جـــامعـة مـــولـــود مـــعـمري– تـيـــزي وزو
كـــليـة الـحقـــوق والـــعلـوم السيـــاسيـــة
قـسم: الـحقوق

ضمانات أمن مواقع التجارة الإلكترونية

أطروحة لنيل شـهادة دكتـوراه في الـعلـوم
تـخصص: القـانـون

من إعـداد الطالـب:
دحـمانـي سميـــر

تحت إشـراف:
د. كـسـال سـامية

لـجنـة المنـاقشـة:

د. أ.د يسعد حورية، أستاذة، جامعة مولود معمري ـ تيزي وزو .....رئيسة.
د. كسال سامية، أستاذة محاضرة"أ"، جامعة مولود معمري ـ تيزي وزو..... مشرفة ومقررة.
د. حمودي ناصر، أستاذ محاضر"أ"، جامعة أكلي ولحاج ـ البويرة .....ممتحنا.
د.حمادوش أنيسة، أستاذة محاضرة"أ"، جامعة مولود معمري ـ تيزي وزو ..... ممتحنة.
د.معيفي عبد العزيز، أستاذ محاضر"أ"، جامعة عبد الرحمان ميرة ـ بجاية .....ممتحنا.
د.بركات كريمة، أستاذة محاضرة"أ"، جامعة أكلي ولحاج ـ البويرة ..... ممتحنة.

تاريخ المناقشة: 2020/07/02.

إهـــداء

أهدي عملي هذا إلى الوالدين الكريمين، أطال اللّه في عمرهما وحفظهما من كلّ سوء، ووفّقني لأكون في مستوى تضحياتهما.

إلى كل من شجعني في إنجاز هذه الأطروحة،

وإلى كل طالب علم.

إلى كل الأساتذة والمعلمين الذين أشرفوا على تعليمي عبر مختلف الأطوار التعليمية.

كما أهديه أيضا إلى جميع الإخوة والأخوات.

ســمير

اعترافا بالفضل والجميل أتقدّم بجزيل الشكر وعميق التقدير والامتنان إلى الأستاذة المُشرِفة الدكتورة **كسال سامية**، عرفانا وتقديرا على توجيهاتها وملاحظاتها القيّمة، التي على إثرها زوّدتني بالنصائح والإرشادات التي أضاءت أمامي طريق البحث والتقصي، خلال جميع مراحل انجاز هذا العمل.

فجزاها الله عني كلّ خير.

كما لا أنسى أن أقدم شكري وامتناني إلى جميع أساتذة كلية الحقوق والعلوم السياسية بجامعة مولود معمري بتيزي وزو، كما أقدّم شُكري لمُوظفي المكتبة.

سمير

قـــائمـــة أهـم الـمختصـرات

أوّلا- باللّغة العربية:

ج ر: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

ر. ر. ج. ت: الرائد الرسمي للجمهورية التونسية.

س.ض.ب.إ.إ: سلطة ضبط البريد والاتصالات الإلكترونية.

م.خ.إ: مقدمي أو مزودي خدمات الإنترنت.

م.خ.ت.إ: مقدم أو مزود أو مؤدي خدمات التصديق أو التوثيق الإلكتروني(ة).

ثانيا- باللّغة الفرنسية:

ASSI : **A**gence de la **S**écurité des **S**ystèmes d'**I**nformation.

AFNIC : **A**ssociation **F**rançaise pour le **N**ommage **I**nternet en **C**oopération.

AGCE : **A**utorité **G**ouvernementale de **C**ertification **É**lectronique.

ANCE : **A**utorité **N**ationale de la **C**ertification **É**lectronique.

ARPCE: **A**utorité de **R**égulation de la **P**oste et des **C**ommunications **É**lectroniques.

AC : **A**utorité de **C**ertification.

AE : **A**utorité d'**E**nregistrement.

C.J.U.E : **C**our de **J**ustice de l'**U**nion **E**uropéenne.

CNIL : **C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés.

DPC : **D**éclaration de la **P**olitique de **C**ertification.

ICP : **I**nfrastructure à **C**lés **P**ubliques.

IGC : **I**nfrastructure de **G**estion de **C**lés.

J.O.R.F : **J**ournal **O**fficiel de la **R**épublique **F**rançaise.

J.O.U.E : **J**ournal **O**fficiel de l'**U**nion **E**uropéenne.

LCEN : **L**oi pour la **C**onfiance dans l'**É**conomie **N**umérique.

LCR : **L**iste des **C**ertificats **R**évoqués.

LFSCSE: **L**oi **F**édérale sur les **S**ervices de **C**ertification dans le domaine de la **S**ignature **É**lectronique(Suisse).

LPD : **L**oi fédérale sur la **P**rotection des **D**onnées(Suisse).

MB: **M**oniteur **B**elge.

PC : **P**olitique de **C**ertification.

PSCE : **P**restataires de **S**ervice de **C**ertification **É**lectronique.

RGPD : **R**èglement **G**énéral de la **P**rotection des **D**onnées.

RS : **R**ecueil **S**ystématique du droit fédéral suisse.

SICE : **S**éminaire **I**nternational sur la **C**ertification **É**lectronique.

TC : **T**iers de **C**onfiance.

ثالثا– باللغة الإنجليزية:

ccTLD: **c**ountry **c**ode **T**op-**L**evel **D**omains.

DNS: **D**omain **N**ame **S**ystem.

eIDAS: **E**lectronique **ID**entification **A**uthentification and trust **S**ervices.

ENISA: **E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency.

ICANN: **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers.

IANA: **I**nternet **A**ssigned **N**umbers **A**uthority.

gTLD: **g**eneric **T**op-**L**evel **D**omain.

MLM: **M**ulti **L**evel **M**arketing.

NIC: **N**etwork **I**nformation **C**enter.

PKI: **P**ublic **K**ey **I**nfrastructure.

SLD: **S**econd **L**evel **D**omain.

TLD: **T**op **L**evel **D**omain.

UDRP: **U**niform **D**omain **N**ame **D**ispute **R**esolution **P**olicy.

VPN: **V**irtual **P**rivate **N**etwork.

مقدمـــة:

أحدثت ثورة تكنولوجيا المعلومات والاتصالات تغييرات حديثة في نمط حياة المجتمعات البشرية على مستوى جميع الأصعدة، وساهمت في ظهور العديد من المفاهيم الحديثة المتعلّقة بالخصوص بالميدان القانوني والاقتصادي، وذلك تزامنا مع التّطور التّقني الهائل والسّريع لمختلف التّقنيات الإلكترونيّة الحديثة المُستخدمة عبر شبكة الإنترنت، التي بدورها استطاعت أن تغيّر المظهر العالمي للتّجارة ومحيط الأعمال بصفة عامة، وكرّست الوجود الفّعلي للتّجارة الإلكترونيّة التي تُشكّل الجُزء الغالب في سوق خدمات الإنترنت.

أدّت هذه التّحولات بالعالم الحديث إلى إحلال مختلف التّقنيات التّكنولوجيّة والمعلوماتيّة في سلوك البشريّة، ولا يمرّ يوم واحد حتّى نسمع بمولود تكنولوجي حديث على مستوى جميع المجالات الحيويّة، حيث توصّل الفكر البشري إلى تطوير جيل جديد من الحواسيب القويّة، وهو الحاسوب الكمّي(Ordinateur quantique)[1] الذي يعتمد على وحدة الكَيُوبِتْ-qubit) (qbit لقياس كميّة البيانات، حيث بإمكانه القيام بسرعة فائقة معالجة وتخزين كميّة هائلة من المعلومات في آن واحد، تفوق بملايين الأضعاف كميّة المعلومات المُعالجة بالحاسوب التّقليدي الذي يعتمد على وحدة(Bit)، ويرى خبراء أمن المعلومات أنّ الإعتماد على تقنية الحوسبة الكميّة تجعل شبكة الإنترنت في المستقبل القريب آمنة وغير قابلة للاختراق[2].

---

1) Un **Ordinateur quantique** est l'équivalent des ordinateurs classiques mais qui effectuerait ses **calculs** en utilisant directement les lois de la **physique quantique** et, à la base, celle dite de superposition des états quantiques, afin d'effectuer des opérations sur des données. À la différence d'un **ordinateur classique** basé sur des **transistors** qui travaille sur des données binaires (codées sur des bits, valant 0 ou 1), le **calculateur quantique** travaille sur des **qubits** dont l'état quantique peut posséder une **infinité** de valeurs.
Pour avoir plus d'informations sur le sujet, voir : **Thierry LOMBRY**, « Comment fonctionne un ordinateur quantique », article publié sur futura-sciences.com, le 26/10/2015. https://www.futura- sciences.com/sciences/dossiers/physique/, consulté le 08/01/2016.

2) **Dan CALZ**, « Un Internet quantique plus rapide et plus sûr serait possible », article publié le 11/02/2019 à 11h 52, sur le site : https://www.devlopper.com/actu/24883/, consulté le 13/02/2019.

تُحظَى البرمجيات المعلوماتيّة(Software) بأهميّة قُصوى في شتى مجالات الاقتصاد الرقمي، نظرا للدقّة المتناهية، والسّرعة الفائقة للمهام والخدمات التي تتيحها لأطراف التعامل الإلكتروني، إذ تعتبر هذه البرمجيات الجزء غير الملموس من نظام الحاسب الآلي، الذي يصبح عديم الفائدة من دونها، كما أنّها تُوفِّر مناخ خصب لشبكات الاتصالات التي تربط فيما بين مختلف أجهزة الحاسوب، وتُؤمِّن عمليات نقل المعلومات أو الملفات الإلكترونيّة المتداولة فيما بين الأجهزة بسرعة وكفاءة عالية، وتضمن عملية التّحكم فيها من خلال جهاز مركزي في الشّبكة يُعرف بالخادم(Serveur)، الذي بدوره يسمح للأجهزة الأخرى بالوصول إلى المعلومات عند الحاجة إليها بطريقة مؤمّنة على مستوى الشّبكات.

تُشكّل شبكات الاتصالات الحديثة الوسط الذي تتلاقى فيه البيانات الإلكترونيّة المتداولة، وتُخزن فيها مختلف المعلومات الأساسية والحسّاسة لأطراف التعامل الإلكتروني، ولضمان ديمومة هذه الشّبكات، فإنّ الوضع الرقمي الراهن يستدعي الحاجة إلى حماية سلامة محتوياتها واستمرارية عملها، فإذا تعطّلت هذه الشّبكات لوقت قصير فقط، تتوقّف معها أعمال مختلف المؤسّسات الحكوميّة والشّركات التّجارية المنتشرة عبر العالم، ويُكبّد أصحابها، أو المستفيدون منها، أضرارا وخسائر فادحة تؤدّي في بعض الأحيان إلى الإفلاس، وكل ذلك ينعكس سلبا على انخفاض مستوى الخدمات المقدّمة للمواطنين، وجودة السّلع المعلوماتية المتاحة، وبالتالي فإنّ نجاح مناخ الأعمال يعتمد على التّصميم الجيّد لشبكات الاتصال وتأمين استمرارية عمل قواعد البيانات.

إنّ شبكة الإنترنت ماهية إلاّ شبكة من بين عدة شبكات اتصالات، تُدار كلّ واحدة بمعزل عن الأخرى بشكلٍ غير مركزي، إذ أنّ تشغيل هذه الشّبكات لا يعتمد على أيًّا منها، وتستخدم تقنيات شبكيّة داخليّة مُختلفة، وما يجمع فيما بين هذه الشّبكات هو إمكانية الاتّصال بينها، عن طريق بوابات مرتبطة وفقا لمواصفات قياسيّة مُشتركة، لذا تعتبر هذه

Benoît CRÉPIN, « Vers un Internet quantique », article publié le 31/01/2019, sur le site : https://www.industrie-techno.com/, consulté le 02/02/2019.

التّقنية العالية أداة اتّصال عالميّة مفتوحة، صاحبت معها ابتداءً من التّسعينيات، ظهور العديد من التّقنيات الحديثة في إبرام وتنفيذ المعاملات التّجاريّة، وفي أساليب التّرويج بمختلف السّلع والخدمات عبر الإنترنت، وطرق دفع مستحقاتها، التي أصبحت تتم بوسائل دفع إلكتروني حديثة مغايرة عن الطرق التّقليديّة.

كما مكّنت شبكة الإنترنت الشّركات التّجاريّة من تحديث وسائل إدارة أنشطتها التّجاريّة، مع تلبية احتياجات المستهلكين، وإتاحتهم لخيرات التّسويق بشكل واسع، على نحو يُمكّنهم من معرفة وتفضيل أصناف وميزات كلّ سلعة أو خدمة، قبل اتّخاذ القرار الأخير في الشّراء.

فبفضل هذه التّقنيّة تحوّلت أسواق دول العالم إلى أسواق إلكترونيّة افتراضيّة، مفتوحة على أطراف المبادلة التّجارية، بغض النظر عن الموقِع الجُغرافي لكل طرف (البائع أو المشتري)، أو التّقنية التّكنولوجيّة المستعملة في إبرام أو تنفيذ تصرفاتهم التّجارية[1].

ساهمت تقنيّة المعلومات في ظهور أسواق إلكترونيّة افتراضيّة، تُتيح خدمات مُبرمجة مسبقا لأطراف التّبادل الإلكتروني، بحيث يستطيع الزبون أن يُلِمَّ بجميع المعلومات المتعلّقة بمزايا مختلف السّلع والخدمات المتاحة من طرف المحترف أو البائع، عبر موقع إلكتروني معدّ خصّيصا لهذا الغرض، إذ يوفّر هذا الأخير(الموْقِع الالكتروني) للشّركات الاقتصاديّة القُدرة على توفير السّلعة أو الخدمة بالكمّ والوقت والسّعر المناسب، مع منافسة الشّركات الأخرى التي تُتيح نفس السّلع أو الخدمات، ضمن مواقِع إلكترونيّة مُستهدفة لفئة معيّنة من المستهلكين، الشيء الذي يُتيح للمستهلك أو المشتري الحريّة في اختيار السّلعة أو الخدمة المرغوبة، والتّفاوض عليها عبر شبكات الاتّصالات الالكترونيّة الحديثة، التي تُوفّر السّهولة واليُسر في عمليات إبرام الصّفقات وتبادل المعلومات الإلكترونيّة.

---

[1] **محمد مدحت عزمي**، المعاملات التجارية (الأسس القانونية والتطبيقات)، مركز الإسكندرية للكتاب، الإسكندرية، مصر، 2009، ص ص 200، 201.

لقد أدّت عولمة الأنشطة التّجارية والأسواق الماليّة إلى تطوّر تكنولوجيا المعلومات، وأنظمة الاتصالات الحديثة بشكلٍ كبير، وإلى ظهور المصارف الالكترونيّة، وتوسيع العمليات التّجارية الالكترونيّة، والخدمات المصرفيّة المُقدّمة إلكترونيا للعملاء عبر الويب.

وممّا لا شك فيه، أنّ المصارف الإلكترونيّة تلعب دوراً مهماً ومحورياً في التّنمية الاقتصاديّة لأيّ دولة في العالم، كما أنّها ساهمت في تغيير المفهوم التّقليدي للمصرف، واستحدثت نوعية الخدمات المصرفيّة، وطريقة تقديمها للعملاء، كما أنّها جعلت التّجارة الالكترونيّة بمثابة المُرادف التّقني لهذه المصارف الالكترونيّة، من خلال تقديم مختلف الخدمات والتّسهيلات بأقل التّكاليف وبسُرعة مُذهلة، عبر الإنترنت[1].

إنّ حتمية البّحث عن وسائل وتقنيات حديثة للدّفع عبر الإنترنت، أصبحت من المتطلّبات التي فَرَضَهَا عصر الرّقمنة، وذلك بعدما كانت الوسائل التّقليدية المستعملة في الدّفع لا تستجيب لمُستجدّات الوضع الرّاهن، الذي عرف ظهور نُظم وتطبيقات ماليّة حديثة ومُتطوّرة، ساهمت في جذب العديد من المتعاملين بالتّجارة عبر الإنترنت، لذا تُعَدُّ تقنيات الدّفع الإلكتروني الحديثة (النّقود الرّقميّة، البطاقات الذّكيّة، الشّيك الإلكتروني، الخ...)، عُنصرا أساسيا ومُهمّا في تفعيل وإنعاش نشاطات التّجارة الإلكترونيّة، والعمليات المصرفيّة عبر شبكة الإنترنت، حيث تُمكّن هذه التّقنيات أطراف التّعامل الإلكتروني من توفير الجُهد والاقتصاد في الوقت، عند القيام بعمليات البيع والشّراء، وتسديد المستحقّات أو الاشتراكات من دون التّنقّل إلى عين المكان.

كما يُوفّر المَوْقِع الإلكتروني للمصرف العديد من الخدمات المصرفيّة للعملاء، كعرض الخدمات الماليّة بعدّة لغات(الأمازيغيّة، العربيّة، الفرنسيّة، الإنجليزيّة، الخ...) لتيسير استخدامها(الخدمات)، وتسهيل عمليات تحويل الأموال بين حسابات العملاء، وإجراء

[1] **محمد مدحت عزمي**، مرجع سابق، ص ص 42-44.

عمليات المقاصة الإلكترونيّة فيما بين المصارف، وإمكانية شراء وبيع الأسهم والسّندات الماليّة بالبورصات، وقيام العملاء بسداد التزاماتهم عبر الإنترنت، مع إمدادهم بجميع المعلومات المتعلّقة بأرصدتهم بالمصرف، من دون التّنقّل إلى مقرّه الرئيسي، أو أحد فروعه.

تُمثّل المواقِع الالكترونيّة أهميّة ماليّة واقتصاديّة كبيرة للمشروعات، والمُحرّك الأساسي لمعاملات التّجارة الإلكترونيّة، حيث ساهمت بشكل كبير في تمييز المشروعات التّجارية على شبكة الإنترنت، وتنويع خدمات الاتّصالات، على غرار خدمات الدّخول والاتّصال والإيواء والبّحث عن المعلومات وتسجيل أسماء النّطاق الخ...، وساعدت على الانتشار الكثيف والسّريع للمتاجر الافتراضيّة، التي تتطلّب عادة تكاليف مُشابهة لتلك التي يتطلّبها بناء أو إنشاء المتجر العادي، غير أنّ عملية إحداث المواقِع الإلكترونيّة تستوجب الاستعانة بخبراء تكنولوجيا المعلومات، وذي درجة عالية من الكفاءة في تقنيات إعداد البرمجيات المعلوماتية المتعلّقة بالتّسويق الإلكتروني، وبأمن الشّبكات والإنترنت[1].

تُمكّن مُحرّكات البحث(Moteurs de recherche) مختلف المستخدمين من الوصول المباشر للمعلومات المطلوبة، بِمُجَرَّدِ الحصول على المَوقِع الإلكتروني وتَصَفُّحِهِ، كما أنّ استخدام عِدَّة لُغات بحث تُسهّل المُهمّة للمستهلك أو المشتري في الحصول على أكثر من سلعة أو خدمة عبر شبكة الإنترنت في وقت آنٍ ووجيز.

وبالتالي فإنّ مُحرّك البحث ما هو إلاّ برنامج معلوماتي يُمكّن الوصول إلى قواعد البيانات على مستوى شبكة الإنترنت، للبحث على معلومات رئيسية مزوّدة بتقارير حول موضوع البحث، حيث يُسهّل عملية فهرسة(Indexer) صفحات الويب(Pages web) ومحتوياتها، التي تُظهِر استجابات الكلمات الدّالة(Mots-clés) المطلوبة من طرف المستخدم، سواء للبحث عن المواقِع الإلكترونيّة(Sites) أو الحصول على معلومات في داخل

1) **Romain V. GOLA**, Droit du commerce électronique :(Guide pratique du e-commerce), Gualino, Lextenso éditions, France, 2013, p. 100.

هذه المواقِع بحدّ ذاتها، فقد تكون مُحرّكات البحث مواقِع الويب نفسها مثل (Google, Altavista, etc.)، أو تكون خدمة فعّالة في داخل الموقِع الإلكتروني، تسمح للمستخدمين بالبحث وتقديم استفسارات عن مختلف المعلومات، فمن بين أهمّ محرّكات البحث المعروفة حاليا نجد كلٍّ من: (Google, Yahoo !, MSN, Altavista, Lycos, etc.).

يعتبر التّسويق الالكتروني(Cybermarketing) من أبرز وأهم نشاطات التّجارة الالكترونيّة التي تتم عبر الإنترنت، حيث يعتمد عليه أطراف العمليّة التّسويقيّة من أجل تسهيل وتبادل السّلع والخدمات، من خلال استخدام أساليب وتقنيات تكنولوجيّة عالية المستوى، تُساعِد البائع أو التّاجر على تصميم وإعلان وتسعير وبيع وتوزيع وترويج مختلف المنتجات والخدمات عبر موقِع إلكتروني جذّاب، يسمح للمستهلك أو المشتري باقتناء حاجاته بأسرع وقت مُمكِن وبأقّل التّكاليف، وفي أي مكان من العالم، مع دفع ثمنها بوسائل دفع الكتروني حديثة على مستوى الموقِع الالكتروني ذاته، باستخدام حاسوبه الشّخصي أو هاتفه الذّكي.

وبالتّالي فإنّ بيئة التّسويق واسعة ومُتغيّرة بحسب العوامل المُؤثّرة فيها، التي تفرض على الشّركات التّجاريّة تكييف استراتيجياتها التّسويقيّة مع التّطوّرات الرّاهنة والمُستقبليّة، حتى تستطيع ضمان وجودها ونجاحها ووضعها الجيّد عبر مختلف أسواق العالم.

إنّ تحوّل المواقِع الإلكترونية إلى وسيلة استثمار مُربِحة في مجال الأعمال، ساهم بشكلٍ كبير في هيمنة معاملات التّجارة الإلكترونيّة، وازدياد حدّة المنافسة فيما بين المتعاملين الاقتصاديين على مستوى شبكة الإنترنت، نتيجة ارتفاع نسبة المبادلات التّجاريّة والمصرفيّة، وتعاظم الإنتاج الرّقمي، من برامج وقواعد البيانات والأعمال الرّقميّة الأخرى، التي عادةً ما تتطلّب مجهودا ذهنيّا مميّزا، وتوظيف موارد ماليّة وبشرية وتقنيّة ضخمة، من قِبل المنتج أو المُبتكر صاحب الحق.

ومع ازدياد حجم الإنتاج الرّقمي، تضاعفت أعمال التّعدي عبر الحدود، التي تفرض على مُشرّعي مختلف الدول توسيع نطاق المعاهدات الدوليّة الخاصّة بحماية حقوق الملكيّة

الفكريّة، لتشمل المصنّفات الرّقميّة الالكترونيّة، التي تشتمل على فهارس وصفحات وأسماء المواقع الإلكترونيّة، ومحرّكات البحث، ووصلات النّصوص الفائقة، والأنظمة التّطبيقيّة المختلفة، والرّسوم والصّور والفيديوهات والوسائط المتعدّدة الخ...، التي تستوجب تكييفها وإعطائها الوصف القانوني الملائم لها، لغرض حمايتها.

وقد صاحب ارتباط الشّبكات المحليّة بشبكة الإنترنت، ظهور أساليب وتقنيات حديثة في التّجسّس والقرصنة على مواقع الإنترنت، وفك شفرات التّشفير لتجاوز بروتوكولات الاتّصالات المُستخدمة فيها، وإحداث نظم خيالية أو وهمية للاستقبال والتّوجيه، تسمح بِالْتِقَاطِ الرّسائل وعناوين المواقع الالكترونيّة والتّظاهر بامتلاكها، وما يُثير الانتباه حاليا، أنّ العديد من أصحاب مواقع التّجارة الإلكترونيّة، لا يعلمون أنّه قد تم اختراقها إلاّ بعد حصول الكارثة أو عملية الاختراق.

كما أنّه مع تنامي استخدام البرمجيات الخبيثة، وبالخصوص تلك المتعلّقة بالتّلصّص المنشورة مجاناً على مواقع الويب، أصبح بمقدور أيّ شخص أن يقوم بإجراء مسح تلقائي لمواقع التجارة الإلكترونية، والبحث عن نقاط الضّعف فيها، بغية استغلالها في ترويج أو إدارة نشاط خارج القانون، أو حتى تعطيل خدماتها(المواقِع)، فأغلبية الشّركات الاقتصاديّة المتنافسة في ميدان الصّناعة والخدمات، تسعى إلى الحصول على الأسرار الصّناعية والتّجارية المملوكة لخصومها من الشّركات، بمجرّد اختراق منظوماتها الأمنيّة أو الدّفاعيّة، وذلك لغرض تحقيق أرباح ومنافع أو تقوية نفوذها في الأسواق، من دون الحاجة إلى عملية زرع موظّف جاسوس في إحدى الشّركات المنافِسة.

تُثير المعاملات عبر مواقع التّجارة الإلكترونيّة، مجموعة من المسائل النّاشئة عن انعدام الثّقة فيما بين أطراف التّعامل الإلكتروني، الذين لا يتلاقون بصفة مباشرة عند إبرام مختلف الصّفقات التّجاريّة، وسرية وأمن البيانات الإلكترونيّة المتداولة عبر شبكة الاتّصالات الإلكترونيّة، وعدم توفّر البُنية التّحتية، التي تحتاج إليها شبكات الاتصالات والمعلومات،

وفقا لمعايير معترف بها عالميا، ضِفْ إلى ذلك، افتقار مواقع التّجارة الإلكترونيّة لمتطلّبات الحماية والأمن التي من شأنها أن تجذب العملاء.

وعليه، فمفهوم الأمن المعلوماتي(Sécurité Informatique) أو (Sécurité de l'information)[1] من الزّاوية التّقنية يعتبر مفهوماً واسعاً، يَشْمُلُ أمن الأنظمة الإلكترونية وأنظمة التّشغيل، وتأمين(Sécuriser) جميع عمليات الاتّصال بالشّبكات والمواقع الالكترونية، ومعالجة المعلومات وانتقالها وتخزينها واسترجاعها، الخ....

فأمن المعلومات من زاوية أكاديمية يعتبر العِلم الذي يبحث في استراتيجيات تأمين وحماية المعلومات المتداولة عبر الإنترنت من المخاطر التي تُهدّدها، من خلال توفير الإجراءات والوسائل والتّقنيات اللاّزمة لضمان حماية البيانات المتداولة أو المُخزّنة من المخاطر الداخليّة والخارجيّة[2].

---

[1] وفقا لقاموس المعاني يقصد بكلمة **أمن:** أَمَانْ، أَمْنَة، أَمَنَة، التي تعني: **1**- مصدر أمِنَ/ أمِنَ مَنْ. **2**- طُمَأْنِينَة، حَالَة هَادِئَة نَاتِجَة من عَدَمِ وجود خطر، بكلّ أَمَان يعني: بِدون أَدْنَى خطر. **3**- حِراسة، رِعاية، حفظ، تَأْمِين، حماية. للمزيد أكثر من المعلومات، أنظر المواقع الإلكترونية التالية: https://www.almaany.com/ar/dict/ar-ar/ ou https://www.maajim.com/dictionary/ (تم الاطّلاع عليها في 2016/02/12.)

تُقابل كلمة الأمن باللغة الفرنسية كلمتي (**Sécurité**) أو (**Sécuriser**)، حيث يُقصد بالمصطلح الأول: **1-** Situation de quelqu'un qui se sent à l'abri du danger, qui est rassuré. **2-** Absence ou limitation des risques dans un domaine précis.
3- Prévenir un accident ou un événement dommageable ou à en limiter les effets.
Synonyme : paix, sûreté, tranquillité, confiance, ataraxie, etc. **Contraire** : danger - insécurité - précarité, anxiété, etc.

بينما تعني كلمة (**Sécuriser**): **1-** Donner une impression **de sécurité**, de tranquillité, de confiance en soi. **2-** Donner à quelque chose de la **sécurité**, de la stabilité. **3- Informatique** : sécuriser un ordinateur, un site, etc.
Synonyme : rasséréner - rassurer- tranquilliser. https://www.larousse.fr/dictionnaires/francais/ ou https://www.larousse.fr/dictionnaires/francais-arabe/ (consulté le 12/02/2016.)

[2] **Wilson GOUDALO**, « Vers une ingénierie avancée de la sécurité des systèmes d'information d'entreprise : une approche conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques », thèse de doctorat, spécialité : Informatique,

كما يعتبر الأمن المعلوماتي من الزّاوية القانونيّة، من بين أهداف وأغراض تشريعات حماية المعلومات ومعاملات التّجارة الالكترونيّة من الأنشطة غير المشروعة وغير القانونيّة، حيث يُشكّل الشّغل الشاغل لكلّ دولة أو أيّ مسؤول عن كيان أو مؤسّسة معينة، وذلك مع تزايد وانتشار الجرائم الالكترونيّة المرتكبة، التي شملت أنشطة التّجسّس الصّناعي، والأمني، والمُتاجرة بالمعطيات الشّخصية للأفراد بشكل غير مشروع، الخ...[1].

انطلاقا من ذلك، فإنّ الأمن المعلوماتي يرتبط ارتباطاً وثيقاً بأمن مواقع التّجارة الالكترونيّة، الذي يتطلب تحديد المخاطر التي تتعرّض لها هذه المواقِع، ونقاط الضعف أو الثّغرات المتواجدة ومن ثمّ الإجراءات والتّدابير التي يجب توفيرها لضمان حماية المعلومات المتداولة أو المُخزّنة فيها من مختلف التّهديدات الداخليّة والخارجيّة.

انطلاقا ممّا سبق، تُطرح الإشكالية التالية:

ما مدى فعالية التّدابير التّقنيّة والقانونيّة المكرّسة لضمان أمن مواقع التّجارة الالكترونيّة من المخاطر التي تهدّدها ؟

وللإجابة عن هذه الإشكاليّة المطروحة، فإننا نتّبع المنهج الاستنباطي – التّحليلي، والمنهج المقارن كلّما تطلّب الأمر ذلك، حيث تمّ توضيح من خلال المنهج الاستنباطي –

Génie Informatique, Université de Valenciennes et du Hainaut-Cambrésis, France, 2017, pp. 07-10.

Margaret ROUSE, « Sécurité de l'information (infosécurité, infosec) », article publié sur le site : https://www.lemagit.fr, consulté le 02/01/2016.

أنظر كذلك: **يونس عرب**، "أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها"، ص 01. مقال منشور عبر الموقع الإلكتروني التالي: http://www.arablaw.org/Download/Information_Security.doc

[1] **Wilson GOUDALO**, « Vers une ingénierie avancée de la sécurité des systèmes d'information d'entreprise : une approche conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques », thèse de doctorat, spécialité : Informatique, Génie Informatique, Université de Valenciennes et du Hainaut-Cambrésis, France, 2017, pp. 07-10.

التّحليلي مكانة مواقع الويب ودورها في تفعيل معاملات التّجارة الإلكترونيّة، مع إبراز مختلف المخاطر والتّهديدات الإلكترونيّة المحيطة بها، وتحليل مختلف النّصوص القانونيّة الوطنيّة والأجنبيّة، التي تعني بحماية وتأمين مواقع التّجارة الالكترونيّة من كل أشكال الاعتداء والتّهديد، وكذلك تحليل النّصوص القانونيّة المتعلّقة بالمسؤوليتين المدنيّة والجزائيّة ودراسة مدى ملاءمة تطبيقها على المسؤوليّة الالكترونيّة، السّالفة الذكر، كما يساعد إتّباع المنهج المقارن معالجة مختلف النّصوص الأجنبيّة الحديثة التي تخدم الموضوع، ومدى مواكبة المشّرع الجزائري للتّطورات الرّاهنة في مجال التّجارة الالكترونيّة.

ويقتضي دراسة موضوع "**ضمانات أمن مواقع التّجارة الالكترونيّة**" تقسيمه إلى بابين رئيسيين، نتعرض في الباب الأول إلى "**مواقع التّجارة الالكترونيّة والمخاطر التي تهدّدها**"، ونتعرض في الباب الثاني إلى "**الحماية التّقنيّة والقانونيّة لمواقع التّجارة الإلكترونيّة**"

حيث أنّ تعميم الرّقمنة وتحوّل شبكة الإنترنت إلى وسيلة ماليّة مُربِحة في مجال الأعمال، ساهم بشكلٍ كبير في نُمُوِّ تطبيقات التّجارة الإلكترونيّة وتطوّر المعدّات والشّبكات، وازدياد حدّة المنافسة على مستوى هذه الشّبكة، نتيجة ارتفاع نسبة المبادلات التّجاريّة والمصرفيّة عبر المواقِع الإلكترونيّة، التي تحتل مكانة كبيرة في التّجارة الإلكترونيّة، حيث تُمثّل هذه المواقع الالكترونيّة أهميّة ماليّة واقتصاديّة لمشروعات المتعاملين الاقتصاديين على شبكة الإنترنت، بالرغم من المخاطر المُحيطة بها **(الباب الأول)**.

لذا تُشّكِل مواقع التّجارة الإلكترونيّة البيئة التي تتلاقى فيها شبكات نُظم المعلومات وتنساب فيها مختلف الأخطار، التي تهدّد استقرار وأمن البيانات الإلكترونيّة المتداولة أو المخزّنة فيها، كالإصابة بالفيروسات والبرامج الضّارة والتّعرض لمحاولات الاحتيال والاختراق والتّجسّس والقرصنة، وانتهاك حقوق الملكيّة الفكريّة الرّقميّة أو أسماء مواقع الإنترنت الخ...، التي تفرض على أرض الواقع حتمية إرساء سياسة أمنيّة موثّقة وإجراءات تشريعيّة وتنظيميّة لتأمين مواقع التّجارة الإلكترونيّة وحمايتها من مختلف التّهديدات **(الباب الثاني)**.

البـاب الأول

مواقِـــع التّجـارة الإلكترونيّة

والمخاطـر التي تهدّدهـا

لا ريب أنّ ما يشهده العالم المعاصر من تقدّم تكنولوجي في شتى وسائل الاتصالات، لهو حقّا يستحق أن نسميه بالثّورة الصّناعيّة الثّالثة، التي أحدثت نقلة نوعيّة في وسائل الاتّصالات وسرعة المعلومات، وحوّلت العالم إلى كون صغير(Petit Univers)، تتبادل فيه المعلومات إلكترونيّا وبسرعة فائقة عبر الإنترنت، التي بدورها كرّست الوجود الحقيقي والفّعلي للتّجارة الإلكترونيّة، وساهمت في ظهور أسواق إلكترونيّة تنافسيّة، واسعة، لمختلف السّلع والخدمات، لذا أضحت التّجارة الإلكترونيّة بالنّسبة لمختلف الشّركات، كضرورة مُلحّة ومطلب أساسي لتطوير قدراتها الإنتاجيّة وإستراتيجياتها التّسويقيّة عبر مختلف الأسواق، وذلك بالاستعانة بأهم خدمات شبكة الإنترنت، لاسيما خدمة الويب التي تعتبر كوسيلة من وسائل الاتّصال والتّرويج والدّعاية والإعلان والتّسعير، لمختلف السّلع والخدمات، وما تتيحه من خيارات التّسوّق وتسهيلات الدّفع للمستهلك عبر مواقع التّجارة الإلكترونيّة **(الفصل الأول)**.

إنّ المخاطر المنبثقة من التّجارة الإلكترونيّة، تتبع أصلا من مخاطر شبكة الإنترنت بسلبياتها الخطيرة، التي تلحق أضرارا جسيمة لأطراف التّعامل الإلكتروني – التّاجر والمستهلك– حيث تطرح إلى الواجهة مسألة الثّقة فيما بينهم، وسلامة وسريّة المعلومات أو البيانات الإلكترونيّة المتداولة في البيئة الرّقميّة وإمكانية إنكارها **(الفصل الثاني)**.

الفصل الأول
الإطار المفاهيمي لمواقع التّجارة الالكترونيّة

تعتمد الشّركات على استراتيجيات مصممة عبر شبكة الانترنت، بشكل يتيح لها خيارات وبدائل متعدّدة حسب احتياجاتها المتغيّرة في زمن العولمة والتّطوّرات التّكنولوجيّة السّريعة، إذْ لم يَعُدْ حاليّا على مَقْدُورِ أيّ شركة مُباشرَة نشاطاتها على النّحو التّقليدي الذي كانت تُمارس وفقه نشاطاتها من قَبْلِ، لذا فإنّ خدمات الإنترنت أحدثت تغييرات جذريّة في إدارة الشّركات وكيفيات نقل معلوماتها، وتنسيق أنشطتها التّجارية، التي من شأنها أن ترفع من قدراتها التّسويقيّة والتّنافسيّة، مع تلبية وفهم المتطلّبات الموضوعيّة المتسارعة للزّبائن، على السلع والخدمات عبر المواقع الإلكترونيّة، وانطلاقا من ذلك تعتبر شبكة الويب من أهم خدمات الإنترنت الأكثر استخداما وشيوعا في نشاطات التّجارة الإلكترونيّة **(المبحث الأول)**.

يُعْرَفُ عن التّسويق الإلكتروني على أنّه عملية تجاريّة أساسيّة ومُعقّدة، تحتوي على مجموعة من الإجراءات والوسائل والتّقنيات، المُستعملة من طرف الشّركة لترويج وتنمية أنشطتها التّجاريّة عبر موقعها الإلكتروني، لغرض إشباع حاجيات الزّبائن من سلع وخدمات، وتحقيق التّوازن بين الإنتاج والاستهلاك، فعن طريق المزيج التّسويقي تستطيع الشّركة أن تعرّف بالسّلعة أو الخدمة المتاحة، مع تعزيز سمعتها التّجاريّة وفرض وجودها الفّعلي والحقيقي على مستوى العالم الافتراضي **(المبحث الثاني)**.

المبحث الأول
ماهية مواقع التّجارة الإلكترونيّة

ترتكز تقنية الويب في المجال الاقتصادي على الذّكاء الصّناعي في عمليات التّصنيف والبحث وإدارة وتصفُّح مواقع التّجارة الالكترونيّة، التي تسهّل عملية الحصول على المعلومات المتعلّقة بمختلف السّلع والخدمات، باستخدام تكنولوجيا الرّقميّة في ظرف قياسي وجيز، وبالتالي تعتبر مواقع التجارة الالكترونية مفتاح تحقيق أهداف الشّركات أو المؤسّسات الاقتصاديّة، التي يستوجب عليها مراعاة مجموعة من القواعد العامة عبر الإنترنت، كالقدرة على تصميم موْقِع إلكتروني موثوق وجذّاب، يحدّد فيها رغبات العملاء وطريقة عرض

مختلف السّلع والخدمات من أجل تلبية احتياجاتهم، مع دراسة قوّة ضعف المنافسين وتحديد الخدمات التي يقدمونها للعملاء عبر الإنترنت، في إطار بنية تحتيّة فعّالة، يتمكّن من خلالها المورّد الإلكتروني من التّرويج بمختلف السّلع والخدمات، مُتخطّيا في ذلك الحدود الجغرافية للرّقعة الأرضيّة، مع اقتصاد التّكاليف والسّهولة في التّنفيذ، كما يتمكّن المستهلك من الدخول الفوري إلى المتجر الافتراضي في أيّ وقت، من أجل تحديد مواصفات ومتطلّبات السّلعة أو الخدمة التي ينويها أو يحتاجها بطريقة مرنة وسهلة، مع اتخاذ القرار المناسب في قبول أو رفض الإيجاب في ظرف قصير وبأقلّ التّكاليف **(المطلب الأول)**.

كما تعتمد مواقع التّجارة الإلكترونيّة على نظام معلوماتي متكامل يتيح لأطراف التّعامل الإلكتروني إمكانية تبادل بياناتهم الإلكترونيّة، وانجاز وإتمام مختلف النّشاطات التّجاريّة، باستخدام تكنولوجيا الثّورة الرّقميّة، التي ساهمت في ظهور مفاهيم ومصطلحات تكنولوجيا جديدة، في ظل تطوّر البنية التّحتيّة لشبكات الاتّصالات، التي تسهّل عمليات تدفّق البيانات والمعلومات ومعالجتها وتخزينها واستحداثها، وبالتالي فإنّ فعالية تطبيقات التّجارة الالكترونيّة متوقّفة على قوّة وتطوّر نُظم معلومات شبكات الاتصالات، والمهارات والمؤهّلات الضّروريّة المعتمدة فيها **(المطلب الثاني)**.

المطلب الأول

مفهوم مواقع التّجارة الإلكترونيّة

يعتبر الموقع الإلكتروني فكرة جديدة ارتبط ظهورها بظهور الإنترنت التي عرفت تطبيقاتها تطوّرات سريعة وانتشارا واسعا في مجال التّجارة الإلكترونيّة **(الفرع الأول)**، في حين تعتمد عملية إحداث المَتاجر الافتراضيّة على تقنيات الويب الحديثة في عمليات إحداث وتصنيف وتحويل صفحات الويب من مجرّد صفحات ثابتة إلى صفحات ديناميكيّة **(الفرع الثاني)**، حيث يجب أن تستجيب مواقِع التّجارة الإلكترونيّة للمُتطلّبات اللاّزمة التي تضمن فعالية ونجاح واستمرارية المعاملات التّجارية عبر شبكة الانترنت **(الفرع الثالث)**.

الفرع الأول
تعريف مواقع التّجارة الالكترونيّة، أنواعها وأهميّتها

لقد اختلفت المفاهيم والآراء بشأن المواقع الإلكترونيّة بحسب الزّاوية أو المعيار المعتمد في تعريفها**(أوّلا)**، في حين يعتبر الموقع الإلكتروني من بين أهم وسائل التّواصل عبر الإنترنت**(ثانيا)**، وذلك نظرا للدّور الفعّال الذي يلعبه في المعاملات الإلكترونيّة وبالخصوص التّجارة الإلكترونيّة **(ثالثا)**.

أوّلا- تعريف المواقع الإلكترونيّة:

تعتبر المواقع الإلكترونيّة من بين المواضيع الحديثة التي اختلفت الآراء حول تعريفها، فبعض آراء الفقه تعتمد في تعريفها إلى المعيار التّقني**(1)**، والبعض الآخر يستند في تعريفه إلى المعيار الشّكلي**(2)**، بينما الاتجاه الآخر من الفقهاء اعتمد على المعيار الوظيفي**(3)**.

1)- تعريف الموقع الإلكتروني وفقا للمعيار التّقني:

استند هذا الاتجاه في تعريفه للموقع الإلكتروني على المعيار التّقني الذي من خلاله وصفه البعض منهم على أنّه: "مجرد تحويل أو نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحا يتواءم واسم المشروع أو المنظّمة"[1]، والبعض الآخر من أنصار هذا الرّأي عرّف المَوقِع الإلكتروني على أنّه:" عبارة عن مجموعة من الحروف تُكتب بشكل مُعيّن يتم ترجمتها إلى أرقام وتشير إلى مَوقِع مُعيّن على الشّبكة." [2]

إنّ السبب في اعتماد أنصار هذا الرّأي على هذا التّعريف، يعود إلى الصّعوبة التي يجدها المُستخدِم في حفظ وكتابة الأرقام الكبيرة التي لا تفهمها سوى لغة الحواسيب، حيث أنّ شبكة الإنترنت تحتضن العديد من المواقع الإلكترونيّة، ولتسهيل عملية الدّخول إلى مواقع

---

[1] **فاتن حسين حوى**، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 53.

[2] **شريف محمد غنام**، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني(Domain Name)، دار الجامعة الجديدة، مصر، 2007، ص 12.

الإنترنت قرّرت المنظّمات والشّركات المتخصّصة في مجال الإنترنت، خلق نظام أسماء المواقع الذي من خلاله تُستبدل الأرقام التي تفهمها الحواسيب، بلغة الحروف التي يَفْهَمُونَهَا البَشَرُ ويُسَهِّلُ التّعامل معها وحفظها[1]، وبالتالي فإنّ نظام أسماء المواقع(DNS) يُسَهِّلُ عملية البحث على مواقع الإنترنت، ويقوم بترجمة عناوين بروتوكولات الإنترنت(IP) المكتوبة بلغة الأرقام إلى عناوين أسماء مَواقِع مكتوبة بأحرف أبجدية، فمثلا يُعبِّر عنوان بروتوكول الإنترنت(IP) "192.0.34.163" على المَوقِع الإلكتروني التالي: "www.icann.org" [2].

2)- تعريف الموقع الإلكتروني وفقا للمعيار الشّكلي:

يعتمد أنصار هذا الاتجاه في تعريف الموقع الإلكتروني على مكونات اسم الموقع الإلكتروني الذي يتكوّن من جزأين أساسيين: "جزء ثابت وجزء متغيّر"، فالجُزء الثّابت يتعلّق ببروتوكول الاتّصال(http://www.) الذي يحتوي على بروتوكول نقل النّص الفائق((HyperText Transfer Protocol(http) المُستعمل للاتصال، وصيغة World Wide) (Web(www.) التي تستعين بتقنيات النّص الفائق للوصول إلى موارد الشّبكة العنكبوتيّة العالميّة، بينما يُسمى الجُزء المُتغيِّر باسم المَوقِع الإلكتروني(Domain name) وهو الجُزء الذي يلي مباشرةً الجزء الثّابت، فمن خلاله تستطيع الشّركة أو المنظّمة تمييز مشروعها عن غيرها من المشروعات، حيث ينقسم اسم النّطاق إلى نوعين[3]:

فالنّوع الأول يتعلق باسم النّطاق من المستوى الأول((Top Level Domain name(TLD) الذي يوجد إلى اليمين من آخر نُقطة في اسم الموقِع الإلكتروني، الذي يمكن أن ينتهي بحرفين من رموز الدّول على غرار (dz.) للجزائر و(fr.) لفرنسا، أو يُعَبِّرُ المقطع عن طبيعة الشّركة أو المنظّمة، فمثلا(com.) يتعلق بالشّركات التّجاريّة، و(org.) للمؤسّسات، الخ...،

---

[1] **حابت آمال**، "التجارة الإلكترونية في الجزائر"، دكتوراه في العلوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري . تيزي وزو، 2015، ص ص 213، 214.

[2] **Lionel BOCHURBERG**, Internet et commerce électronique (Sites web- Contrats- Responsabilités- Contentieux), 2e édition, DELMAS, France, 2001, p. 41.
Eric CHARTON, Sites Internet : conception et réalisation, op.cit., p. 61.

[3] **Romain V. GOLA**, op.cit., p. 39.

بينما الجُزء الثّاني يتعلّق باسم النّطاق من المُستوى الثّاني (Second Level Domain(SLD))، الذي يتكوّن من الحروف الأولى من اسم المشروع أو المنظّمة أو حروف كل اسم « icann.org »، فمثلا موقِع المنظّمة العالميّة للملكيّة الفكريّة « http://www. icann.org»، يتكوّن من ببروتوكول الاتصال(http://www.) الذي يُمثِّل الجُزء الثّابت من اسم الموقع الإلكتروني، حيث يُعَبِّرُ المقطع(org.) الذي يلي مباشرة الجزء الثّابت على اسم الموقع الإلكتروني من المُستوى الأول، بينما المقطع(wipo) يُمثِّل اسم الموقع الإلكتروني من المُستوى الثّاني.

3)– تعريف الموقع الإلكتروني وفقا للمعيار الوظيفي:

استند أنصار هذا الاتجاه في تعريف الموقع الإلكتروني إلى الوظيفة التي يؤديها هذا الموقع، فمنهم من عرفه على أنّه[1]:" عنوان فريد ومميّز يتكوّن من عدد من الأحرف الأبجديّة اللاتينيّة أو الأرقام التي يمكن بواسطتها الوصول لموقع ما على الإنترنت"، فالموقع الإلكتروني يعتبر كوسيلة الاتّصالات عبر شبكة الإنترنت.

والبعض الآخر عرفه على أنّه:" عنوان منفرد على شبكة الإنترنت يسمح بتحديد الموقع وتمييزه عن غيره، وإذا أردنا تحديده فهو موقع أو عنوان على شبكة الإنترنت"[2]، بينما الرأي الآخر يرى أن الموقع الالكتروني هو:" عنوان للمشروعات عبر شبكة الإنترنت، وهو عنوان افتراضي لأنّه لا يحدد مواقع المشروعات على أرض الواقع ولكنّه يُحدّدها على شبكة الإنترنت." [3].

---

[1] **رامي علوان**، "المنازعات حول العلامات التجارية وأسماء مواقع الإنترنت"، مجلة الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات، عدد 2005/22، ص 55.

[2] **هدى حامد قشقوش**، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، مصر، 2000، ص 78.

[3] **فاتن حسين حوى**، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 53.

ثانيا– أنواع المواقع الإلكترونيّة.

يمكن تقسيم المواقع الإلكترونيّة من النّاحية التّقنيّة إلى مواقع إلكترونيّة ثابتة ومواقع إلكترونية تفاعليّة(**1**)، ومن ناحية المستويات إلى مُستوى أوّل ومُستوى ثاني(**2**).

1)– أنواع المواقع الإلكترونيّة من النّاحية التّقنيّة:

يوجد من النّاحية "التّقنيّة" نوعان من المواقع الإلكترونيّة، فالأولى تتعلّق بالمواقع الثّابتة(**Sites statiques**) التي تعتمد عادة في برمجتها على لغة(HTML)، إذ تتميّز بالسّهولة وقِصر وظيفتها المتعلّقة فقط بعرض المحتويات الثّابتة من صور ونصوص الخ...، حيث يتطلّب تغيير هذه المُحتويات تَدخُّل مُبرمِجو(Programmeurs) المَواقِع، لغرض إعادة فتح وسوم الصفحات وتعديلها أو إلغائها عبر مُحرّر ويب(Éditeur Web).

إنّ عملية تحرير صفحات ويب المتعلّقة بالمواقع الثّابتة تحتاج من النّاحية التّقنيّة إلى الاستعانة بأحد برامج مُحرّري نصوص الويب (WYSIWYG, DreamWeaver, FrontPage, Bloc-Notes, Notepad++, PSPad, etc.)، الذي يُساعِد على كتابة الوسوم (Balises de formatage ou «Tags ») وتحرير صفحات الويب التي يتم معاينتها ورؤيتها عبر متصفّح الويب(Google Chrome, Mozilla Firefox, Internet Explorer, etc.)، حيث تأخذ هذه الصفحات دائما امتداد « .html » أو « .htm» [1]

---

[1] أنظر **الملحقين رقم(07) و(08)**، ص 487.

للتعرف أكثر على لغة برمجة(HTML) أنظر ما يلي:

Moustapha MBENGUE, « Création et gestion de sites web et de portails documentaires », pp. 30- 47. Article disponible à partir de l'adresse suivante : http://docplayer.fr/7997805-Creation-et-gestion-de-sites-web-et-de-portails-documentaires.html, consultée le 13/02/2016.

Daniel - JEAN DAVIDE, HTMLE5 et CSS3, par la pratique (construire un site internet de qualité professionnelle), édition ellipses, Paris, France, 2014, p. 16.

Cédric BERGÉ, Je crée mon site Internet avec Dreamweaver 8 et Flash 8, éditions EYROLLES/DEMOS, Paris, France, 2006, pp. 26, 27.

Olivier ABOU, Créer son site web (de la construction d'une équipe jusqu'à la mise en ligne d'un site d'entreprise), Microsoft press, France, 2001, pp, 13-17.

Eric CHARTON, Sites Internet : conception et réalisation, édition Simon et Schuster Macmillan, Paris, France, 1997, pp. 161- 163.

أمّا النّوع الثّاني من المواقع الإلكترونيّة يتعلق بالمواقع التّفاعليّة(**Sites dynamiques**) التي تتميّز بخصائص تَحكُّم أكثر فاعلية وقوّة، حيث تعتمد إلى جانب لغة(HTML) وتقنية(CSS) على لغات وتقنيات أخرى مثل (PHP, MYSQL, JavaScript, AJAX, Python, etc.) التي تعمل على جانب الخادم أو موزع الويب، الشيء الذي يجعلها في تطوّر وتُسهّل عملية تغيير أو إضافة أو حذف مُحتوياتها، مع خلق تواصل مستمر بين الزّائر والمَوْقِع الإلكتروني التّفاعلي، فعلى سبيل المثال سمحت لغة برمجة صفحات الويب التّفاعليّة((Hypertext Preprocessor(**PHP**)، بإحداث عدد كبير من المواقع الالكترونيّة المشهورة(Facebook, Yahoo, Google, You tube, Wikipedia, etc.)[1].

تحتوي مواقع الويب التّفاعليّة على مجموعة من صفحات مرتبطة ببعضها البّعض، ومُخزّنة على مستوى الخادم الذي يَعرِضُهَا في الحاسوب عبر برنامج متصفّح الويب، وبالتّالي فإنّ المواقع التّفاعليّة تحتاج إلى جانب البرامج المعلوماتية السّابقة المُستخدَمَة في تقنيات تحرير ومعاينة صفحات الويب الثّابتة، إلى خادم(Serveur) مُتّصِل بالانترنت، أو القيام بتنصيب خادم محلّي(Local host) مثل(WampServer, Appserv,etc.) على جهاز الحاسوب في حالة عدم الاتصال بالإنترنت، فبما أنّ مِلفات لغة(html ou xhtml) لها وسوم خاصة بها، فإنّ لغة برمجة(php) لها وسوم خاصّة بها ومِلفاتها(php) يمكن أن تتضمّن

Daniel, AMOR, La révolution e-business, Pearson Éducation France, Paris, France, 2000, pp. 275, 276.

Daniel - JEAN DAVIDE, HTMLE5 et CSS3, par la pratique (construire un site internet de qualité professionnelle), op.cit., pp. 23- 27.

Daniel - JEAN DAVID, Développer son site web, édition ellipses, Paris, France, 2007, pp. 26- 34.

Eric CHARTON, créer votre site web, campus press, Paris, France, 2004, pp. 36- 46.

[1] للمزيد من المعلومات حول الموضوع، أنظر المَوقِع التالي: http://php.net/manual/fr/book.dom.php(تم الإطّلاع عليه في 2016/02/12.)

Voir aussi : **Philippe RIGAUX**, Pratique de MySQL et PHP(Conception, et réalisation de site web dynamique.), 4e édition, Dunod, Paris, France, 2009, pp. 20- 23.

على وسوم لغة برمجة(html)، الشيء الذي يعطي إمكانية قوية في التّحكم والعَرض، وأيّ كود يُكتب خارج هذه الوسوم فيتم طباعته مباشرة ولا يتم تنفيذه كشفرة(php)[1].

2)- أنواع المواقع الإلكترونيّة من حيث المستويات:

تنقسم المواقع الإلكترونيّة من حيث عدد المستويات، إلى مواقع إلكترونيّة من المستوى الأوّل(أ)، ومواقع إلكترونيّة من المستوى الثّاني(ب).

أ- المواقع الإلكترونيّة من المستوى الأول(Domaine de premier niveau):

إنّ نظام أسماء المواقِع(DNS) عبارة عن قاعدة بيانات(Base de données) مُنتشرة بمُستويات مختلفة في بِنْيَة هرميّة من جذور الخوادم الرّئيسية(Root servers)، التي تُمثّل النطاقات الجذرية(Root domains) أو(Serveurs racine du DNS)، باعتبارها كأعلى مُستوى في البِنية الهرمية حيث يُشار إليها بالنقطة(.)[2]، وبالتالي فإنّ تقنية التّسمية في النّطاق تعتمد على عملية التّجميع الهرمي لأسماء النّطاقات التي تَعرِف عدّة مُستويات مختلفة في بنية هرميّة، حيث يشمل المستوى الأوّل على النّطاق الجّذري(Root domain) المُشار إليه بالنّقطة(.)[3]، والجدير بالذّكر أنّ الخوادم الرّئيسية لأسماء النّطاقات تُديرها أو

---

[1] أنظر **الملحق رقم (03)**، ص 488.

Voir aussi : **François- XAVIER BOIS**, Sites web dynamiques (PHP, MySQL, JavaScript™, Ajax), MA édition, France, 2012, pp. 74- 78.

Nicolas MOYROUD, « Introduction au langage PHP », pp. 06- 23. Article disponible sur : http://www.ird.fr/informatique-scientifique/.../php/cours_introduction_php.pdf, consulté le 10/02/2018.

William STEINMETZ, Brian WARD, PHP clé en main (76 scripts efficaces pour enrichir vos sites web), Pearson éducation France, 2008, pp. 4-21.

Lary ULLMAN, PHP 6 et MySQL 5(Créez des sites web dynamique), Dunod, Paris, France, 2008, pp. 2-5, 9- 16, 25-31, 38- 42, 91- 96.

[2] **Nathalie DRYFUS**, Marques et Internet (Protection, valorisation, défense.), éditions Lamy, France, 2011, pp. 20, 21.

Hélie - SOLANGE GHERNAOUTI, Sécurité Internet : Stratégies et technologies, Dunod, Paris, France, 2000, p. 192.

Olivier GOURBESVILLE, « Faut-il avoir peur d'Internet ? », Revue Pour, 2007/3 (n° 195), pp. 22, 23.

[3] أنظر **الملحق رقم (04)**، ص 488.

Voir aussi : **Hans KLEIN**, « ICANN et la gouvernance d'internet. La coordination technique comme levier d'une politique publique mondiale », Les Cahiers du numérique 2002/2 (Vol. 3), pp. 103-106.

تُسيّرها حاليًّا ثلاثة عشرة(13) منظّمة أو هيئة، اثنان(02) منها أوروبية، واحدة(01) من اليابان، والعشرة(10) الباقية من الولايات المتّحدة الأمريكيّة[1].

أمّا النّطاق الذي يأتي مُباشرة تحت الجِّذر(Sous la racine) يُمثِّل مُستوى القِمَّة للنّطاقات(Domaine de tête) ويُدعى كذلك بنطاق المُستوى الأوّل الأعلى (Top-Level Domains(**TLDs**)) أو(Domaines de haut niveau) الذي يتكوّن من حرفين أو ثلاثة حروف، تُعَبِّرُ عن نوع المُنظّمة أو الشّركة أو الموقِع الجغرافي أو أيّ شيء آخر، وبالتّالي فإنّ أسماء النّطاقات العليا(**TLD**) يمكن تقسيمها إلى ثلاثة أنواع، والمتمثّلة فيما يلي:

أ-1- أسماء المواقع العليا المُكوّنة من رموز الدّول (country code Top-Level Domain «ccTLD»: يخصص هذا المجال لكل دولة من دول العالم أو إقليم مستقل، حيث يتكوّن من حرفين من اسم تلك الدّولة أو ذلك الإقليم وفقا لمعيار الآيزو ISO 3166) (Standard 3166، مثل(.ch) لسويسرا، و(.fr) لفرنسا، و(.be) لبلجيكا، و(.dz) للجزائر، (.us) للولايات المتحدة الأمريكية، و(.uk) للمملكة البريطانيّة المتّحدة، و(.ca) لكندا الخ... أو المستوى الأعلى حسب الانتماء القاري أو الجهوي(Extensions régionales) مثل(.eu) للإتحاد الأوروبي و(.asia) لقارة آسيا، وكذا مُستويات أسماء المواقع العُليا العامّة (generic Top-Level Domain (gTLD)) مثل(.com) و(.org) و(.net) و(.bz) الخ...[2].

أ-2- أسماء المواقع العليا القاريّة(Extensions régionales - Supranationales): يُقصد بها المواقع الإلكترونيّة التي تُشير إلى أنشطة دوليّة حسب الانتماء القارّي، حيث

---

[1] للمزيد من المعلومات أنظر المواقع الالكترونية التالية: ftp://rs.internic.net/domain/named.cache ou https://www.root-servers.net

Voir aussi: **Jacques BERLEUR, Yves POULLET**, « Réguler Internet », Revue Études, 2002/11 (Tome 397), p. 366.

[2] **رامي علوان**، مرجع سابق، ص 250.

Voir aussi: **Vincent FAUCHOUX, Pierre DEPPREZ**, Le droit de l'internet : Lois, Contrats, Usages, Litec, France, 2009, pp. 08, 09.

للمزيد من المعلومات أنظر المواقع الإلكترونية التالية: http://www.iana.org/domains/root/db ou https://www.icann.org/tlds/ ou http://www.iana.org/cctld/cctld-whois.htm

يمكن لأي شخص طبيعي أو معنوي الذي يثبت إقامته في قارّة أو جهة معيّنة خارجة عن إقليم دولته الأصليّة، أن يقوم بتسجيل اسم نطاقه الأعلى ضمن النّطاق الأعلى القارّي أو الجهوي، فمثلا اسم النّطاق الأعلى(eu.) للاتّحاد الأوروبي و(asia.) لقارّة آسيا، الخ...

أ-3- أسماء المواقع العليا العامّة(gTLD): ترتبط هذه الأسماء من حيث المبدأ حسب طبيعة الشّركة أو المؤسّسة أو المنظّمة التي ترغب في تسجيل اسم النّطاق أو بنشاطها الرّئيسي، حيث يُعبَّر عن هذه المَواقِع برمز يتكوّن عادة من ثلاثة حروف أو أكثر، فبعدما أن تم حصر استخدام النّطاقات(mil.) و(gov) و(edu.) على الجامعات والسّلطات الإدارية والعسكرية الأمريكية، أصبحت باقي المجالات الأخرى مُتاحة للتّسجيل لأيّ شخص أو مؤسّسة أو منظّمة أو دولة أو إقليم(باستثناء النّطاقات المقيّدة)، فمثلا(com.) للمواقع التّجاريّة و(net.) لمواقع مُزوّدي خدمات الإنترنت، و(biz.) لمواقع الأعمال، و(aero.) لشركات الطّيران، و(coop.) لتعاونيات الأعمال، و(int.) لمواقع المنظّمات الدّوليّة، و(info.) لمواقع الاستخدامات العامّة، و(pro.) لمواقع المحترفين، و(fm.) لمحطّات الرّاديو، الخ...[1].

ب - المواقع الإلكترونيّة من المستوى الثّاني(Domaine de deuxième niveau):

يُدعَى اسم النّطاق الذي يأتي مباشرة بَعْدَ اسم نطاق المستوى الأوّل(**TLD**) بنطاق المستوى الثّاني((Second Level Domain(**SLD**)، الذي يتكوّن من الجزء الذي يقع على يسار آخِر نقطة في اسم المَوقِع، حيث يمكن للهيئة المسؤولة عن تسجيل وإدارة أسماء المواقع من المستوى الأوّل توزيع الخدمة على مستويات أدنى، وبتعبير آخر يُمكِن لنطاقات المستوى الأعلى(TLD) أن تحتوي على نطاقات المستوى الثّاني(SLD)، كما يُمكِن كذلك لهذه الأخيرة أن تتضمّن بدورها على نطاقات فرعيّة(Sub domains)، فمثلا يمكن إنشاء أسماء نطاقات فرعيّة من المستوى الثّاني ضمن اسم النّطاق الأعلى المُكوّن من رمز دولة

---

[1] **رامي علوان**، مرجع سابق، ص ص 251، 252.

للمزيد من المعلومات حول الموضوع، أنظر الموقع الإلكتروني التالي: https://www.icann.org/tlds/

أنظر كذلك، **الملحق رقم (05)**، ص 489.

الجزائر(dz.)، كالشّركات التّجاريّة(com.dz.)، والمنظّمات الحكوميّة(org.dz.)، ومنظّمات الإنترنت(net.DZ.)، والجّمعيات(asso.dz.)، الخ...

ثالثا- الأهميّة التّجارية للمواقع الإلكترونيّة.

إنّ أهميّة مواقع التّجارة الالكترونيّة تتجلّى من خلال العناصر التّالية:

1- تسهيل الدّخول إلى الموقع التّجاري: إنّ نظام أسماء المواقع الإلكترونيّة يسهل الاتّصال بشبكة الإنترنت من خلال استبدال الأرقام التي تفهمها لغة الحواسيب، بمجموعة من الحروف التي تُمثّل اسم المشروع التّجاري، حيث يُخصّص لكل مَوقِع تِجَارِي مُرتبط بشبكة الإنترنت عنوان إنترنت أو رقم خاص به[1].

2- إعلان المشروعات التّجارية عبر الإنترنت: يُمكن لأي شخص أن يَتَّخِذَ من الإنترنت موطنا افتراضيا يُعْلِنُ فيه نشاطه التّجاري باستخدام نظام أسماء مواقع الإنترنت، حيث لا يُمكن للمستهلك الدّخول إلى المَوقِع التّجاري إلاّ باستخدام اسم النّطاق الخّاص به[2].

3- تمييز المشروعات التّجاريّة عبر الإنترنت: إنّ عملية تسجيل أسماء مواقع الإنترنت تخضع لقاعدة الأسبقية في التّسجيل التي تقضي بأنّه لا يجوز لأكثر من مشروع أن يكون له موقع إلكتروني نفسه، حيث يجب أن يكون لكل مشروع تجاري موقع إلكتروني يُميّزه عن غيره من المشروعات الأخرى، وأن لا يمس بأحد حقوق الملكيّة الفكريّة الصّناعيّة(العلامة، الاسم والعنوان التّجاري...) المحميّة بموجب القوانين الخاصّة بها[3].

4- ترويج مختلف السّلع والخدمات: يعتبر الموقع الإلكتروني التّجاري كأداة فعّالة لترويج السّلع والخدمات عبر الإنترنت، وإتاحة المعلومات حولها بالقدر الكافي نصًّا وصُورةً أو حتى باستخدام مقاطع الفيديو، أو التّعوِيل على التّقنيات الحديثة الأخرى المُستخدمة في الدّعاية لهدف جذب اهتمام العملاء وكسب ثقتهم لاتّخاذ قرار الشّراء في الوقت المناسب.

---

[1] **رامي علوان**، مرجع سابق، ص ص 247، 248.

[2] **عبد الله عبد الكريم عبد الله**، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2008، ص 288.

[3] **فاتن حسين حوى**، مرجع سابق، ص 62.

5– ضمان إجراءات الشّراء والدّفع الإلكترونيين: إنّ مواقع التّجارة الإلكترونيّة تسهل وتضمن للمستهلك إجراءات دفع تكاليف السّلع والخدمات، باستخدام إحدى وسائل الدّفع الالكتروني المتاحة عبر المنصّة الإلكترونيّة، من دون التّنقّل أو بذل أي جُهد إضافي.

6– تشجيع وتطوير الميزة التّنافسيّة للشّركة: تساهم مواقع التّجارة الإلكترونيّة في تحسين القدرة التّنافسيّة للشّركة من خلال استغلال الفرص التّسويقيّة المتاحة، التي تمكّنها من جذب العملاء الجُدد والدّخول إلى الأسواق الجديدة، بغية تحقيق المزيد من الأرباح وتحسين سُمعتها التّجارية مع تعزيز حصتها وتواجدها في الأسواق[1].

الفرع الثاني
خطوات إحداث مواقع التّجارة الإلكترونيّة

المتجر الإلكتروني عبارة عن مِنَصَّة إلكترونيّة لبيع وشراء السّلع والخدمات عبر شبكة الإنترنت، حيث تتطلّب عملية إحداثها من النّاحية التّقنيّة مراعاة الخطوات التّالية: التّخطيط المسبق للمشروع **(أولا)**، احترام دفتر الشّروط **(ثانيا)**، شراء اسم النّطاق **(ثالثا)**، إيواء الموقع التّجاري الإلكتروني **(رابعا)**، تصميمه **(خامسا)**، التّرويج له **(سادسا)**، التّصريح به لدى الهيئة المكلّفة بحماية المعطيات الشّخصية **(سابعا)**، استغلال وصيانة الموقِع **(ثامنا)**.

أولا– التّخطيط المُسبق لمشروع إحداث المتجر الافتراضي:

يجب على الرّاغب في إحداث متجر افتراضي أن يقوم بدراسة مُسبقة لمشروعه، أخذا بعين الاعتبار المجال والأهداف والتّكاليف المُنتظرَة من المشروع، والإمكانيات الماليّة والبشريّة والتّقنيّة المُسّخرة فيه، والإحاطة بكلّ ما يَسْتَوْجِبُهُ مُحْتَوَى المَوقِع الإلكتروني من إيواء وعِناية خاصّة، وتخطيط أو تصميم مُفصّل ومدروس بِدقّة، والتّكاليف النّاجمة عن حمايته، وصيانته، وتحديثه، الخ...، وكذا مدى إمكانية الاعتماد على مُزوِّد خدمات إنترنت يُشرِف

---

1) **Alain d'IRIBARNE, Robert TCHOBANIAN**, « PME et TIC : quels sites web pour quelles PME ? », Revue Réseaux ; 2003/5 n° 121, pp. 149-154.
Philippe IRRMANN, Jean BROUSSE, Maurice LEVY, Dominique SCAGLIA, L'informatique au service du marketing, Masson éditeur, Paris, France, 1976, pp.151, 152.

لوحده وبنفسه على تحقيق جميع مراحل ومتطلّبات مشروع بناء المَتجر الافتراضي، وفقا للشّروط المحدّدة مُسبقا في دفتر الشّروط الخّاص بعقد إحداث الموقع الإلكتروني، أو اللّجوء إلى إبرام عدّة عقود خدمات إنترنت مع مزوّدين آخرين على غرار العقود المتعلّقة: باسم النّطاق(Création d'un nom de domaine)، والإيواء(Ébergement)، والإحالة(Référencement)، والصّيانة(Maintenance)، الخ...[1].

ثانيا- احترام دفتر الشّروط الخّاص بإحداث المتجر الافتراضي:

إنّ عملية بناء المتجر الافتراضي عبر الإنترنت، تستوجب من النّاحية القانونيّة إبرام سِلْسِلَة من العقود الفنيّة مع مُزوّدي خدمات الإنترنت التي تُحَدَّدُ فيها حقوق والتزامات كل طرف في العقد، حيث تفرض عادة على صاحب المشروع تحمّل العديد من الأعباء أو المصاريف المترتّبة عن دفتر الشّروط الخّاص بِكُلِّ عقد، ولتفادي كلّ المخاطر القانونيّة والتّقنيّة النّاجمة عن عدم الانسجام والتّناسق فيما بين الخدمات المتاحة أو عدم تحقيقها، يجب على صاحب المشروع، أن يَقَعَ اِخْتِيَارِهِ على مُزوِّد خدمات إنترنت يُشرف لِوَحْدِهِ على الخدمات الأساسية، المُتعلّقة بجميع مَرَاحِلِ إحداث واستغلال المتجر الافتراضي عبر الإنترنت، التي يتيحها سواء في إطار عقد مُوحَّد(Un contrat unique) أو عن طريق إبرام سلسلة من العقود الفنّيّة(Contrats séparés) مع نفس المُزوّد[2].

ثالثا- شراء اسم النّطاق:

يجب على صاحب مشروع إحداث المتجر الافتراضي أن يقوم بشراء اسم النّطاق(DN)، الذي من المُسْتَلْزَمِ أن يُعَبِّرَ عن نَوْعِ النّشاط مع التّأكد من عدم استخدامه مُسبقا من قِبَلِ الأطراف الآخرين، مع إضافته الامتداد الذي يَدُّلُ على نوع الشّركة، فلكي يتمتّع صاحب اسم

---

1) **Jakob NEILSEN, Hoa LORANGER**, Sites web: priorité à la simplicité, Pearson, Paris, 2007, pp. 150- 155.
Jean-Paul TRIAILLE, « Le Contrat de création d'un site Web », pp. 03, 04. Article publié le 08/03/2001 sur : https://www.droit-technologie.org, consulté le 15/04/2017.
2) **Vincent FAUCHOUX, Pierre DEPPREZ**, op.cit., pp. 263, 266, 267.
Hubert BITAN, « Le site de commerce électronique : approche technique et juridique », Gazette du Palais- 18/04/2000 - n° 109, p. 05.

النّطاق بحق استعماله، يجب عليه أن يَحْتَرِمَ قاعدة الأسبقيّة في تسجيل الاسم لكي يَخْدُمَهُ« premier arrivé, premier servi »، المُتبّعة في جميع إجراءات التّسجيل حَسْبَ جِهة التّسجيل ونوع المَوقِع المرغوب تسجيله[1]، سواء كان يتعلق بالنّطاق العام العالي(gTLD)، أو باسم نطاق وطني(ccTLD) أو تابع لجهة معيّنة (Extensions régionales)، مع احترام إجراءات التّسجيل المحدّدة بموجب اتفاقية تسجيل اسم النّطاق[2].

لذا يجب على كلّ راغب في اختيار اسم النّطاق أن يقوم قبل تسجيله، بإجراء بحث مُسبق في قاعدة بيانات« Whois »، المتواجدة عبر المِنصّة الإلكترونية للمُسجّل أو مكتب التّسجيل المُعتمد، لغرض الحصول على المعلومات الكافية حول أسماء النّطاق المُسجّلة والغير المُسجّلة، حيث تتراوح مُدّة تسجيل اسم النّطاق عادةً ما بين سنة(01) إلى عشرة(10) سنوات وذلك مقابل أجر محدّد مع إمكانية تجديد تلك المُدّة كلّما قَرُبَتْ نهايتها، حيث يظهر المَوقِع الالكتروني(http://www.icann.org) مُباشرةً بعد إتمام إجراءات تسجيله، في نافذة المتصفّح الالكتروني((Uniform Ressource Locator(URL)).

رابعا- إيواء الموقع التّجاري الإلكتروني:

يجب على صاحب مشروع إحداث المتجر الافتراضي الاستعانة بمقدّم خدمات الإيواء((Hébergeur web(web hosting)، الذي يشرف على مهام تخزين محتوى المواقع الإلكترونيّة على خوادمه الرّئيسيّة بشكل مُباشر ودائم، مع إتاحة الوسائل التّقنيّة اللاّزمة التي تسمح بِبَثٍّ مختلف الصّور والنّصوص والأصوات الخ... المتعلّقة بنمط الخدمة ونوعيّة السّلعة المتاحة على شبكة الإنترنت[3]، حيث يقوم متعهد الإيواء بتخصيص مساحة قرص أو

---

1) **Nicole TORTERELLO, Pascal LOINTIER**, Internet pour les juristes, édition DALLOZ, Paris, France, 1996, pp. 236- 244.
Eric CHARTON, créer votre site web, op.cit., pp. 175 et suiv.
للمزيد من المعلومات حول إجراءات تسجيل أسماء النطاق أنظر الموقع التالي: https://www.gandi.net/whois/

2) أنظر **الملحق رقم (06)**، ص 489.

3) **Sandrine CARNEROLI**, Les contrats commentés du monde informatique : Logiciels, Bases de données, Multimédia, Internet, 2e édition, Larcier, Belgique, 2013, pp. 123, 135, 136- 145.

شريط مرور لبث المعلومات، مع تزويد صاحب المَتجر الافتراضي بمفتاح دخول(code d'accès) للتعريف بهويته، وببرنامج خاص يسمح له بالاتصال بمزود الخدمة أو إضافة أو حذف أو تغيير ما يريده من المعلومات.

خامسا– تصميم الموقع التّجاري الإلكتروني:

إنّ آليات تصميم مواقع التّجارة الإلكترونيّة(Web design) تختلف من موقِع إلى آخر بحسب تقنيات البرمجة المُستخدمة في تطبيقات الويب(PHP, HTML, etc.)، حيث يجب أن يحتوي التّصميم على مُحتوى صفحات ويب جيّدة ومُتجانسة مع نظام تصفّح سهل التّحميل للمستهلك، الذي لا يحتاج إلى أيّ جُهد للوصول إلى الصّفحة المُراد الوصول إليها، فعادة ما ينصرف المستهلك عن المتجر الافتراضي لسبب صعوبة تحميل صفحاته وطول فترة الانتظار[1]، وبالتّالي يصبح المَتجر الافتراضي عديم الفائدة في حالة ما إذا تضمّن على تصميم رائع ومُحتوى رديء لا يستجيب لتَوقّعات ومُتطلّبات المُستهلكين، لذا ينبغي أن يجتمع التّصميم الفعّال والمُحْتَوَى الجيِّد لضمان نجاح مواقِع التّجارة الإلكترونيّة[2].

سادسا– التّرويج للموقع التّجاري الإلكتروني:

يجب على صاحب المَوقِع الإلكتروني أن يعمل على ترويجه في عدّة محرّكات البحث ومحتويات الأدّلة أو الفهارس المعلوماتيّة(Annuaires)، بواسطة العقد المناسب الذي يُعرف بعقد الإحالة(Contrat de référencement)، الذي بموجبه تتم عملية تسجيل الموقع الإلكتروني بطريقة آلية أو يدوية، لهدف تضمينه والاعتراف به ضمن قواعد بيانات محرّكات

---

1) **Bruno DURAND**, « L'épicerie en ligne. Les atouts des petits commerces indépendants », Revue des Sciences de Gestion, 2005/4 (n°214-215), pp. 145, 146.

2) **Emmanuel KESSOUS**, « Le commerce électronique et la continuité de la chaine logistique. De l'approvisionnement des sites à la livraison aux consommateurs », Revue Réseaux 2001/2 n° 106, pp. 117, 118.

Sylvie HÉROUX, Jean-François HENRI, « Reporting sur le Web : optimisation de la gestion de contenu des sites web », Revue des Sciences de Gestion, 2011/6 n° 252, pp.60, 64, 65.

François OLLÉON et autres, « Monter son projet de gestion de contenu », Revue Documentaliste-Sciences de l'Information, 2008/3 (Vol. 45), pp. 56- 59.

Jean-MARC HARDY, Gaetano PALERMO, Réussir son site web en 60 fiches, 3e édition, Dunod, Paris, France, 2010, pp. 34, 35, 38, 39, 42- 45, 46, 47, 50-53.

البحث أو فهارس البحث على شبكة الإنترنت[1]، حيث يتعيّن على مُبرمِجو صفحات الويب أن يقوموا بانتقاء أحسن الكلمات الدّالة اللاّئقة بمحتوى المَوقِع التّجاري الإلكتروني، التي من شأنها أن تضفيه مرتبة أحسن من بين المواقع التّجاريّة الإلكترونيّة الأخرى أو تُسهّل أو تُسرِّع في عمليات البحث عن السّلعة أو الخدمة المُتاحة على مستوى المَتجر الافتراضي[2].

سابعا- التّصريح لدى الهيئة المكلّفة بحماية المعطيات الشّخصية:

يجب على صاحب المتجر الافتراضي أن يأخذ بعين الاعتبار أحكام التّشريعات والتّنظيمات المتعلّقة بحماية المعطيات الشّخصية للأشخاص الطبيعيين، أين يتعيّن عليه الالتزام بالتّصريح لدى الهيئات المعنيّة بحماية المعطيات الشّخصية، باعتبار التّاجر الافتراضي كمسؤول على المعالجة الآلية للمعطيات الشّخصية[3].

ثامنا- استغلال وصيانة الموقع التّجاري الإلكتروني:

إنّ عملية شراء أو الحصول على اسم موقع الإنترنت لا يعني بالضّرورة الحصول على موقع إلكتروني بكامل معاييره ومواصفاته التّقنيّة، بل يُعطي فقط لصاحبه حق التّصرف في اسم نطاق الإنترنت في حدود فترة تسجيله، حيث ينبغي على صاحب الموقع التّجاري الإلكتروني أن يقوم باستغلاله فعليا بمجرّد استكمال أو نفاذ الخطوات الباقيّة لإحداثه، مع القيام بصيانته في إطار عقد الصّيانة الذي يحدد حقوق والتزامات كل طرف فيه[4].

---

1) **Cyril ROJINSKY,** « Les techniques contractuelles du commerce électronique », Revue Legicom, 2000/1, n° 21-22, pp. 107, 108. **Romain V. GOLA**, op.cit., pp. 440-442.
Philippe LE TOURNEAU, Contrats informatiques et électroniques, Dalloz, 8e édition, France, 2014, pp. 462- 468. **Lionel BOCHURBERG**, op.cit., pp. 105, 106.

2) **Olivier ANDRRIEU**, Réussir son référencement web, éditions Eyrolles, Paris, France, 2012, pp. 7, 8, 9, 10, 104- 107, 108- 117.

3) **Fabrice MATTATIA**, Traitement des données personnelles- le guide juridique (La loi informatique et libertés et la CNIL Jurisprudence), éditions EYROLLES, France, 2013, pp. 55- 60, 68- 74. **Hubert BITAN**, op.cit., p. 07.
Jean-GUY DE RUFFRAY et autres., « Droit de l'information », Revue Documentaliste-Sciences de l'Information, 2013/4 (Vol. 50), pp. 18,19.

4) **Etienne WÉRY**, « Comment rédiger en pratique un contrat de commerce électronique ? », pp. 17- 25. Article publié le 16/10/2000 sur : https://www.droit-technologie.org, consulté le 12/09/2017.

الفرع الثالث

متطلبات إحداث مواقع التّجارة الإلكترونيّة

لضمان تقديم خدمة فعّالة ومضمونة للعملاء يجب على المُورّد الإلكتروني احترام الشّروط القانونيّة المتعلّقة بممارسة التّجارة الإلكترونيّة**(أوّلا)**، والمتطلّبات المتعلّقة سواء بالعرض الإلكتروني**(ثانيا)**، أو الإشهار والدّفع الإلكترونيين**(ثالثا)**، وكذا المتطلّبات المتعلّقة بالعقد الإلكتروني**(رابعا)**.

أوّلا– شروط ممارسة التّجارة الإلكترونيّة:

إنّ ممارسة أي نشاط تجاري لدى أيّة دولة كانت، يجب أن تُراعى فيه الأحكام التّشريعية والتّنظيميّة المُنظّمة لذلك النّشاط لضمان استمراريّة وبقاء المتجر الافتراضي[1]، حيث قام المشّرع الجزائري بإصدار القانون رقم 18–05 المؤرخ في 10 ماي 2018 المتعلق بالتّجارة الإلكترونيّة[2]، الذي حدّد بموجب أحكام نص المادتين 08 و09 منه الشّروط المتعلّقة بمزاولة أيّ نشاط تجاري إلكتروني في الجزائر، التي من خلالها يجب على المعني بالأمر أن يقوم بتسجيل نشاطه التّجاري الإلكتروني حسب الحالة، سواء في السّجل التّجاري أو في سجّل الصّناعات التّقليديّة أو الحرفيّة، وكذا تسجيل اسم المَوقِع التّجاري الإلكتروني عبر

---

[1] **رشا محمد تيسير الحطاب، مها يوسف خصاونة**، "تطبيق النظام القانوني للمحل التجاري على الموقع التجاري الإلكتروني"، مجلة الشريعة والقانون، كلية القانون، جامعة اليرموك، عدد 2011/02، ص ص 347– 353. https://www.journal.uaeu.ac.aeissues/.

[2] **قانون رقم 18–05** مؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، ج ر عدد 28 الصادر في 16 ماي 2018.

تنص **المادة 06** منه، على ما يلي: " يُقصد في مفهوم هذا القانون بما يأتي:

– **المستهلك الإلكتروني:** كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الإلكترونية من المورد الإلكتروني بغرض الاستخدام النهائي.

– **المورد الإلكتروني:** كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الإلكترونية. [...].

– **اسم النطاق:** عبارة عن سلسلة من أحرف و/أو أرقام مقيّسة ومسجلة لدى السجل الوطني لأسماء النطاق، وتسمح بالتعرف والولوج إلى الموقع الإلكتروني."

امتداد(Com.dz) وإيوائه لدى مؤدي خدمات استضافة مُقيم في الجزائر، مع إيداعه لاسم النّطاق المُسجّل لدى مصالح المركز الوطني للسّجل التّجاري، وينبغي على المُورِّد الإلكتروني أن تَتَوَفَّرَ لديه وسائل تسمح للمُستهلك الإلكتروني بالتّأكد من مدى سلامة وصحة اسم مَوقِع الإنترنت المُسجَّل في الجزائر، حيث يَضَعُ المركز الوطني للسّجل التّجاري في مُتَنَاوَلِ المستهلكين الإلكترونيّين بطاقية وطنية مَنشُورة عبر الإنترنت، تَضُمُّ جميع المُورّدين الإلكترونيّين المُسّجلين في السّجل التّجاري أو في سجّل الصّناعات التّقليدية والحرفيّة[1].

تجدر الإشارة في هذا السّياق، أنّ المشّرع الجزائري قام بتعديل بعض أحكام القانون رقم 04-08 المؤرخ في 14 أوت 2004 المتعلّق بشروط ممارسة الأنشطة التّجاريّة، بموجب القانون رقم 18-08 المؤرخ في 10 جويلية 2018، الذي من خلاله استحدث بموجب المادتين 5 مكرر1 و5 مكرر2[2]، بوابة إلكترونية يُشرف عليها المركز الوطني للسّجل

---

[1] تنص المادة 08 من القانون رقم 18-05، سالف الذكر، على ما يلي:" يخضع نشاط التجارة الإلكترونية للتسجيل في السجل التجاري أو في سجل الصناعات التقليدية والحرفية، حسب الحالة، ولنشر موقع إلكتروني أو صفحة إلكترونية على الإنترنت، مُستضاف في الجزائر بامتداد "com.dz". يجب أن يتوفر الموقع الإلكتروني للمورد الإلكتروني على وسائل تسمح بالتأكد من صحته."

وتنص المادة 09 من نفس القانون، على ما يلي:" تنشأ بطاقية وطنية للموردين الإلكترونيين لدى المركز الوطني للسجل التجاري، تضم الموردين الإلكترونيين المسجلين في السجل التجاري، أو في سجل الصناعات التقليدية والحرفية. لا يمكن ممارسة نشاط التجارة الإلكترونية إلاّ بعد إيداع اسم النطاق لدى مصالح المركز الوطني للسجل التجاري. تنشر البطاقية الوطنية للموردين الإلكترونيين عن طريق الاتصالات الإلكترونية وتكون في متناول المستهلك الإلكتروني."

[2] قانون رقم 04-08 مؤرخ في 14 أوت 2004، يتعلق بشروط ممارسة الأنشطة التجارية، ج ر عدد 52 الصادر في 18 أوت 2004، المعدل والمتمم بموجب القانون رقم 18-08 المؤرخ في 10 جويلية 2018، ج ر عدد 35، الصادر في 13 جويلية 2018.

تنص المادة 5 مكرر1 على ما يلي:" تنشأ بوابة إلكترونية لتسهيل إجراءات إنشاء المؤسسات. يكلف المركز الوطني للسجل التجاري بمهمة تسيير البوابة الإلكترونية المخصصة لإنشاء المؤسسات. تحدد كيفيات تسيير وسير البوابة الإلكترونية وكذا كيفيات التسجيل والتحويل واستلام الوثائق الإلكترونية ومنح رقم التعريف المشترك، عن طريف التنظيم."

تنص المادة 5 مكرر 2 على ما يلي:" تتضمن البوابة الإلكترونية المذكورة أعلاه، استمارة موحدة. يقوم المركز الوطني للسجل التجاري بالمصادقة على الاستمارة الموحدة المملوءة والممضاة والمصادق عليها بالطريق الإلكتروني من طرف منشئ المؤسسة بعد تأكيدها وتسجيلها من طرف الإدارات المكلفة بالسجل التجاري والضرائب والإحصائيات والضمان

التّجاري لتسهيل إجراءات إنشاء المؤسّسات عبر الإنترنت، بينما تُحدَّد عن طريق التّنظيم كيفيات تسيير وسير البّوابة وكيفيات التّسجيل والتّحويل واستلام الوثائق الإلكترونيّة، وكذا منح رقم التّعريف المُشترك الذي يتم الحصول عليه، بعد قيام مُنشئ المؤسّسة بملء وتوقيع(إلكترونيا) الاستمارة المُوحّدة المُتاحة عبر البّوابة الإلكترونيّة، التي يُصادق عليها المركز الوطني للسّجل التّجاري بطريقة إلكترونيّة، وذلك بعد تأكيدها وتسجيلها من طرف الإدارات المُكلّفة بالسّجل التّجاري والضّرائب والإحصائيات والضّمان الاجتماعي.

ثانيا– المتطلبات المتعلّقة بالعرض الإلكتروني:

ألزم المشّرع الجزائري المورّد الإلكتروني بضرورة مراعاة متطلّبات التّجارة الإلكترونيّة، الواردة في أحكام الفصل الثالث(الباب الثاني) من نفس القانون، كضرورة إعداد عرض تجاري إلكتروني بطريقة مرئية ومقروءة ومفهومة يتضمّن على الأقل على البيانات الواردة في أحكام المادة 11 من نفس القانون[1]، كإعداد وصف كامل لمختلف مراحل تنفيذ المعاملة الإلكترونيّة ومدّة صلاحية العرض، وتحديد الأرقام المتعلّقة بالهاتف والتّعريف الجّبائي والسّجل التّجاري للمورّد الافتراضي، وعناوينه الماديّة والالكترونيّة ورقم البطاقة المهنيّة للحرفي، وطبيعة وأسعار السّلع والخدمات المُقترحَة مع احتساب جميع الرّسوم، وعند الاقتضاء طريقة حساب السّعر في حالة عدم تحديده مُسبقا، وكذا تحديد الشّروط العامّة المتعلّقة بالبيع، لاسيما الأحكام المتعلّقة بحماية المعطيات ذات الطابع الشّخصي، وشروط الضّمان التّجاري وخدمة ما بعد البيع، وشروط وآجال العدول، وتلك الشّروط المتعلّقة بفسخ العقد عند الاقتضاء، وكذلك طريقة تأكيد وإلغاء الطلبيّة المُسبقة(Précommande) وكيفيات وإجراءات الدّفع، وآجال وموعد تسليم المنتوج وطريقة إرجاعه أو استبداله أو تعويضه.

الاجتماعي. وبعد المصادقة على الاستمارة الموحدة، يكون للمعني حق التسجيل لدى الإدارات المعنية المذكورة أعلاه، والحصول على رقم تعريف مشترك."

[1] راجع المادة 11 من القانون رقم 18–05، المؤرخ في 10 ماي 2018، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

ثالثا- المتطلبات المتعلّقة بالإشهار والدّفع الإلكترونيين:

إنّ الرّسالة الإعلانيّة الإلكترونيّة تستهدف العملاء للدّخول إلى مَوقِع التّجارة الإلكترونيّة حيث يستوجب على المورّد الالكتروني، مراعاة المتطلّبات المتعلّقة بالإشهار الإلكتروني(**1**)، وكذا المتطلّبات القانونيّة والتّقنيّة المتعلّقة بالدّفع الإلكتروني(**2**).

1)- المتطلبات المتعلّقة بالإشهار الإلكتروني:

يُقصد بالإشهار الإلكتروني، وفقا للفقرة 06 من المادة 06 من القانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتّجارة الإلكترونيّة، كل "إعلان" يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتّصالات الإلكترونيّة، وبالتّالي ألزمت أحكام المادة 34 من نفس القانون، المُورّد الالكتروني، بعدم القيام بنشر أيّ إشهار أو ترويج عن طريق الإنترنت لكلّ سلعة أو خدمة ممنوعة من التّسويق بموجب التّشريع والتنظيم المعمول به، مع وجوب احترام المتطلبات المتعلقة بالإشهار الإلكتروني الواردة في أحكام المادة 30 من نفس القانون، كأن تكون الرّسالة الإشهارية واضحة وتسمح بتحديد الشّخص الذي تم تصميم الرّسالة لحسابه ولا تَمُس بالآداب والنّظام العامين، وفي حالة ما إذا كان العرض تجاريا أو تنافسيا أو ترويجيا، يجب أن يُحَدَّدَ فيه ما إذا كان يشمل تخفيضات أو هدايا أو مكافآت، وكذا التّأكد من أنّ جميع الشّروط الواجب استيفاءها للاستفادة من العرض التّجاري ليست مُضلّلة وغير غامضة.

كما يُمنع على الموّرد الإلكتروني وفقا لأحكام المواد 31 و32 و33 من القانون رقم 18-05، المتعلّق بالتّجارة الإلكترونيّة، استعمال معلومات شخص طبيعي بأيّ شكل من الأشكال، من دون موافقته المُسبقة على تلقي استبيان مباشر(Prospection directe) عن طريق الرّسالة الإلكترونيّة أو أي اتصال إلكتروني آخر، حيث يجب على الموّرد أن يَضَعَ تحت تصرّف أيّ شخص، منظومة إلكترونيّة تسمح له بالتّعبير عن رغبته في عدم تلقّي أيّ رسالة إشهارية منه(E-fournisseur) وذلك من دون فرض أيّة مصاريف أو مبرّرات، وفي حالة ما إذا طلب الشّخص المعني ذلك، يجب على المورّد أن يقوم بتسليم وصل استلام بطريقة إلكترونيّة يؤكّد من خلاله لذلك الشّخص تسجيل طلبه، مع اتخاذ جميع التّدابير اللازمة لتلبية رغبته في غضون 24 ساعة، فإذا طرأ أيّ نزاع بشأن الإشهار الإلكتروني،

يجب على المورّد أن يُثْبِتَ أنّ إرْسَالَ الإشهارات الإلكترونيّة قد تَمَّ بالموافقة المُسبقة والحُرّة، مع استيفاء المقتضيات الواردة في المادة 30 من نفس القانون.

2)- المتطلبات المتعلقة بالدّفع الإلكتروني:

تتّم عملية الدّفع في معاملات التّجارة الإلكترونيّة عند تسليم المنتوج أو عن بُعد عبر مِنصات دفع إلكترونية، مُستغلَّة حصريا من طرف مصارف معتمدة من قِبَلِ المصرف المركزي وبريد الجزائر، ويجب أن يكون وصل مِنصّة الدّفع الإلكتروني مُؤَمَّناً بواسطة نظام تصديق إلكتروني، حيث تخضع جميع المِنصّات المُنشأة والمُستغلة لرقابة المصرف المركزي الجزائري، بُغية ضمان مدى استجابتها لمتطلّبات التّشغيل البيني، وكذا سلامة وسرّية وأمن البيانات الإلكترونية المتداولة عبر شبكة الإنترنت[1].

وعليه، قام المشّرع الجزائري بموجب المادة 07 من القانون رقم 18-05، المتعلّق بالتّجارة الإلكترونيّة[2]، بإعفاء من إجراءات مراقبة التّجارة الخارجيّة والصرف كلّ بيع لسلعة أو خدمة عن طريق الاتّصالات الإلكترونيّة، يتم(البيع) فيما بين مُورِّد إلكتروني مُقيم في الجزائر ومُستهلك إلكتروني موجود في بلد أجنبي، على أن لا تتعدّى قيمة هذه السّلعة أو الخدمة ما يُعادلها بالدّينار الحدّ المنصوص عليه في التّشريع والتّنظيم المعمول بهما، حيث

---

[1] تنص **المادة 27** من القانون رقم 18-05 المؤرخ في 10 ماي 2018، الذي يتعلق بالتجارة الإلكترونية، على ما يلي: " يتم الدفع في المعاملات التجارية الإلكترونية إمّا عن بُعد أو عند تسليم المنتوج، عن طريق وسائل الدفع المُرخص بها، وفقا للتشريع المعمول به. عندما يكون الدفع إلكترونيا، فإنّه يتم من خلال منصات دفع مخصصة لهذا الغرض، منشأة ومستغلّة حصريا من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر وموصولة بأي نوع من أنواع محطات الدفع الإلكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية. يتم الدفع في المعاملات التجارية العابرة للحدود، حصريا عن بُعد، عبر الاتصالات الالكترونية."

وتنص **المادة 28** منه، على ما يلي:" يجب أن يكون وصل موقع الإنترنت الخاص بالمورد الإلكتروني بمنصة الدفع الإلكترونية مؤمنا بواسطة نظام تصديق إلكتروني."

وتنص **المادة 29** منه، على ما يلي: " تخضع منصات الدفع الإلكتروني المنشأة والمستغلّة طبقا للمادة 27 أعلاه، لرقابة البنك الجزائر لضمان استجابتها لمتطلبات التشغيل البيني وسرية البيانات وسلامتها وأمن تبادلها."

[2] راجع المادة 07 من القانون رقم 18-05، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

يجب أن يتّم تحويل مُستحقات البيع بعد دفعها من طرف المستهلك الأجنبي إلى حساب المُورّد الإلكتروني المُقِيم بالجزائر المُعتمد لدى المصرف المركزي أو لدى بريد الجزائر.

كما تمّ إعفاء من إجراءات مراقبة التّجارة والصّرف، كل شراء يتّم عبر الاتّصالات الإلكترونيّة، لمختلف السّلع أو الخدمات الرّقميّة ذات الاستخدام الشّخصي، يقوم به المستهلك الإلكتروني المُقيم في الجزائر لدى مُورِّد إلكتروني مُقيم في بلد أجنبي، على أن لا تتجاوز قيمة هذه السّلع أو الخدمات ما يُعادلها بالدّينار الجزائري الحدّ المنصوص عليه في التّشريع والتّنظيم المعمول بهما، ويتم الدّفع الإلكتروني لمستحقات الشّراء باستعمال الحساب المصرفي بالعملة الصّعبة للمستهلك الإلكتروني المُقيم بالجزائر، حيث يتّم تحديد شروط وكيفيات تطبيق هذه المادة(07) عن طريق النّصوص التّنظيميّة.

رابعا– المتطلبات المتعلّقة بالعقد الإلكتروني:

يجب أن يشمل مُحتوى العقد الإلكتروني البيانات الواردة في أحكام قانون التّجارة الإلكترونيّة**(1)**، الذي من خلاله يجب على المُورّد الإلكتروني مراعاة مُتطلّبات الطلبيّة المُسبقة**(2)**، حيث يتحمّل أطراف العقد الإلكتروني مجموعة من الحقوق والالتزامات**(3)**.

1)– المتطلبات المتعلقة بمُحتوى العقد الإلكتروني:

يجب أن تكون كلّ معاملة تجارية وفقا لنص المادة 10 من القانون رقم 18–05 المتعلق بالتجارة الإلكترونية، مسبوقة بعرض تجاري مع توثيقها بموجب عقد إلكتروني يُصادق عليه المستهلك الإلكتروني، ويجب أن يَتَضَمَّنَ العقد الإلكتروني على المعلومات الواردة في أحكام المادة 13 من نفس القانون[1]، كالخصائص التّفصيلية للسّلع والخدمات ومُدّة العقد حسب الحالة وشروط وكيفيات الدّفع والتّسليم وإعادة المنتوج، والشّروط المتعلقة بالضّمان وخدمات ما بعد البيع، وفسخ العقد الإلكتروني وكيفيات معالجة الشّكاوى والجهة القضائيّة المختصة في حالة النّزاع، وعند الاقتضاء يجب تحديد شروط وكيفيات الطلبيّة المُسبقة وكذا الشّروط والكيفيات الخاصّة المتعلقة بالبيع بالتّجريب.

[1] قانون رقم 18–05، مؤرخ في 10 ماي 2018، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

2)- المتطلبات المتعلّقة بالطلبيّة المُسبقة:

يُمكِن للمُورّد الإلكتروني قبل إبرام العقد الإلكتروني، أن يَقْتَرِحَ للمُستهلك الإلكتروني في إطار الطلبيّة المُسبقَة(Précommande) تعهّد بالبيع في حالة عدم تَوافُر المنتوج، حيث يجب أن تَمُرَّ الطلبيّة المُسبقة وفقا لأحكام المادة 12 من القانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلّق بالتّجارة الإلكترونيّة، عبر ثلاث مراحل إلزاميّة[1] وهي كالتّالي:

في المرحلة الأولى يجب من خلالها أن يكون المُستهلِك الإلكتروني على علم ودراية تامّة بجميع الشّروط التّعاقديّة التي تُمكّنه فيما بعد من إبرام العقد الإلكتروني.

ويقوم المستهلك في المرحلة الثّانية بالتّحقق في تفاصيل الطلبيّة وبالخصوص حول كل ما يتعلّق بماهيّة السّلع والخدمات المُتاحة، والسّعر الإجمالي والوحدوي والكميات المطلوبة، مع منحه إمكانية تعديل اختياراته في الطلبيّة، أو تصحيح الأخطاء المحتملة فيها أو حتى إلغائها(اختياراته)، حيث يجب أن لا تتضمن الخانات المُعدّة للملء على أيّة مُعطيات تهدف إلى توجيه اختيار المستهلك الإلكتروني.

وفي المرحلة الثّالثة، يقوم المستهلك الالكتروني بالتّعبير صراحة عن اختياراته وتأكيدها في الطلبيّة المُسبقة التي تؤدّي إلى تكوين العقد الإلكتروني.

فبمجرّد تَوَفُّرِ السّلعة أو الخدمة تَتحوّل الطلبيّة المُسبقة(Précommande) بصفة ضمنيّة إلى طلبيّة مُؤكّدة(Commande Validée)، التي على إثرها يُمكِن للمستهلك الإلكتروني دفع ثمن السّلعة أو الخدمة المختارة، وفي حالة دفع الثّمن قَبْلَ تَوفُّر المنتوج في المخزون، يجب على المورّد الإلكتروني إرجاع الثّمن المدفوع وذلك دون المساس بحق المستهلك الإلكتروني في التّعويض، كما يمكن للمستهلك الإلكتروني أن يطلب من ذلك المُوّرِد إبطال العقد والتّعويض عن الضّرر الذي لحقه، في حالة عدم احترامه(المُورِّد الإلكتروني) لأحكام المادتين 10 و13 من القانون رقم 18-05 المتعلّق بالتّجارة الإلكترونيّة[2].

---

[1] تنص **المادة 7/06** من القانون رقم 18-05، سالف الذكر، على ما يلي: "**الطلبية المُسبقة:** هو تعهد بالبيع يمكن أن يقترحه المورد الإلكتروني على المُستهلك الإلكتروني في حالة عدم توفر المنتوج في المخزون."

أنظر كذلك نص المادة 12 من القانون رقم 18-05، سالف الذكر.

[2] راجع المادتين 14 و15 من القانون رقم 18-05، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

3)- المتطلبات المتعلّقة بأطراف العقد الإلكتروني:

بمجرد إبرام العقد الإلكتروني يتحمل كل من المورّد الإلكتروني (أ) والمستهلك الإلكتروني (ب) مجموعة من الالتزامات، تتمثل فيما يلي:

أ- الالتزامات المتعلقة بالمُورّد الإلكتروني:

تقع على عاتق المُورّد الإلكتروني مجموعة من الالتزامات، والمتمثّلة فيما يلي:

أ-1- الالتزام بحماية المعطيات ذات الطّابع الشّخصي: يجب على المورّد الالكتروني الذي يقوم بجمع وتخزين المعطيات الشّخصيّة للمستهلك الإلكتروني، أو أي عميل آخر محتمل، الالتزام بالأحكام القانونيّة والتّنظيميّة المتعلّقة بحماية المعطيات ذات الطّابع الشّخصي، حيث ينبغي عليه ألاّ يجمع إلاّ البيانات الضّروريّة المتعلّقة بإبرام المعاملات التّجاريّة، والحصول المُسبق على الموافقة الصّريحة للمستهلك قبل جمع بياناته الشّخصيّة، مع ضمان أمن نُظم المعلومات وسريّة بياناته الشّخصية المُخزّنة[1].

نص المشّرع الجزائري بموجب المادة 43 من القانون رقم 15-04 المؤرخ في 2015/02/01 المحدّد للقواعد العامة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، وكذا المادة 42 من القانون رقم 18-07 المؤرخ في 10 جويلية 2018 المتعلّق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي، على عدم جمع البيانات الشّخصية من طرف(م.خ.ت.إ) إلاّ بعد الحصول على الموافقة الصريحة للمعني، ولا يجوز لمقدّم الخدمة في هذه الحالة إلاّ جمع البيانات الشّخصية الضّروريّة لمنح وحفظ شهادة التّصديق الإلكتروني فقط ولا يمكن استعمال هذه البيانات لتحقيق أغراض أخرى[2].

---

[1] راجع المادة 26 من القانون رقم 18-05، سالف الذكر.

[2] تنص المادة 43 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06 الصادر في 10 فيفري 2015، على ما يلي:" لا يُمكن على مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلاّ بعد موافقته الصريحة. ولا يمكن مقدم خدمات التصديق الإلكتروني أن يجمع إلاّ البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى."

انطلاقا من ذلك، ألزمت المادة 07 من القانون رقم 18–07 المؤرخ في 10 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي[1]، المسؤول على المعالجة الآلية للمعطيات الشّخصيّة الحصول مُسبقا على الموافقة الصّريحة للشّخص المعني بالأمر، حيث يُمكن لهذا الأخير أن يتراجع عن موافقته في أيّ وقت، ففي حالة ما إذا كان الشّخص المعني فاقد أو ناقص الأهلية فإنّ إجراءات الحصول على موافقته تخضع للقواعد المنصوص عليها في القواعد العامة – التّقنين المدني–، في حين لا يمكن للغير الاطّلاع على المعطيات الشّخصيّة الخاضعة للمعالجة الآلية، إلاّ من أجل تحقيق أو إنجاز الغايات المرتبطة بمهام المسؤول عن المعالجة والمرسل إليه، وبعد الموافقة المسبقة للشّخص المعني، غير أن موافقة هذا الأخير لا تكون مُلزمة في حالات المعالجة الآلية الضّروريّة المذكورة بموجب الفقرة الأخيرة من المادة(5/07).

فإلى جانب ذلك، ألزمت المادة 38 من القانون رقم 18–07، سالف الذكر، المسؤول على المعالجة الآلية بضرورة إرساء التّدابير التّقنيّة والأمنيّة الملائمة لحماية المعطيات الشّخصية من الإتلاف العرضي أو غير المشروع أو الضّياع العرضي أو التّلف أو النّشر

وتنص المادة 42 من القانون رقم 18–07 المؤرخ في 10 جويلية 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، الصادر في 10 جويلية 2018، على ما يلي:" ما عدا في حالة موافقتهم الصريحة، يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني، من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها."

للمزيد من المعلومات راجع: **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية (شرح قانون المبادلات والتجارة الإلكترونية)، الكتاب الأول، دار الكتب القانونية، مصر، 2007، ص ص 248، 249.

[1] تنص **المادة 07** من القانون رقم 18–07، سالف الذكر، على ما يلي:"[...]. غير أنّ موافقة الشخص المعني لا تكون واجبة، إذا كانت المعالجة ضرورية: – لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة، – لحماية حياة الشخص المعني، – لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه، – للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه، – لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعه على المعطيات، – لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/ أو حقوقه وحرياته الأساسية."

أو الولوج غير المرّخصين، وذلك خاصة في حالة ما إذا استوجبت المعالجة إرسال المعطيات عبر شبكة معيّنة وحمايتها من أيّ شكل من أشكال المعالجة غير المشروعة، حيث يجب أن تضمن هذه التّدابير مستوى ملائما من السّلامة والأمان، وذلك بالنّظر إلى المخاطر المتعلّقة بالمعالجة وطبيعة المعطيات الواجب حمايتها[1].

أ -2- **الالتزام بالإعلام:** يجب على المورّد الإلكتروني في إطار العرض التّجاري أن يضع تحت تصرف المستهلك الإلكتروني جميع المعلومات الضّروريّة لإبرام العقد الإلكتروني، كإعلام المستهلك بالمعلومات المتعلّقة بالمورّد الإلكتروني التي تُتيح إمكانية الاتصال به عند الحاجة(رقم الهاتف، الأرقام المتعلقة بالتّعريف الجبائي، والسّجل التّجاري، وكذا المعلومات الماديّة والالكترونيّة.)، وإعلامه كذلك بجميع شروط التّعاقد والعناصر الجوهريّة بالعقد الإلكتروني، والمعلومات المتعلّقة بطبيعة وخصائص السّلعة أو الخدمة المتاحة، وطرق حساب السّعر وتأكيد الطّلبيّة أو إلغائها مسبقا، وكذا تحديد كيفيات الدّفع وآجال التّسليم والعدول(Rétractation)، والشّروط المتعلّقة بالضّمان التّجاري وخدمة ما بعد البيع وإرجاع أو استبدال أو تعويض المنتوج أو فسخ العقد عند الاقتضاء، الخ... [2].

أ-3- **الالتزام بتسليم المنتوج:** يجب على المورّد الإلكتروني بعد إبرام العقد الإلكتروني أن يقوم بإرسال نُسخة إلكترونيّة من العَقْدِ إلى المُستهلك الإلكتروني، مع تسليم هذا الأخير للفاتورة المتعلّقة ببيع المنتوج عبر الانترنت بصيغتها الالكترونيّة، حيث يمكن للمستهلك أن يطلب الفاتورة بشكلها الورقي، كما يجب على المُورّد احترام آجال التّسليم والقيام بتسليم المنتوج الذي طلبه المُستهلك، حيث لا يمكن للمورّد طلب دفع ثمن ومصاريف تسليم منتوج في حالة عدم طلبه من طرف المستهلك[3].

---

[1] راجع المادة 38 من القانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

[2] راجع المواد 11، 12، 13 من القانون رقم 18-05، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

[3] تنص المادة 19 من القانون رقم 18-05، سالف الذكر، على ما يلي:" بمجرد إبرام العقد، يلزم المورد الإلكتروني بإرسال نسخة إلكترونية من العقد إلى المستهلك الإلكتروني."

أ-4- الالتزام بضمان العيب الخفي للمنتوج ومطابقته للطلبيّة: في حالة تسليم سلعة أو خدمة تحتوي على عيب خفي أو غير مُطابقة للطلبيّة، يجب على المورّد الإلكتروني أن يستعيد منتوجه، حيث يجب أن يُعيد المستهلك الإلكتروني إرسال المنتوج في غلافه الأصلي في خلال مدّة أربعة(04) أيام ابتداء من تاريخ التّسليم الفّعلي للمنتوج، مع الإشارة إلى سبب الرّفض، حيث تكون تكاليف إعادة الإرسال على عاتق المورّد الإلكتروني، وفي هذه الحالة يجب على هذا الأخير أن يقوم إمّا بتسليم جديد مُوافق للطلبيّة، أو إصلاح المنتوج المُعيب أو استبدال المنتوج المُعيب بمنتوج آخر مُماثل غير مُعيب، أو يقوم بإلغاء الطلبيّة مع إرجاع المبالغ المدفوعة خلال خمسة عشرة(15) يوم من تاريخ استلامه للمنتوج، وذلك من دون المساس بحقّ المستهلك الإلكتروني في المطالبة بالتّعويض عن الضّرر الذي لحقه[1].

أ-5- الالتزام بإرسال سجّلات المعاملات التّجارية إلى المركز الوطني للسّجل التّجاري: وفقا لأحكام المادة 25 من القانون رقم 18-05 المتعلّق بالتّجارة الإلكترونيّة، يجب على كل مُورِّد إلكتروني القيام بحفظ سجّلات المعاملات التّجارية المُنجزَة بتواريخها وإرسالها إلكترونيا إلى المركز الوطني للسّجل التّجاري، حيث يُحدّد التنظيم كيفيات تطبيق هذه المادة.

ب- الالتزامات المتعلّقة بالمستهلك الإلكتروني:

يتحمّل المستهلك في نطاق معاملات التّجارة الإلكترونيّة مجموعة من الحقوق والالتزامات المترتبة عن العقد الإلكتروني، والمتمثّلة فيما يلي:

ب-1- الالتزام بدفع ثمن السّلعة أو الخدمة: يجب على المستهلك الإلكتروني أن يقوم وفقا لأحكام المادة 16 من القانون رقم 18-05 المتعلّق بالتّجارة الإلكترونيّة، بدفع الثّمن المُتّفق عليه في العقد الإلكتروني بمُجرّد إبرامه، وذلك ما لم ينص العقد على خلاف ذلك[2].

وتنص المادة 20 من نفس القانون، على ما يلي:" يترتب على كل بيع لمنتوج أو تأدية خدمة عن طريق الاتصالات الإلكترونية، إعداد فاتورة من قبل المورد الإلكتروني، تسلّم للمستهلك الإلكتروني. يجب أن تعد الفاتورة طبقا للتشريع والتنظيم المعمول بهما. يمكن أن يطلب المستهلك الإلكتروني الفاتورة في شكلها الورقي."

[1] راجع المادتين 22 و23 من القانون رقم 18-05، سالف الذكر.

[2] تنص المادة 16 من القانون رقم 18-05، سالف الذكر، على ما يلي:" ما لم ينص العقد الإلكتروني على خلاف ذلك، يلتزم المستهلك الإلكتروني بدفع الثمن المتفق عليه في العقد الإلكتروني بمجرد إبرامه."

ب-2- الالتزام بتوقيع وصل استلام المنتوج: يجب على المستهلك الإلكتروني، وفقا لأحكام المادة 17 من نفس القانون، أن يقوم بتوقيع وصل استلام السّلعة أو الخدمة عند التّسليم الفِّعلي للمنتوج أو تأدية الخدمة موضوع العقد الإلكتروني، ولا يُمْكِنُهُ رفض توقيع وصل الاستلام في حالة ما إذا طلب ذلك المورّد الالكتروني، حيث يجب على هذا الأخير أن يقوم بتسليم نُسخة من ذلك الوصل إلى المُستهلك الإلكتروني[1].

ب-3- العدول عن العقد: قرّرت معظم قوانين الاستهلاك الحديثة منح المستهلك الإلكتروني الحق بالتّراجع عن البيع خلال فترة زمنيّة محدودة، إذا ما وجد ما يُبَرِّرُ له التَراجُع من دون أن يَتَحَمَّلَ أيّة نتائج، حيث يُعتبر الحق في العدول مُقرّر فقط للمُستهلكين، بغية حمايتهم من مخاطر الغّش والخداع أو التّغرير والتّأثير المُترتّبة عن العقود المُبرمة عن بعد[2].

يعود مصدر حق العدول عن العقد إلى القانون، الذي كرّس شروط وإجراءات مباشرة هذا الحق، حيث حدّدت المادة 1/09-2 من التّوجيه الأوروبي رقم 2011/83 المؤرخ في 25 أكتوبر 2011 المتعلّق بحقوق المستهلكين، المُعدّل للتوجيه رقم 1993/13 والتّوجيه رقم 1999/44، و**المُلغي** للتّوجيه رقم 85/577 والتّوجيه رقم 97/07[3]، المُدّة القانونيّة لمباشرة حق العدول عن العقد بأربعة عشرة(14) يوم، تسري من تاريخ إبرام العقد أو من تاريخ تسليم السّلعة للمستهلك أو الشّخص المُمثّل له، حيث يحق للمُستهلك أثناء هذه المُدّة العدول عن العقد، من دون أي تعليل لأسباب خيار التّراجع أو تحمّل التّكاليف الأخرى المحدّدة بموجب أحكام المواد 2/13 و14 من نفس التّوجيه(رقم 2011/83)[4].

---

[1] راجع المادة 17 من القانون رقم 18-05، سالف الذكر.

[2] للمزيد من المعلومات أنظر: **عمر خالد زريقات**، مرجع سابق، ص ص 358- 362.

Romain V.GOLA, op.cit., pp. 308-314.

[3] **Directive 2011/83/UE** du parlement européen et du conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et **abrogeant** la directive **85/577**, JOUE n° L 304/64 du 22/11/2011.

Art.31: « La directive 85/577/CEE et la directive 97/7/CE, telle que modifiée par la directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs et par les directives 2005/29/CE et 2007/64/CE, sont **abrogées** à compter du 13 juin 2014. […].»

[4] **Art.09 (Directive 2011/83/UE** du parlement européen et du conseil, relative aux droits des consommateurs,…) : « **1-** En dehors des cas où les exceptions prévues à l'article 16

في حالة إغفال المِهَنِي بواجب إعلام المستهلك بحق العدول عن العقد، وفقا لنص المادة 1/10-2 من نفس التّوجيه(رقم 2011/83)، يمكن للمستهلك مباشرة هذا الحق خلال مدّة اثنتي عشرة(12) شهر تسري من تاريخ انتهاء المدّة القانونيّة التي حدّدتها المادة 2/09 من نفس التّوجيه، وفي حالة إعلام المهني للمستهلك بحق العدول عن العقد، فإنّ مباشرته لهذا الحق تكون خلال مهلة أربعة عشرة(14) يوم تسري من تاريخ إعلامه بحقّه في العدول، وبالتّالي يجب على المستهلك وفقا لأحكام المادة 11 من نفس التّوجيه، الالتزام بإعلام المِهَنِي بقرار العدول قبل نهاية المُدّة القانونيّة المُقرّرة له، وذلك سواء بملء الاستمارة الخاصّة بالعدول وفقا للنّموذج المُحدّد في الملحق(I) الجزء(B) من نفس التّوجيه، أو استعمال تصريح يُوَضِّحُ فيه قرار العدول، حيث يُمكن للمستهلك إرسال أحدهما مُباشرة عبر الموقِع الإلكتروني للمِهَنِي الذي يَمْنَحُهُ وصل تسليم فوري لقرار العدول عن العقد.

---

s'appliquent, le consommateur dispose d'un délai de **quatorze jours** pour se **rétracter** d'un contrat à distance ou d'un contrat hors établissement **sans** avoir à **motiver** sa décision et **sans** encourir **d'autres coûts** que ceux prévus à l'article 13, paragraphe 2, et à l'article 14. **2**- Sans préjudice de l'article 10, le délai de rétractation visé au paragraphe 1 du présent article expire après une période de quatorze jours à compter: **a)** en ce qui concerne les contrats de service, du jour de la conclusion du contrat; **b)** en ce qui concerne les contrats de vente, du jour où le consommateur ou un tiers autre que le transporteur et désigné par le consommateur prend physiquement possession du bien ou: **i)** dans le cas de biens multiples commandés par le consommateur dans une seule commande et livrés séparément, du jour où le consommateur ou un tiers autre que le transporteur et désigné par le consommateur prend physiquement possession du dernier bien; **ii)** dans le cas de la livraison d'un bien composé de lots ou de pièces multiples, du jour où le consommateur ou un tiers autre que le transporteur et désigné par le consommateur prend physiquement possession du dernier lot ou de la dernière **pièce**; **iii)** dans le cas des contrats portant sur la livraison régulière de biens pendant une période de temps définie, du jour où le consommateur ou un tiers autre que le transporteur et désigné par le consommateur prend physiquement possession du premier bien;
c) en ce qui concerne les contrats portant sur la fourniture d'eau, de gaz et d'électricité lorsqu'ils ne sont pas conditionnés dans un volume délimité ou en quantité déterminée, ainsi que de chauffage urbain et de contenu numérique non fourni sur un support matériel, du jour de la conclusion du contrat. […]. ».
Voir aussi : les Arts. **L221-18 et L221-20** du **Code de la consommation** - Dernière modification le 02 février 2019 - Document généré le 13 février 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr

كما نص المشّرع التّونسي بموجب أحكام الفصل 30 من القانون عدد 2000/83 المؤرخ في 09 أوت 2000 المتعلّق بالمبادلات والتّجارة الإلكترونيّة[1]، على إمكانية المستهلك في العدول عن الشّراء في أجل عشرة(10) أيام عمل تسري من تاريخ تسليم البضائع للمستهلك أو من تاريخ إبرام العقد بالنّسبة للخدمات، حيث يتعيّن على البائع إرجاع المبلغ المدفوع إلى المستهلك في خلال عشرة(10) أيام عمل، تسري من تاريخ إرجاع البضاعة أو العدول عن الخدمة، على أن يتحمّل المستهلك للمصاريف النّاجمة عن إرجاع البضاعة.

لم ينص المشّرع الجزائري صراحة في أحكام القانون رقم 18-05 المتعلّق بالتّجارة الإلكترونيّة، على حق المستهلك الإلكتروني في العدول عن العقد، ولا على ضوابط ممارسته لهذا الحق، بل نص عليه بموجب المادة 19 من القانون رقم 18-09 المؤرخ في 10 جوان 2018، المعدل والمتمم للقانون رقم 09-03 المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، التي منحت للمستهلك الحق في التراجع عن اقتناء منتوج ما من دون تعليل أيّ سبب أو دفع مصاريف إضافية، حيث ترك المشرّع للتّنظيم تحديد شروط وكيفيات ممارسة حق العدول، وكذا آجال وقائمة المنتوجات المَعْنِيَّة[2].

تجدر الإشارة في هذا السّياق، أنّ غالبية التّشريعات المُنظّمة للاستهلاك نصّت على بعض الاستثناءات الواردة على حق المستهلك في العدول عن العقد، وذلك على غرار

---

[1] راجع أحكام الفصل 30 من القانون عدد 83-2000 المؤرخ في 09 أوت 2000، الذي يتعلق بالمبادلات والتجارة الإلكترونية، ر. ر. ج. ت، العدد 64، الصادر في 11 أوت 2000.

[2] قانون رقم 18-09 مؤرخ في 10 جوان 2018، يعدل ويتمم القانون رقم 09-03 المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، ج ر عدد 35 الصادر في 13 جوان 2018.

تنص المادة 19 منه، على ما يلي:" يجب أن لا يمس المنتوج المقدم للمستهلك بمصلحته المادية، وأن لا يسبب له ضررا معنويا. العدول هو حق المستهلك في التراجع عن اقتناء منتوج ما دون وجه سبب. للمستهلك الحق في العدول عن اقتناء منتوج ما ضمن احترام شروط التعاقد، ودون دفعه مصاريف إضافية. تحدد شروط وكيفيات ممارسة حق العدول وكذا آجال وقائمة المنتوجات، عن طريق التنظيم."

قانون رقم 09-03 مؤرخ في 25 فيفري 2009، يتعلق بحماية المستهلك وقمع الغش، ج ر عدد 15 الصادر في 08 مارس 2009.

الفصل 32 من القانون التّونسي رقم 2000/83 المتعلّق بالمبادلات والتّجارة الإلكترونيّة، الذي نصّ على أنّه لا يمكن للمستهلك، باستثناء حالات العيوب الظّاهرة أو الخفيّة، أن يباشر حقّه في العدول عن الشّراء في حالة توفير البائع للخدمة بعد أن طلبها المستهلك قبل انتهاء أجل العدول عن الشّراء، أو قيام البائع بتزويد المستهلك بمنتوجات حسب خاصّياته الشّخصية أو لا يُمكِن إعادة إرسالها أو قابلة للتّلف أو الفساد لانتهاء مدّة صلاحياتها، أو في حالة قيام المستهلك بشراء الصّحف والمجلاّت أو نزعه للأختام المتعلّقة بالتّسجيلات السّمعية أو البصريّة أو البرمجيات والمعطيات الإعلاميّة المُسلّمة أو نقلها آليا[1].

المطلب الثاني

علاقة شبكات الحاسوب بمواقع التّجارة الالكترونيّة

تتضمن الشّبكات المعلوماتيّة على مجموعة من الوسائل الماديّة والبرمجيات المُخصّصة للاتّصالات بين الحواسيب، ونقل مختلف المعلومات والبيانات المُتداوَلة فيها، حيث تعود دوافع ظهورها لتحقيق غايات أو أهداف معيّنة **(الفرع الأول)**، حيث تعتبر الجوانب المُكوّنة للشّبكات بمثابة العلبة السّوداء لمواقِع التّجارة الإلكترونيّة **(الفرع الثاني)**، التي تستعين بمزوّدي خدمات شبكة الإنترنت كمتدّخلين من ذوي الكفاءات والخبرات في مجال تكنولوجيا الاتّصال والإعلام، لضمان السّير الحسن والفعّال لعمليات الاتّصال والاطّلاع على مختلف البيانات والمعلومات الإلكترونيّة المتداولة **(الفرع الثالث)**.

1) Voir aussi : l'**Art.16** de la Directive européenne n° 2011/83 relative aux droits des consommateurs du 25 octobre 2011, et **l'Art. L221-28** du Code de la consommation Français (Dernière modification le 02 février 2019).

الفرع الأول
دوافع ظهور شبكات الحاسوب

إنّ الشّبكة الحاسوبية عبارة عن وسيلة ربط بين الحواسيب مع أدوات وبرامج معلوماتيّة مخصّصة للتّعامل مع هذه الشّبكات، وذلك لغرض تسهيل تبادل البيانات والمعلومات وغيرها من الموارد المعلوماتيّة على النّحو الذي يسمح لمختلف المستفيدين من التّواصل المباشر، فمن بين أهم الأسباب التي أدّت إلى ظهور شبكات الحاسوب نجد ما يلي:

أ)– ضرورة تبادل ونقل البيانات والمعلومات فيما بين أجهزة الحاسوب على النّحو الذي يسمح بتدفّق المعلومات، وتطوير العلاقات مع شركاء الأعمال سواء في داخل الشّركة أو المؤسّسة أو خارجها[1]؛

ب)– الحاجة إلى تحسين وزيادة مردوديّة الإنتاج، من خلال مشاركة المعلومات والمصادر على الشّبكة عبر مساحات جغرافيّة أوسع، حيث يمكن نقل الملفات مع إجراء التّخاطب اللّحظي بين مجموعة من المستخدمين، وكذا إرسال واستقبال رسائل البريد الإلكتروني، من وإلى الشّركاء في مواقع مختلفة عبر أنحاء الرّقعة الأرضيّة، وذلك في نفس الوقت وبسرعة فائقة وتكلفة زهيدة[2]؛

ج)– الحاجة إلى التّواصل عن بُعد، من خلال المشاركة في البرمجيات المعلوماتيّة التي تسمح للمستخدمين باستخدام نفس البرامج، والأنظمة المتواجدة على أجهزة مُحدّدة في الشّبكة والولوج إلى نفس المعطيات، وبالتالي التّناسق في البيانات المتواجدة في الجهاز الواحد على نحو يسمح بانجاز الأعمال، التي لا تتطلّب التّأخير بشكل متزامن ومن دون ضياع الوقت؛

---

1) **Jean-François PILLOU, Fabrice LEMAINQUE**, Tout sur les réseaux et Internet, 2e édition, Dunod, Paris, 2010, pp. 4, 5.
2) Ibid.

د)- إنّ التّقنيات التّقليديّة المُستخدمة في تسويق وبيع مختلف السّلع والخدمات لم تَعُدْ تتأقلم مع التّطوّرات والمستجدّات التي شهدتها الثّورة الرّقميّة حاليا، وبالخصوص الشّبكات التي تسمح للشّركات التّجارية بتجهيز وتسويق منتجاتها للعملاء، وإعداد طلبات الشّراء، مع دفع قيمة المستحقّات عبر الإنترنت بكل ثقة وأمان[1]؛

هـ)- تعتمد الشّبكات على معايير ومواصفات أمان عالية المستوى تسمح بفصل الشّبكات(الإنترانت والإكسترانت)، لغرض تأمين وحماية المعالجة الآلية للمعلومات، ومنع الدّخلاء من الدّخول لغير المرّخصين بهم، هذا من جهة، ومن جهة أخرى، تفادي عمليات الاختراق غير المشروعة، التي تستهدف البيانات أو المعطيات الإلكترونيّة الحسّاسة الخاصّة بالمُستخدمين أو العملاء عبر الشّبكة المفتوحة(الإنترنت)[2].

---

[1] **علاء عبد الرزاق السالمي**، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2017، ص ص 306، 307.

[2] **Internet** : Un réseau télématique international **d'origine américaine**, constituant à ce jour le plus grand réseau du monde, Internet est accessible aux professionnels comme aux particuliers.

- **Intranet** : Un réseau informatique interne à une entreprise, **identique** à **Internet** de par sa structure et les moyens d'y accéder, mais réduit à l'usage des employés d'une même entreprise. L'intérêt d'un tel réseau réside dans la capacité qu'il possède à transmettre les données, mais aussi et surtout dans sa possibilité de faire transiter des **informations confidentielles** ou à destination des seuls employés de l'entreprise. Ainsi, tout employé peut communiquer des notes de service, lire des manuels en ligne, consulter des catalogues ou suivre les projets en cours. Le réseau peut être étendu aux clients, aux fournisseurs, aux succursales ou aux filiales de l'entreprise : on parle alors **d'extranet**.

- Extranet : Un réseau privé de **type intranet**, accessible de l'extérieur, les réseaux extranet, basés sur une **architecture client / serveur**, sont très répandus car ils répondent aux besoins des nouveaux modes de communication des entreprises, l'accès à un réseau **extranet** est limité, seules certaines personnes peuvent y accéder et parfois uniquement à partir de lieux prédéfinis, les contrôles d'accès se font par l'utilisation d'un code d'identification (généralement le nom de l'utilisateur) et d'un mot de passe qui est un code secret censé être connu exclusivement par l'utilisateur, l'objectif d'un **extranet** est de profiter des possibilités offertes par la **technologie Web**. La première de ces possibilités a trait aux accès distants, le **site extranet** est identifié par une adresse électronique appelée **URL** (Uniform Resource Locator), à l'aide de cette adresse, il suffit de se connecter au site en utilisant un navigateur

الفرع الثاني
أنواع شبكات الحاسوب

يمكن أن تضم الشّبكة مجموعة من أجهزة حاسوب، تكون قريبة جدّا من بعضها البعض، كتواجدها مثلا في غرفة واحدة، أو من المُمْكِنِ أن تَتَوَاجَدَ في أماكن بعيدة، كالشّبكات بين المدن أو الدول، وحتّى القارات، أين يتم وصل هذه الشّبكات عادة بالإنترنت أو الأقمار الصّناعيّة(Satellites) بحسب تصميماتها[1]، وتنقسم شبكات الحاسوب إلى عدّة أنواع تختلف فيما بينها بناءً على علاقة الأنظمة ببعضها البعض **(أوّلا)**، كم تختلف من النّاحية الجغرافيّة **(ثانيا)**، ومن النّاحية الشّكليّة **(ثالثا)**.

Web tel que Microsoft Internet Explorer ou Netscape Navigator, et ceci de n'importe quel endroit de la planète disposant d'une ligne téléphonique ou d'une ligne spécialisée.
Le deuxième avantage d'un extranet est l'utilisation de documents sécurisés au standard HTML (HyperText Markup Language) ou XML (Extensible Markup Language), Cependant, cette protection vis-à-vis d'éventuelles intrusions externes n'est pas parfaite et les sites extranet sont parfois les cibles des pirates informatiques, appelés communément hackers. http://www.internet.gouve.fr/

[1] **قانون رقم 18-04** مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد 27 الصادر بتاريخ 13 مايو 2018.

تنص المادة **10** من القانون 18 -04، على ما يلي:... -**1 اتصالات الكترونية:**" كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرمغناطيسية."

-**5 الإنترنت:**" شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال IP وعمل معا بهدف تقديم واجهة موحدة لمُستعمليها."

-**21 شبكة الاتصالات الالكترونية:**" كل منشأة أو مجموعة من منشآت تضمن إمّا إرسالا، أو إرسال وإيصال إشارات إلكترونية، وكذا تبادل معلومات التحكم والتسيير المتصلة بها، ما بين النقاط الطرفية لهذه الشبكة، وعند الاقتضاء، الوسائل الأخرى التي تضمن إيصال الاتصالات الإلكترونية، وكذا التحويل والتوجيه.

تعد شبكات اتصالات الكترونية خصوصا: شبكات الأقمار الصناعية والشبكات الأرضية والأنظمة التي تستعمل الشبكة الكهربائية شريطة أن تُسْتَعْمَلَ لإيصال الاتصالات الإلكترونية."

-**22 شبكة الاتصالات الالكترونية المفتوحة للجمهور:**" كل شبكة للاتصالات الالكترونية مُنشأة أو مُستعملة لتقديم خدمات الاتصالات الالكترونية أو خدمات اتصالات للجمهور بطريقة إلكترونية."

أوّلا– تصنيف الشّبكات وفقا لعلاقة الأنظمة ببعضها البعض:

يمكن تقسيم شبكات الحاسوب بناءً على هذا التّصنيف إلى نوعين:

1)– شبكة النّد للنّد(Peer to Peer): في هذه الشّبكة(Pair à Pair) يتم ربط مختلف الأجهزة ببعضها البعض من دون الخادم أو الموزّع، حيث يتم من خلالها تبادل الملفات ورسائل البريد واستخدام الموارد الماديّة للحواسيب كالطّابعات(Imprimantes)، والموديم(Modems) والماسحات(Scanners) وغيرها من الأجهزة[1].

2)– شبكة العميل/الخادم(Client/serveur): تُصنّف هذه الشّبكة ضمن الأنظمة المفتوحة(Systèmes ouverts) التي يتم إحداثها وفقا لطريقة الإعداد العميل/الخادم، أين يتم من خلالها ربط مختلف أجهزة الحواسيب بخادم أو موزّع واحد أو أكثر، يتميّز بمعايير ومواصفات خاصّة، تتيح إمكانية تشارك وتبادل الخدمات فيما بين أجهزة الحواسيب[2]، حيث تكون حسابات المُستخدمين مركزيّة وينبغي على أنظمة التّشغيل الرئيسيّة للشّبكة Network) (Operating System أن تَضْمَنَ التّحكم في نشاط جميع الأجهزة، وتسمح للبرامج والأجهزة بالتّواصل، مع ضمان حماية البيانات الإلكترونيّة المتداولة داخل الشّبكة.

وعليه، يعتبر الخادم أو الموزّع الجهاز الرّئيسي داخل شبكة الحواسيب، أين يتم فيه الاحتفاظ أو تخزين البيانات الإلكترونيّة وحسابات المُستخدمين الخ...، حيث يقوم بتقديم الخدمات بحسب الدّور المُناط إليه في داخل الشّبكة، فقد يكون الخادم مُخصّص للاحتفاظ بملفات المُستخدمِين(File Serveur)، أو خادم الطّابعة المركزيّة التي يستخدمها جميع مُستخدمي الشّبكة(Print Serveur)، أو يكون الخادم مُخصّص للبريد الإلكتروني Mail) (Serveur، الخ...[3].

---

[1] **غسان قاسم داود اللامي، أميرة شكرولي البياتي،** تكنولوجيا المعلومات في منظمات الأعمال(الاستخدامات والتطبيقات)، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2010، ص 92.

[2] المرجع نفسه، ص ص 92– 94.

[3] **Serveur** (informatique) : **ordinateur** ou **programme** prenant en charge certaines fonctions pour le compte des autres systèmes d'un réseau informatique.
Un ordinateur serveur ne peut pas fonctionner sans **logiciel serveur** associé, par exemple, un ordinateur serveur supportant le service Web se compose d'un ordinateur spécialement

ثانيا– أنواع شبكات الحاسوب من النّاحية الجغرافيّة:

تتعدّد شبكات الحاسوب من الناحية الجغرافيّة بحسب حاجيات الشّركة أو المؤسّسة، والتي يمكن تقسيم أنواعها على النّحو التالي:

1)– الشّبكة المحليّة(Local Area Network (LAN)):

الشّبكة المحليّة عبارة عن مجموعة من أجهزة الحاسوب المرتبطة فيما بينها، عن طريق وسيط مشترك وتتصل مع بعضها البعض باستخدام مجموعة من البروتوكولات المشتركة، إذ تتقيّد هذه الشّبكة بمكان أو مَوْقِع واحد مثل بناية أو بنايات متجاورة، فعادة ما تملك الشّركة الواحدة شبكة محليّة خاصّة بها تحتوي على شبكات محليّة صغيرة، في كل قسم أو فرع من فروعها (الشّركة) مع خادم خاص لكل منهم (القسم أو الفرع)، ويتم ربط كلّ هذه الشّبكات الصغيرة بمُحوّل(Switch) أو مجمع مركزي(Hub) مرتبط بطريقة سلكية أو لاسلكية[1]،

---

configuré pour supporter la charge d'activités, ainsi que d'un logiciel appelé serveur HTTP (du nom du protocole supporté, HyperText Transfer Protocol), le plus célèbre et le plus répandu des logiciels serveurs **HTTP** est **Apache**.
On désigne également par serveur (ou logiciel serveur), les programmes offrant des services ou fonctions à d'autres programmes (architecture client / serveur). C'est le cas des logiciels serveurs supportant des fonctions d'accès à distance via un protocole de communication particulier (FTP, HTTP, rlogin, etc.), mais aussi de logiciels offrant des services de calcul (convertisseurs de monnaies, etc.). https://fr.www.wikepidia.org/wiki/serveur/(consulté le 07/02/2016.)

[1] من بين الشبكات المحلية اللاسلكية نجد شبكة "الويفي" (Wi-Fi « Wireless Fidelity » par analogie au terme « Hi-Fi » pour « High Fidelity » apparu dans les années 1930.)، التي عبارة عن مجموعة من بروتوكولات الاتصال اللاسلكية المنظمة وفقا لمعيار الإيسو(IEEE 802.11 (ISO/CEI 8802-11))، كتقنية تقوم عليها معظم شبكات الاتصال اللاسلكية المحلية(Wireless LAN (réseau local sans fil))، فشبكة الويفي تستخدم موجات الراديو لتبادل المعلومات بدلا من الأسلاك والكوابل التي تسمح بربط العديد من الأجهزة المعلوماتية (Ordinateur, Routeur, Smartphone, Modem Internet, etc.) لتبادل البيانات أو المعطيات الإلكترونية فيما بينها، فمصدر تسمية علامة "الويفي" جاء من هيئة (Wi-Fi Alliance « Wireless Ethernet Compatibility Alliance »، (WECA))، المكلفة بمهام تحديد خصوصيات التفاعل فيما بين الأجهزة وفقا لمعيار (IEEE 802.11 (ISO/CEI 8802-11)) وبيع علامة(Wi-Fi) للمعدات التي تستجيب لهذه المواصفات، فعن طريق خدمة الويفي يمكن إحداث شبكة اتصال لاسلكية محلية يتم نقل واستقبال البيانات فيما بين أجهزة الاتصال بسرعة عالية تصل إلى(**1,3 Gbit/s**) [Pour le **802.11ac** normalisé depuis décembre 2013(« **IEEE 802.11ac** » est la dernière évolution du standard de transmission sans fil 802.11, qui permet une connexion sans fil haut débit dans la bande de fréquences inférieure à 6 GHz (communément appelée bande des 5 GHz). Le 802.11ac offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz,

بخادم رئيسي على النّحو الذي يمنع الازدحام على الخادم ويُحسِّن من أداء الشّبكة[1]، وبالتالي فإنّ هذا النّوع من الشّبكات يُستخدم عادة من طرف الشّركات، أو المؤسّسات الصّغيرة والجامعات الخ... [2]، من أجل تسهيل عملية نقل المعلومات بين الأقسام أو الفروع

---

soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz (de 5170 MHz à 5835 MHz). La norme a été ratifiée en janvier 2014.)[حيث يتراوح نطاق التغطية لهذه الشبكة ما بين 32 مترا في الداخل و95 مترا في الخارج ما لم يوجد عائق يعرقل سريانها، كحائط الاسمنت مثلا، في حين تزداد هذه الأرقام كلما تم استخدام أجهزة التقوية، وعليه يُمكِن لمزودي خدمات الإنترنت إحداث شبكة "ويفي" محلية متصلة بشبكة الإنترنت في نطاق تغطية يضم عدد كبير من المُستخدمين(وذلك مجانًا أو بمقابل مادي)، حيث تُشكل هذه المناطق نقاط اتصال "الويفي" (**Bornes points d'accès Wi-Fi** ou « **Hot spots** »).

[1] **علاء عبد الرزاق السالمي**، مرجع سابق، ص ص 307، 308، 309.

[2] من بين الأماكن الشائعة "للويفي" نجد المقاهي والمطاعم والمطارات والفنادق والجامعات والمكتبات وبعض وسائل النقل كالقطارات والطائرات والسفن والمترو والحافلات، وغيرها من الأماكن العامة التي تتيح إمكانية الاتصال بالإنترنت لكل زائر لديه جهاز محمول كالكمبيوتر المحمول أو اللوحة الرقمية، أو الهواتف الذكية أو أي جهاز اتصال مُهيّأ ببطاقة ويفي في داخله مُعدّة لاستقبال الموجات التي تُوفّر خدمة الويفي.

وعليه أصبحت خدمة "الويفي" في الوقت الحالي تلعب دورا مُهِمًّا في العديد من الأماكن الحسّاسة كالمستشفيات والمواقع الأمنية، حيث يمكن للطبيب أو رجل الأمن اللجوء إلى استخدام تطبيقات برمجية معينة لخدمة المرضى أو التعرّف(بالنسبة لرجل الأمن) على هوية الأشخاص غير المرغوب فيهم من دخول أماكن حسّاسة وغيرها، كما أنّها تسمح بالاتصال بشبكة الإنترنت العالمية في حالة التّواجد داخل نطاق شبكة الويفي حيث تتيح الإمكانية للمسافر مثلا البقاء متصلا بالإنترنت أثناء السفر، في حين نجد أنّ عملية إعداد شبكة "الويفي" سريعة وسهلة وتكلفتها أرخص من تكلفة الشبكات السلكية التي تحتاج إلى تمديدات للأسلاك وحفر للجدران الخ...، فبالرغم من المزايا المتاحة لمستخدمي شبكة "الويفي" إلاّ أنّ هذه الأخيرة تتوافر على مجموعة من السلبيات كتدني مستوى أدائها ومحدودية نطاق أو مجال تغطيتها وسهولة اختراق البيانات أو المعطيات الشخصية للأفراد، كما أنّ مُجمل تكنولوجيات الميكرو راديو(Micro-ondes) حاليا وبالخصوص (GSM, WiMAX, UMTS (la 3G), ou encore HSDPA (la 3G+), DECT, et le Wi-Fi) محل انشغال العديد من العلماء، نظرا للمخاطر الصحية التي يمكن أن تلحقها لصحة الإنسان الخ... لمزيد من المعلومات أنظر المواقع الإلكترونية التالية:

http://www.generation-nt.com/imprimer/dossier-radiofrequences-sante-mobiles-article-95591-1.html et https://web.archive.org/web/20120114023754/http://www.sante-radiofrequences.org/index.php?id=5 (consultés le 12/02/2016.) et http://www.it espresso.fr/next-generation-hotspot-le-futur-de-linternet-mobile-passe-par-le-wi-fi-43671.htm et http://www.larousse.fr/dictionnaires/francais/wi-fi/10910038(consultés le 14/02/2016.) et http://www.smallnetbuilder.com/wireless/wireless-features/32238-ac1900-innovation-or-3d-wi-fi(consulté le 16/02/2016.)

بشكل سريع، في حين تعتبر شبكة الإيترنت(Ethernet) من الطرق الشّائعة التي تستخدِم النّموذج الخطّي(Réseau en bus) في توصيل الشّبكات المحليّة[1].

2)- الشّبكة الإقليميّة(Local Metropolitan network(MAN)):

الشّبكة الإقليميّة عبارة عن شبكة بيانات تُغطّي منطقة أكبر من المنطقة التي تُغطّيها الشّبكات المحليّة(LAN)، وأصغر من المنطقة التي تغطيها الشّبكة الواسعة(WAN)، بحيث صُمِّمت الشّبكة الإقليميّة من أجل نقل البيانات عبر مناطق جغرافيّة بفاعليّة وسرعة فائقة، والتي يمكن لها أن تحتوي على عدد من الشّبكات المحليّة(LAN) مربوطة مع بعضها، فمن بين عيوب الشّبكة الإقليميّة نجد أنّها مُكلّفة وصيانتها صعبة[2].

3)- الشّبكة الواسعة(Wide Area Netwwork(WAN)):

الشّبكة الواسعة عبارة عن مجموعة شبكات صغيرة متّصلة فيما بينها عن طريق أجهزة الحاسوب الموجودة في مناطق متباعدة جغرافيًّا، وتتوضّع على مساحة جغرافيّة واسعة في إقليم أو مجموعة من الدول أو قارّة أو حتى عبر الكرة الأرضيّة[3]، لذا تُستخدم هذه الشّبكة لربط العديد من الأجهزة وتوجيه وتبادل كميّات هائلة من البيانات الإلكترونيّة، حيث تُستخدم بشكلٍ واسع من قبلِ متعاملي أجهزة الهواتف النّقالة لربطها بشبكة الإنترنت بصورة سريعة

---

[1] **ناصر خليل**، التجارة والتسويق الإلكتروني، دار أسامة للنشر والتوزيع، الأردن، عمان، 2009، ص ص 160، 175.

علاء حسين الحمامي، سعد عبد العزيز العاني، تكنولوجيا أمنية المعلومات وأنظمة الحماية، دار وائل للنشر والتوزيع، الأردن، عمان، 2007، ص 71.

Jean-François PILLOU, Fabrice LEMAINQUE, Tout sur les réseaux et Internet, 2e édition, Dunod, Paris, France, 2010, p. 12.

[2] **Jean-François PILLOU, Fabrice LEMAINQUE**, Ibid.

غسان قاسم داود اللامي، أميرة شكرولي البياتي، مرجع سابق، ص ص 94، 95.

محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص 53.

سعد غالب ياسين، تحليل وتصميم نظم المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2010، ص 259.

[3] **ناصر خليل**، مرجع سابق، ص 161.

علاء حسين الحمامي، سعد عبد العزيز العاني، مرجع سابق، ص 72.

Jean-François PILLOU, Fabrice LEMAINQUE, op.cit., p.13.

باستخدام تقنية(General Packet Radio Service(GPRS))، لغرض تعميم خدماتها المتاحة في المطارات والأماكن الهامّة والمرافق السّياحيّة الخ...، كما تَستعمِل شركات الطّيران الشّبكات الواسعة لربط ونقل كميّات هائلة من البيانات المتداولة فيما بين مكاتبها المُوزّعة عبر أنحاء العالم، فمن بين عيوب الشّبكة الواسعة نجد أنّها تحتاج إلى برامج وأجهزة مُكلفة جدّا مع صعوبة تشغيلها وصيانتها.

4)- شبكة الإنترنت(Internet):

تعتبر الإنترنت ثمرة جهود العقل البشري التي نشأت في ظروف الحرب الباردة بين المعسكر الشّيوعي والرّأسمالي(أ)، حيث تطوّرت خدماتها عبر العالم بشكل سريع بعد ظهور ونشأة فكرة الويب(**ب**).

أ)- نشأة الإنترنت: تعتبر الإنترنت البنية التّحتية للشّبكات، تحتوي بداخلها عددا لا يُحصى من الشّبكات التي تربط العديد من أجهزة الحاسوب والأجهزة الأخرى ببعضها البعض عبر العالم، عن طريق خطوط الهاتف أو الأقمار الصّناعيّة، بحيث تنبثق جذور هذه الشّبكة(الإنترنت) أصلا من شبكة الاتّصالات المعروفة بالأربنات(ARPANET)، التي اكتشفتها وكالة الأبحاث والمشاريع الأمريكيّة (ARPA, Advenced Research Project Agency) في عام 1969 بطلبٍ من وزارة الدّفاع الأمريكيّة(Pentagon)، وذلك من أجل تحقيق أغراض عسكريّة بحتة في زمن الحرب الباردة، مع الإتّحاد السّوفياتي سابقاً(URSS)[1] عن طريق جمع شمل أكبر عدد مُمْكِن من أجهزة الحاسوب والتّحكم في

---

[1] **L'Union des républiques socialistes soviétiques**, abrégé en (**URSS**) ou en Union soviétique, est un **État fédéra**l, formé de **quinze(15) républiques socialistes soviétiques fédérées**, ainsi que d'un certain nombre de **républiques** et **régions autonomes**, qui a existé du **30 décembre 1922** jusqu'à **sa dissolution** le **26 décembre 1991**.
L'ex- **RSFS** de Russie (**R**épublique **S**ocialiste **F**édérative **S**oviétique de Russie), devenue **Fédération de Russie en 1991**, est actuellement considérée comme l'héritière de l'**URSS** du point de vue diplomatique, et a notamment hérité de son siège de membre permanent au conseil de sécurité des Nations unies. http://www.monde-diplomatique.fr/index/pays/URSS (consulté le 10/01/2016.)

إرسال تعليمات التّصويب إلى قواعد الصواريخ لتفادي أيِّ هجوم نووي مُبَاغِتْ على الولايات المتّحدة الأمريكيّة(USA)[1].

تَغيّر مفهوم شبكة الأربنات(ARPANET) في التّسعينيات، وتوسّع نطاقها بعدما أن ظهرت الشّبكة العنكبوتيّة العالميّة(Web)، التي ألغت الحدود فيما بين الدول وحوّلت العالم إلى كونٍ صغير، تتبادل في إطاره مختلف المعلومات والبيانات بطريقة إلكترونيّة على مستوى جميع الأصعدة[2]، حيث أصبحت شبكة الإنترنت تضم جميع الشّبكات السّالفة الذّكر(LAN/ MAN/ WAN) التي انتشرت وتوسّعت في الآونة الأخيرة، بعدما أن تطوّرت وتنامت معها تطبيقات الويب التي تسهّل الاتّصالات على مستخدمي الشّبكة في شتى المجالات، وبالخصوص في ميادين الاقتصاد الرّقمي.

ب)– علاقة الويب بالإنترنت: إنّ الويب ما هو إلاّ خدمة من بين الخدمات المُختلِفة المُتاحة عبر الإنترنت، وكوسيلة لِبَثّ المعلومات والحصول عليها عبر تلك الشّبكة (الإنترنت)، حيث يسمح للمستخدم من خلال المُتصفّح بالوصول إلى المعلومات وتَصفُّح المُستندات التي تحتوي على صفحات الويب، الصّور، الأصوات والمرئيات، الخ...، إذْ يرجع الفّضل في نشأته(الويب) لأوّل مرّة إلى العالم الفيزيائي ذي الأصول البريطانيّة "تيموتي جون بيرنرلي"(Timothy John BERNERS-LEE)، الذي اشتغل في سنة 1980 كمستشار ومهندس برمجيات داخل المركز الأوروبي للأبحاث النّوويّة(CERN) المتواجد على الحدود الفرنسيّة والسّويسريّة، حيث اقترح في عام 1989 إلى رئيسه الإداري(Mike SENDALL) مشروع تبادل المعلومات يُدعى بالنّص العالمي المُترابط، الذي يجمع بين النّص الفائق(Hypertexte) واستخدام الإنترنت، وذلك من أجل السّماح للمستخدمين بالعمل معاً وتوحيد معارفهم.

---

[1] **Thomas SCHULTZ**, Réguler le commerce électronique par la résolution des litiges en ligne (Une approche critique), BRUYLANT (L.G.D.J), Bruxelles, Belgique, 2005, pp. 18, 19.

[2] **Daneil AMOR**, op.cit., pp. 06, 61, 62.

Alexandre SERRES, « Aux sources d'Internet : l'´emergence d'ARPANET », thèse de Doctorat, en Sciences de l'Information et de la Communication, Université Rennes 2 - Haute Bretagne (U.F.R), Arts Lettres Communication, 2000, pp. 242- 257.

Nicole TORTERELLO, Pascal LOINTIER, op.cit, p. 02.

وفي ماي 1990، قام العالم البريطاني بتغيير تسمية ذلك المشروع بصيغة (World Wide Web)، وذلك تزامنا مع التحاق زميله البلجيكي المهندس في الإعلام الآلي "روبيرت كايو"(Robert CAILLIAU) وبعض علماء الفيزياء العاملين في داخل مركز البحث(CERN)، الذين قاموا بتطوير التّقنيات الأساسيّة، التي جعلت الإنترنت متاحة فعليا لجميع المُستخدمين عبر العالم، وبالتالي "فبيرنرلي" وزملائه لم يربطوا كافة أجهزة الحاسوب في العالم ببعضها البعض، لكنّهم طوّروا التّقنيات الثّلاثة التي مَنَحت للمُستخدمِين إمكانية إيجاد وتبادل المعلومات بين الأنظمة المعلوماتيّة المُتّصلَة ببعضها البعض بشكل أفضل[1]، حيث تتمثّل التّقنية الأولى في مُعرِّف المَوارِد المُوحّد((Uniform Resource Locator(URL) الذي بواسطته يتم الذهاب إلى عنوان موقِع إنترنت مُعيّن، حيث يمنح(URL) كل مصدر على الشّبكة عنوانا متفرّدا خاصاً به يُكتب على شريط العنوان الخاص بالمتصفّح((Navigateur Internet(Web)).

أمّا التّقنية الثّانية تتمثّل في لغة تشفير أو ترميز النّص الفائق أو المُتشعِّب (Hypertext Markup Language(HTML))، التي تُستخدم فقط في إنشاء وتطوير صفحات مواقع الويب وليس في خلق البرامج المعلوماتيّة، حيث تُعتبر لغة برمجة(HTML) بمثابة الوقود الذي يحتاجه المتصفّح لعرض النّصوص والصّور والأصوات والبرامج التّفاعليّة، وغير ذلك، بينما التّقنيّة الثّالثة تتمثّل في بروتوكول نقل النّص الفائق (HyperText Transfer Protocol(http))، الذي يُستعمل للاتّصال بشبكة الإنترنت والوصول إلى مواردها.

وفي أكتوبر 1994 أسّس مُخترِع الويب(Timothy John BERNERS-LEE) تَكتُّل شبكة الويب العالمية((Consortium(W3C)، الذي ساهم في خلق وإعداد قواعد ومواصفات أو معايير تكنولوجيا الويب الأساسيّة، التي من شأنها أن تُحَسِّن التّفاعل بين مستخدمي الشّبكة وضمان التّوافق والاتّفاق فيما بين أعضاء القطاع الصّناعي في اعتماد معايير جديدة وتوفير نماذج مُوحّدة للمستخدمين، كما قام العالم البريطاني ومجموعة من رفقائه في معهد

[1] للمزيد من المعلومات حول الموضوع، أنظر الموقع الإلكتروني التالي: https:/www. Futura-sciences.com/tech/(consulté le 05/01/2016.)

"ماساشوسيتس" للتّكنولوجيا(Massachusetts Institute of Technology(MIT)) بابتكار لغة جامعة لإنشاء مواقع عبر شبكة الإنترنت[1].

5)- الشّبكات الافتراضيّة الخاصّة((VPN)ou(RPV)):

إنّ الشّركات التي تملك مكتب رئيسي ومكاتب متعدّدة موزّعة عبر أنحاء مختلفة من بلد معيّن أو خارجه يعمل في إطارها موظّفوها، كانت تعتمد على شبكة خطوط الهاتف المتّصلة بالخادم والمودم الموجودان في مقرّها لنقل اتّصالات الموظّفين، أو المستخدمين البعيدين بحيث تتميّز هذه الشّبكة بنوع ما من الأمان، مع كثرة التّكاليف النّاجمة عن المبالغ الضّخمة النّاجمة عن الخدمة(إيجار الخطوط) وسرعة الاتّصال البطيئة، كما أنّ البيانات الإلكترونيّة التي يتم تداولها عبر شبكة الإنترنت تكون عرضة لمختلف التّهديدات والاختراقات، لذا ظهرت فكرة الشّبكات الافتراضيّة الخاصّة[2](Virtual Private Network(VPN)) أو (Réseau Privé Virtuel(RPV)) كوسيلة أمان حديثة ساهمت بتقليص أو تخفيض تكاليف نقل البيانات أو المعطيات الإلكترونية، بين مختلف الشركات أو المؤسسات وفروعها البعيدة عن مقرها الرئيسي، وبين المستخدم الذي يريد الوصول إلى معلوماته الخاصة المتواجدة في جهاز حاسوبه المنزلي.

انتشرت وكثرت استخدامات هذه الشبكات في أوساط الشركات والمستخدمين وذلك تزامنا مع انتشار الإنترنت، في أنحاء العالم باعتبارها شبكة الشبكات، وكوسيط فعال لنقل المعلومات من مكان إلى آخر وبأسعار زهيدة[3].

---

1) **Harry HALPIN**, « La souveraineté numérique. L'aristocratie immatérielle du World Wide Web », Revue Multitudes, 2008/4 (N° 35), pp. 206, 207, 209, 210. **Jacques BERLEUR, Yves POULLET**, op.cit., p. 365.

2) عرّف المشرع الجزائري الشبكة الخاصة الافتراضية للاتصالات الالكترونية بموجب **الفقرة 24** من **المادة 10** من القانون رقم 18-04، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، على أنّها:" شبكة تَستغِل منشأة قاعدية للاتصالات الالكترونية قائمة من قَبْلِ، وتتقاسم هذه الشبكة المسالك الأساسية على مستوى هذه المنشأة القاعدية مع الحركة المتبادلة فيها، لكنها محمية بمختلف آليات مراقبة النفاذ والتشفير."

3) **Jean-François PILLOU, Fabrice LEMAINQUE**, op.cit., pp. 228, 229.

أنظر **الملحق رقم(07)**، ص 490.

تتطلب تقنية إحداث هذا النّوع من شبكات الاتّصالات، الاعتماد على برمجيات معلوماتيّة حديثة خاصّة بالشّبكات الافتراضيّة(VPN)، تقوم بإدارة أو ضمان خصوصيّة الاتّصالات القائمة أو المتبادلة عبر شبكة الإنترنت، التي تجمع فيما بين كلّ شبكات الاتّصالات الدّاخليّة(Intranets) والخارجيّة(Extranets)، التي بدورها لا تسمح للعامّة بالدّخول إليها لكونها غير مرتبطة بالإنترنت بشكلٍ مباشر ومفتوح، إلاّ أنّه أحيانا يُسمح بالدّخول إليها من طرف المستخدمين من خارج الشّركة الذين يتمتّعون بصلاحية الدّخول، كالزّبائن والمورّدين ومندوبي المبيعات الخ...، فبما أنّ اتصالات هؤلاء المستخدمين تتم عبر شبكة الإنترنت، إلاّ أنّ هذه الاتّصالات تكون معزولة عن مستخدمي هذه الشّبكة(الإنترنت)، فيتم تحقيق تقنيّة العزل باستخدام عدّة بروتوكولات خاصّة بشبكات الاتّصالات الافتراضيّة[1]، التي تقوم بتأمين وضمان عمليّة نقل وتبادل المعطيات أو البيانات الإلكترونيّة المشّفرة من نقطة إلى أخرى، عبر أنفاق خاصّة مؤمّنة مُرتبطة بالخادم المركزي المتواجد بالمقّر الرّئيسي للشّركة، وبالتالي فإنّ طريقة الدّخول إلى الشّبكات الدّاخليّة أو الخارجيّة هي نفس طريقة الدّخول إلى الإنترنت، بحيث يستوجب على المستخدمين كتابة العنوان الصّحيح في متصفّح الإنترنت مع إدخال كلمة السّر الخاصّة بهم، في حين تتطلّب إدارة أمن هذه الشّبكات الاستعانة بخليط برمجيات الجدار النّاري(Firewall) التي تقوم بحماية الشّبكة والمعلومات

---

1) Les principaux protocoles de tunneling sont les suivants :
- **PPTP** (Point-to-Point Tunneling Protocol) : est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F** (Layer Two Forwarding): est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **L2TP**(LayerTwo Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC2661), pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec:** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Ibid., pp.230-235.

Jean-François PILLOU, « VPN - Réseaux Privés Virtuels (RPV) », pp. 2,3. Article publié le 15/09/2015, sur : http://www.commentcamarche.net/vpn-reseaux-prives-virtuels-rpv-514-mddyo0.pdf, consulté le 23/01/2016.

Jean-Christophe GALLARD, « Sécurité et Réseaux : Partie « Réseaux »- architecture et solution de sécurité », pp. 61- 63. Article disponible à partir de l'adresse: http://www.jgallard.free.fr/RSX112.pdf, consultée le 21/01/2016.

الخاصّة بالشّركة، وتمنع الوصول غير المُصرّح به للشّبكة، من مُستخدمي شبكة الإنترنت غير المسّجلين، ممّا يوفّر حماية عالية للشّبكة ضدّ عمليات الاقتحام غير المشروع[1].

ثالثا– أنواع شبكات الحاسوب من النّاحية الشّكلية:

يقصد من التّصميم الشّكل(La Topologie) الذي يكون عليه توصيل شبكات الحاسوب مع بعضها البعض، وبعبارة أخرى الطريقة المُستخدمة لربط وتوصيل أجهزة الحواسيب بكوابل الشّبكة حيث تُحدّد بحسب برتوكول طبقة البيانات ونوع السّلك أو الكابل الذي تختاره، في حين تتدرج هذه الأشكال وفقا لشبكات النّقل الرّئيسية التّالية:

أ)– الشّبكة الخطّية(Réseau en bus):

تتميّز هذه الشّبكة بجغرافية المسرى(Bus) الذي من خلاله يتم ربط مختلف أجهزة الحاسوب بالنّاقل الخطّي، الذي يتألّف من كابل وحيد على مستوى الشّبكة تتصل به كلّ الأجهزة في شكل سلسلة مرتبطة نظريا بخط مستقيم[2]، ومن مميزات هذه الشّبكة أنّه بإمكان المرسل أن يرسل عبر جهاز الكمبيوتر رسالة إلكترونيّة، إلى أيّ نقطة أو عقدة(Nœud) وتنتقل هذه الرّسالة عبر جميع العقد المتواجدة عبر الشّبكة، بحيث لا يستطيع أي شخص كان من قراءتها، سوى الشّخص الذي تُرسل إليه هذه الرّسالة(المرسل إليه)، إضافة إلى ذلك، نجد أنّ شبكة النّاقل الخطّي تتميّز بسهولة التّركيب ورخيصة التّكاليف[3].

كما تحتوي شبكة النّاقل الخطّي على مجموعة من السّلبيات التي تؤثّر على سرعة ونمط أداءها، فأيّ خطأ في التّوصيل أو الإنهاء أو حصول انقطاع على مستوى النّاقل الخطّي سيؤثّر بالضّرورة على عمل كافة الشّبكة[4]، كما أنّ الإشارات التي لا تستطيع تجاوز نقطة

---

[1] للمزيد من المعلومات حول الموضوع، أنظر المواقع الإلكترونية التالية:
https://www.commentcamarche.net/initiation/vpn.php3 ou https://www.commentcamarche.net/forum/ (consultés le 29/01/2016.)

[2] **ناصر خليل**، مرجع سابق، ص 172.
علاء حسين الحمامي، سعد عبد العزيز العاني، مرجع سابق، ص 74.

[3] أنظر **الملحق رقم (08)**، ص 490.

[4] **علاء عبد الرزاق السالمي**، مرجع سابق، ص 314.

أو عُقدة معيّنة، يتعذّر عليها الوصول إلى كافة الأجهزة التي تَلِي تلك النّقطة أو العقدة، وذلك بالرّغم من استخدام شبكة المسرى التّقنية المعروفة بالوصول المتعدّد بتحسّس الحامل مع كشف التّصادم (Carrier Sense Multiple Access / Collision Detection (CSMA/CD))، فإذا أراد أيّ مُرسِل إرسال رسالة إلكترونيّة عبر جهاز الحاسوب، فإنه يقوم بتحسّس الكابل حول ما إذا كان شاغرا لكي تُرسَل هذه الرّسالة، أو ينتظر حتى النّهاية في حالة إذا كان الكابل مشغولاً، ففي حالة ما إذا قام أكثر من جهاز بإرسال رسائل إلكترونيّة في نفس اللّحظة، فتتلاقى بصورة عَشوائيّة مما يتعذّر إرسالها عبر مختلف النّقاط، ممّا يضطّر صاحبها إلى إعادة المحاولة من جديد[1].

ب)– الشّبكة النّجميّة(Réseau en étoile):

تتميّز الشّبكة النّجميّة بتواجد مُوزّع أو خادم مركزي(Concentrateur ou Hub) تجتمع أو ترتبط به جميع الأسلاك أو الكابلات الخاصّة بأجهزة أو مكوّنات هذه الشّبكة[2]، كما يمكن أن ترتبط به كذلك جميع المجمّعات المركزية في الشّبكة، بحيث تمرّ عبره جميع الرّسائل أو الإشارات من دون استخدام أو المرور على العقد أو النّقاط، فأي خلل أو عطب في هذه الأخيرة(Nœuds) لا يؤدي حتما إلى شلل أو فشل في منظومة عمل الشّبكة النّجميّة، فإذا فشل كابل أو وصلة جهاز معيّن عبر الشّبكة، فلن يتأثّر سوى ذلك الجهاز المتّصل بذلك الكابل أو الوصلة، لكون أنّ جميع مسارات الاتّصالات فيها متمركزة في الموزّع أو الخادم المركزي[3]، فعن طريقه يتم توجيه الرّسائل أو الإشارات إلى الجهاز أو الأجهزة المطلوبة[4].

ومن بين مميزات الشّبكة النّجميّة، نجد أنها تسهّل عملية عزل أو إضافة العُقَد، أو النّقاط المتواجدة فيها، وتسهّل تحديد أي مشكلة أو عطب في داخلها(الشّبكة)، كما أنّ لهذه الأخيرة أيضا سلبيات تتمحور حول ما إذا حصل عطب أو فشل في الموزّع المركزي، ستنهار حتما، ولو كان ذلك من النّاحية العمليّة نادرا، كما أن الموزّع المركزي بحاجة إلى تدعيمه وتقويته

---

1) **Jean-François PILLOU, Fabrice LEMAINQUE**, op.cit., pp. 6.
2) Ibid.

3) **سعد غالب ياسين**، مرجع سابق، ص 254.

4) أنظر **الملحق رقم (09)**، ص 490.

بمختلف أجهزة الحاسوب كالمحوّلات(Routeurs)، والمبدّلات(Switch) بالرّغم من ارتفاع التّكاليف الخ...[1].

ج)- الشّبكة الحلقيّة(Réseau en anneau):

تتشابه هذه الشّبكة مع الشّبكة الخطّية(Réseau en bus) لكون أن جميع النّقاط أو العُقَدْ(Nœuds) التي ترتبط فيما بينها تكون في خط واحد، إلاّ أن الشّبكتان تختلفان من حيث الشّكل، بحيث تكون الشّبكة الحلقيّة في شكل دائرة أو حلقة تتصل من خلالها أجهزة الحاسوب في اتجاه واحد فقط، بحيث تنتقل الإشارات من نقطة أو عقدة لأخرى وتتصل كلّ عقدة مع عقدتين بشكل مباشر، أي عقدة ترسل لها وعقدة تستقبل منها، وبالتالي فكل جهاز في هذه الشّبكة يستقبل إشارة ويستجيب لها بناءً على ذلك، ويُعيد توليدها من جديد لكي يقوم بإرسالها للجهاز الذي يليه وذلك في إطار مسار واحد[2].

لتفادي التّضارب فيما بين الرّسائل الإلكترونيّة، تستخدم الشّبكة الحلقيّة بروتوكول اتّصال يدعى بعلامة الحلقة(Anneau à jeton) أو (Token Ring)[3]، بحيث تدور هذه العلامة من عقدة إلى عقدة أخرى في حالة شغور قناة الشّبكة الحلقيّة، فإذا أراد أحد العُقَد في بإرسال رسالة إلكترونيّة، فينتظر حتى يمسك بالعلامة التي يعدّل مسارها ويرسلها مع الرّسالة في اتجاه العقدة أو النّقطة التي تقبل الاستقبال، ففي هذه الحالة لا يكون بمقدور أي شخص في هذه اللّحظة أن يقوم بالإرسال حتى ينتهي الإرسال الأوّل، كما تمنح الشّبكة الحلقيّة إمكانية إرسال الرّسالة الإلكترونيّة إلى عدّة جهات مستقبلة، وتلغي بالتالي الرّسائل التي تقوم بأكثر من دورة واحدة، فمن بين مميّزات الشّبكة الحلقيّة نجد أنها سهلة التركيب ورخيصة التّكاليف، وقادرة على العمل حتى في حالة تواجد عطب أو فشل أحد الكابلات أو الوصلات[4].

---

[1] **عامر إبراهيم قنديلجي، إيمان فاضل السامرائي**، شبكات المعلومات والاتصالات، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، 2012، ص 71.

[2] **غسان قاسم داود اللامي، أميرة شكرولي البياتي**، المرجع نفسه، ص ص 98، 99.

أنظر **الملحق رقم (10)**، ص 491.

[3] **Jean-François PILLOU, Fabrice LEMAINQUE**, op.cit., pp. 7.

[4] **ناصر خليل**، مرجع سابق، ص ص 173، 176، 177.

د)- الشّبكة المتشابكة(Réseau maillé):

يمتاز هذا النّوع من الشّبكات بتعدّد التّوصيلات المرتبطة فيما بين أجهزة الحاسوب وتشّعب مسارات الاتّصالات فيها[1]، ففي حالة ما إذا انهار الاتصال في توصيل أو كابل معين، فسيُعوَّض بالتالي ذلك الانقطاع بإتّباع أو سلوك مسارات أخرى بديلة، من أجل الوصول إلى الهدف المرغوب، وهذا ما يُحسّن من عمل وأداء هذه الشّبكة، وما يُعاب على هذه الشّبكة أنّها قليلة الاستعمال ونادرا ما يتم إحداثها لكون كُلفتها غالية وكثرة التّوصيلات المطلوبة فيها وتشّعبها، فمن بين إيجابيات هذه الشّبكات نجد أنّها تُستعمل كثيرا في الربط بين أنواع أخرى من الشّبكات المحليّة[2].

هـ)- الشّبكة الهجينة أو الهرميّة(Réseau hybride - Hiérarchique):

تعتبر هذه الشّبكة من أحد أشكال الشّبكة الخطّية(المسارية) أو النّجميّة، بحيث يكون تصميمها في شكل شجرة، ترتبط أو تتصل من خلالها عدّة عُقد بشكل هرمي بعقدة الجّذر أو الرّئيسي، التي يمكن أن تكون كخادم قوي أو حاسب مركزي في رأس الهرم[3]، فمن بين مميّزات هذه الشّبكة، نجد أنّها سهلة التّوسّع ومرنة في تحديد وعزل العقد التي يحصل فيها عطل أو خلل، وبالتالي فإنّ هذا النّوع من الشّبكات نجده مناسبا للشّركات أو المؤسّسات(التّجاريّة والصّناعيّة)، التي يتصل في إطارها مستخدميها بمختلف مكاتبها أو فروعها الموزّعة إقليميا أو محليا داخل أو خارج إقليم الدّولة، الذي يتواجد فيها الخادم الرّئيسي للشّركة أو المؤسّسة، فإذا حصل أيّ خلل أو عطل على مستوى ذلك الخادم، تنهار الشّبكة بأكملها [4].

---

[1] **غسان قاسم داود اللامي، أميرة شكرولي البياتي**، مرجع سابق، ص 100.

[2] أنظر **الملحق رقم (11)**، ص 491.

[3] **غسان قاسم داود اللامي، أميرة شكرولي البياتي**، مرجع سابق، ص 101.

[4] أنظر **الملحق رقم (12)**، ص 491.

الفرع الثالث

المتدخّلين في إطار خدمات شبكة الإنترنت

إنّ عدد المُتدخّلين في شبكة الإنترنت لا يُحصى ولا يُعدّ، فمنهم من يضمن نقل المعلومة أو خدمة الإيواء(Hébergement) أو البحث عن المعلومة(La recherche)، ومِنهم من يضمن خدمات التّصديق الإلكتروني(Certification électronique) أو علامة المواقع الإلكترونيّة(Labellisation) ومِنهم من يَعرِض وسائل التّشفير(La cryptographie) إلى غيرهم، وأهم هؤلاء المتدخّلين هم كالتّالي: مُسجّل أسماء مواقع الإنترنت(**أولا**)، المستعمل (**ثانيا**)، مزوّد الدّخول (**ثالثا**)، مزوّد الإيواء (**رابعا**)، مزوّد المحتوى (**خامسا**)، مزوّد خدمة النّقل (**سادسا**)، مزوّد خدمة البحث (**سابعا**)، مزوّد خدمات التّصديق الإلكتروني (**ثامنا**).

أولا– مُسجّل أو مكتب تسجيل أسماء مواقع الإنترنت (Registrar ou Bureau d'enregistrement):

يُقصد به الشّخص أو الهيئة التي تُتِيحُ خدمات تسجيل أسماء مواقع الإنترنت، وفقا للعقد الذي يربطها مع السّجل(Registre) أو هيئة التّسجيل(Instance d'enregistrement)، المسؤولة عن إدارة وتنظيم وتسجيل اسم النّطاق المعني، حيث يجب على المُسجّل أو مكتب التّسجيل قبل الشّروع في مزاولة مهامه، أن يَتَحَصَّلَ على اعتماد من قِبَلِ هيئة التّسجِيل وفقا للشروط والإجراءات المُحدّدة من طرف هذه الأخيرة[1].

---

[1] **Règlement (CE) n° 733/2002** du parlement européen et du conseil du 22 avril2002, concernant la mise en œuvre du domaine de premier niveau .eu, J.O.U.E, L 113/1 du 30.4.2002.

Art. 02 : « **a)**- «**Registre**», l'entité chargée de l'organisation, de l'administration et de la gestion du TLD .eu, y compris la maintenance des bases de données correspondantes et les services de recherche publics qui y sont associés, l'enregistrement des noms de domaine, l'exploitation du registre des noms de domaine, l'exploitation des serveurs de noms du registre du TLD et la diffusion des fichiers de zone du TLD;

b)- «**Bureau d'enregistrement**», la personne ou l'entité qui, dans le cadre de contrats conclus avec le registre, fournit aux demandeurs des services d'enregistrement de nom de domaine. »

Règlement (CE) n° 874/2004 de la commission du 28 avril 2004, établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier

ثانيا– المستعمل أو المستفيد(Utilisateur):

يمكن أن يكون المستعمل شخص طبيعي أو معنوي يستفيد من الخدمات المتاحة من طرف(م.خ.إ)، التي يُعوّل عليها أطراف التّبادل الإلكتروني في إبرام مختلف صفقات التّجارة الإلكترونيّة، وكذا عقود البيع والشّراء والدّفع عبر شبكة الإنترنت، الخ... [1].

ثالثا– مُزوّد الدّخول أو الاتّصال(Fournisseur d'accès):

لكي ينتفع المستهلك بخدمات شبكة الإنترنت، يجب عليه الاتّصال بمزوّد خدمة الاتّصال أو الدّخول، لغرض الاستفادة بخدمة الرّبط بشبكة الإنترنت أو الشّبكات الخاصّة، أين يتّفق معه(Fournisseur d'accès) مُسبقا حول جميع بنود العقد، التي عادة ما تتضمّن العناصر الفنيّة والقانونيّة التي لها صلة بخدمة الرّبط، ويكون ذلك بمقابل، حيث يلتزم المزوّد، من خلال هذا العقد، بضمان خدمة الاتّصال بالخوادم أو المُوزّعات(Serveurs)،

---

niveau .eu et les principes applicables en matière d'enregistrement, J.O.U.E, L 162/40 du 30/4/2004.

Art. 04 (**Accréditation des bureaux d'enregistrement**) : « **Seuls les bureaux d'enregistrement accrédités** par le **registre** sont **autorisés** à offrir des services d'enregistrement pour des noms dans le domaine de premier niveau **.eu**. La procédure d'accréditation des bureaux d'enregistrement est déterminée par le registre; elle doit être raisonnable, transparente et non discriminatoire, et doit garantir des conditions de concurrence effectives et équitables. Les bureaux d'enregistrement doivent avoir accès aux systèmes d'enregistrement automatisés du registre et utiliser ces systèmes. Le registre peut établir d'autres exigences techniques de base pour l'accréditation des bureaux d'enregistrement.

Le **registre** peut demander aux bureaux d'enregistrement d'acquitter par anticipation les droits d'enregistrement, qui sont établis chaque année par le registre sur la base d'une estimation raisonnable des conditions du marché.

Le **registre** doit faire en sorte que le **public** puisse facilement prendre **connaissance** de la procédure, des conditions d'accréditation des bureaux d'enregistrement et de la liste des bureaux d'enregistrement accrédités. Chaque **bureau d'enregistrement** s'engage contractuellement envers le **registre** à respecter les conditions d'accréditation, et en particulier à se conformer aux principes de politique d'intérêt général établis dans le présent règlement. »

Voir aussi : La liste des **registraires accrédités par l'ICANN** est disponible à l'adresse suivante : http://www.internc.net/regist.html

[1] **علي كحلون**، المسؤولية المعلوماتية (محاولة لضبط مميّزات مسؤوليّة المتدخلين في إطار التطبيقات المعلوماتية وخدماتها)، مركز النشر الجامعي، تونس، 2005، ص 74.

التي تُمكّن المستهلك من استشارة بنوك المعلومات(صور، أصوات، نصوص، فيديوهات، الخ...) التي تحتويها مواقِع الإنترنت، إلى جانب الخدمات الأخرى التي تُتيحها الإنترنت[1].

رابعا- مُزوّد الإيواء(Fournisseur d'hébergement):

إنّ هيكلة اسم النّطاق تتطلّب الاستعانة بفنيات وتقنيات مُزوّد خِدمة التّخزين أو الإيواء، الذي من المُمْكِنِ أن يكون في نفس الوقت مُزوّد الدّخول أو الاتّصال، وذلك لضمان بقاء واستمرارية الموقِع الإلكتروني بصفة فعليّة على شبكة الإنترنت، حيث يُشرف ذلك المُتعهِّد(Fournisseur d'hébergement)[2] على مُهِمَّةِ تخزين البيانات والمعلومات،

---

[1] **عمر خالد زريقات**، عقود التجارة الإلكترونية: عقد البيع عبر الإنترنت(دراسة تحليلية)، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007، ص ص 83- 85.

علي كحلون، مرجع سابق، ص 75.

Philippe LE TOURNEAU, op.cit., p. 432.

[2] La plupart des offres d'hébergement sont regroupées en grandes catégories :

1- Les hébergements partagés ou mutualisés : Chaque serveur héberge plusieurs sites, jusqu'à plusieurs milliers, et ce dans le but de mutualiser les coûts. Le principal avantage est le prix, le principal inconvénient est que le client mutualisé n'est pas l'administrateur du serveur, il est donc souvent tributaire du bon vouloir de l'hébergeur s'il souhaite une technologie particulière. Dans certaines configurations d'hébergement mutualisé, l'utilisateur peut être administrateur d'un serveur virtuel sur lequel son site est déployé. Il continue cependant à partager les ressources système avec les autres clients mutualisés.

2- Les hébergements dédiés : Le client dispose alors de son propre serveur, et peut en général l'administrer comme il le souhaite, ce qui est le principal avantage de ce type d'offre. Le fournisseur du serveur reste cependant propriétaire du serveur. Les inconvénients sont : le prix beaucoup plus élevé que les hébergements mutualisés, et le besoin de compétences pour administrer la machine correctement.

3- L'hébergement virtuel dédié via un hyperviseur ; qui offre au client la souplesse d'un dédié (le client administre sa machine à sa convenance) en lui fournissant une machine virtuelle qui utilise une partie des ressources d'un serveur (physique) par des techniques de virtualisation (informatique).

4- Les hébergements dédiés dits « managés », avec « serveur dédié infogéré » ou « clés en main » : Le client dispose de son propre serveur mais les techniciens de l'hébergeur s'occupent de sa gestion système. Cette solution est parfaite si vous n'avez aucune connaissance technique sur son administration. Il suffit de déposer son site. Ce type d'hébergement cherche à s'adapter aux besoins.

5- La colocation : L'hébergeur met, dans son centre de traitement de données, un espace à disposition du client, de sorte qu'il puisse placer son propre serveur à l'intérieur (La plupart du temps dans des armoires spéciales nommées racks ou « baies »). L'hébergeur met également à disposition du client un câble d'alimentation électrique et un câble Ethernet pour qu'il puisse alimenter et connecter son serveur à Internet. Ce système est censé coûter moins cher, puisque

وصفحات الويب التي يتيحها أصحاب المواقع الإلكترونيّة على مستوى خوادمه أو موزّعاته المُرتبطة بصفة دائمة بشبكة الإنترنت، التي يتمكّن من خلالها المستهلكين من الاطّلاع على مضمونها المعلوماتي على مدار السّاعة، حيث يجب على متعهّد الإيواء التقيّد بقواعد السلامة والأمن الكفيلة بحماية شبكة الإنترنت[1].

خامسا– مُزوّد المُحتوى(Fournisseur de contenu):

يُعْرَفُ مزودّ المحتوى كذلك بمُورِّد المعلومات، الذي قد يكون صاحب المادة المعلوماتية الذي يَتَّخِذُ صِفة المُؤلّف والنّاشر لهذه المادّة، أو يكون صاحب المُحْتَوَى المُرسِل أو صاحب المَوقِع الإلكتروني أو مُزوِّد خدمات، كما يمكن أن يقتصر دور مُورّد المُحتوى على جمع المادّة المعلوماتية، من خلال التَوسُّط فيما بين مؤلف تلك المادة ومُستخدمِي شبكة الإنترنت الراغبين في الإطّلاع على مضمونها، حيث يَتَّخِذُ في هذه الحالة صفة النّاشر للمادّة المعلوماتية عبر شبكة الإنترنت (عقد نشر يربطه بصاحب المادّة المعلوماتيّة)، الخ...

ومن هنا يمكن أن يكون مُورّد المعلومات شخص طبيعي(المدوّن(Éditeur d'un Blog)) أو معنوي مُنشئ للمعلومة(Plates-formes de blog) أو له علاقة بمحتوى تلك المعلومة[2]، حيث يتميَّز عن مُتعهّد الإيواء في كون أنّ الأوّل(Fournisseur de contenu) يُشرف على خدمة النّشر أو التّوريد للمعلومات، بينما الثّاني(Fournisseur d'hébergement) يُشرف على خدمة تأجير أو إعارة مكان أو مساحة على مستوى خادمه أو القرص الصّلب(الحاسوب)، حيث يعتبر متعهد الإيواء في هذه الحالة بمثابة المؤجّر أو المُعير

---

la location du serveur n'est pas comprise, mais les systèmes de sécurité et des badges dans les centres de traitement de données peuvent coûter plus cher que la location.
Nicolas CHU, réussir un projet de site web, 3e édition, EYROLLES, Paris, France, 2005, pp. 72- 77.

أنظر كذلك: **لزهر بن سعيد**، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2014، ص ص 56، 57.

[1] **علي كحلون**، مرجع سابق، ص 76.

Philippe le TOURNEAU, op.cit., p. 438.

[2] **علي كحلون**، مرجع سابق، ص ص 74، 75.

Romain V. GOLA, op.cit., pp. 493, 494.

للمكان، فبالرّغم من أوجه الاختلاف إلاّ أنّ كلٍّ من مورّد المُحتوى ومتعهّد الإيواء يلتقيان في إطار المساهمة في تقديم الخدمة المعلوماتيّة للجمهور[1].

سادسا– مزوّد خدمة النّقل(Transmetteur):

يُطلق عليه كذلك تسمية مزوّد البنية التّحتيّة(Fournisseur d'infrastructure)، الذي يُشرف على إجراءات الربط المادّي والفنّي فيما بين شبكات الاتصال عن بُعد، حيث تتولى هذه الخدمات الهيئات العامّة للاتّصال لكل دولة، على غرار اتّصالات الجزائر واتّصالات تونس وهيئة الاتّصالات الأردنية، وفرانس تيليكوم(France télécom) في فرنسا، باعتبارها كناقل مادّي للبيانات والمعلومات المتداولة عبر الإنترنت، حيث تلتزم في إطار عقد نقل المعلومات بتقديم الوسائل والأجهزة التقنيّة(Les câbles, routeurs, etc.) اللاّزمة لإجراء وتأمين عملية النّقل المادّي للبيانات الإلكترونيّة المتبادلة فيما بين أطراف التّعامل الإلكتروني، وكذا ضمان الرّبط المشترك بين مختلف شبكات الاتّصال عبر الإنترنت[2].

سابعا– مزوّد خدمة البحث (Fournisseur de recherche):

يشرف هذا المزوّد على التّطبيقات المعلوماتية التي تتيح للمستهلك أو المستخدم، إمكانية البحث ومعرفة وجمع البيانات والمعلومات عبر شبكة الإنترنت، عن طريق مُحرّكات البحث(Moteurs de recherche) والفهارس أو الأدّلة(Annuaires, répertoires, indexes)، حيث تسمح محرّكات البحث(Google, Yahoo!, Lycoc, Altavista, etc.) للمستهلك بالوصول إلى مختلف البيانات والمعلومات المطلوبة بطريقة آلية، بمجرّد كتابة موضوع

---

[1] **أحمد قاسم فرح**، "النظام القانوني لمقدمي خدمات الإنترنت– دراسة تحليليّة مقارنة–" مجلة المنارة، المجلد 13، عدد 09، 2007، ص ص 327، 328.

[2] **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية الحكومة الإلكترونية، (الكتاب الثاني)، دار الفكر الجامعي، الإسكندرية، مصر، 2003، ص 349.

Alain STROWEL, Nicolas IDE, « Responsabilité des intermédiaires : actualités législatives et jurisprudentielles », pp. 09,11. Article publié le 10/10/2000 sur le site: https://www:droit-tchnologie.org, consulté le 03/03/2018.

البحث أو الكلمات الدّالة عليه في المكان المُناسب[1]، بينما تتضمّن الفهارس على مجموعة من المواقع الإلكترونيّة المُنظَّمَة بصفة تسلسليّة وهرميّة، تُتيح (الفهارس) للمستهلك إمكانية البحث عن المواضيع المتعلّقة بهذه المواقِع بمجرّد الضّغط بالمكان المناسب للوصول إلى محتوى الموقِع المطلوب.

وتُمكّن هذه الفهارس المستهلكين من الإطّلاع على مواقع التّجارة الإلكترونيّة والانتفاع بمُحتواها، حيث بإمكان أصحاب المتاجر الافتراضيّة الانخراط في الدّليل أو الفهرس بمجرّد موافقة الجّهة المكلّفة بإدارته(Annuaires, répertoires, indexes)[2].

تعتمد محرّكات البحث على روابط الإحالة(Liens hypertextes)، التي تُمثِّل أو تُعَبِّرُ على وسوم أو أكواد لغة برمجة(Code HTML) المُستخدمة في تنظيم صفحات ويب المواقع الإلكترونيّة على نحو يسمح للمُتصفّح(Navigateur)، بالانتقال من صفحة ويب إلى أخرى، سواء كانت في نفس المَوقِع الإلكتروني(Lien interne) أو بموقِع آخر (Lien externe)، وبتعبير آخر، فإذا أحالت الرّوابط إلى صفحات ويب داخلية بنفس الموقِع فهي داخلية، أمّا إذا أحالت الرّوابط إلى صفحات موجودة بمواقع خارجية فهي إحالة خارجية التي من خلالها يتّخذ رابط الإحالة(liens hypertextes) المَخْفِي، شَكل وَسْمْ (Code HTML du lien) يَتضّمنُ على اسم الموقِع الإلكتروني المُحَال إليهِ، فعن طريق رابط الإحالة يتمكّن المُستهلك من الوصول إلى المواقِع الإلكترونيّة بمُجرّد الضّغط على مكان التّرابط الذي يتّخذ شكل صورة أو فيديو أو كلمات، الخ...[3]

---

1) **Alain STROWEL, Nicolas IDE**, (actualités législatives et jurisprudentielles), Ibid., pp. 09, 10.
Thibault VERBIEST, « Entre bonnes et mauvaises références. A propos des outils de recherche sur internet », pp. 2-5. Article publié le 31/05/2000 sur le site: https://www:droit-tchnologie.org, consulté le 12/03/2018.

2) **Thibault VERBIEST**, op.cit., p. 6.
Philippe LE TOURNEAU, op.cit., p. 462.
فاطمة الزهراء محمد عبده، "محركات البحث على شبكة الإنترنت"، مجلة الكترونية محكمة في المكتبات والمعلومات(Cybrarians journal)، عدد 02، سبتمبر 2004، ص ص 06-12. مقال منشور على الموقع التالي:
https://www.cybrarians.info/journal/no2/searchengines.htm

3) **Romain V.GOLA**, op.cit., pp. 513- 515.

وعليه، تنقسم روابط الإحالة(Type de code HTML) حسب طريقة البرمجة La) technique de linking) المُستعملة، إلى أربعة تقنيات والمتمثّلة فيما يلي[1]:

أ)- الرّوابط السّطحية((Le lien en surface (Surface linking)): من خلالها يقوم الرّابط الخارجي لصفحة الموقِع الإلكتروني(Le site établissant le lien)، بالإحالة إلى صفحة ويب الاستقبال الأصليّة(La page d'accueil originale) للموقِع الإلكتروني الآخر المُحال إليهِ(Le site relié)، وبمعنى آخر، أن تقع الإحالة إلى موقِع خارجي(Le site relié) مرورًا عبر صفحة الاستقبال الأصليّة التّابعة له.

ب)- الرّوابط العميقة((Le lien en profondeur (Deep linking): فإذا كان الرّابط السّطحي يُحِيلُ المُستهلك إلى صفحة الاستقبال الأصلية للموقِع الإلكتروني المُحَال إليهِ، فإنّ الرّابط الخارجي العميق(Lien externe en profondeur) يُحِيلُ إلى صفحات الويب الثّانوية لذلك المَوقِع(Le site relié)، مِن دُونِ المرور عبر صفحة الاستقبال الأصليّة له.

ج)- الرّوابط الإطارية(("Le cadrage (ou "framing): يتّخِذ إطار صفحة الويب عادة شكل شعار(Logo) أو اسم(Nom) الشركة المُستغلة للموقِع الإلكتروني أو إعلانات (Bannières publicitaires) الخ...، يتضمن على محتوى صفحات تابعة لمواقع إلكترونيّة أخرى، حيث يسمح رابط الإطار(Lien cadre ou cadrage) سواء بعرض صفحات ويب نفس الموقِع الإلكتروني أو عرض صفحات ويب لمواقِع أخرى في إطار الموقِع الإلكتروني الأصلي للرّابط(Site qui établit le lien)، وبمعني آخر، بمُجرّد النّقر على رابط الصّورة أو الإعلان أو الشّعار، يتّم عرض مُحتوى صفحات ويب الموقِع المُحال إليهِ(Site relié) دون الخروج من إطار عنوان وصفحة الموقِع الأصلي الذي تمّ النّقر فيه على رابط الإحالة، فعندما يتصفّح المُستهلك لمُحتوى صفحات المَوقِع المُحال إليهِ، فإنّ عُنوان هذا

Alain STROWEL, Nicolas IDE, « La responsabilité des intermédiaires sur internet: Actualités et question des hyperliens (2ème partie: la responsabilité en matière d'hyperliens) », pp. 03, 04. Article publié le 02/02/2001 sur le site: https://www:droit-tchnologie.org, consulté le 11/03/2018.

1) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit, pp. 05, 06, 07.

الأخير(L'URL de Site relié)، لا يَظْهَرُ على مُتصّفح المَوقِع الأصلي الذي تمّت فيه الإحالة، حيث لا يُدركُ المُستهلك عنوان الموقِع المُحال إليهِ عند تصفُّحه لمُحتواه[1].

د)- الرّوابط الآليّة(("Inlining" ou « Embedded link ») Le lien automatique):

يُدعى كذلك بالرّابط التّفاعلي(Lien dynamique) الذي من خلاله يقوم صاحب الموقِع الإلكتروني في إطار لغة البرمجة، بإدراج ضمن صفحة الويب "صورة" تُعبِّرُ عن شِعار أو اسم تجاري أو غيره، تابعة لصفحات أخرى مُتواجِدة بنفس الموقِع الإلكتروني أو بمواقِع أخرى، ويكون لهذه الصّورة عنوان إلكتروني خاص بها(Adresse URL)، حيث يَحْصُلُ التّنقُّل إلى صفحات الصّورة في إطار الموقِع الأصلي بطريقة آلية من دون تدخّل المُستهلك في ذلك، وبمعنى آخر، فإنّ متصفّح الويب يستجيب آليا لِلُغة البرمجة ويُحيل إلى مكان تواجد الصّورة(Le serveur où l'image est stockée)، وبالتالي، فلتفعيل الرّوابط السّطحية والعميقة والإطاريّة تستدعي تدخُّل المُستهلك، بينما يتّم تفعيل الرّوابط الآليّة بطريقة آلية من طرف المُتصّفح من دون تدخُّل المستهلك[2].

وبالرغم من الدّور الأساسي الذي تلعبه تقنيات روابط الإحالة في تفعيل نشاط مواقِع التّجارة الإلكترونيّة وخدمات مزوّدي البّحث، إلاّ أنّها أثارت نقاشات قانونية حول طرق الإحالة المستعملة في بعض هذه التّقنيات، التي تُشكّل اعتداء على المصنّفات الرّقميّة المحميّة وخرق قواعد المنافسة المشروعة أو المساس بالحقوق الأخرى المملوكة للغير[3].

ثامنا- مزوّد خدمات التّصديق الإلكتروني(PSCE- AC):

يُطلق عليه كذلك مصطلح المُوثّق الإلكتروني، باعتباره كوسيط موثوق به محايد عن أطراف العقد الإلكتروني[4]، يضمن تبادل المعلومات والبيانات عبر شبكة الإنترنت من

---

1) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., pp. 05, 06, 07.

2) Ibid., pp. 05, 06.

3) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., p. 08.

4) **Règlement (UE) n° 910/2014** du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au

خلال تحديد وتوثيق هوية أطراف التصرف الإلكتروني (Identification+Authentification)، وتأكيد سلامة وسرية محتوى البيانات المتداولة(Intégrité-Confidentialité)، مع ضمان عدم إنكار التّصرف الإلكتروني-Non) (Répudiation من جانب أطراف العقد الإلكتروني، حيث يُشرف(م.خ.ت.إ) على الخدمات المتعلّقة بتزويد المتعاقدين بشهادات التّصديق الإلكتروني الموصوفة بعد التّحقق من المعلومات المُقدّمة، وإصدار مفاتيح التّشفير(العامّة والخاصّة) للمُوقِّع، وتحديد لحظة إبرام العقد الإلكتروني، وكذا تأمين المواقع الإلكترونيّة وإيقاف أو إلغاء الشّهادات، الخ....

---

sein du marché intérieur (eIDAS) et **abrogeant la directive 1999/93/CE**. JOUE L 257/73 du 28/08/2014.

Art. 03-19: « **Prestataire de services de confiance**», une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié.»

Loi sur la signature électronique, **SCSE du 18 mars 2016**, RS 943.03 (État le 1er janvier 2017).

Art. 2 « Définitions Au sens de la présente loi, on entend par: […] ; **k.** fournisseur de services de certification (**fournisseur**): un organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques; […]. »

قانون عدد 83 لسنة 2000 مؤرخ في 9 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية، ر.ر.ج.ت عدد 64، الصادر في 9 أوت 2000.

الفصل: 4/02:"مزود خدمات المصادقة الإلكترونية: كلّ شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني."

وتنص المادة 12-11/02 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، سالف الذكر، على ما يلي: "**الطرف الثالث الموثوق:** شخص معنوي يقوم بمنح شهادات تصديق الكتروني موصوف، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي."

– "**مؤدي خدمات التصديق الإلكتروني:** شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني."

المبحث الثاني
التّسويق في مواقع التّجارة الإلكترونيّة

استطاعت التّقنيات التّكنولوجيّة الرّقميّة المنتشرة بكثرة في شتى مجالات المعاملات الالكترونيّة، أن تُحَوِّلَ الوظائف التّسويقيّة إلى مفهوم حديث، ساهم في ظهور آليات وتقنيات جديدة في تسويق السّلع والخدمات، وتبادلها بطرق إلكترونيّة عبر شبكة الإنترنت، التي تعتبر كوسيلة مُهمّة من وسائل قطاع التّسويق الإلكتروني، الذي انطلق بدوره بسرعة مُذهِلة في الآونة الأخيرة، نظرا لما يتيحه في انخفاض التّكاليف، والقدرة في التَوسُّع عبر مختلف أسواق العالم في إطار نمط جديد في شبكة الأعمال أكثر فاعليّة مع التّكنولوجيا الرّقميّة، الذي يخضع لنفس المبادئ الأساسية المعروفة في التّسويق التّقليدي **(المطلب الأول)**.

نتيجة لما سبق، فإنّ وظائف التّسويق الإلكتروني المفتاح الأساسي لتحقيق أهداف الشّركات، التي جعلت من قنوات التّسويق الحديثة مدارا جديدا للاتصال بالعملاء وإقامة علاقات معهم عبر مَواقِع شبكة الإنترنت، التي تُعْرَضُ من خلالها العديد من المنتجات والخدمات، وتُوفّر بيئة خصبة لممارسة الحملة الدعائيّة، كما تُوفّر استشارات وحُلُولاً لحُسن سير الإعلانات الإلكترونيّة التي تستجيب بسُرعة لتَوقُّعات فئة مُستهدَفة من المستهلكين **(المطلب الثاني)**.

المطلب الأول
مفهوم التّسويق الإلكتروني

أصبحت الأسواق في وقتنا الحاضر بحاجة إلى مختلف المنتجات والخدمات التي تتطلب تقنيات وأساليب تسويق حديثة، لإعلانها أو ترويجها لغرض جذب واستهداف مختلف العملاء، حيث يتمتّع التّسويق الإلكتروني بخصائص تُمَيِّزُهُ عن تلك التي يتمتّع بها التّسويق التّقليدي**(الفرع الأول)**، وتعتبر تقنيّة التّسويق الالكتروني من إحدى تطبيقات التّجارة الالكترونيّة التي تعتمد عليها الشّركات من أجل تحقيق أهدافها التّجارية المرغوبة**(الفرع الثاني)**، حيث يمكن التّرويج لمختلف السّلع والخدمات باستخدام تقنيات التّسويق الحديثة عبر شبكة الإنترنت**(الفرع الثالث)**، وبالتّالي يعتبر التّسويق الإلكتروني كجزء من معاملات

التّجارة الإلكترونيّة التي تفرض على أطراف عملية التّسويق الإلكتروني مُواجهة مجموعة من التّحديات أو عوائق البيئة الافتراضيّة، التي تتبادل في إطارها البيانات أو المعلومات الإلكترونيّة(**الفرع الرابع**).

الفرع الأول
تعريف التّسويق الإلكتروني وخصائصه

يُعتبر التّسويق الإلكتروني من بين المفاهيم الأساسية المعاصرة المنبثقة عن تكنولوجيات الثّورة الرّقميّة(**أولا**)، التي جعلته ينفرد بمجموعة من الخصائص التي تُميّزُه عن التّسويق التّقليدي(**ثانيا**).

أولا- تعريف التّسويق الإلكتروني:

يرى بعض المختصين في مجال التّسويق أنّ مصطلح التّسويق عبر شبكة الإنترنت(Internet marketing) باعتبارها شبكة الشّبكات، مرادفا لمصطلح التّسويق الإلكتروني(E-marketing) لكون هذا الأخير يستعمل الإنترنت كثيرا كوسيلة مهمّة من الوسائل أو التّقنيات الحديثة الأخرى المنبثقة عن تكنولوجيا الاتّصال والإعلام، بينما البعض الآخر منهم يرى أنّ مفهوم التّسويق الإلكتروني أوسع وأشمل نطاقا عن التّسويق عبر الإنترنت، لكون أنّ تكنولوجيا التّسويق الإلكتروني كانت موجودة قبل نشأة وتطوّر الويب وتشمل جميع الأجهزة الإلكترونيّة(التّلفاز، الرّاديو، الهاتف النّقال، الحاسب الآلي،...)، كما أنّ التّسويق الإلكتروني عبر الإنترنت أصبحت الآن أداة فعّالة من أدوات التّسويق تفوّقت في قدرتها التّسويقية على أدوات التّسويق الإلكتروني الأخرى[1].

وعليه فإنّ الثّورة الرّقميّة فرضت في محيط الأعمال مصطلح حديث يتمثّل في التّسويق الالكتروني(Cybermarketing)، الذي يتكوّن في أصله الانجليزي من مُصطلحين: فالأوّل يتمثّل في(Cyber) الذي يُقصد به كلّ ما هو مُتواجد عبر شبكة الإنترنت، أمّا الثّاني يتعلّق

[1] **محمد طاهر نصير**، التسويق الإلكتروني، دار الحامد للنشر والتوزيع، عمان، الأردن، (د. ت. ن)، ص ص 39، 40.

بـ(Marketing) الذي يعني مجموعة من التّقنيات التي تسمح بتقييم احتياجات ومتطلّبات المستهلك لهدف إعداد استراتيجيات التّسويق، كما يُقصد من ذلك المصطلح كلّ ما يتعلّق بتهيئة الظّروف الأساسيّة لبيع المنتجات أو الخدمات، وبالتّالي فإنّ كلمة(Cybermarketing) ترادفها باللّغة العربية كلمة التّسويق الإلكتروني أو الافتراضي النّاتج عن تزاوج التّسويق التّقليدي مع التّقنيات الحديثة للمعلومات والاتصالات.

لقد تعدّدت آراء الباحثين والفقهاء حول مفهوم التّسويق الإلكتروني، فمنهم من عرّفه على أنّه:" إدارة التّفاعل بين المنظّمة والمستهلك في فضاء البيئة الافتراضيّة من أجل تحقيق المنافع المشتركة" [1].

والبعض الآخر عرف التّسويق الإلكتروني على أنّه:" استخدام شبكة الإنترنت وشبكات الاتصال المختلفة والوسائط المتعدّدة في تحقيق الأهداف التّسويقيّة، مع ما يترتّب على ذلك من مزايا جديدة وإمكانيات عديدة."[2]

وعرفه الآخرون على أنّه:" الاستخدام الأفضل للتّقنيات الرّقميّة، بما في ذلك تقنيات المعلومات والاتصالات لتفعيل إنتاجية التّسويق وعملياته المتمثّلة في الوظائف التّنظيميّة والعمليات والنّشاطات الموجّهة لتحديد حاجات الأسواق المستهدفة، وتقديم السّلع والخدمات إلى العملاء وذوي المصلحة في المنظّمة." [3].

فمن خلال كل هذه التّعاريف يُمكِن تعريف التّسويق الالكتروني على أنّه: "**أسلوب تجاري حديث يعتمد على استخدام تقنيات تكنولوجيّة ووسائط إلكترونية عبر أنظمة حاسوبيّة أو شبكيّة مختلفة، لغرض جذب أكبر عدد مُمكِن من العملاء والحفاظ على ولائهم لاقتناء السّلع والخدمات المتاحة وفقا لاحتياجاتهم ومتطلّباتهم.**"

---

[1] **يوسف أحمد أبو فارة**، التسويق الإلكتروني: عناصر المزيج التسويقي عبر الإنترنت، دار وائل للنشر والتوزيع، عمان، الأردن، 2004، ص 135.

[2] **عبد الله فرغلي علي موسى**، تكنولوجيا المعلومات ودورها في التسويق التقليدي والإلكتروني، دار ايتراك للنشر والتوزيع، القاهرة، مصر، 2007، ص ص 127، 128.

محمد الصيرفي، التسويق الإلكتروني، دار الفكر الجماعي، الإسكندرية، مصر، 2008، ص 13.

[3] **بشير العلاق**، التسويق الإلكتروني، دار اليازوري للنشر والتوزيع، عمان، الأردن، 2010، ص 16.

ثانيا– خصائص التّسويق الإلكتروني:

يعتبر التّسويق الالكتروني من بين أحد إفرازات عصر الرّقمنة، الذي يعتمد بشكل أساسي على شبكة الإنترنت، في ممارسة كافة الأنشطة التّسويقية كالإعلان والبيع والتّوزيع وإجراء بحوث التّسويق، تصميم المنتجات وتسعيرها الخ...، ويسعى كذلك إلى تسهيل عملية التّبادل الالكتروني لمختلف المنتجات أو الخدمات بين المنتج والمستهلك بشكل أسرع وأقل تكلفة عن التّسويق التّقليدي، حيث يتمتّع التّسويق الإلكتروني بِنُكْهَةٍ مُعيّنة من الخصائص التي تُميّزه عن التّسويق التّقليدي، والمتمثّلة فيما يلي:

– تعتبر الوظيفة التّسويقية من أبرز وأهم نشاطات التّجارة الإلكترونيّة عبر شبكة الإنترنت، التي تُستخدم فيها تقنيات وأساليب حديثة لتسويق مختلف المنتجات والخدمات في إطار قنوات التّسويق التي غيّرت من نمط إدارة الأنشطة التّجاريّة.

– النّفاذ بسهولة إلى مختلف الأسواق العالميّة ممّا يسمح للشّركات أو المؤسّسات الصّغيرة أو المتوسّطة التي تُعاني العُزلة في الأسواق المحليّة، إلى الانفتاح بسرعة على أسواق العالم من دون أيّة حدود أو قيود مع إمكانية مزاحمة الشّركات الضّخمة في جذب العملاء.

– التّسويق الالكتروني هو مفتاح تحقيق أهداف ورغبات المؤسّسات التي تسعى دائما من خلاله إلى تحديد الفئات التي يجب استهدافها بمنتجاتها أو خدماتها، والبحث عن رغبات واحتياجات كل عميل أو مستهلك وتقييمه، مع ترقُّب وضعيّة المنافسين من أجل إعداد إستراتيجيات جديدة للتّسويق[1].

– تحقيق المنفعة الكافية لأطراف العملية التّسويقية، من خلال سعي البائع إلى عرض خدمات تعزيزية مرافقة للمنتجات أو الخدمات بحسب تفضيلات المستهلك أو العميل، الذي بدوره يتأثّر بالمرونة والمستوى العالي المستخدم في عرض السّلعة أو الخدمة على نحو يؤدّي به إلى تكرار أو عدم تكرار عملية الشّراء.

– تُستعمل في تقنية التّسويق الإلكتروني آليات وتقنيات حديثة في تكنولوجيا الإعلام والاتّصال، لإبرام وتنفيذ مختلف الأنشطة التّجاريّة عبر الإنترنت، التي تمتاز بالتّكلفة

[1] **ناصر خليل**، مرجع سابق، ص ص 237، 238.

المنخفضة وسرعة التّنفيذ، وذلك بالمقارنة مع التّسويق التّقليدي الذي مازال يعتمد على الوسائل والآليات التّقليدية في التّسويق[1].

– تحقيق الميزة التّنافسية فيما بين الشّركات أو المؤسّسات من خلال تصميم موقع إلكتروني جذّاب مُتكيّف مع إستراتيجية تسويق مدروسة، ومُستنبَطة من حاجيات ومتطلّبات الزّبائن والظروف الدّاخليّة والخارجيّة المتعلّقة بالأسواق بصفة عامّة.

الفرع الثاني
أهميّة التّسويق الإلكتروني

أصبحت شبكة الإنترنت في وقتنا الحالي الرّئة النّابضة لمعاملات التّجارة الإلكترونيّة، والمصدر الأساسي الذي يُعوَّل عليهِ للحصول على مختلف المعلومات أو المبادلات التي تتم خصوصا بين أطراف التّجارة الإلكترونيّة، حيث فتحت لهم هذه التّقنيّة العالية، مساحات جديدة تمكّنهم من استثمارها في مجال تسويق المنتجات أو الخدمات[2]، إذ تتيح تقنيّة التّسويق الإلكتروني القدرة على اقتناء أيّة سلعة أو خدمة معيّنة، مع الحصول عليها في ظرف قصير وبأقل جهد أو استثمار من رأس المال، وانطلاقا من ذلك فإنّ تقنية التّسويق الإلكتروني تمنح مجموعة من المزايا لأطراف المبادلة التّجارية سواء بالنسبة للمستهلك أو العميل **(أولا)**، أو بالنسبة للشّركات أو المؤسّسات **(ثانيا)**.

أولا– المزايا الموجّهة للمستهلك أو العميل:

تعتبر الإنترنت وسيلة تسويق حديثة توفر بيئة واسعة خصبة لجميع العملاء، من أجل الاستفادة من المنافع التي يُحقّقها نشاط التّسويق الإلكتروني، باعتباره كجزء من التّجارة الالكترونيّة، فمن بين المزايا التي يُتيحها التّسويق الإلكتروني للمستهلك نجد ما يلي:

---

[1] **بشير عباس العلاق**، التسويق عبر الإنترنت، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2002، ص ص 22، 97.

[2] **محمد عبد حسين الطائي**، التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص ص 396 – 398.

- إمكانية الدخول إلى جميع الأسواق العالميّة، مع سهولة تَخطِّي الحدود الجُغرافيّة المرسومة لكل دولة، وذلك من أجل التّعرف والحصول على مختلف المنتجات أو الخدمات المتاحة عبر مواقع التّجارة الإلكترونيّة، التي تُوفر لهم خدمات لحظيّة ليلا ونهارا[1]، واتّصال دائم من دون انقطاع أو التّقيُّد بمواعيد العمل الخاصّة بالمتاجر التّقليدية، وذلك على مدار السّاعة طوال أيّام الأسبوع.

- أصبح من السّهل للمستهلك معرفة أية معلومات تخصّ منتج أو خدمة معيّنة عبر مواقع التّجارة الإلكترونيّة، التي تتيح له الدّخول الفوري، مع سرعة التّصفّح والقدرة على اقتناء تلك السّلعة أو الخدمة من دون أيّ انتظار، والثّقة في دفع ثمنها بطرق دفع إلكترونيّة آمنة[2].

- تحسين جودة القدرة الشّرائية لدى المستهلكين، من خلال فرص البحث والتّجوّل عبر الأسواق الافتراضيّة المنتشرة محليا أو على المستوى الدّولي، وإمكانية اختيار أفضلها بما يتناسب مع رغبات واحتياجات كل واحد منهم، وذلك وفق سعر وجودة وخصائص ومواصفات كل سلعة أو خدمة مطلوبة[3].

- تُوفّر قنوات التّسويق الالكتروني خدمة مباشرة للعملاء من خلال اختصار خطوات عملية التّسويق، والتّفاعل فيما بينها حول السّلعة أو الخدمة المرغوب فيها، كما تسهّل تنفيذ عمليات البيع والشّراء من البداية إلى النّهاية، بل وحتّى ضمان خدمات ما بعد البيع[4].

- تمكّن تقنيّة التّسويق الإلكتروني المستهلكين من التّسوق في عدّة أماكن مع تحقيق المنفعة لهم، إذ أنّ جلّ استراتيجيات التّسويق تنصب حول فهم حاجيات ورغبات كل مستهلك قبل طرح المنتوج أو السّلعة عبر الإنترنت، وهذا ما يؤثّر على جودة القرارات الشّرائية[5].

---

1) **Bertrand QUÉLIN**, « Rapport sur les rapports - Développement du commerce électronique et économie d'internet. », Revue d'Économie industrielle, vol. 84, 2e trimestre 1998. pp. 108-110.

2) **نظام موسى سويدان، شفيق ابراهيم حداد**، التسويق: مفاهيم معاصرة، دار الحامد للنشر والتوزيع، عمان، الأردن، 2003، ص ص 374- 376.

3) **عامر محمود الكسواني**، التجارة عبر الحاسوب، ماهيتها- إثباتها- وسائل حمايتها- القانون الواجب التطبيق عليها في كل من الأردن ومصر وإمارة دبي(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص ص 35- 38.

4) **عامر محمود الكسواني**، مرجع سابق، ص ص 36، 37 .

5) المرجع نفسه.

ثانيا– المزايا الموجّهة للشّركات أو المؤسّسات:

يجب على الشّركات التّجاريّة أو أيّ تاجر أو متعامل اقتصادي إعداد تخطيط استراتيجي فعّال يسمح له بمُباشرة عمليات التّسويق عبر الانترنت، التي تترتّب عنها مجموعة من المزايا أو الفوائد والمتمثّلة فيما يلي:

– مساعدة الشّركة على قياس وتحليل وتقييم الفرص التّسويقيّة، وتحديد أهداف أكثر واقعيّة من شأنها أن تُسهّل عمليات إبرام الصّفقات والمبادلات التّجاريّة بتقنيات تكنولوجيّة حديثة عالية المستوى، مع تحسين الأداء التّسويقي واستغلال فرص الدخول إلى مختلف الأسواق الالكترونيّة عبر العالم[1].

---

[1] يعتبر موقع جوميا.كوم(jumia.com) من أكبر المتاجر الافتراضية في إفريقيا، تأسس في عام 2012 في لاغوس بنيجيريا((Lagos(Nigeria) من قِبل كلّ من Jérémy HODARA, Sacha POIGNONNEC, Tunde KEHIND, Raphael AFAEDOR, Leonard STIEGELER.)، كمؤسسين لمُجمّع أفريكا إنترنت (Africa Internet Group(AIG)) الذي يساهم فيه المتعامل الاقتصادي الألماني(Rocket Internet) بنسبة 20% من رأس مال(يساهم كذلك في المُجمّع كلّ من شركتي(Milicom et MTN))، حيث قام هذا الأخير(Rocket Internet) بإنشاء مؤسسات مُصغّرة(Start-up) في قارة إفريقيا على غرار كلّ من(Zalando, Kaymu et Jovago, etc.)، في حين تتواجد جوميا في العديد من الدول الإفريقية (L'Algérie, le Maroc, la Tunisie, le Kenya, l'Égypte, l'Ouganda, le Cameroun, le Sénégal, le Ghana, l'Angola et la Tanzanie et la Côte d'Ivoire, etc.)، ويتوافر موقع جوميا على اللّغة العربية والفرنسية والانجليزية والبرتغالية، وعليه يعتبر الموقع(jumia.com) من أكبر مواقع التسوّق في قارة إفريقيا(Jumia est surnommé l'Amazon africain) وبالخصوص الجزائر(jumia.dz)، أين تبذل جوميا أقصى جهدها لتوفير أفضل تجربة للتسوق عبر الانترنت عبر أنحاء القطر الجزائري، حيث تُتيح حاليا منتجاتها بأسعار تنافسية مقارنة بالمواقع الأخرى وتُوفّر مختلف المنتجات إلى العملاء مباشرة(الملابس والأجهزة الالكترونية والحواسيب والهواتف الذكية الخ...)، مع إمكانية الدفع عند الاستلام مع تكريس الحق في إرجاع السلعة مجانا خلال 7 أيام من تاريخ الاستلام، وعليه أطلقت جوميا خدمة المتجر داخل المتجر(Shop in Shop) التي تسمح للشركات الراغبة في تسويق منتجاتها في أن تقوم بشراء متجر الكتروني داخل مَوقِع جوميا، وهذا ما يساهم في الاقتصاد من تكاليف التجهيز وأجور العمال ودفع فواتير المياه والكهرباء الخ...، فإذا كان أفضل متجر عادي يزوره 200 ألف زبون شهريا فإنّ المتجر عبر جوميا يزوره ما يقارب مليون زبون شهريا، ففي مارس 2016 استطاعت جوميا أن تجذب انتباه المستثمرين الأجانب حيث قامت كل من شركة(Goldman Sachs, AXA et Orange) باستثمار حوالي 326 مليون دولار أمريكي لتطوير خدمات موقع جوميا، وفي جوان 2016 أصبحت جوميا علامة تجارية مشهورة ومن أكبر مواقع التسوق التي تُوفّر العديد من المنتجات والخدمات للمستهلكين في إفريقيا (**Kaymu** devient Jumia Market, **Jovago** devient Jumia Travel, **Hellofood** devient Jumia Food, **Vendito** devient Jumia Deals, **Lamudi** devient Jumia House, **Everjobs** devient Jumia Jobs, **Carmudi** devient Jumia Cars, **AIGX** devient Jumia Services.)، في حين حقّق موقع جوميا في سنة 2015 رقم أعمال يقدر بـ 134,6 مليون أورو.

- تحسين العلاقات التّسويقية بين الشّركات وأهمّ عناصر بيئتها التّسويقيّة(العملاء)، من خلال استخدام أحدث التّقنيات التّكنولوجيّة في تصميم الرسائل التّرويجيّة التّفاعليّة(نصيّة أو صوتيّة)، وتبادلها مع العملاء بصورة سريعة وفوريّة، مما يُزيد من فاعليّة وكفاءة العمليّة التّرويجية على استهداف وجذب فئة معيّنة من المستهلكين[1].

- تشجيع وتحسين القدرة التّنافسية للمؤسّسات، من أجل الاستفادة من المشروعات الكبيرة أو الصّغيرة الحجم، وتدعيم إمكانياتها لخلق ميزة تنافسيّة تساعدها على الإبقاء على حصتها في الأسواق، مع تحليل مواطن الضّعف والقوّة في الشّركة بالمقارنة مع منافسيها.

- يساعد التّسويق الالكتروني على فهم واستباق رغبات وأهداف الزّبائن، مع توجيه قيادة تدّفق السّلع والخدمات من المنتج إلى المستهلك من أجل الحفاظ على التّوازن بين تطوّر الإنتاج ونموّ الاستهلاك، مع تحقيق مشاركة المستهلك في عمليات خلق وتطوير منتجات جديدة من خلال تقنيات التّفاعل التي توفّرها بيئة الإنترنت[2].

للمزيد من المعلومات أنظر:

Laure BELOT, « Quatorze start-up qui font bouger l'Afrique », article de journal Le Monde, publié le 03/03/2015 sur le site: http://www.lemonde.fr/afrique/article/2015/04/02/quatorze-start-up-qui-font-bouger-l-afrique_4608623_ 3212.html, consulté le 03/03/2017.

Benjamin POLLE, « E-commerce : Jumia double son chiffre d'affaires en 2015 mais reste dans le rouge », article de journal Jeune Afrique, publié le 19 avril 2016. http://www.jeuneafrique.com/319093/economie/e-commerce-jumia-double-chiffre-daffaires-2015-reste-rouge/, consulté le 04/05/2017.

Rémy DARRAS, « Africa Internet Group fait de Jumia la marque unique de ses principales sociétés », article de journal Jeune Afrique, publié le 23 juin 2016. http://www.jeuneafrique.com/335955/economie/africa-internet-group-renomme-71-societes-jumia/ (consulté le 06/05/2017.)

أنظر كذلك الموقع الإلكتروني التالي: https://www.jumia.dz/ (consulté le 02/02/2017.)

[1] **محمد فريد الصحن، نبيلة عباس**، مبادئ التسويق، الدار الجامعية للطبع والنشر والتوزيع، الإسكندرية، مصر، 2004، ص ص 358، 359، 370، 371.

[2] **ربحي مصطفى عليان**، البيئة الإلكترونية(E- Environment)، الطبعة الثانية، دار صفاء للنشر والتوزيع، عمّان، الأردن، 2015، ص ص 256، 257.

– تحسين كفاءات التّسيير في الشّركة أو المؤسّسة الاقتصاديّة، من خلال التّصميم الجيّد لموقعها الإلكتروني الذي من خلاله تُحدّد الطّرق المناسبة لعرض المنتجات والخدمات واستراتيجيات الاتّصال مع الزُّوار والإفصاح عن السّياسات السّعريّة وطرق الدّفع المُمْكِنة[1].

– تشجيع البحوث والدّراسات التّسويقية من أجل تحديد العملاء المستهدفين والاستجابة بسرعة لتوقّعاتهم، من خلال الحصول على آرائهم وفحص ودراسة شكاويهم ومعرفة المنافسين المحتملين لغرض تعديل، أو إعداد عروض جديدة لمختلف المنتجات أو الخدمات وتحسين فعالية الجوانب المختلفة لعناصر المزيج التّسويقي[2].

– تحدّي التّغييرات المستمرّة في حركة الأسواق من خلال الاستعانة بمختصين لإعداد إدارة جيّدة وخطط تسويقيّة جذّابة، من شأنها أن تؤثّر على اتجاهات المستهلك من النّاحية الذّهنية، أو على مُيولِه من خلال الشّعور بالرّاحة والثّقة النّاتجة عن المعلومات المقدّمة عن السّلع والخدمات المُعلَنة عبر المَوقِع التّجاري.

الفرع الثالث

تقنيات التّسويق الحديثة عبر الإنترنت

إنّ التّغييرات التي شهدها عالم الأعمال في وقتنا الرّاهن، سواء في نمط الإنتاج ونشاطات تبادل السّلع والخدمات، أو في تقنيات الاتّصالات، ما هو إلاّ نتاج ثورة تكنولوجيا المعلومات والاتّصالات، التي ساهمت في ظهور أنماط جديدة في إدارة مناخ الأعمال، وأحدثت تطوّرات هائلة في أساليب وتقنيات التّعامل مع العملاء، عبر مختلف شبكات الاتّصالات الحديثة وبالخصوص شبكة الانترنت، التي فجّرت مجتمع المعرفة ووسّعت من فجوة قنوات الاتّصالات وتبادل المعلومات، وساهمت في ظهور وتطوير تقنيات تسويق حديثة لمختلف السّلع والخدمات عبر مواقع التّجارة الالكترونيّة، على غرار التّسويق عبر محرّكات البحث(Saerch Engine Marketing) **(أوّلا)**، أو برامج المشاركة

---

[1] **بوياح عالية**، "دور الإنترنت في مجال تسويق الخدمات(دراسة حالة قطاع الاتصالات)"، مذكرة الماجستير في العلوم التجارية، تخصص: التسويق، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، 2010، ص 80.

[2] **ربحي مصطفى عليان**، مرجع سابق، ص ص 258، 259.

التّسويقيّة(Affiliate Marketing) **(ثانيا)**، والتّسويق عبر مواقع التّواصل الاجتماعي (Social Network Marketing) **(ثالثا)**.

أولا- التّسويق عبر محرّكات البحث(Saerch Engine Marketing(SEM)).

إنّ محرّكات البحث عبارة عن قواعد بيانات ضخمة تتضمّن وَصْفْ مُصغّر حول عناوين المواقع الإلكترونيّة وَصَفحات الويب المختلفة، التي تسمح للمستخدم بالبحث عن البيانات أو المعلومات المطلوبة بطريقة آلية بمجرّد كتابة موضوع البحث في المكان المناسب، حيث تعتمد هذه المحرّكات على زواحف الويب(Robot-Spider) التي تُمكّن من إجراء تفتيش دقيق ومختصر حول المعلومات التي تُتيحها مُرَتَّبَةً حسب أهمّيتها وشُهرتها.

وعليه، تعتبر محرّكات البحث كأداة فعّالة في مجال التّسويق الإلكتروني، حيث تسمح للمُتسوّق البحث عن المعلومات المتعلّقة بمختلف السّلع والخدمات في ظرف وجيز، بمجرّد الضّغط على الكلمات الدّالة في محرّك البحث، ولضمان عملية نجاح عملية التّسويق عبر محرّكات البحث، يستوجب على صاحب المتجر الافتراضي التّخطيط لإستراتيجية كاملة للتّسويق عن طريق هذا الأسلوب(SEM)، مع الأخذ بعين الاعتبار متطلّبات التّصميم الفعّال للمتجر الافتراضي(العنوان اللاّئق، المحتوى الجيّد، روابط الإحالة الخارجيّة والدّاخليّة، الكلمات الدّالة،...)، التي تُعتبر من بين العناصر المُهِمَّةِ لتحسين مرتبة المَوقِع الإلكتروني ضمن ترتيب أفضل في قائمة نتائج البحث(search Results) لمُحرّكات البحث، سواء كانت طبيعيّة(Organic search) أو نتائج مدفوعة الأجر(Paid Search)، لغرض جذب وتحقيق الثّقة المطلوبة لدى العملاء المُستهدفين، مع تشجيع الميزة التّنافسيّة وتحسين السّمعة التّجاريّة للمتجر الافتراضي.

للوصول إلى العملاء المُستهدفين وتحقيق المزيد من الأرباح، تسعى الشّركات إلى إتّباع استراتيجيات تسويق عبر محرّكات البحث، من خلال تقنيّة تهيئة الموقِع الإلكتروني لمحرّكات البحث المجّانيّة(Search Engine Optimization(SEO))، التي تتضمّن على مجموعة من التّقنيات، على غرار روابط الإحالة الدّاخليّة(on-page seo) وأيضا الرّوابط الخارجيّة(off-page seo)، وكذا وضع الكلمات المفتاحية أو الدّالة للوصول بالموقع

الإلكتروني إلى المركز الأوّل من نتائج البحث، لجذب الزوّار المستهدفين للموقِع وتحقيق الأرباح من دون إنفاق أيّة تكاليف[1].

وبالتّالي فإنّ هذا النّوع من التّسويق عبر محرّكات البحث قد يحتاج في كثير من الأحيان إلى الصّبر، للحصول على النتائج في محرّكات البحث أو حتى حظر الموقِع التّجاري الإلكتروني من نتائج البحث، نظرا للعراقيل التي تُواجِهُهَا التّقنيات المعمول بها وعدم تطبيقها من طرف عناكب محرّكات البحث(Black hat seo)[2].

لذا يتّجه أصحاب المتاجر الافتراضيّة إلى تقنية الإعلانات المدفوعة في محرّكات البحث(Google AdWords, Bing AdWords, etc.)، التي من خلالها يقوم المُعلِن بالدّفع لمحرّك البحث مقابل كل نقرة يقوم بها المستخدمين على الإعلان(Pay Per Click(PPC)) أو الدّفع مقابل كل اتّصال عن طرق الهاتف(Pay Per Call(PPC))، أو يتم الدّفع لمحرّك البحث مقابل كل 1000 نقرة تظهر فيها نتائج البحث عبر محرّكات البحث (Coût Pour Mille affichages/impressions(CPM))، وبالتّالي يُعتبر محرّك البحث(https://www.google.com)[3] من أنجع وسائل الدّعاية على شبكة الإنترنت وأشهر

---

[1] للمزيد من المعلومات حول التسويق الالكتروني، أنظر الموقع الإلكتروني التالي:
https://www.marketers-voice.com/2017/01/seo_27.html (consulté le 24/05/2017)

[2] للتعرف أكثر حول هذه العراقيل أنظر المواقع الإلكترونية التالية:
https://www.marketers-voice.com/2017/02/what-is-the-build-links-and-the-benefit-from-it.html ou
https://www.marketers-voice.com/2017/07/avoid-Black-hat-seo.html (consultés le 27/05/2017)

[3] غوغل(**Google**) شركة أمريكية فرعية(Filiale) تابعة لمُجمّع(**Alphabet**) منذ أوت 2015، مُتخصصة(**Google**) في مجال الخدمات التكنولوجية عبر الإنترنت، يقع مقرها الرئيسي بمدينة(Mountain View) بولاية كاليفورنيا (Californie)، تم تأسيسها في مرآب سيارات(Garage Google, Menlo Park, Californie) في 1998 على يد كلّ من((LARRY Page(âgé de 24 ans) و(SERGUEÏ Brin(âgé de 23 ans))، عندما كانا طالِبيْن يحضّران لشهادة الدكتوراه بجامعة ستانفورد(Stanford) الأمريكية في عام 1995 (Son DG depuis **2015** est, **PICHAI Sundararajan**)، حيث كانت بداية شركة غوغل منذ جانفي 1996 في صورة مشروع بحث ينطوي على إيجاد مُحرّك بحث جديد تحت تسمية باك روب(BackRub) يقوم بتحليل العلاقات بين مواقع الشبكة، وترتيب نتائج البحث حسب عدد مرّات ظهور المصطلح الذي يتم البحث عنه داخل الصفحة، وذلك بطريقة أفضل من تلك التي توفرها محركات البحث التابعة للشركات المنافسة(AltaVista, Yahoo! et Bing) وبالخصوص شركة(Altavista)، حيث اقتنعا حول فرضية دراستهما المُنْصَبَّة على أنّ الصفحات التي تتضمن روابط تشير لصفحات أخرى ذات صلة، هي الصفحات الأكثر ارتباطا

منصّات الإعلانات المدفوعة في عملية التّسويق عبر محرّكات البحث(SEM)، إذ يُتيح للمعلنين خدمة برامج معلوماتية مُتطوّرة تُساعدهم على تسويق مختلف السّلع والخدمات، كبرنامج(Google AdWords) الذي يُحِيل الزبائن المحتملين بشكل مباشر إلى السّلعة أو الخدمة المُروَّج لها، حيث تظهر هذه الإعلانات في صورة مُصغّرة(يمينا أو يسارا) إلى جانب نتائج البحث المرتبطة بِالْمَوْقِعِ التِّجَارِي، ويُساعد صاحب هذه الإعلانات على التَّحكُّم في التّكاليف عن طريق تقنيات التّسعير المُتاحة[1].

كما يسمح برنامج(Google AdSense) لأصحاب المتاجر الافتراضيّة عرض إعلاناتهم المكتوبة أو المصوّرة(Text, Images, Vidéos Advertisements)، مقابل حِصّة من قيمة الإعلان التي يدفعها المُعْلِنُ لشركة(Google)، حيث يحقّق ذلك البرنامج (Google AdSense) للموقع التّجاري المُعلَن مكتسبات إضافيّة من خلال إضافتها ميزة ويب(Google)، وتقديم إعلانات نصيّة وصُوَرِيَّة مُستهدِفة بدقّة إلى صفحات نتائج البحث

بعملية البحث التي من خلالها قاما بوضع أساس محرك البحث الخاص بهما، مستخدمين آنذاك موقع الويب الخاص في جامعة ستانفورد باستعمال اسم النطاق(google.stanford.edu)، حيث قاما في 15 سبتمبر 1997 بتسجيل ملكية اسم النطاق(google.com)، وبالتالي إنظمت شركة غوغل في 2004 إلى بورصة نازداك(NASDAQ) التي من خلالها كان أدائها جيّدا بعد أوّل اكتتاب عام لأسهمها، وذلك بسبب المبيعات العالية للشركة والإيرادات المُحقّقة في سوق الإعلان إلى جانب تقنيات البحث الأخرى المتاحة، وعليه فإنّ موارد شركة غوغل تجنيها من خلال برامجها الإعلانية التي تُمثّل نسبة 99% من إيراداتها، فعن طريق خدمة (AdWords)تسمح شركة غوغل للشركات المُعلنة على شبكة الويب بعرض إعلاناتها في نتائج محرك البحث حيث يتم تقدير التكاليف التي يجب على الشركات تقديمها، سواء وفقا لنظام السداد مُقابل كلّ مرة نقر أو نظام السداد مقابل كلّ مرة استعراض للإعلان، كما تتيح خدمة (AdSense for search) لمالكي مواقع الويب إمكانية عرض الإعلانات على مواقعهم مع تحقيق أرباح في كلّ مرّة ينقر أحد المُستخدمين على هذه الإعلانات.

للمزيد من المعلومات أنظر المواقع الالكترونية التالية:

http://www.boursorama.com/bourse/profil/profil_finance.phtml?symbole=GOOG et https://www.google.com/intl/en/about/company/ et http://www.nasdaq.com/symbol/goog(consultés le 29/05/2017.)

[1] أنظر **الملحق رقم (13)**، ص 492.

Kevin MELLET, « Marketing en ligne », Revue Communications, 2011/1 (n° 88), pp. 106, 107.

للتعرف أكثر على تفاصيل هذه الخدمة أنظر المواقع الإلكترونية التالية: http://adwords.google.com ou https://www.1min30.com/advertising-adwords-display/cpc-cpm-cpa-cpl-comment-choisir-combien-investir-75616 ou https://agency-inside.com/2016/04/definition-marketing-acronymes-cpc-cpm-cpl-cpa-cpv/

ومحتواها، كما يجمع هذا البرنامج بين إعلانات الدّفع بالنّقرة والدّفع بالظّهور (CPC -CPM) التي من خلالها يُدفع المال باحتساب عدد النّقرات المشروعة على الإعلانات التي قام بها الزّائرين وعدد المرّات التي ظهر فيها الإعلان على المواقع[1].

ثانيا- برنامج المشاركة التّسويقيّة(Affiliate Marketing Program).

يعتمد أصحاب المتاجر الافتراضيّة على برنامج المشاركة التسويقية (Affiliate Marketing) الذي يتيح للأطراف المُشارِكة فِيهِ، إمكانية الحصول على الأرباح من خلال المبيعات التي يحقّقونها لفائدة الشّركة الأصليّة المُعْلِنَة(Affilieur)، حيث تقوم هذه الأخيرة بتجنيد أو ضمّ عدد أكبر من المشاركين(Les affiliés) في إطار ذلك البرنامج، الذين تُكلّفهم بتسويق السّلع أو الخدمات مقابل عمولة يتحصّلون عليها على كل عملية بيع تمّت عن طريقهم. (Sont rémunérés par une commission sur les ventes ou en fonctions des contacts commerciaux (leads) générés à partir de leurs liens (formulaires, installations d'application,…), etc.)، حيث يقوم برنامج الشّركة(Affiliate Marketing) بتتبُّع جميع الزُوّار القَادمِين من روابط المُشاركِين مع تسجيل العمولات المُستحقّة لصاحب كل رابط تمّت وفقه صفقة البيع (Le tracking en affiliation) [2].

فمثلا شركة(amazon.com) ترغب من خلال برنامج المشاركة التّسويقيّة (Affilieur-Annonceur)، تسويق منتجاتها مع تحقيق مبيعات كثيرة على نطاق واسع، حيث تقترح على أصحاب المواقِع الإلكترونيّة المعروفة، ومُحرّكات البحث المشهورة (Google, yahoo !, etc.) كمشاركين(Affiliés) عمولة(Rémunération) مقابل تسويق مُنتجاتها عبر روابط

---

[1] للمزيد من المعلومات حول هذه الخدمات أنظر الموقع التالي: http://www.google.com/adsense

[2] **Girard GAUTIER**, « Monter une stratégie marketing de réseau », pp. 1-3. Article publié à partir de l'adresse: http://www.netalya.comfrArticle2.aspCLE=173# , consultée le 10/09/2017.
Etienne WÉRY, « Le référencement sur internet : que dit la loi ? », pp. 03, 04. Article publié le 03/09/2014 sur le site : https://www.ulys.net, consulté le 04/02/2017.
Philippe LE TOURNEAU, op.cit., pp. 469, 470.
Romain V.GOLA, op.cit., p. 448.

الإحالة إلى موقِع أمازون، حيث يتم ذلك بموجب عقد خاص بالمشاركة التّسويقيّة (Contrat d'affiliation directe) الذي بموجبه تُحدّد حقوق وواجبات كلّ طرف فيه[1].

وعليه، يمكن لشركة أمازون(Affilieur) أن تُبرمَ عقد المشاركة التّسويقيّة بطريقة مباشرة(Contrat d'affiliation directe) مع كل مشارك بصفة فرديّة(Affiliés)، أين تُتيح لكل واحد منهم جميع التّقنيات المتعلّقة ببرنامج المشاركة التّسويقيّة، كما يمكن كذلك لشركة أمازون(Affilieur) أن تبرم عقد المشاركة التّسويقيّة بطريقة غير مباشرة (Contrat d'affiliation indirecte(Master affiliation))، مع وسيط خاص (Intermédiaire d'une plate forme d'affiliation)، الذي يُحدّد الشّروط العامّة(التّقنيّة والماليّة...) المتعلّقة ببرنامج المشاركة التّسويقيّة وكذا العلاقة التي تربطه(Intermédiaire) مع المشاركين(Affiliés)، فمثلا الوسيط الفرنسي(Affilinet) يشرف على شبكة برامج مشاركة تسويقية تضم حوالي أربعمائة وسبعين ألف(470000) موقِع مُشارك(Affiliés)، ويُسيِّر حوالي ألف وستمائة(1600) برنامج مشاركة تّسويقيّة[2].

انطلاقا من ذلك، يجب على صاحب المَوقِع المُشارِك(Affilié) أن يلتزم أساسا بِحُسْنِ استخدام روابط المشاركة التّسويقيّة المتاحة من قِبلِ الشّركة المُعلِنة(Affilieur) باعتبارها صاحبة المنتجات المُروَّج لَهَا، وذلك وفقا لأحكام العقد الخاص الذي يربطها مع صاحب الموقع المشارك، كاحترام الشّعارات(Logos)، الصّور(Images)، الأيقونات(Icônes) الخ...، والسّهر على عدم تشويه أو المساس بسُمعة المنتجات المُرَوَّجِ لها أو استخدام أساليب الخداع أو الاحتيال تُجَاهَ الزبائن، من خلال توجيههم إلى روابط أخرى غير تابعة للشّركة المُعلِنَة(Affilieur)، أو يقوم بحدّ ذاته(Affilié) بعمليات النّقر على الإعلانات لغرض

---

[1] للمزيد من المعلومات أنظر الموقع الإلكتروني التالي:
https://www.definitions-marketing.com/definition/contrat-d-affiliation/ (consulté le 10/01/2017)

[2] أنظر **الملحق رقم (14)**، ص 492.

للمزيد من المعلومات أنظر الموقع الإلكتروني التالي: http.www.affili.net

Voir aussi : **Didier MAZIER**, PrestaShop : créer un site de e-commerce, édition ENI, France, 2011, pp. 265-267.
Nicolas CHU, op.cit., pp. 132, 133.
Romain V.GOLA, op.cit., p. 449.

التّزوير في عدد الزائرين المُستقطبين، أو حتى تسجيل نَفْسَهُ بُغية الحصول على العمولات، أو تكليف عدد من الأشخاص بمُهمّة النّقر بصفة مُستمرّة على روابط المُشاركة، وكذا يجب عليه(Affilié) أن لا يقوم بتعديل "وسوم لغة برمجة(HTML)" التّابعة لمنصّة برامج المشاركة التّسويقيّ.

والجدير بالذّكر، أن صاحب المَوقِع المُشارِك(Affilié) لا يضمن حُسن تنفيذ أو سير الصّفقات التّجاريّة المُنبثقة عن برنامج المشاركة التّسويقيّة(Affiliate Marketing)، كما أنّه لا يتحمّل المسؤولية تجاه الزّبائن، إلاّ في الحالات الاستثنائية المتعلّقة بالاشتراك في عمليات الاحتيال والتّدليس أو الإعلانات الكاذبة الخ... [1].

بالمقابل، يتعيّن على الشّركة المُعلِنَة(Affilieur) أن تَحْتَرِمَ بدورها أحكام عقد برنامج المشاركة التّسويقيّة الذي من خلاله، يجب أن تلتزم بعدم استخدام كلمات أو عبارات أو أسماء نطاقات تابعة لأصحاب حقوق الملكيّة الفكريّة، وأن تُزوّد أصحاب المواقع المشاركة(Affiliés) بجميع المعلومات والوسوم(Codes) الضّروريّة لإحداث روابط الإحالة(Liens hypertextes)، وإتاحة جميع الإحصائيات المتعلّقة بعمليات البيع المحقّقة أو المنجزة عبر كل موقِع مُشارِك مع تحديد هويّته وعدد الزّائرين الخ...، لتسهيل عملية احتساب ودفع العمولة المُستحقّة لكل صاحب مَوقِع مُشارك(Affilié).

فعن طريق تقنيات الدّفع بالنّقر، يستطيع صاحب المَوقِع الإلكتروني المشارك الذي يُقدّم خدمة قيّمة نافعة للزّائرين، أن يتحصّل على عمولة أو مكافئة بمجرّد قيام الزّائر بالنّقر Pay) per clic(Rémunération au clic)) على أحد روابط الإحالة مُباشرةً Liens) hypertextes(Texte, image, vidéo, etc.))) ، أو بعد نقر الزّائر على رابط الإحالة وشرائه للمنتوج(Pay per sale(Rémunération au chiffre d'affaires généré))على موقِع الشّركة

1) **Romain V.GOLA**, op.cit., pp. 451, 452.

المُعلنة(Affilieur)، أو عند نقر الزّائر على رابط الإحالة ومَلْئِهِ للنّموذج أو إجابته للأسئلة المقترحة من طرف الشّركة المُعلِنَة (Pay per lead(Rémunération au prospect)) [1].

ثالثا- التّسويق عبر مواقع التّواصل الاجتماعي(Social media marketing).

تُعتبر منصّات التّواصل الاجتماعي من بين وسائل التّسويق الإلكتروني الأكثر فاعليّة، حيث تتضمّن على كمّ هائل من المعلومات حول مختلف السّلع والخدمات، فمن خلال خاصيّة "المُشاركة" يمكن للمُسوِّق نشر الإعلانات عبر شبكة التّواصل الاجتماعي على مستوى واسع في وقت قصير ودون أدنى عناء، مع استهداف رغبات العملاء من خلال السّلعة أو الخدمة التي يتم تسويقها.

لضمان نجاح عملية التّسويق عبر منصّات التّواصل الاجتماعي، يجب على صاحب المتجر الافتراضي، إتّباع إستراتيجية فعّالة للتّسويق، من خلال معرفة المنصّات الاجتماعيّة البارزة التي يجب استخدامها للتّرويج بمختلف السّلع أو الخدمات، وإعداد محتوى جيّد ومُحكم مع فهم رغبات واحتياجات العملاء المُستهدفين، من خلال تحديد المواضيع والعبارات التي من شأنها أن تحث المستخدمين على التّفاعل مع الإعلانات المعروضة عبر كل منصّة تواصل اجتماعي، وكذا تحديد الطّرق النّاجعة للتّواصل مع العملاء، وعدم الاكتفاء بخاصيّة واحدة(الرّسائل القصيرة، الفيديو، والرّسائل الصّوتيّة، والصّور، الخ...)، لغرض جذب العملاء

---

1) **Romain V.GOLA**, op.cit., p. 452.
Les modes de rémunération d'un programme d'affiliation peuvent être variés, ils peuvent être notamment tout ou partie des modes suivants :
- **CPA** (Cost Per Action ou rémunération par action) : exemple, une commission sur un achat ;
- **CPL** (Cost Per Lead ou rémunération par formulaire) : exemple, une demande de crédit, une inscription à une newsletter... ;
- **CPC** (Cost per click ou rémunération par clic) : exemple, un clic sur une bannière ou un lien texte. Les sites d'e-commerce utilisent les plateformes d'affiliation pour mettre à disposition de leurs affiliés des **liens textes**, des **bannières**, et des **catalogues produits**. Ces catalogues produits sont utilisés par les comparateurs de prix, et les acteurs du reciblage publicitaire. Lorsque plusieurs affiliés ont été acteurs sur une vente, la société d'affiliation attribue la vente à l'un des affiliés en fonction des règles établies par l'annonceur (en général il s'agit d'attribution au dernier clic).
Source : https://fr.wikipedia.org/wiki/Affiliation_(internet)/ (consulté le 04/03/2017)

إلى الصّفحات التّرويجية وإخطارهم بأي إعلان جديد حول السّلعة أو الخدمة المُراد تسويقها، مع تزويدهم بشكل مُستمر بآخر مُستجدات السّلع أو الخدمات المروّج لها، والجدير بالذّكر أنّ أغلب مواقع التّجارة الإلكترونيّة تتوافر لديها روابط إحالة خاصّة بمنصّات التّواصل الاجتماعي(Facebook, Twitter, Google+, Youtube, Flickr, Instagram, etc.)[1].

وعليه، فتقنيات التّسويق عبر منصّات التّواصل الاجتماعي مُتعدّدة ومُتنوّعة بحسب كل منصّة، فعن طريق الرّسائل الصّغيرة لشبكة(Twitter) يُمكن لصاحب المتجر الافتراضي التّرويج لمنتجاته على مستوى فردي، أين يتم من خلالها وصف وشرح آلية عمل السّلعة أو الخدمة المُروَّج لها مع طريقة استعمالها، حيث يمكن للمسوّق كذلك التّرويج بمنتوجاته باستخدام روابط أو صور أو فيديوهات عبر تلك الشّبكة(Twitter) [2].

---

[1] للمزيد من المعلومات أنظر: **جهاد بالكحلاء**، "كيف تنجح في التسويق عبر مواقع التواصل الاجتماعي؟"، مقال منشور بتاريخ 25 مارس 2019، عبر موقع عربي 21. https://arabi21.com/story/997093/ (تم الاطلاع عليه في 11 ماي 2019.)

Voir aussi : **Gabriel DABI-SCHWEBEL**, « L'importance des réseaux sociaux dans le marketing digital », article publié sur 1min30.com le 05 mai 2017. https://www.1min30.com/developpement-web/limportance-des-reseaux-sociaux-dans-le-marketing-digital-119459, consulté le 05/06/2017.

Joaquim ROBBE, « Notre Guide complet sur le marketing des médias sociaux », article publié le 16 janv. 2019(Mis à jour le 24 janv. 2019) à 16:00, sur le site: https://www.e-marketing.fr/Thematique/social-media-1096/breve/notre-guide-complet-sur-le-marketing-des-medias-sociaux-329928.htm#, consulté le 20/02/2019.

[2] للمزيد من المعلومات حول الموضوع، أنظر الموقع الإلكتروني التالي:

https://blog.hootsuite.com/fr/marketing-sur-twitter-le-guide-ultime/(consulté le 04/03/2017.)

Voir aussi : **Clara WALTER**, « Le marketing sur Twitter : les bonnes pratiques », article publié le 06 avril 2017 sur le site: https://www.restoconnection.fr/le-marketing-sur-twitter-les-bonnes-pratiques/, consulté le 10/02/2017.

ظهر مَوقِع تويتر(**Twitter**) في 21 مارس 2006 على يد كل من (Jack Dorsey, Evan Williams, Biz Stone et Noah Glass)، وتم إطلاق الخدمة في جويلية 2006، وتتوافر لديه(Twitter) حوالي 40 لغة تسمح للمستخدمين بالاشتراك في تويتر بشكل مباشر مع تكوين ملف شخصي باسم الحساب، ويضم تويتر منذ 05 مارس 2017 حوالي 313 مليون مُستخدم، حيث يقع المقرّ الرئيسي للشركة بولاية سان فرانسيسكو(الولايات المتحدة الأمريكية) وتستحوذ الشركة على 35 مكتب مُوزّع عبر العالم، وبالتالي فإنّ تاريخ نشأة موقع تويتر يعود إلى أوائل عام 2006 كمشروع بحث أجرته الشّركة المصّغرة(Startup) الأمريكية(Odeo) التي قام بتأسيسها كلّ من(Noah Glass et Evan Williams) بولاية سان فرانسيسكو، حيث قام(Noah Glass) بتسويق برنامج تطبيقي(AudBlog) على مستوى الهواتف يسمح بنشر ملفات

وإلى جانب ذلك، تُقدّم صفحات شبكة(Facebook) تفصيلا أكثر حول مختلف السّلع أو الخدمات المُروّج لها، وذلك بالمقارنة مع حسابات شبكة "تويتر"، حيث تسمح بنشر وعرض الكثير من الإعلانات بصفة مباشرة بمجرد نشرها عبر الصّفحة الرّئيسيّة، مع تزويد المشتركين بمعلومات إضافية حول السّلعة أو الخدمة المروّج لها عبر روابط الفيديو أو الصّور أو أيّ خاصيّة أخرى[1].

سمعية، بينما(Evan Williams) أسّس شركة(Pyra Labs) صاحبة الأرضيّة أو المنصّة الإلكترونيّة (Blogs Blogger) حيث قامت شركة غوغل(Google) بشراء هذه الشّركة(Pyra Labs) في 2003، ففي أكتوبر 2006 تم شراء شركة(Odeo) من طرف شركة(Obvious Corp) في حين قام(Jack Dorsey) في أفريل 2007 بتأسيس شركة مستقلة بتسمية(Twitter)، ليشرف على إدارتها فيما بعد كل من(Evan Williams) في أكتوبر 2008 و (Dick Costolo) في 04 أكتوبر 2010.

وهكذا انضمت شركة تويتر إلى بورصة نيويورك في 31 أكتوبر 2013 تحت شعار(TWTR) وقامت كذلك بشراء العديد من المعدات والشركات حيث حازت في 28 جانفي 2013 على جهاز تحليل(Crashlytics)، الذي يسمح بكشف والتّصدي لأي طارئ من شأنه أن يُوقِفَ البرنامج التّطبيقي للهواتف الذّكية(iOS et Android)، وفي 11 أفريل 2013 أعلنت الشركة(Twitter) عن شرائها لخدمة موسيقية(WeAreHunted.com) بمناسبة مهرجان الموسيقى(Coachella) المُقام بولاية كاليفورنيا، وفي شهري سبتمبر وأوت من عام 2013 أعلنت الشركة(Twitter) عن شرائها لخدمة(MoPub) بمبلغ يُقدّر بحوالي 350 مليون دولار أمريكي، وخدمة(Curatorr) الخاصة بالتحليل الآني للرسائل المتداولة عبر شبكات التّواصل الاجتماعي حول برامج التلفيزيون أو الإشهار، فإلى جانب ذلك أعلنت شركة تويتر في 05 فيفري 2013 عن شرائها لشركة(Bluefin Labs) المُتخصّصة في تحليل المحادثات حول برامج التلفيزيون، كما قامت في جوان 2014 بشراء شركة(Namo Media) المتخصّصة في مجال الإعلانات على مستوى الهواتف الذكيّة، وفي خلال شهري فيفري ومارس 2015 قامت شركة تويتر بشراء شركتين مصغرتين(Niche) و(Periscope).

- لمزيد من المعلومات أنظر المواقع الإلكترونية التالية:

http://argent.canoe.ca/nouvelles-bourse/laction-twitter-senvole-pour-ses-debuts-boursiers-7112013 et http://www.lavenir.net/article/detail.aspx?articleid=DMF20130412_00295498 et http://www.reuters.com/article/2014/06/05/us-twitter-namomedia-idUSKBN0EG20Y20140605(consultés le 18/04/2016.)

[1] يعود تاريخ ظهور موقع(Facebook) إلى موقع(Facemach) الذي ابتكره الأمريكي مارك زوكربيرك **(Mark ZUCKERBERG)** في أكتوبر 2003 عندما كان طالبا في السنة الثانية في جامعة هارفارد (Université Harvard) الأمريكية، حيث يستخدم الموقِع آنذاك صورا تم نسخها وجمعها من دليل الصور المُتاح على الإنترنت الخاص بتسعة من طلبة السكن الجامعي، ووضع صورتين بجانب بعضهما البعض مع دعوة المُستخدمين إلى اختيار الشخص "الأكثر جاذبية"، حيث قام في 2004 بتأسيس موقع(TheFacebook.com)، الذي اقتصرت العضوية(التسجيل) فيه منذ البداية على طلبة كلية هارفارد كوليدج(أقدم كليات جامعة هارفارد)، حيث فتح الموقع أبواب التسجيل فيما بعد(منذ 26

كما تحتوي الشّبكة الاجتماعيّة(+Google) على العديد من المزايا المتواجدة في شبكة(Facebook)، مع إلحاق الصّفحة التّسويقيّة مع تقنيات(Google) المعروفة على غرار(Google AdWords, Google Maps, Youtube, etc.)، التي تسمح بنشر الإعلان على نطاق أوسع مع تقديم توضيحات حول السّلعة أو الخدمة بشكل أكثر تفصيلا، حيث أصبح المُحتوى المرئي من بين أدوات التّسويق الفعّالة عبر منصّة اليوتيوب(Youtube) باعتبارها كموطن رئيسي لفيديوهات التّرويج لمختلف السّلع والخدمات، التي حُظيت باهتمام المُسّوقين لهدف جذب العملاء الجُدد وزيادة المبيعات[1].

سبتمبر 2006) لجميع الأفراد البالغين من العمر(13) سنة فأكثر الذي لديهم عنوان بريد إلكتروني صحيح، حيث أعلنت شركة فيس بوك في جوان 2017 تجاوزها لسقف 2 مليار من عدد المستخدمين للشبكة، كما حقّقت الشركة في ماي 2012 فوائد كثيرة تقدر بـ 104 مليار دولار، التي تحصّلت عليها من قيمة الأسهم المطروحة في سوق البورصة المقدّرة بـ 421 مليون دولار أمريكي أي ما يعادل مبلغ 38 دولار للسهم الواحد، في حين بلغت موارد الشركة في 2015 إلى 44% من الأرباح أي ما يُعادل 17928 مليون دولار أمريكي التي تجنيها من إعلانات الشعار، حيث تعتبر شركة مايكروسوفت الشريك الحصري لشركة فيس بوك في تقديم خدمة الإعلانات، وهكذا طرحت شركة فيس بوك تطبيقات مجانية على مستوى أجهزة الهواتف الذكية والمواقع الإلكترونية التي تتيح الخدمات عبر الإنترنت، حيث أعلن موقع فيس بوك في نوفمبر 2007 عن إطلاق تطبيق(Facebook Beacom)، كمبادرة تسويقية تتيح للمواقع المختلفة إمكانية الإعلان عن الأنشطة التي يقوم بها المستخدمون في ملفاتهم الشخصية في موقع فيس بوك في صورة إعلانات اجتماعية بهدف الترويج للمنتجات، وبالمقابل قامت نفس الشركة بشراء العديد من الشركات Oculus, (Janvier 2014), (Branch Media VR(Mars 2014), etc.)، والتطبيقات البرمجية التي تُمكّنها من تنويع الخدمات المتاحة للمستخدمين. - لمزيد من المعلومات أنظر:

Antonio CASILLI, « Être présent en ligne : culture et structure des réseaux sociaux d'Internet», Revue Idées économiques et sociales, 2012/3 (N° 169), pp. 20-23, 24-27.

أنظر كذلك: **أوليغ عوكي**، فايسبوك للجميع(دليل إلى التسلية مع الأصدقاء وإلى الترويج للمشاريع على فايسبوك)، الدار العربية للعلوم ناشرون، 2009، ص ص 24-33، 105-110، 124، 125، 126، 167- 170، 172-176، 203-207.

[1] **Jeannette KOCSIS,** « Médias sociaux: 4 stratégies de marketing social essentielles (des tactiques personnalisées pour Facebook, Twitter, Google+ et LinkedIn) », article publié le 1er mai 2012 sur : https://www.targetmarketingmag.com/article/4-social-marketing-strategies-facebook-twitter-google-linkedin/all/, consulté le 07/O6/2016.

الفرع الرابع
تحديات التّسويق الإلكتروني

بالرغم من المزايا التي تُتيحها تقنيّة التّسويق عبر الإنترنت حاليا لأطراف العملية التّسويقية، سواء كانوا المُسوّقين(صاحب المتجر الإلكتروني)، أو المتسوّقين(العميل أو المستهلك) إلاّ أنّهم تَعترِضُهم مجموعة من التّحديات أو العوائق والمتمثّلة فيما يلي:

1)- اختلاف المجتمعات من حيث الأبعاد الاجتماعية والدّينيّة: تُشكّل الأبعاد الاجتماعيّة والدّينيّة تحديّا خاصاً على المسوّقين، حيث توجد الكثير من الأمور المسلَم بها في المجتمعات الغربيّة ولا تصلح تطبيقاتها في المجتمعات العربيّة أو المُسْلِمَة، كاشتراط هذه الأخيرة تسويق المنتجات التي تراها حلال من النّاحية الشّرعيّة، الخ...[1].

2)- التحدّي الخاص باختلاف اللّغات والثّقافات فيما بين المجتمعات: إنّ اختلاف الثّقافات واللّغات فيما بين المجتمعات يفرض على الشّركة أو المؤسّسة صاحبة الموقع التّجاري الإلكتروني التّعويل على عدّة لغات أجنبيّة، حتّى ولو كان ذلك في داخل دولة واحدة، (الهند لوحدِها لديها إلى جانب اللّغتين الرّسميتين: هندي Hindi(Langue officiel du gouvernement central) والانجليزية، إلى أكثر من 20 لغة رسميّة جهويّة، وكذا سويسرا، بلجيكا، كندا،...)، لهدف تسهيل معرفة معاني الكلمات المستعملة في اسم المنتجات والعلامة التّجارية، ومحتويات المنتوج، الإعلانات، الخ...، ومواكبة التّشريعات والتّنظيمات المتعلّقة بالممارسات التّجارية في إقليم كل دولة.

3)- ارتفاع تكاليف إعداد وتصميم وإدارة مواقع التّجارة الإلكترونيّة: تتطلب عملية إنشاء وتطوير مَوقِع إلكتروني تجاري مُحترِف عبر شبكة الإنترنت، إلى خِبرات وكَفاءات ومُؤهلات في الميدان مع ضرورة إعداد دراسات تسويقيّة وفنيّة مُحكَمة لجذب اهتمام العملاء أو المستهلكين، وتعزيز القدرة التّنافسية للشّركة.

---

[1] **ناصر خليل**، مرجع سابق، ص 25.

4)- فقدان الإطار المُنظّم لنشاطات مزوّدي خدمات الإنترنت: إنّ عدم تنظيم بعض الدول - على غرار الجزائر- للخدمات التي يتيحها المزوّدين عبر شبكة الإنترنت(الإيواء، الاتّصال، توريد المعلومات، البحث...)، بات يُشكّل عائقا جوهريا أمام المؤسّسات أو الشّركات التي ترغب في تسويق منتجاتِها عبر شبكة الإنترنت.

5)- العراقيل المتعلّقة بتدفّق الإنترنت: إنّ ضُعف كفاءة استخدام شبكة الإنترنت وانتشارها في بعض الدول وبالخصوص الدول النّامية(الدول العربية، الإفريقية...)، يؤثر سلبًا في عمليات تسويق المنتجات والخدمات لسبب تدنّي مستوى تدفّق شبكة الإنترنت.

6)- التّأقلم مع تقنيات التّسويق الإلكتروني: يمثّل ضعف الوعي عائق أمام المسوقين أو المتسوقين تجاه التّسهيلات أو المزايا التي تتيحها تقنيات التّسويق الإلكتروني، وعدم معرفة التّعامل أو التّجاوب مع تقنيات تكنولوجيا الاتّصال والإعلام، التي تستوجب التّأقلم معها لإجراء المعاملات الإلكترونيّة عبر شبكة الإنترنت[1].

7)- مُواجهة مستجدّات حركة الأسواق: يتطلّب التّسويق عبر شبكة الإنترنت بالنّسبة للشّركات أو المؤسّسات، إتّباع خطط مدروسة وإدارة جيّدة لمواجهة التّغييرات المستمرّة الطّارئة، في حركة الأسواق المحليّة أو الدوليّة التي تستوجب عليها الإحاطة والإلمام بجميع العوامل المؤثّرة فيها، والظّروف المحيطة بالعملاء وبالمنافسين[2].

8)- فقدان الثّقة والأمان: إنّ نجاح عملية التّسويق عبر الإنترنت مُتوقّف على توافر عُنصرَا الثّقة والأمان اللّذان يعتبران من بين الضّمانات الرّئيسيّة، لإرساء مُناخ ثقة آمِن لمعاملات التّجارة الإلكترونيّة التي تتم في بيئة إلكترونيّة افتراضيّة مملوءة بالمخاطر المتعلّقة، بانتحال هويّة أطراف التّعامل الإلكتروني، واختراق بياناتهم الإلكترونيّة وإنكار عملية تبادل أو بيع أو دفع قيمة المستحقّات عبر شبكة الإنترنت[3].

---

1) **Gilles PACHÉ**, « La logistique de distribution du commerce électronique : des défis économiques, managériaux et écologiques à l'horizon », Revue Gestion 2002/5 (Vol. 27), pp. 41- 43.

2) **بن خليفة مريم**،" التسويق الإلكتروني وآليات حماية المستهلك"، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص: قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 02، 2015، ص ص 25، 27.

3) **Sylvie ROLLAND**, « Impact de l'utilisation d'Internet sur la qualité perçue et la satisfaction du consommateur », thèse de doctorat en sciences de gestion, Université Paris IX-

9)- مراعاة القوانين الأجنبيّة المُنَظِّمَة للنشاطات التّجارية في داخل كلّ دولة: يُشّكل هذا التّحدي كحاجز حقيقي أمام أطراف العملية التّسويقيّة عبر الانترنت، نتيجة التّناقضات المتواجدة بين تسهيل وتنمية معاملات التّجارة الإلكترونيّة، وبين المعالجة الضّريبيّة لها، والقانون الواجب التّطبيق أثناء النّزاعات، وكذا اختلاف مواقف الدول تجاه استخدام بعض وسائل الدّفع الإلكتروني عبر الإنترنت(كالعملات الافتراضيّة مثلا)، وهذا ما يُعقّد من إجراء عمليات التّسويق عبر الإنترنت[1].

10)- مُواكبة الهندسة الماليّة الحديثة: يجب على مواقع التّجارة الإلكترونيّة أن تُوَاكِبَ ما أحدثته الهندسة الماليّة في عصرنة الخدمات المصرفيّة، وظهور نظم وتطبيقات مالية حديثة غير معروفة من قَبْلِ تحتوي على تكنولوجيا معقّدة وفقا لمستويات معيّنة من الثّقة والأمان، حيث ساهمت الثّورة الرّقميّة في ظهور آليات حديثة للدّفع الإلكتروني عبر الإنترنت باستخدام العُملات الرّقميّة الافتراضيّة التي تستوجب وضع إطار تنظيمي وقانوني لها.

11)- فقدان مُتعة التّسوق والتّفاعل الاجتماعي: يؤدي التسوّق عبر الإنترنت في بعض الأحيان إلى فقدان مُتْعَة التسوّق المعروفة التي كانت تجدها بعض العائلات أو الأسر في ممارسة عملية التّسوّق، والتّفاعل الاجتماعي المباشر فيما بين البائع والمشتري، كما أنّه يساهم في تقليص فرص التّفاعل الأسري نتيجة تضاؤل فرص التّسوّق التّقليديّة التي تعتبر بالنّسبة لبعض أفراد العائلات الفرصة الوحيدة للتّنزُّه أو التّسلية أو التّلاقي فيما بينهم، ضِفْ إلى ذلك فقدان أو ضعف ثقافة استخدام وسائل الدّفع الإلكترونيّة الحديثة لدى فئة المجتمع، حيث تعتبر من بين أحد الوسائل الأساسيّة المستخدمة لنجاح التّجارة الإلكترونيّة[2].

12)- التّحدّي الخاص بالتّرجمة الموازية للّغات: تواجه التّرجمة الآلية لوثائق صفحات مواقع الويب التّجارية المُسترجعة من طرف محرّكات البحث، انتقادات لاذعة بوصفها ترجمة

Dauphine, U.F.R, Sciences des organisations, Centre de recherche DMCP (Dauphine-Marketing-Stratégie-Prospective), 2003, pp. 83- 90.

ربحي مصطفى عليان، مرجع سابق، ص ص 285- 287.

[1] **يوسف حسن يوسف**، التسويق الالكتروني، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص ص 126، 127.

[2] **محمد فريد الصحن، نبيلة عباس**، مرجع سابق، ص 375.

أوّلية وغير مُعمّقة، وذلك نظرا لسطحيّة المجال المعرفي لهذه المحرّكات، وعدم قُدرتها على التّرجمة المُختصّة التي تعتمد على مصطلحات خاصّة في المجالات المعرفيّة الدّقيقة واقتصار هذه المحرّكات، على تقنيات قوائم المصطلحات المُوازية مع خوارزميات نحويّة بسيطة للقيام بالتّراجم المُوازية إلى عدّة لغات أجنبية من دون التّعمّق في معرفة الوثائق والتّحليل الموضوعي لها.

13)– التّباين في تكلفة الإعلانات الإلكترونيّة: يرجع ذلك إلى صعوبة قياس تكلفة الإعلانات الإلكترونيّة وتقييم تأثيرها على المستهلكين، نظرا لافتقارها لوسائل ومعايير القياس المعتمدة في ذلك، وعدم تكامل البيانات الخاصّة بهذه الإعلانات وعدم تناسقها[1]، وكذا صعوبة تقدير الأمور الهامّة ذات الصلة بقياس حجم السّوق وعناصر المزيج التّسويقي، وتفاوت أساليب احتساب تكلفة الإعلانات التي تتباين بحسب مرتبة الموقع الإلكتروني على محرّكات البحث، أو عدد مرّات النّقر على الإعلان، أو عدد زوّار المَوقِع الذين دَوَّنَهُمْ الخادم(Serveur).

من خلال ما سبق، نصل إلى أنّه من السّهل من النّاحية التّقنية على أيّ شخص مبتدئ إنشاء أو إحداث موقع إلكتروني، من خلال استخدام أحد محرّري النّصوص مثلا-Bloc) (notes ومتصفّح الويب(Internet Explorer) لمُعاينة النتائج على شاشة الحاسوب، أو يقوم بالاستعانة على إحدى البرامج المعلوماتية المجّانيّة التي تُساعِد على إحداث وتصميم أيّ موقع إلكتروني بسيط، إلاّ أنّ مُهمّة بناء وتصميم مَوقِع مُتقدّم أو مُحترِف للتّجارة الإلكترونيّة تبدو صعبة وليست سهلة للغاية كما يبدو في الموقع الإلكتروني البسيط.

فلإحداث موقع ناجح للتّجارة الإلكترونيّة يتطلّب اللّجوء إلى خبرات وموارد وكفاءات متخصّصة، في انجاز كامل المراحل الخاصّة ببناء وتشغيل الموقع التّجاري، كما يستوجب على صاحب المشروع أن تكون لديه إدارة فاعلة وكفوءة مع امتلاك رؤى سليمة واضحة وأهداف مُحدّدة، وسياسات وخيارات إستراتيجيّة جديدة ناجحة، تمكّن من تحقيق الأهداف

---

[1] **Thomas BEAUVISAGE** et autres, « Notes et avis des consommateurs sur le web. Les marchés à l'épreuve de l'évaluation profane », Revue Réseaux, 2013/1, n° 177, pp. 137-144, 151-153.

والغايات التّسويقيّة المَرجُوَة، ومواجهة مختلف التّحدّيات والعوامل المُحيطة ببيئة التّسويق الإلكتروني التي تستوجب الوعي والإدراك بأهمية تطبيقات التّجارة الإلكترونيّة، مع الأخذ بعين الاعتبار التّهديدات الأمنية التي تُعرقِل حسن سير معاملات التّجارة الإلكترونيّة، وكذا احترام الأحكام التّشريعيّة والتّنظيميّة السّارية المفعول لدى الدّولة المعنيّة.

المطلب الثاني

عناصر المزيج التّسويقي الإلكتروني

تُساهم إستراتيجية التّسويق الإلكتروني في رسم معالم التّخطيط الإستراتيجي للمؤسّسة الاقتصاديّة، التي يستوجب عليها تحديدها من أجل تسويق منتجاتها أو خدماتها في ظروف ملائمة وبكفاءة وفعالية، حيث توفّر تقنيات التّسويق الإلكتروني الفاعليّة في التّعامل فيما بين أطراف العملية التّسويقيّة والتّجاوب بأكثر مرونة مع عناصر المزيج التّسويقي-Mix) (marketing، وبالتّالي يُمكن تقسيم عناصر المزيج التّسويقي الإلكتروني إلى كلّ من المنتوج الإلكتروني(**الفرع الأول**)، والسّعر الإلكتروني(**الفرع الثاني**)، ومزيج التّرويج الإلكتروني(**الفرع الثالث**)، والتّوزيع الإلكتروني(**الفرع الرابع**).

الفرع الأول

المنتوج الإلكتروني(E-Product)

يمكن تحديد المفهوم التّسويقي للمنتوج الإلكتروني بشكل أساسي على أنّه وسيلة لإشباع حاجة أو منفعة مُعيّنة للمستهلك، يحتوي على مجموعة من الخصائص الماديّة الملموسة وغير الملموسة، التي تنطبق على عنصر السّلعة، باعتبارها كمنتوج مادّي وعنصر الخدمة كمنتوج غير مادي، وبالتّالي يعتبر المنتوج من الأمور الهامّة التي يجب على أيّة مؤسّسة أو شركة الاهتمام به، لكونه يعتبر كعنصر أساسي في إدارة وتخطيط إستراتيجية تسويقه عبر مواقع التّجارة الإلكترونيّة، عن طريق القيام ببحوث ودراسات لمعرفة احتياجات ورغبات المستهلكين المستهدفين أو المرتقبين، حتى يتمكّن المسوّقين من إعداد أو تكوين رؤى واضحة تمكّنهم من إعداد أو صيانة الاستراتيجيات والآليات التي توصل إلى تحقيق منتجات ذي خصائص ومواصفات وفقا لتلك الاحتياجات.

علاوة على ذلك فإنّ المنتوج الإلكتروني المادّي أو غير المادّي يمكن تداوله بطريقة آلية عبر شبكة الإنترنت، والذي يتطلّب وضع إستراتيجيات محكمة ومدروسة، وذلك قبل اتّخاذ قرار إدخاله إلى مختلف الأسواق، في حين يُقصد بإستراتيجيّة المنتوج كلّ ما تُدخله الشّركة أو المؤسّسة الاقتصاديّة على المنتوج، لهدف إخراجه في أحسن صورة تحقّق له الميزة التّنافسيّة مع المنتجات المثيلة له، وبالتّالي فإنّ دورة حياة أي منتوج(السلع أو الخدمات) تستوجب تقديم إستراتيجيات بديلة لمزيج المنتجات[1] والمتمثّلة فيما يلي:

أ)- إستراتيجيّة التّمييز: قد يتم اللّجوء إلى استخدام هذه الإستراتيجيّة في حالة تواجد منافسة شديدة لمنتجاتها أو الرّغبة في التّوسّع نتيجة ازدياد عدد الأسواق، أو حدوث تغييرات جديدة في أذواق المستهلكين أو استغلال الطّاقة الإنتاجية الزّائدة، أو البحث عن حاجات لم تُلَبَّى بعد أو التّطوّر التّكنولوجي في ميدان الصّناعة الخ...، التي من خلالها تسعى الشّركة أو المؤسّسة إلى اقتناص الفرص عن طريق توفير سلعة أو خدمة جديدة متميّزة عن باقي المنتجات المنافسة لها، أَخِذَةً فيها بعين الاعتبار شكل المنتجات، حجمها، تصميمها، علامتها التّجاريّة، غلافها، مواصفات جودتها، خدمات ما بعد البيع الخ...، وذلك من دون التّخلي عن ما هو موجود من عناصر سابقة مُميِّزة للمنتوج، فالمنتوج الجديد يمكن أن يكون منتوج غير مُتوفّر في مكان أو عند منافسين آخرين، أو يدعّم الزبائن بخدمات متميّزة أو يؤدّي وظيفة أو منفعة جديدة نسبياً، أو يمثّل تطوّرا مهمًّا من زاوية المستهلك المستهدف وذلك بالمقارنة مع المنتجات الحالية.

ب)- إستراتيجيّة التّنويع: تسعى الشّركة أو المؤسّسة من خلال هذه الإستراتيجيّة إلى توسيع الفرص وإعطاء خيارات أوسع أمام المستهلكين، عن طريق توسيع وتنويع مزيج المنتجات تحت نفس العلامة التّجاريّة، وذلك سواء كانت هذه المنتجات المُقدّمة جديدة، أو لها علاقة

---

[1] **محمد فريد الصحن**، التسويق(المفاهيم والإستراتيجيات)، الدار الجامعية، الإسكندرية، 1998، ص ص 243- 246.

محمود جاسم الصميدعي، إستراتيجية التسويق(مدخل كمي وتحليلي، دار ومكتبة الحامد للنشر والتوزيع، عمّان، الأردن، 2000، ص ص 194- 197.

سابقة مع المنتجات القديمة، من النّاحية التّسويقيّة والتّكنولوجيّة أو ليست لها علاقة بالمنتجات القديمة.

ج)- إستراتيجيّة التّعديل: يمكن اللّجوء إلى هذه الإستراتيجيّة لمُسايرة التّطوّر التّكنولوجي في المجال الصّناعي، أو يكون ذلك نتيجة لعدم نجاح بعض المنتجات أو مراعاة التّعديلات التي تفرضها ظروف موسميّة، أو تواجد تغييرات في رغبات أو حاجات المستهلكين، بحيث تقوم الشّركة بإجراء تعديلات في منتجاتها عن طريق تحديث أو تطوير بعض الصّفات المميّزة لمنتجاتها الحالية[1].

د)- إستراتيجيّة الِانْكِمَاشْ: تسعى هذه الإستراتيجيّة إلى تبسيط بعض أشكال المنتجات أو استبعاد بعض العناصر المُميّزة لها، لغرض إقصاء أو إسقاط المنتجات غير المُربحة، ومراعاة متطلّبات الأسواق، عن طريق إنتاج منتجات مطلوبة، تُلبي حاجيات ورغبات المستهلكين، وبالتّالي تسعى الشّركة من خلال هذه الإستراتيجيّة إلى تركيز أو توجيه جهودها على المنتجات التي تحقّق منها أرباحا عالية على المدى البعيد، وذلك بالمقارنة مع المنتجات الحالية التي تحقّق أرباحا ضئيلة، كما يمكن الشّركة الاقتصاديّة أن تلجأ إلى إستراتيجيّة الانكماش في حالة الظّروف الاقتصاديّة الصّعبة المحيطة بها، أو عدم توافر المواد الأوّليّة اللاّزمة للعمليّة الإنتاجيّة، أو تواجد نُقص من حيث الطّاقة الإنتاجيّة الخ...

الفرع الثاني

التّسعير الإلكتروني(E-Pricing)

يعتبر التّسعير عبر الإنترنت عُنصرًا مُهِماً في مُكوّنات المزيج التّسويقي والعنصر الوحيد الذي يُمثّل الإيراد للشّركة أو المؤسّسة، وذلك بالمقارنة مع العناصر الأخرى(المنتوج، التّوزيع، التّرويج) التي تمثّل تكاليف عليها، فيُقصد بالسّعر الشّكل النّقدي الذي يُعبِّر عن القيمة المعطاة لسلعة أو خدمة معيّنة، إذ يمنح المستهلكين فرصة الاختيار فيما بين المنتجات المعروضة ويؤثر على إدراكهم من حيث مدى تطابقه(السّعر) مع الفوائد المتوقّعة

[1] **محمود جاسم الصميدعي**، مرجع سابق، ص ص 194- 197.

وتوافقه مع مواصفات المنتجات وجودتها وقيمتها الحقيقيّة، التي تختلف من شخص إلى آخر ومن سوق لآخر، فعادة ما تقوم بعض الشّركات التّجاريّة بعرض أو ترويج مختلف المنتجات وفقا للرغبات أو الاحتياجات العشوائيّة للمستهلكين[1]، في حين تتّسم عملية تسعير السّلع أو الخدمات عبر شبكة الإنترنت بالدّيناميكيّة والمرونة، وسرعة تغييرها من حين لآخر، فهي بالتّالي لا تعرف الاستقرار، وعليه فإنّ عملية تحديد السّعر تُؤثر فيه مجموعة من العوامل التي منها ما هو خاضع لإدارة الشّركة ومنها ما هو خارج عن سيطرتها أي لا تستطيع التّحكُّم فيه.

من بين أهم هذه العوامل نجد تلك المتعلّقة بالتّكاليف النّاجمة عن السّلع أو الخدمات التي تتحمّلها الشّركة، كتكاليف الإنتاج، التّسويق، النّقل، التّرويج، التّخزين، الرّسوم الجمركيّة، الضّرائب الخ...، التي تسعى الشّركة دائما إلى تغطيتها، مع إضافة هامش ربح معقول أثناء عملية تحديد السّعر، وذلك مهما قامت الشّركة بتسويق منتجاتها محليا أو دوليا بالطّرق التّقليديّة أو عبر شبكة الإنترنت، لذا يجب أن تسعى الشّركة إلى الحصول على احتياجاتها بأقل التّكاليف مع انتقاء أفضل المورّدين عبر شبكة الإنترنت[2].

كما يستعين المستهلك حاليا بالتّقنيات الحديثة لشبكة الإنترنت للحصول على معلومات صحيحة حول أسعار المنتجات، وإجراء المقارنة فيما بينها، حيث ظهرت برمجيات حديثة(Shop bot, My simon, eboodle, etc.) تسمح لمستخدمي شبكة الإنترنت الحصول

---

1) **Antoinette ROUVROY, Thomas BERNS,** « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Revue Réseaux, 2013/1 n° 177, pp. 176-179.

- Comme le dit **Éric SCHMIDT**, Directeur général de Google : « Nous savons en gros qui vous êtes, en gros ce qui vous intéresse, en gros qui sont vos amis [c'est-à-dire on connaît votre « banc de poissons »]. La technologie va être tellement bonne qu'il sera très difficile pour les gens de voir ou de consommer quelque chose qui n'a pas été quelque part ajusté pour eux (c'est-à-dire qu'une **prédiction en apparence individualisée** serait **possible**). »

Au contraire, bien sûr, l'objectif n'est pas tant d'adapter l'offre aux **désirs spontanés** (pour peu qu'une telle chose existe) des individus, mais plutôt d'adapter les désirs des individus à l'offre, en adaptant les stratégies de vente (la manière de présenter le produit, d'en fixer le prix…) au profil de **chacun**. Ibid.

2) **يوسف حسن يوسف**، التسويق الالكتروني، مرجع سابق، ص ص 106-108.

على معلومات دقيقة وتفصيليّة عن الأسعار المتاحة وأفضل البائعين في الفئة المختارة، كما يمكن للزّائرين التّعرف عبر الشبكة على مزايا المزادات العلنيّة، وكذلك العروض التّرويجيّة المتاحة في أكثر من 150000 متجر افتراضي في آن واحد، أو إرشاد المستهلك إلى أكثر من 12000 متجر افتراضي لإجراء المقارنة فيما بين الأسعار مع إتاحته فرصة اختيار السّعر الأقل والجودة الأفضل[1].

وعليه، فإنّ عملية تحديد السّعر تتأثّر بشكل كبير بعامل المنافسة، الذي يجب على الشّركة التّنبؤ به لإجراء المقارنة بين سعر منتجاتها، وأسعار منتجات المنافسين، من حيث الجودة والنّوعية والمواصفات وتفادي المشاكل المؤدّية إلى حروب الأسعار، لذا يُمكن للشّركة في حالة ما إذا لم تكن لها خبرة كافية في تحديد الأسعار، أن تسترشد بأسعار الشّركة التي أخذت المبادرة على إستراتيجيّة قِيَادَة أسعار المنتجات في الأسواق المستهدفة، من خلال وضع أسعار مماثلة لهذه الأسعار، أو تقوم الشّركة بوضع أسعار منخفضة بالمقارنة مع أسعار المنافسين، وذلك بغية الدّخول إلى الأسواق، أو أنّ منتجاتها لا تتمتّع بالمواصفات التي تتمتّع بها المنتجات الأخرى، أما إذا كانت الشّركة تتمتّع بشُهرة وسُمعة كبيرتين وأنّ منتجاتها تتميّز بنوعيّة وجودة عالية ومواصفات تمنحها مزايا تنافسيّة في مختلف الأسواق، يمكن لها في هذه الحالة، وضع سعر أعلى وانتهاج إستراتيجيّة قِيَادَة الأسعار التي تسترشد بها باقي الشّركات[2].

وبما أنّ السّعر يعتبر أحد عناصر المزيج التّسويقي، فإنّ عملية تحديده يجب أن تكون متناسبة أو متطابقة مع باقي هذه العناصر، ولا يمكن أن يُحَدَّدَ بِمَعْزَلٍ عنها، فمن الطّبيعي في حالة ما إذا كانت المنتجات تتمتّع بمستوى معيّن من المواصفات والجودة العالية، فإنّ الشّركة ستختار بالتّالي السّعر الأعلى المناسب لهذه المنتجات، كما أنّه إذا قامت الشّركة بحملة ترويجية لمنتجاتها، بإمكانها رفع السّعر في حالة زيادة الطّلب عليها، فإذا كان

---

[1] **بشير العلاق**، التسويق الإلكتروني، مرجع سابق، ص ص 134، 135، 151، 152.

[2] **بشير العلاق**، التسويق الإلكتروني، مرجع سابق، ص ص 136، 140، 141.

Robert LEDUC, Initiation aux techniques commerciales, entreprise moderne d'édition, Paris, France, 1976, pp. 126- 131.

العرض كبير والطلب على المنتجات قليل، فإنّ السّعر سينخفض وذلك وفقا لقانون العرض والطّلب[1].

انطلاقا من ذلك، تلعب إستراتيجيّة التّسعير دورا مهمًّا في تحقيق الأهداف التّسويقيّة للشّركة، عند قيامها بطرح منتجات جديدة في مختلف الأسواق، والتي يستوجب عليها القيام بدراسة طبيعة هذه الأسواق ودرجة مرونة الطّلب فيها لاعتماد سياسة الأسعار المنخفضة، وذلك بُغيَة التَّغَلْغُلِ فيها(الأسواق) والحصول على أكبر حصّة مُمكِنة فيها، بالشّكل الذي يؤدّي إلى زيادة الأرباح في الأمد الطويل، لأنّ الأسعار تؤثّر بشكل كبير على مرونة الطّلب، فإذا ارتفعت فسيؤدّي ذلك حتما إلى انخفاض الطّلب على المنتجات، والعكس صحيح، كما أنّه في حالة ما إذا قامت الشّركة بتوزيع المنتجات عبر شبكة الإنترنت مباشرة إلى المستهلكين فبإمكانها تخفيض أسعارها، وذلك لسبب انخفاض تكاليف التّرويج وحذف تكاليف وأرباح طرق التّوزيع الأخرى[2].

بالإضافة إلى ما سبق، تعتبر المزادات العلنيّة التي تتم عبر شبكة الإنترنت من العوامل التي تؤثّر في عملية تحديد الأسعار[3]، حيث يمكن من خلالها لأيّ شخص أو شركة أن

---

1) **Robert LEDUC**, op.cit., pp. 126- 131.

محمود جاسم الصميدعي، مرجع سابق، ص ص217، 218.

2) **محمود جاسم الصميدعي**، المرجع نفسه.

3) تعتبر الشركة الأمريكية(eBay.com) من بين الشركات الكبرى المتخصصة في البيع بالمزادات عبر الإنترنت أين تُمثّل دور الوسيط بين البائع والمشتري، تم إنشائها في عام 1995 من طرف الطالب(Pierre OMIDYAR) تحت تسمية(AuctionWeb) أو(Réseau d'enchères)، حيث تم تغيير هذه التسمية في عام 1996 إلى إيباي(eBay) الذي يعبّر اختصارا بـ(Echo Bay Technology)، ويقع مقر الاجتماعي حاليا بسان جوزي في ولاية كاليفورنيا (San José dans le Silicon Valley en Californie)، حيث تُشغّل حوالي 13000 عامل ويُقدّر رقم أعمالها في عام 2010 بحوالي 9,5 مليار دولار أمريكي في 2010، وعليه قامت شركة إيباي منذ نشأتها ببيع أول سلعة طُرحت للبيع بالمزاد عبر موقعها الالكتروني تتمثل في جهاز لايزر بمواصفات رديئة(Pointeur laser défectueux) بمبلغ 14,83 دولار أمريكي، وذلك لجذب انتباه العملاء ومختلف وسائل الإعلام حول مهام الشركة، وفي أواخر التسعينيات(1999) أعلنت الشركة(إيباي) عن شرائها لخدمة الدفع عبر الإنترنت(Billpoint) التي تم تعويضها فيما بعد بخدمة الدفع(Paypal) في 2002، كما قامت شركة إيباي بشراء العديد من المواقع الإلكترونية للبيع بالمزادات العلنية على غرار (Half.com(Juin 2000), iBazar(Août 2001), etc.)، وكذا شراء شركة(PayPal) بقيمة 1,5 مليار دولار أمريكي

تقوم بعرض منتجاتها(قطع أثريّة، عتاد لأَشْهَرِ الشّخصيات، سيّارات قديمة، كنوز الخ...) لبيعها عن طريق المزاد العلني عبر الإنترنت، الذي يُوفّر الفرص للمستهلكين في اختيار سلع أو خدمات قد لا تعرض إلاّ عن طريق هذه المزادات[1]، في حين يستعدّ أو يتسارع الأشخاص إلى اقتناء هذه المنتجات، حتى ولو كانت أسعارها باهضة، وذلك على نحو يعود بالفائدة على أطراف عملية البيع.

الفرع الثالث

المزيج التّرويجي عبر الإنترنت(E-Promotion)

يُعتبر التّرويج من بين أحد عناصر المزيج التّسويقي، الذي من خلاله تعمل الشّركة أو المؤسّسة على بذل كافة المجهودات، للتّأثير بشكل مباشر أو غير مباشر على المستهلكين المستهدفين لإثارة دوافعهم وأذواقهم ورغباتهم، من أجل اتّخاذ قرار شراء السّلع أو الخدمات

للأسهم، وفي 2005 اشترت الشركة(eBay) الموقع البريطاني(Gumtree) المتخصص في الإعلانات الصغيرة في مجالات العقار والرحلات والتشغيل الخ...، إلى جانب شركة سكايب(Skype) التي اشترتها بقيمة 2,6 مليار دولار أمريكي، الخ...، وبالتالي فإنّ نظام المزايدة العلنية لموقع إيباي تتم وفقا لمبادئ مزايدة(Vickrey) التي تعطي الأولية في الشراء للمشتري الأخير الذي قام بدفع أعلى قيمة، وكذا السّعر الذي أتاحه المشتري الثاني (Offrant plus une petite somme (par exemple, 50 centimes))، حيث تتيح شركة إيباي لكلّ شخص بالغ قانونيا إمكانية المشاركة في المزايدة بعد القيام بإجراءات التسجيل عبر موقعها الالكتروني، أين يتم التّحقق من صحة العنوان الإلكتروني لصاحبه(المشتري) في حالة الشراء، والتحقق في هوية الأعضاء(البائعين) عن طريق البريد العادي(ما يبرر الإقامة(Justificatif de domicile)) أو التعريف المصرفي(Par la carte de crédit)، حيث يتحمل كل طرف مسؤوليته في حالة عدم احترام أحكام التشريع الساري المفعول وكذا تنظيمات شركة إيباي(تعرضت شركة إيباي في 2014 إلى عملية قرصنة شملت جميع حسابات مستخدميها، أين طلبت منهم الإلتزام بضرورة تغيير جميع كلمات المرور الخاصة بهم)، وعليه فإنّ مداخيل شركة إيباي(eBay) تأتي من خلال اقتطاعها لحصة(Commission) عن كلّ عملية تجارية قام بها البائع مقابل الخدمة المتاحة له من طرف الشركة(eBay)، حيث يبقى المشتري مُعفى من دفع أيّة تكاليف إضافية، وتتم عملية دفع قيمة المزايدة وفقا لتقنية الدفع التي يُحدّدها البائع التي يمكن أن تتمثل في الشيك، البطاقة المصرفية، الاقتطاع بصفة أوتوماتكية أو عن طريق تقنية باي بال(PayPal)، أو حتى الدفع العادي الخ...

للمزيد المعلومات أنظر المواقع الإلكترونية التالية:

http://www.boursier.com/actions/actualites/news/ebay-des-encheresd-art-en-ligne-avec-sotheby-s-620525.html et http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=403863 22300-77 et http://www.journaldunet.com/ebusiness/commerce/ebay-hacke-france-0514.shtml(consultés le 16/04/2016.)

[1] **بشير العلاق**، التسويق الالكتروني، مرجع سابق، ص ص 142- 145.

المروّج بها وفقا لإمكاناتهم وتوقّعاتهم[1]، وعليه تنطوي عملية التّرويج على تحديد وإبراز خصائص ومُميّزات عناصر السّلع أو الخدمات المروّج لها، لغرض استمالة سلوك المستهلكين بأنّ ما يتم التّرويج إليهم من منتجات قادر على إشباع حاجياتهم ورغباتهم، لذلك يسعى التّرويج إلى تحقيق تلك الأهداف من خلال عناصر مزيجه، التي تختلف أهميّتها من شركة لأخرى بحسب منتجاتها والإمكانيات التّكنولوجيّة المُسّخرة فيها، في حين تعتبر عناصر المزيج التّرويجي كجزء من عناصر المزيج التّسويقي الإلكتروني والمتمثّلة فيما يلي:

أولا- البيع الشّخصي(المباشر) عن طريق الإنترنت(La vente directe):

يعتبر البيع الشّخصي(La vente de personne à personne) عنصرا مباشرا من عناصر المزيج التّرويجي الذي يُعبِّر عن المجهودات الشّخصية المبذولة، لحثِّ وجذبِ العملاء المرتقبين لغرض اقتناء أو شراء سلعة أو خدمة معيّنة، وفقا لأحكام التّشريعات والتّنظيمات المعمول بها[2]، في حين يعتبر البيع الشّخصي عن طريق مواقع التّجارة الإلكترونيّة وسيلة أساسيّة للاتّصال الشّخصي للتّاجر الافتراضي بالمستهلكين الإلكترونيين، إذ يلعب دور مُهِّم في تحسين الخدمة ويُعطي سُمعة جيّدة للشّركة وتشريف صورتها في أوساط العملاء.

لذا تُعد خدمات البيع المباشر لمختلف النّشاطات والمنتجات من بين الأساليب التّرويجيّة الرّئيسيّة التي تعتمد عليها الشّركات الصّناعيّة والتّجاريّة لإقناع العملاء، حيث يمكِن لها أن تبيع مختلف السّلع والخدمات بطريقة مباشرة إلى المستهلك النّهائي، عبر تقنيّة التّسويق الشّبكي(Multi Level Marketing(MLM)) أو التّسويق المتعدّد المستويات (Marketing par réseau- Vente multiniveaux- Vente en réseau par cooptation- Vente à paliers multiples, etc.)، باعتبارها كقناة من قنوات التّسويق المباشر المبني على أساس التّسويق

---

[1] **زياد محمد الشرمان، عبد الغفور عبد السلام**، مبادئ التسويق، الطبعة الثانية، دار الصفا للنشر والتوزيع، عمان، الأردن، 2001، ص 181.

محمد إبراهيم عبيدات، مبادئ التسويق، دار المستقبل للنشر والتوزيع، عمان، الأردن، 1989، ص 243.

[2] **A. BRUGEL**, « La vente directe : La vente de personne à personne », Gazette du palais, n°18, 19/1995, p. 32.

التّواصلي فيما بين الموزّعين، ويظهر ذلك من خلال دراسة سلاسل التّسويق الشّبكي القانونيّة(**1**)، وسلاسل التّسويق الشّبكي غير القانونيّة(**2**).

1)- سلاسل التّسويق الشبكي القانونيّة:

إنّ التّعامل بتقنية البيع المتعدّد المستويات(MLM) يستوجب مراعاة التّشريعات والتّنظيمات المتعلّقة بحماية المستهلك، واحترام قواعد التّسويق والبيع والممارسات التّجاريّة المشروعة إلى جانب التّشريعات الأخرى المعنيّة السّارية المفعول، حيث تعتمد الشّركات التّجارية والصّناعيّة من خلال هذه التّقنيّة على شبكة من البائعين(التجّار) أو المُوزّعين المستقلّين (Distributeurs Indépendants ou vendeurs à Domicile Indépondants(VDI))، في إطار علاقة تعاقدية تسمح لكلّ واحد منهم بدعوة أو ضمّ(Coopter) عملاء أو موزعين آخرين لشراء وإعادة بيع السّلع أو الخدمات، مُقابل الحصول على حوافز وعمولات(Commissions-remises)[1]، في حين يُمكِن لأيّ بائع أو موزّع مُنضّم أو مُشارك في شبكة البيع(MLM) أن يقوم بتطوير شبكة من الزّبائن(العملاء) بأسفله(parrainer) بنفس الطّريقة التي التحق بها هو، وبعبارة أخرى فإنّ المستهلك أو الموزّع الأوّل يتحصّل على عمولة كحافز، مُقابل تجنيد مشترين آخرين لشراء المنتوج، حيث يتحصّل كلّ مستهلك أو عميل يجذب مستهلكين أو عملاء جُدُد لشراء المنتوج، على نِسبة معيّنة من العمولة في حالة قيامهم بإعادة بيع المنتجات وفقا لسلاسل تسويق قانونيّة[2].

وعليه فإنّ البيع المباشر يتحقّق من خلال السّلاسِل التّسويقية القانونيّة(MLM) التي يقوم في إطارها الجميع بعملية البيع للمنتجات بصفة مباشرة، حيث لا ينحصر البيع بالمُسوّقين وتجنيد المسوّقين الآخرين، إذْ تعتمد سلاسل البيع القانونيّة المتعدّدة المستويات أساسا على السّلع أو الخدمات التي تتميّز بأسعار تنافسيّة ونوعية جيّدة تستجيب لرغبات المستهلكين وتُحْتَرَمُ فيها قواعد التّسويق والبيع على أساس الفاتورة، وكذا نظام الإلحاق أو الانضمام (La

1) **Daniel HURSTEL**, « Principes juridiques : la vente multiniveaux serait-elle remise en cause ? », Gazette du palais, n° 18, 19/ 1995, pp. 41- 44.
2) **Nicolas LEFRANC**, « Vente en réseaux : le markéting multiniveaux », Gazette du palais, n° 18, 19/ 1995, pp. 38, 39.

(cooptation الذي تتوقّف فيه المُستويات حول مدى قُدرَة المُوزّع(التّاجر) أو المُوزّعين على جذب مُوزّعين(مُشترين) جُدُدْ، حيث تتم عملية بيع وتوزيع المنتجات من دون الحاجة إلى محلّ(Magasins) أو الاستعانة بتقنيات البيع عن بُعد (Vente à distance-Correspondance)، كما تُمَثِّلُ الصّورة الشّريفة لشخصية الموّزع أو السّمعة التّجاريّة للشّركة المُوزّعة أحد عوامل نجاح عملية البيع المتعدّد المستويات(MLM)، حيث تُحدّد قيمة العمولة(Commission) الممنوحة لكل موزّع على أساس "هامش ربح" مبيعات المنتجات التي حقّقها الموّزع السّابق المنخرط في شبكة البيع، وكذا على المبيعات المحقّقة من جانب الموزّعين الذين قام بإلحاقهم(Cooptation) إلى الشبكة (Au titre de rémunération de leur travail d'animation)[1].

2)- سلاسل التّسويق الشبكي غير القانونيّة:

تحوّلت تقنية البيع المتعدّد المستويات في الآونة الأخيرة إلى وسيلة لتحقيق الأرباح فقط ولم تُعد وسيلة من وسائل التّسويق، حيث ظهرت خُطط تسويق شبكية(MLM) تشترط مُستويات مُعيّنة غَالِباً ما تكون بصفة هرميّة (Systèmes dits(Boule de neige ou pyramidaux))، تبدأ بشخص واحِد على قمّة الهرم، الذي يتّسع نُزُولاً أو هُبُوطاً حسب عدد المشتركين الذي يساهمون في زيادة المستويات الدُنْيَا في الشّبكة الهرميّة(MLM)، حيث ينقسم التّسويق الشّبكي الهرمي إلى صورتين أساسيتين:

أ)- التّسويق الهرمي من دون منتوج(La vente pyramidale):

تعتمد تقنيّة التّسويق الهرمي من دون منتوج(La vente pyramidale) على أسلوب النّد للنّد(Pair à Pair) أو(Peer-to-Peer)، على مستوى شبكة الحواسيب(Réseau numérique) بطريقة مباشرة وفقا لنظام سلسلة الكُتَلْ المعروفة بالبَلُوكْ شَيْنْ(Block chain)، التي ماهيّة إلاّ قاعدة بيانات تحتوي على سلسلة من الكُتل المرتبطة فيما بينها بصفة هرميّة، حيث تُسجَّل وتُخزَّن فيها العديد من البيانات أو المعلومات المتداولة فيما بين المستخدمين عبر شبكة الإنترنت، أين تُدار سلسلة الكُتَلْ بطريقة آمنة ومُستقلَّة على نحو لا يسمح بتعديل

1) **Nicolas LEFRANC**, op.cit., p. 38.

المعلومات المُخزّنة لاحقاً[1]، وعليه فإنّ تقنية سلسلة الكُتَلْ تتجسّد من النّاحية التّقنيّة في إطار سوق العملات الرّقميّة الافتراضيّة(Bitcoin, Namecoin, Litecoin, Peercoin, etc.)، أين يتم فيها إحداث هرم تسلسلي على أساس الاشتراك في النّقد الافتراضي أو العملة المُجرّدة(Monnaie virtuelle)، حيث تتداول وتُشترى فيه قِيم العملات الرّقميّة المشّفرة بالمفتاح العام والخاص(Crypto-monnaies) فيما بين نظم شبكات الحاسوب، خَارِجَ رقابة المصارف المركزيّة ومن دون أيّ إطار تشريعي وتنظيمي أو تدخّل حكومي، حيث يتم استبدال قيمتها فيما بعد مُقابل العمولات الماديّة الرّسميّة للدول[2].

ب)– التّسويق الهرمي القائم على المنتوج:

تعتمد تقنيّة البيع الهرمي على المنتوج كغطاء للتّضليل أين يتحقّق البيع للمسوّقين فقط داخل الهرم التّسويقي، ولا يُحقّق أو يُشكل نِسبة معيّنة من المبيعات، وما يشكّك من مصداقيّة البيع الهرمي أنّ الأشخاص التي هي على رأس الشّبكة التّسويقيّة(الهرم) يحقّقون أرباحا وثروات هائلة لا تُقدّر، وذلك على حساب العملاء الذين هم في المستويات الدُّنيا، بينما يمكن لأيّ شخص على مستوى السّلاسل التّسويقيّة القانونيّة أن يُحَقِّقَ الرّبح أكثر من الّذين هم في مستويات أعلى منه[3].

فمثلا شركة تصنع هواتف ذكية وتُريد بيع كلّ هاتف بقيمة(80 أورو)، حيث تقوم بمنح فُرص التّسويق الشّخصي لكلّ شخص يقوم بشراء منتوجها مقابل عمولة قدرها(10 أورو) عن كلّ مُشْتَرٍ يأتي به أو يأتي به هذا الأخير، حيث يقوم "محند" بإقناع كلّ من محمّد وعلي بشراء الهاتف الذّكي مع حثّهما على تسويقه حتى يظفرا بالحوافز(المكافأة)، يشتري "محمد وعلي" الهاتف الذّكي، ويكسب "محند" الحافزين المودعين(10 أورو× 02(المشتريين)= 20

---

[1] **Y. POULLET et H. JACQUEMIN**, « Blockchain : une révolution pour le droit ? », Journal des Tribunaux, 10 novembre 2018, 137e année - N° 6748, pp. 802- 806.

[2] أنظر **الملحق رقم (15)**، ص 493.

Voir aussi : **Jean-Paul DELAHAYE,** « Le Bitcoin, première crypto-monnaie », Bulletin de la Société informatique de France, numéro 4, octobre 2014, pp. 68, 74, 75.

[3] **أمير فرج يوسف**، الجرائم التجارية الإلكترونية وأساليب مكافحتها، وكيفية حماية المستهلك الإلكتروني وأطراف العقد الإلكتروني التجاري، مكتبة الوفاء القانونية، الإسكندرية، 2013، ص ص 121– 124.

أورو)، فإذا قام "محمّد" بإقناع ثلاثة من زملائه بشراء المنتوج والتّسويق له فيحصل هو الآخر على ثلاثة حوافز(10 أورو×03= 30 أورو) حيث يحصل "محند" على نفس الحافز أو المكافئة باعتباره "المُسوِّق والمشتري الأوّل على رأس الشبكة"، فإذا قام الثّلاثة المجنّدين بإقناع كلّ واحد منهم ثلاثة مشتريين آخرين مع حثّهم على تسويق المنتوج، فسيحصل كل واحد منهم على ثلاثة حوافز(10 أورو×03= 30 أورو) على أن يكون نصيب "محمد"(10 أورو× 09= 90 أورو) حيث ينال "محند" على رأس الشّبكة نفس العمولة(90 أورو) [1] .

انطلاقا من ذلك، فإنّ نظام البيع الهرمي مبني على أساس شراء حق "التّسويق" أو "التّوظيف" الذي يعتبر القلب النّابض والرّكيزة الأسّاسيّة التي يقوم عليها نظام التّسويق الشّبكي الهرمي[2]، حيث يقوم أحد الأشخاص من خلال المنتوج بتجنيد أشخاص مشتركين الذين يدفعون مصاريف الدّخول في الهرم، إمّا عن طريق حقوق التّسجيل أو مصاريف الانضمام أو شراء المنتوج مُقابل وعود مُستقبلية(كسب ثروات، التّكوين، الهدايا، الخ...)[3]، حيث تُبَالِغُ الشّركات الماليّة والتّجاريّة ومُسوّقوها بالتّرويج بمنتجاتها وإحاطتها بأثمان باهظة غير معقولة بالنّظر إلى قيمتها الحقيقيّة أو الأصليّة، ولا تُراعي أنظمة التّسويق الشّبكي القواعد الأسّاسيّة في تسويق المنتجات كقانون العرض والطّلب ودورة حياة المنتوج، الخ...، ممّا يؤدّي إلى إشباع السّوق وإغراقه بهذه المنتجات وإحداث المضاربة والتّضخّم النّقدي وبالتّالي عجز المسوّقين عن الإتيان بعملاء جُدد، بالإضافة إلى ذلك نجد أنّ الدّافع الحقيقي لدى المشترين هو "الحافز" أو "العمولة"، التي يكسبونها في حالة إقناع أو تسجيل مشتركين جُدد، ولا يهتمون بالمنتوج الذي يُستخدم فقط كوسيلة لدخول الهرم، ممّا يثير الشّكوك لدى

---

[1] أنظر **الملحق رقم (16)**، ص 493.

[2] للمزيد من المعلومات حول الموضوع، أنظر المواقع الالكترونية التالية:

http://www.mlmwatch.org/ ou http://www.mlm-thetruth.com/mlm-tax-study/(consultés le 10/07/2016.)

Stephen Barrett, M.D, « The Origin of Multi Level Marketing ». Article disponible sur: http://www.mlmwatch.org/01General/mlmstart.html, consultée le 02/09/2016.

[3] **Marc PUECH**, « Jurisprudence du parrainage en matière de vente multiniveaux », Gazette du palais, n° 18, 19/ 1995, pp. 46- 49.

رجال الدّين والقانون حول مدى شرعيّة ومِصدَاقيّة التّسويق الشّبكي الهرمي من النّاحية القانونيّة والشّرعيّة.

ففي حالة ما إذا قصد المُشترِك عمولة التّسويق بدلا من السّلعة أو الخدمة، فَيَسْقُطُ بالتّالي المفهوم القانوني للمعاملة التّجارية عنها، كأن يقوم بدفع مبلغ مالي لشراء باقة 300 أورو بعد التّسجيل في أحد مواقع أو منصّات الصّرف الإلكتروني، المتخصّصة في بيع العملات الافتراضية لغرض الحصول على مبالغ ماليّة زهيدة قد تأتي أو لا تأتي له، وهذا ما يُشكّل القِمار والرّبا، فالرّابح الكبير في اللُّعبة يكون دائما الشّخص الأوّل السّابق أو الأوّل في التّسجيل عبر الشّبكة(MLM)، كما لا يضمن المُسوّق الذي دفع المال في المُستويات الأخيرة الإتيان أو إقناع بعملاء آخرين، حيث تتوقّف العملات بتوقّف بعض المشتركين في الهرم، الأمر الذي يستوجب تجنيد وتسجيل مُسوّقين إضافيين لإكمال عملية التّوازن بين المُشتركين.

فمن بين السّلاسل غير المشروعة للتّسويق الشّبكي نجد البيع الهرمي (Vente pyramidale) المعروف بسلسلة بونزي(**Chaîne de PONZI**)[1]، التي ماهيّة إلاّ عملية استثمار تعتمد على ممارسات الغّش والتّدليس الممنوعة من النّاحية القانونيّة، حيث يُعوّل عليها شخص معيّن أو شركات التّسويق التي تقوم بدفع عمولات للمستثمرين على حساب رأس المال الذي يستثمره أو يدفعه المستثمرين الآخرين لها، عند انخراطهم في الشبكة الهرميّة وذلك عِوضًا من دفعها(العمولات) من الفوائد أو العوائد المُتَحَصَّلِ عليها من الأرباح الحقيقيّة للاستثمار.

وعليه، فإنّ سلاسل البيع الهرمي لا تستعين بالمنتوج لتحقيق الأرباح، حتى ولو اعتمدت عليه، فيكون ذلك "المنتوج كغطاء" فقط للتّعامل بالبيع الهرمي، واستقطاب أكبر عدد مُمكِن من المشتركين أو المستثمرين إلى الشّبكة الهرميّة، التي ليس لها حدود من حيث عدد

1) **Julien FLOER**, « Ponzi, la plus célèbre des arnaques », article publié le 28/12/2015, sur le site : http://richesse-et-finance.com/ponzi-la-plus-celebre-des-arnaques/, consulté le 13/03/2016.

المستويات، وذلك بالمقارنة مع السّلاسل التّسويقية القانونيّة(MLM) التي تحدّد فيها عدد المستويات[1]، حيث يشرف على سلاسل البيع الهرمي شخص(طبيعي أو معنوي) مُعيّن على رأس الهرم الذي يستخدم المنتوج كوسيلة فقط للدّخول إلى الشّبكة الهرميّة، أين يُباع فيها بسعر غير منطقي أو بسعر غامض أو لا يُصدّقه العقل في بعض الأحيان، كما أنّ دعوة الأصدقاء والأقارب تعتبر من أساسيات عمل البيع الهرمي غير القانوني، مُقابل وعود بثروات وتحقيق مكاسب أو مداخيل عالية جدّا خلال فترة زمنية معيّنة قد يتم الحصول عليها أو لا، بينما في عمليات التّسويق الشّبكي القانونيّة(MLM) يُباع المنتوج لأيّ شخص كان ما دام أنّ المنتوج حقيقي(Un vrai produit) وتُحْتَرَمُ فيه القواعد الأسّاسيّة في تسويقه.

انطلاقا من ذلك، فإنّ معاملات البيع الهرمي ترتكز أساسا على العملات الافتراضيّة المشّفرة(Crypto monnaies) المجهولة، التي تُهيّئ الأرضيّة الخصبة للقيام بأنشطة الغّش التّجاري والتّهرب الضّريبي وغسيل الأموال الخ...، حيث يمكن أن ينهار الهرم الشّخصي نتيجة هروب أصحاب الشّبكة أو اعتقالهم، بعد أن يتّم الكشف عن حقيقة العمليّة التّسويقيّة، وأنّ الهدف منها تسويق البضائع المحظورة قانونياً، أو أنّ الشّركة الماليّة التي تُشرف على عمليات التّسويق الهرمي تُمارس مهامها خارج القانون، ولم تتحصّل على أيّ ترخيص لمزاولة نشاطاتها بصفة قانونيّة[2].

وعليه بقيت تشريعات بعض دول العالم في صَمْتٍ تِجَاهَ بعض تقنيات التّسويق الشّبكي عبر الإنترنت، وبالخصوص أسواق صرف العملات الافتراضيّة المنتشِرة بكثرة في الدول المتقدّمة، على غرار كلّ من سويسرا وبعض دول الاتّحاد الأوروبي(ألمانيا، مالطا، فنلندا، الخ...)، والولايات المتّحدة الأمريكيّة إلى جانب بعض البلدان العربية كتونس، المغرب،

---

1) **David LEFÈVRE**, « 60 informations pour tout savoir sur le MLM », p. 08. Article publié à partir de l'adresse suivante: http://www.kalipub.commediasfiles60-informations-pour-tout-savoir-sur-le-mlm.pdf, consultée le 20/06/2016.

2) أنظر **الملحق رقم (17)**، ص 494.

للمزيد من المعلومات حول التسويق الهرمي، أنظر المواقع الالكترونية التالية:
http://www.pyramidschemealert.org ou http://www.mlm-thetruth.com(consultés le 13/07/2016)

الخ...)، حيث اتّفقت جميعها بالمقابل على أنّ التّعامل التّجاري عبر شبكات البيع الهرمي يُشجِّع الغشّ التّجاري والتّهرّب الضّريبي وغسيل الأموال والمعاملات الماليّة المجهولة(تمويل الإرهاب، المخدّرات...)، كما لم تُصدر أيّ إطار تنظيمي أو تشريعي يُنظم التّعامل بتقنيات التّسويق بالعملات الافتراضيّة، وبقيت فقط تحذّر المُستهلكين من الأخطار المُحيطة بها.

ثانيا– الإعلان الإلكتروني:

يُعرف عن الإعلان الإلكتروني أنّه من بين الوسائل التي تستخدم للاتّصال غير الشّخصي بين المنتجين والعملاء عبر مواقع التّجارة الإلكترونيّة، لهدف تقديم ونقل المعلومات الخاصّة بمختلف السّلع أو الخدمات والاتصال بأكبر عدد مُمكِن من المستهلكين الحالين أو المرتقبين، لإقناعهم على اتّخاذ القرار الشّرائي وفقا لإمكانياتهم ومصالحهم وأهدافهم، وبالتّالي فإنّ الإعلان الإلكتروني يتميّز بقلّة تكاليف الحملة التّرويجيّة لمختلف السّلع والخدمات، وذلك مقارنة مع التّكاليف النّاجمة عن الحملة الإعلانية التّقليديّة، ويُمكّن المُشاهِد من التّفاعل الفّوري مع الإعلان من خلال التّوصّل إلى جميع المعلومات التي يحتاجها عن المنتوج، الشيء الذي يُحفّزه على الاتّصال بالبائع عبر موقعه التّجاري لشراء السّلعة أو الخدمة فورا، كما يستخدم في الإعلان الإلكتروني وسائط إلكترونيّة عبر الشّبكة تُمكّن من توجيه المنتجات إلى العملاء المستهدفين بطرق مدروسة بدقّة، بالإضافة إلى ذلك نجد أنّ الإعلان الإلكتروني يتميّز بمرونته وسهولة سحبه أو تغييره حسب الظّروف الدّاخليّة والخارجيّة المحيطة ببرنامج الحملة الدّعائيّة[1].

تحتوي الكتالوجات الإلكترونيّة(Catalogues) على مجموعة من صفحات الويب التي تُمثّل العمود الفقري لمحتوى إعلانات الحملات الدّعائيّة، المتعلّقة بعرض المعلومات عن منتجات البائع إلكترونيا، إذ تستخدم فيها النّصوص، الرّسومات، الصّور المتحرّكة،

---

[1] **فداء حسين أبودبسة، خلود بدر غيث**، تصميم الإعلان والترويج الإلكتروني، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن، 2009، ص ص 170– 172.

ديفيد ميرمان سكوت، القواعد الجديدة للتسويق والعلاقات العامة،**(ترجمة ديب القيس)**، دار الكتاب العربي، بيروت، لبنان، 2007، ص ص 246، 247، 248.

الفيديوهات، الصّوتيات الخ... حيث تحتوي النّسخة الإلكترونيّة على معلومات دقيقة عن وصف المنتج، الحجم، اللّون، المكوّنات الماديّة، معلومات عن السّعر، وبالتّالي فإنّ الكتالوجات يمكن أن تحتوي على صفحات ويب ثابتة تقوم بعرض المعلومات من خلال نصوص مكتوبة أو صور ثابتة، بينما الكتالوجات الدّيناميكيّة تعمل على عرض المعلومات المتعلّقة بمختلف المنتجات من خلال صور أو فيديوهات متحرّكة أو حيّة[1].

انطلاقا من ذلك، يجب على صاحب المَوقِع التّجاري أثناء قيامه بتصميم الكتالوجات أن يقوم ببناء الواجهة الأماميّة للمتجر الافتراضي، ويُراعي الحاجات والمعلومات التّفصيليّة عن طريق استخدام لغات مناسبة في توجيه المعلومات المختارة، التي من شأنها أن تُأَثِّرَ أو تَترُك انطباعًا جيّدا لدى العملاء، كما ينبغي عليه أن يقوم بعرض قائمة المنتجات في صفحة واحدة رئيسيّة تحتوي على كلمات مُوجَزَة مُعبّرة وصُورا وفيديوهات لوصف للمنتجات، المعروضة للبيع التي تتيح للزّبائن فرصة التّعرف عليها(المنتجات) بِيُسْرٍ، مع تسهيل مهمّة شراء المنتجات التي وقع عليها الاختيار ووضعها في عربات التّسوق الإلكترونيّة، لإتمام الخطوات اللاّحقة لعملية الشّراء بما فيها إتمام عملية التّسديد، بطرق دفع إلكترونيّة آمنة عبر شبكة الإنترنت وتوضيح طرق شحن وتوصيل هذه المنتجات[2].

إنّ نجاح الحملات الإعلانية عبر مواقع التّجارة الإلكترونيّة مرهون بتواجد برامج محرّكات البحث عبر شبكة الإنترنت، التي تمكّن العملاء من الوصول إلى قواعد البيانات للبحث عن المعلومات المتعلّقة بموضوع بحثهم، وبالتّالي يمكن لهذه المحرّكات أن تكون في شكل موقع إلكتروني مخصّص للبحث عن المواقع الإلكترونيّة الأخرى المسجّلة لديه، أو

---

1) **François OLLÉON et autres**, op.cit., pp. 60- 66.

2) **Jeffrey F. RAYPORT, Bernard J. JAWORSKI**, Commerce électronique, édition de la Chenelière McGraw-Hill, Québec, Canada, 2003, pp. 164- 166, 169, 170, 171.

إيمان فاضل السامرائي، تسويق المعلومات وخدمات الانترنت، الطبعة الثانية، درا صفاء للنشر والتوزيع، عمان، الأردن، 2015، ص ص 328- 330.

محمد عبد حسين الطائي، مرجع سابق، ص ص 166- 169.

حميد الطائي، أحمد شاكر العسكري، الاتصالات التسويقية المتكاملة(مدخل استراتيجي)، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009، ص ص 179، 180، 185، 186، 187.

تكون في داخل مواقع التّجارة الإلكترونيّة بذاتها، ففي كلتا الحالتين يستوجب على الزّائرين إدخال الكلمات الدّالة، سواء للبحث عن المواقع التّجاريّة عبر محرّكات بحث مستقلّة، أو البحث عن المحتوى الإعلاني للمنتجات المروّج لها، في إطار خدمة بحث داخل الموقع التّجاري التي تسمح للعملاء بالاستفسار عن المعلومات المتعلّقة بهذه المنتجات.

فوفقا لشركة تحليل ودراسة بيانات الإنترنت(Alexa Internet)، يعتبر مُحرّك البحث(https://www.yahoo.com) إلى جانب محرّك البحث(https:///www.google.com) من بين المواقع الإلكترونيّة الأكثر زيارة عبر شبكة الإنترنت، حيث استطاع الموقع الإلكتروني(!Yahoo) في أكتوبر 2014، أن يتيح حوالي ثلاثة(03) مليار من صفحات الويب في اليوم الواحد، وبلغ عدد زيارات هذه الصّفحات في أكتوبر 2007 إلى 3,4 مليار زيارة يوميا الأمر الذي يجعلها(!Yahoo) واحدة من أكثر المواقع الأمريكيّة الأكثر شُهرة [1].

---

[1] تُشرف الشركة الأمريكية لخدمات الحاسوب(! Yahoo) على بوابة ويب تقدم من خلالها العديد من الخدمات(مجانية أو بأجر)، من أشهرها خدمة البريد الإلكتروني(Boîtes à courrier électronique,)، محرك البحث (Moteur de recherche)، والخدمة الإخبارية(Portails(actualités, finances, etc.)، وخدمات الإيواء(Hébergement web)، والمحادثة الفورية(Messagerie instantanée,)، الخ...، حيث تأسست الشركة على يد خريجي جامعة ستانفورد(Stanford) جيري يانغ(Jerry Yang) ودايفيد فايلو(David Filo) في جانفي 1994، في حين أعلنت كشركة بصفة رسمية في 02 مارس 1995 حيث يتواجد مقرّها الرئيسي في سانيفال بولاية كاليفورنيا الأمريكية((Sunnyvale(Californie)، فأصل ظهور ياهو! يعود إلى دليل ويب (Jerry and David's Guide to the World Wide Web to Yahoo! (« Guide de David et de Jerry pour le World Wide Web »)) الذي تم إحداثه في جانفي 1994 من طرف الطالبان يانغ وفايلو(Yang et Filo)، حيث توصلا إلى إنشاء مُحرّك بحث Yet(**Y**) (**A**nother **H**ierarchical **O**fficious **O**racle)، يسهل من عملية البحث على المواقع الالكترونية عن طريق الكلمات الدالة(Mots-clés)، وبعد تأسيس شركتهم(02 مارس 1995) قبلوا عرض السيد مارك أنديرسون(Marc Andreessen) أحد مؤسسي شركة(Netscape Communications) حول إيواء الموقع الالكتروني ضمن خوادمها (Netscape Communications)، وفي عام 1996 انضمت شركة ياهو! إلى البورصة أين قامت ببيع حوالي 2,6 مليون من أسهمها بقيمة 13 دولار أمريكي للسهم الواحد، حيث حققت رأسمال يقدر بـ 43 مليار دولار أمريكي في بداية مارس 2005، ولتطوير وتحسين تكنولوجيا خدمات البحث قامت شركة ياهو! بشراء العديد من الشركات على غرار شركة(Inktomi) في 2002 محرك بحث كيلكو((Kelkoo(moteur de comparaison de prix) في 2004، وشركة(Interclick) المتخصصة بتقديم الحلول الإشهارية عبر الانترنت(2011) بقيمة 196,4 مليون أورو، الخ...، حيث أعلن مُجمّع ياهو ! في 2014 عن إنشاء متجرين افتراضيين عبر الإنترنت(Yahoo! Food et Yahoo! Tech)،

لذا تسعى الشّركات من خلال كتابة الإعلانات في المواقع الإلكترونيّة إلى تحقيق هدفين متزامنين، الأوّل يتعلّق بترقية مرتبة المَوقِع التّجاري في محرّكات البحث والحصول على أفضل المراتب في محرّكات البحث الذّكية، والثّاني يتمثّل في تحقيق الأرباح والسّعي لاستقطاب أو جذب أكبر عدد مُمْكِنْ من الزوّار إلى المَوْقِع، ويكون ذلك من خلال اختيار كلمات دّالة جاذبة وعبارات مفتاحية حاسمة على صفحات الويب[1].

لكي يتمكّن صاحب الموقع التّجاري من بناء اتّصالات تسويقيّة عبر الإنترنت، يجب أن يستعين بطرق أو تقنيات الإعلان التي تتيحها روابط الإحالة(Hyperliens) لمُحرّكات البحث أو برامج المشاركة التّسويقيّة، لتمكين العملاء من الاتّصال المباشر بموقعه التّجاري بطريقة

وإطلاق خدمة(Yahoo! Sports) في فرنسا التي تتوافر في الهواتف الذكية(iPhone, iPad et Android)، والجدير بالذكر أنّ مجمع ياهو ! أعلن في جانفي 2015 عن نيته في بيع نسبة 15% من الأسهم التي يملكها في مجمّع علي بابا(Alibaba Group) بقيمة تُقدّر بـ 40 مليار دولار أمريكي، في حين أعلنت شركة(Verizon) في جويلية 2016 عن شرائها لأسهم شركة ياهو ! بقيمة تُقدّر بـ 4,8 مليار دولار أمريكي حيث قامت نفس الشركة(Verizon) كذلك بشراء أسهم شركة(AOL) بمبلغ يقدر بـ 4,4 مليار دولار أمريكي.

للمزيد من المعلومات حول الموضوع، أنظر المراجع التالية:

Sarah BELOUEZZANE, « Yahoo! officialise le rachat de Tumblr », article de journal Le Monde, publié le 20/05/2013 sur : http://www.lemonde.fr/technologies/article/2013/05/20/yahoo-veut-racheter-tumblr-pour-rajeunir-son-image_3380686_651865.html, consulté le 03/11/2016.

Johann BRETON, « Yahoo! se paie Vizify, les Numériques », article publié le 6 mars 2014 sur : http://www.lesnumeriques.com/yahoo-se-paie-vizify-n33502.html, consulté le 02/10/2016.

Anne CONFOLANT, « Yahoo France prépare un vaste plan de licenciements », article de journal ITespresso.fr, publié le 21 mars 2016 sur : http://www.itespresso.fr/yahoo-france-prepare-vaste-plan-licenciements-124456.html, consulté le 05/01/2017.

Marion-JEANNE LEFEBVRE, « Yahoo étend son offre médiatique avec deux magazines en ligne », Stratégies/AFP, publié le 9 janvier 2014 sur : http://www.strategies.fr/actualites/medias/227458W/yahoo-etend-son-offre-mediatique-avec-deux-magazines-en-ligne.html, consulté le 20/12/2016.

Philippe GUERRIER, « Yahoo acquiert Interclick pour 270 millions de dollars », article de journal Itespresso.fr, publié le 2 novembre 2011 sur : http://www.itespresso.fr/publicite-yahoo-acquiert-interclick-pour-270-millions-de-dollars-47710.html, consulté le 07/01/2017.

أنظر كذلك المواقع الإلكترونية التالية: http://www.silicon.fr/restructuration-yahoo-au-bord-du-gouffre-137594.html et http://www.ledevoir.com/economie/actualites-economiques/260885/microsoft-yahoo-un-an-et-demi-de-discussions-avant-une-alliance (consultés le 10/02/2017)

[1] **Christophe BOUDRY, Clémence AGOSTINI**, « Étude comparative des fonctionnalités des moteurs de recherche d'images sur Internet », Revue Documentaliste-Sciences de l'Information, 2004/2 (Vol. 41), pp. 98, 99, 103, 104.

آمنة كاستعمال تقنية إعلانات الضّغط(Button advertising)[1]، التي تساعد الشّركة من وضع إعلان صغير في شكل مربّع أو مستطيل يظهر في الرّكن الأسفل من الموقع الإلكتروني، حيث يحتوي في داخله(الشّكل) شعار خاص بالمنتجات لاستهداف المستهلكين المرتقبين، كما يمكن لصاحب الموقع التّجاري أن يستعين بالتّقنيّة الخاصّة بإعلانات الكلمات الدّالة(Key Word Ads)، التي تكون في شكل كلمات موجّهة ومواد إعلان يظهر في شكل دليل يُوجّه عن طريقه الزائرين مباشرة إلى موقعه التّجاري[2]، وأمّا تقنيّة الإعلانات أو النّوافذ المنبثقة(Pop-up Ads) فهي تسمح بعرض إعلانات (لقطات الفيديو أو الصّور) بشكل مفاجئ وبصفة عشوائيّة ضمن صفحات الويب، وذلك عند فتح أحد المواقع أو تصفّحه أو حتى عند غلقه، لذا تثير هذه الإعلانات الانزعاج والجدل والانتقادات نظرا لطبيعتها التّطفّلية[3].

بالإضافة إلى هذه التّقنيات، توجد تقنيات أخرى كالإعلان عن طريق البريد الإلكتروني(mail Advertising)، الذي من خلاله تُحقّق الشّركة الكفاءة عن طريق اختيار قوائم عناوين البريد الإلكتروني المُهتمّة بالمنتجات المُرَوَّجِ لها، حيث تشتمل هذه القوائم على عناوين الرّاغبين في تلقي الرّسائل الإلكترونية التي تتضمّن على المنتجات التي يريدون معرفتها[4]، أمّا إعلانات الرّاية أو اللاّفتات(Advertising Banners) تسعى من خلالها الشّركة إلى وضع إعلان صغير في الرّكن الأعلى من موقعها التّجاري، في شكل مستطيل يحتوي على إعلانات تصويريّة صغيرة ومختصرة، تتضمّن على بيانات مختصرة عن السّلع

---

1) **Yan CLAEYSSEN**, L'e-mail marketing, 3e édition, Dunod, Paris, France, 2008, pp. 18- 20, 195- 200.

2) **ديفيد ميرمان سكوت(ترجمة ديب القيس)**، مرجع سابق، ص ص 241، 242، 243، 244، 245.

محمد عبد حسين الطائي، مرجع سابق، ص 333.

نظام موسى سويدان، شفيق إبراهيم حداد، مرجع سابق، ص 381.

Thibault VERBIEST, La protection juridique du cyber-consommateur (Publicité- Contrat- Contentieux), Litec, Paris, 2002, pp. 09- 18.

3) **Vincent FAUCHOUX, Pierre DEPREZ**, op.cit., p, 132.

4) من بين المواقع الإلكترونية التي تبيع قوائم البريد الإلكتروني الاختيارية عبر شبكة الإنترنت:
http://www.godaoldy.com ou http://www.netcreations.net/ ou http://www.returnpath.biz/

أو الخدمات بأشكال وألوان جذّابة، حيث تتميّز هذه الإعلانات بالحركة والتّفاعل بالشّكل الذي يُغري المشاهد للضّغط عليها[1].

كما يمكن لصاحب الموقِع التّجاري أن يَسْتَعِينَ بتقنيتي الإعلانات المُبوَّبة (Classified Advertising) أو إعلانات الرِّعايَة(Sponsorship)، فالتّقنية الأولى يقوم من خلالها باختيار المواقع الإلكترونيّة الأكثر شُهرة وتجذب العديد من الزّائرين، لعرض مختلف السّلع أو الخدمات فيها، أمّا التّقنيّة الثّانية تسمح للشّركة بدمج منتجاتها(السّلع أو الخدمات) المروّج لها ضمن مُحتوى النّص التّحريري لموقِع مُعيّن على شبكة الإنترنت، وذلك لغرض الإلمام أو الإيحاء للعميل أو المستهلك بوجود علاقة أو صلة بين المنتج المُعْلَنُ عَنْهُ والرّسالة الإلكترونيّة الخاصّة بالموقِع الإلكترونِي، ففي كلتا التّقنيتين يتوجّه الزّائرين بالدّخول مباشرة إلى صاحب الموقع التّجاري، وذلك بمجرّد النّقر على إعلانات المنتجات المُرَوَّجِ لَهَا[2].

ثالثا- الدّعاية والعلاقات العامّة الإلكترونية:

تسعى الشّركة أو المؤسّسة من خلال النّشر إلى رَفْعِ معنوياتها وتحسين صورتها الذّهنيّة وتشريف شُهرتِها، والذي يعتبر(النّشر) من بين الأدوات الرئيسية المستعملة في التّرويج وذلك لهدف نشر الأخبار ومختلف المعلومات المتعلّقة بسياسات الشّركة أو المؤسّسة وتوسّعاتها بخصوص منتجاتها، أما العلاقات العامّة تسعى من خلالها الشّركة إلى خلق المناخ الملائم للأعمال وتحقيق الرّضا والتّفاهم المتبادل مع عملائها، وإرساء علاقات حسنة فيما بين الشّركة والعملاء مع كسب ثقتهم وولائهم لسياساتها التّرويجية المتّبعة في مبيعاتها، أو المساعدة في تقديم منتجات جديدة[3].

---

[1] **فداء حسين أبودبسة، خلود بدر غيث**، مرجع سابق، ص ص 174، 175.

[2] **Thibault VERBIEST**, La protection juridique du cyber- consommateur, op.cit., pp. 09- 16.

إبراهيم بختي، "دور الإنترنت وتطبيقاته في مجال التسويق(دراسة حال الجزائر)"، دكتوراه دولة في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2002، ص ص 83- 85.

محمد عبد حسين الطائي، مرجع سابق، ص ص 331، 333.

[3] **محمد فريد الصحن**، التسويق الإلكتروني، مرجع سابق، ص ص 166، 167.

حميد الطائي، أحمد شاكر العسكري، مرجع سابق، ص ص 98- 101.

Robert LEDUC, op.cit., pp. 85, 86.

فمن خلال العلاقات العامّة تستطيع أصحاب مواقع التّجارة الإلكترونيّة الاتّصال بصفة مباشرة بالعملاء، من خلال مواقعها الشّبكية لاستعراض نشاطاتها أو عرض تقاريرها الشّهريّة أو السّنويّة وإتاحة خلاصات تفيد العملاء عن سير أعمالها ومشاريعها، أو استخدام آليات المؤتمرات الإلكترونيّة(e- conferencing) أو مجاميع النّقاش (Discussion grousp, focus groups.) أو غيرها من أساليب التّواصل المباشرة التي تستهدف العملاء الجدد مع تعزيز صورتها في أذهانهم[1].

لذا يعتمد المُسوّقون على مواقِع شبكات التّواصل الاجتماعي التي تسمح للأفراد بالتّفاعل مع بعضهم البعض، وبناء علاقات اجتماعيّة من خلال التّواصل المباشر عبر شبكة الإنترنت، وذلك مهما كان الجهاز المُستعمَل(الحاسوب، الهاتف الذّكي، لوحة رقميّة...)، حيث تعتبر حاليًّا هذه الشّبكات(التّواصل الاجتماعي) من بين أهم تقنيات التّسويق الأكثر فاعليّة، إذ تُتيح في إطار برامج المشاركة، إمكانية التّواصل مع العملاء في أيّ منطقة من العالم وتحليل السّوق بسهولة، مع استهداف رغبات العملاء في آنٍ واحد، من خلال نشر كمّ هائل من المعلومات المتعلّقة بمختلف السّلع أو الخدمات لكسب ثقة الزّوار مع جذب انتباههم بطريقة تلقائيّة إلى الموقِع التّجاري الإلكتروني، وكذا تزويدهم في أيّة لحظة بآخرِ المستجدّات الطارئة بالسّلعة أو الخدمة المُروّج لها[2].

---

[1] **بشير العلاق**، التسويق الالكتروني، مرجع سابق، ص ص 142، 143، 144، 145.

حميد الطائي، أحمد شاكر العسكري، مرجع سابق، ص ص 95، 96، 97.

للمزيد من المعلومات أنظر المواقع الإلكترونية التالية:

https://investors.ebayinc.com/secfiling.cfm?filingID=1193125-17106847&CIK=1065088#D191389DDEF14A_HTM_TX191389_4 et http://www.pez.at/fr/Company/History (consultés le 20/07/2016.) et http://www.boursier.com/actions/actualites/news/ebay-des-encheresd-art-en-ligne-avec-sotheby-s-620525.html et http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=403863 22300-77(consultés le 22/07/2016.)

[2] **Martine HLADY RISPAL**, Marketing contextuels (Industries- Grande distribution- Web 2.0- Organisation sportives- Arts et culture- Produits biologique- Économie solidaire- Politique des petites communes.), Dunod, Paris, France, 2008, pp. 56, 57, 64.

Anthony PONCIER, « La gestion de l'image de l'entreprise à l'ère du web 2.0 », Revue Internationale d'intelligence économique, 2009/1 (Vol 1), pp. 83- 85, 89- 91.

وعليه، فإنّ مَواقِع التّواصل الاجتماعي تسمح لأصحاب المتاجر الافتراضيّة من خلال خاصيّة المُشاركة(J'aime)، إمكانية التّواصل مع الجماهير حول العالم بشكل مباشر عبر شبكة الإنترنت، مع تحليل الأسواق بسهولة واستهداف رغبات العملاء من خلال التّرويج لمنتجاتهم وضمان وصولها إلى أكبر عدد مُمكن من المُتابعين، حيث تتضمّن مَواقِع التّواصل الاجتماعي على معلومات متعلّقة بالسّلع أو الخدمات المُتاحة التي من شأنها أن تجذب انتباه وأنظار العملاء المحتملين، مع تزويدهم بصفة مُستمِرّة بأحدث المستجدات حول السّلعة أو الخدمة التي يشتركون أو يتابعون فيها من خلال أيّ جهاز متّصل بشبكة الإنترنت، ولتحسين صفحات الشّبكات الاجتماعيّة يتعيّن على القائم بعملية التّسويق أن يستهدف فئة معيّنة من المستهلكين، من خلال توفير المعلومات القيّمة والمُفيدة حول السّلعة أو الخدمة المُروَّج لها عبر شبكة التّواصل الاجتماعي، إنشاء مجموعات للمشاركة في المناقشات التي تدور حول المواقع، مع استخدام العديد من الوصلات كمصادر لجذب المستهلكين لزيارة الموقع التّجاري[1].

انطلاقا من ذلك، يُعتبر موقع فايس بوك(Facebook) من بين أحد أشهر وسائل التّواصل الاجتماعي، باعتباره شبكة اجتماعيّة تتيح للمستخدمين إمكانية نشر مختلف الصّور والفيديوهات والملّفات والوثائق والاتّصال والتّفاعل فيما بينهم، من خلال تقنيّة الانضمام والمشاركة وإرسال الرّسائل وخلق مجموعات للتّواصل فيما بينهم، الخ...، ففي مجال التّجارة الإلكترونية يسمح ذلك الموقع(Facebook) بإنشاء روابط اتّصال مع المتاجر الافتراضيّة لغرض نشر المعلومات المتعلّقة بمختلف السّلع أو الخدمات، من خلال الصّور والفيديوهات، من دون حدود معيّنة، مع عرض المنشور التّرويجي مباشرة للمُعجبِين بعد نشره في الصّفحة الرّئيسيّة للموقِع التّجاري[2].

---

[1] **مروة نبيل حلمي الحايك**، "التسويق عبر شبكات التواصل الاجتماعي وعلاقته في تعزيز إدارة العلاقة مع الزبون في شركات تكنولوجيا المعلومات- قطاع غزة"، رسالة الماجستير في إدارة الأعمال، كلية الاقتصاد والعلوم الإدارية، جامعة الأزهر، غزة، 2017، ص ص 40- 45.

ديفيد ميرمان سكوت(ترجمة ديب القيس)، مرجع سابق، ص ص 236، 237.

[2] للمزيد من المعلومات حول مواقع التواصل الاجتماعي، أنظر:

كما يُعتبر(Twitter) من بين أحد شبكات التّواصل الاجتماعي التي تتيح للمُستخدمين خدمة التّدوين المُصّغر(Microblogage)، من خلال إرسال تغريدات(Tweets) في حدود(140) حرف للرّسالة الواحدة كحدّ أقصى، ويتّم ذلك مباشرة عبر موقع "تويتر" أو عن طريق إرسال رسالة نصيّة قصيرة(SMS) أو برامج المحادثة الفوريّة (Messagerie instantanée) ، أو التّطبيقات التي يتيحها المُطوّرون أو المُبرمِجون (Facebook, Twitterfox, Twhirl, Twitterrific, TwitBird.).

حيث يمكن للأصدقاء قراءة الرّسائل مباشرة من صفحتهم الرّئيسيّة واستقبال ردود الأفعال من خلال الرّسائل النّصيّة القصيرة، التي تبدأ برمز هَاشْتَاغْ(« # »Hashtags) أو دَيَازْ(« # »Dièse)، التي تتعدّد وتتنوّع صِيَغُهَا حسب أهداف ومواضيع مستخدمي خدمة التّدوين، ففي مجال التّجارة الإلكترونيّة تسمح شبكة(Twitter) للشّركات بترويج منتجاتها على مستوى فردي، من خلال إرسال رسائل قصيرة للأفراد تشرح في إطارها آلية عمل المنتوج وطريقة استعماله الخ...، أو تقوم عبر هذه الشّبكة(Twitter) بنشر روابط للتّرويج لمختلف منتجاتها، فمنذ سنة 2012 أصبح رمز ($)يُستخدم في صيغ رسائل التّدوين حول شركات البورصات العالميّة (« **$AAPL** » pour Apple ou bien « **$TWTR** » pour Twitte, etc.)، الخ...[1].

Franck LEROY , Réseaux sociaux et C[ie] (Le commerce des données personnelles) , Actes Sud, 2013, France, pp. 96- 101, 149- 156, 157- 162,

Benjamin GOURDET, « Facebook vaut-il 104 milliards de dollars ? », article publié sur 01n et.com, le 18 mai 2012. http://www.01n et.com/editorial/566339/facebook-vaut-il-104-milliards-de-dollars/), sur 01net.com, consulté le 14/11/2016.

Antoine CROCHET-DAMAIS, « Facebook at Work se lance, et devient Workplace by Facebook », article de Journal Du Net, publié le 13 octobre 2016. http://www.journaldun et.com/solutions/reseau-social-d-entreprise/1186206-facebook-at-work-lance-et-devient workplace-by-facebook-6/, consulté le 18/11/2016.

Fabien SOYEZ, « 83 millions de comptes Facebook sont faux », article de journal Le Figaro, publié le 03/08/2012. http://www.lefigaro.fr/societes/2012/08/03/20005-20120803ARTFIG00397-83-millions-de-comptesfacebook-sont-faux.php, consulté le 21/11/2016.

1) **William AUDUREAU**, « Le réseau social Mastodon, un «Twitter plus proche de l'esprit originel», article de journal Le Monde, publié le 4 avril 2017 sur : http://www.lemonde.fr/pixels/article/2017/04/04/le-reseau-social-mastodon-un-twitter-plus-proche-de-l-esprit-originel_5105900_4408996.html, consulté le 09/05/2017.

رابعا– تنشيط المبيعات الإلكترونيّة:

يُستخدم هذا النّشاط بجانب الإعلان والبيع الشّخصي لغرض تنشيط مبيعات منتجات الشّركة في ظرفٍ قصير، وزيادة معدلات استخدامها عن طريق جذب المستهلكين المرتقبين لاستهلاكها، فمن بين الوسائل المستخدمة في تنشيط المبيعات نجد المسابقات والهدايا والعيّنات المجّانيّة والتّخفيضات في أسعار المنتجات الموّجهة للمستهلكين[1]، كما يمكن أن تُوَّجَهَ هذه الوسائل إلى المُوزّعين والبائعين من أجل تحفيزهم على تصريف المنتجات ورفع فعالية أدائهم، من خلال منحهم جائزة أحسن موزّع مع وَسائل مُساعدة أو مكافئات ماليّة، كما توجد مواقع شبكيّة تجري مقابلات فيما بين الزّائرين وتقدم للفائزين هدايا فوريّة، الخ...

الفرع الرابع

التّوزيع الإلكتروني(E-Place)

يُعْتَبَرُ التّوزيع عنصرا أساسيا في عناصر المزيج التّسويقي الإلكتروني، إذ يُمثّل جميع النّشاطات أو الوسائل التي تعتمد عليها الشّركة، لتوصيل المنتوج إلى العملاء المستهدفين في الوقت والمكان المناسبين، ويتّم ذلك عبر قنوات توزيع تعتمد فيها على شركات وأفراد، يقومون بمجموعة من الوظائف الضّروريّة لإيصال المنتجات من المنتجين إلى الأسواق المستهدفة أو العملاء، كالقيام بعمليات التّمويل المُسبق، والتّوزيع المادّي للمنتجات كنقلها وتخزينها وتجهيز الطّلبيات، وإجراء عمليات التّرويج والاتّصال والتّفاوض الخ...[2].

تتأثّر نُظُمَ التّوزيع بمجموعة من العوامل التي تؤثّر في اختيار إستراتيجيّة التّوزيع، فمنها ما يتعلق بتزايد وتغيّر حاجات ورغبات المستهلكين، نتيجة المُتغيّرات الحاصلة على الظّروف المحيطة بالمنتجات، كحساسيّة هذه الأخيرة نتيجة ظروف النّقل أو البيئة المناخيّة الخ...،

---

[1] **يوسف حسن يوسف**، التسويق الالكتروني، مرجع سابق، 2012، ص 102.

بشير العلاق، التسويق الإلكتروني، مرجع سابق، ص 165.

[2] **Marie-Christine MONNOYER-LONGÉ, Catherine LAPASSOUSE-MADRID,** «Intégrer les sites web dans les stratégies. Concept et modèle », Revue Française de Gestion, 2007/4 (n° 173), p. 152, 153.

مما يستدعي الأمر البحث على عدّة وسطاء لتوزيع هذه المنتجات بسعر مُنخفض، أمّا إذا كانت المنتجات تتميّز بنوعيّة خاصّة، وجودة عالية، فيرتفع سعرها ويتّم توزيعها من خلال قناة توزيع قصيرة، كما أنّ نوع المنتجات وحجم الطّلب عليها والطبيعة الفنيّة لها يؤثّر بشكل كبير على اختيار نمط توزيعها إلى المستهلك النّهائي، كما أنّ الظّروف المحيطة بالأسواق تؤثّر بشكل كبير على نمط اختيار قنوات التّوزيع، كالأخذ بعين الاعتبار التّركيز الجغرافي للأسواق المستهدفة، وحجمها وعدد العملاء المرتقبين فيها، وكساد المنتجات التي تستدعي البحث على قنوات توزيع قصيرة، نتيجة الظّروف الاقتصاديّة المزرية الخ...

فمهما كانت العوامل المؤثّرة في اختيار نمط التّوزيع، فإنّ عملية تسويق المنتجات إلى الأسواق المُستهدفَة، تستوجب تحديد الإستراتيجيّة الملائمة للتّوزيع، التي من خلالها تقوم الشّركة بإتّباع إستراتيجيّة التّوزيع المباشر أو غير المباشر، فالأولى تضمن للشّركة عِدّة خيارات إستراتيجيّة من دون الاعتماد على وسطاء كالبيع عبر متاجر التّجزئة، البيع بالبريد الإلكتروني أو الطّواف بمكاتب المشترين الخ...، أمّا إستراتيجيّة التّوزيع غير المباشرة تستدعي تواجد وسيط أو عدّة وسطاء لإيصال المنتجات من المنتج إلى المستهلك[1].

تجدر الإشارة في هذا السّياق، أنّ استخدام بعض التّقنيات أو الوسائل التّكنولوجيّة الحديثة كالطّائرات بدون طيّار(Drones) المُزوّدة بحمولة(كاميرات، صواريخ أو أيّة سلعة أخرى) وتقنيات التَّحكُّم الذّاتي أو عن بُعد، كانت تُستخدَم مُنْذُ المُهلة الأولى لغرض تحقيق أهداف عسكريّة بحتَة في إطار الحرب الإلكترونيّة، كمُباشرة عمليات الاستطلاع على العدّو من خلال المتابعة والمراقبة اللحظيتين لأرض المعركة، مع اتّخاذ القرار المُناسب لتنفيذ الهجمات، أو تنفيذ عمليات الإعاقة للتّشويش على الصّواريخ والدّفاع الجوّي أو لكشف المراكز الحسّاسة، حيث يمكن استخدامها في بعض الحالات كصواريخ انتحارية في حالة فشل مهامها أو انتهاؤها أو وجود هدف حيوي يتطلّب تدميره بسرعة الخ...

---

[1] **محمود جاسم الصميدعي**، مرجع سابق، ص 248.

حيث يعود أوّل استخدام لها من النّاحية العملية من طرف الولايات المتّحدة الأمريكيّة في زمن الحرب البّاردة، وبالخصوص أثناء الحربين الفيتناميّة(1975/1955) والكوريّة(1953/1950)، وبالتّالي أصبحت مع مرور الزمن تُستخدم تقنيّة الطّائرات بدون طيّار لتحقيق "أغراض مدنيّة" كمُكافحة الحرائق(إطفائها)، وقياس درجة الحرارة وسرعة الريّاح لاكتشاف الأعاصير ومتطلّبات البيئة الأخرى أو لأغراض البحث العلمي، إلى جانب تنفيذ عمليات الإنقاذ والاستكشافات الكونيّة أو في مجال الزّراعة وحفظ النّظام العام والصّحافة الخ...، حيث كَثُرَ استخدامها في هذه الآونة في مجال التّجارة الإلكترونيّة.

انطلاقا من ذلك، قامت شركة أمازون (Amazon.com) في ديسمبر 2013 بعرض خدمة التّوزيع باستخدام الطّائرة بدون طيّار أطلقت عليها تسمية(Amazon Prime Air)، التي تستوجب آنذاك الحصول على ترخيص من طرف الوكالة الفيدراليّة للطّيران (Federal Aviation Administration(FAA)) التي فرضت مجموعة من القواعد الصّارمة التي حدّدت إجراءات وشروط استخدام هذا النّوع من الطّائرات(Drones)، كضرورة تحديد مكان وساعات التّحليق، مع وجوب مُراقبتها(Technicien) والتّدخل الفّوري عند الاقتضاء في أيّة لحظة أثناء مباشرتها لخدمة التّوزيع.

حيث استطاعت شركة(Amazon.com)[1] في ديسمبر 2016، بالتّعاون مع السّلطات الإنجليزيّة، أن تُجَسِّدَ في غضون 13 دقيقة أوّل رحلة تجاريّة على الأراضي البريطانيّة،

---

[1] شركة أمازون.كوم(Amazon.com) عبارة عن موقع إلكتروني للتجارة الإلكترونية والحوسبة السحابية تأسس على يد الأمريكي جيف بيزوس(Jeff BEZOS) في جويلية 1994 بالولايات المتحدة الأمريكية التي يقع مقرّها في مدينة سياتل بولاية واشنطن، حيث استقر اختيار جيف بيزوس(Jeff BEZOS) تسمية متجره الافتراضي بعلامة تجارية مميزة أمازون(Amazon)، نسبة لنهر الأمازون باعتباره كأكبر نهر في العالم الذي يتوافق مع هدف مشروعه في أن يكون متجره كأكبر متجر في العالم، فمنذ عام 2000 ظهر شعار أمازون كسهم يشبه شكل الابتسامة يمتد من حرف(A) إلى(Z) الذي يشير إلى أنّ الشركة قادرة على توفير وبيع كافة المنتجات للمستهلكين.

وهكذا بدأت الشركة خدماتها التسويقية عبر الإنترنت في 16 جويلية 1995 أين قامت ببيع أول كتاب(Douglas Hofstadter) بعنوان(Fluid Concepts and Creative Analogies)، حيث بدأت الشركة نشاطاتها باعتبارها متجرا لبيع الكتب عبر الإنترنت أين أثمر مشروع بيزوس مع صاحب مشروع(Ingram content book) الذي تحصلت منه شركة أمازون على الكتب بالجملة، ووصلت مبيعات الشركة خلال الشهرين الأولين من بداية المشروع إلى(50) ولاية

باستخدام طائرة بدون طيّار على مَتْنِهَا منتجات إلكترونيّة مُوَجَّهَة لزبون مُقِيم في إقليم(Cambridgeshire) مع عودتها سليمة إلى القاعدة التي انطلقت منها[1].

أمريكية و(45) دولة من العالم، وكانت أرباح الشركة آنذاك تقدر بحوالي عشرين ألف(20000) دولار أمريكي في الأسبوع، وعليه كانت شركة أمازون منذ بداية نشأتها تَستحوِذ على خدمات بيع الكتب عبر شبكة الإنترنت.

غير أنّه سرعان ما وسّعت نشاطاتها لتشمل العديد من المنتجات كأقراص الفيديو الرقمي(DVD, etc) وألعاب الفيديو واسطوانات الموسيقى(MP3, MP4, etc.)، وبرمجيات الحاسوب، والإلكترونيات والملابس والأثاث وقِطَع غيار السيارات والأثاث والطعام الخ...، ولتوسيع نفوذها عبر أسواق العالم قامت شركة أمازون بشراء العديد من الشركات التي سمحت للشركة بتنويع منتجاتها وإنشاء مواقع تجارية منفصلة عبر العديد من دول العالم، مع إتاحة العديد من الخدمات عبر الموقع الالكتروني على غرار خدمة أمازون فيديو(Amazon Video) التي استحدثتها في 2006، لتوفير وتزويد خدمات الفيديو بصفة مباشرة حسب الطلب حيث قامت الشركة في 2016 بتوسيع نمط تلك الخدمة المباشرة تحت تسمية(Prime video) لتشمل حوالي مائتي(200) دولة من العالم، التي من شأنها منافسة شركة(Netflix) الرائدة في ذلك المجال على المستوى العالمي.

كما قامت شركة أمازون في 2007 بتسويق قارئ للكتب الالكترونية (Lecteur de livres numériques appelé **(Kindle)**) في شكل برنامج تطبيقي يتيح إمكانية قراءة الكتب على أيّ جهاز حاسوب أو هاتف الذكي، وفي 25 جويلية 2016 توصلت شركة أمازون إلى الاتفاق مع الحكومة البريطانية بشأن الحصول على تراخيص لتوزيع المنتجات عبر خدمة الطائرات بدون طيّار(Amazon Prime) لتُعمّم تلك الخدمة في المستقبل عبر أنحاء دول العالم. للمزيد من المعلومات حول الموضوع، أنظر المواقع الالكترونية التالية:

https://www.challenges.fr/economie/consommation/pourquoi-l-incroyable-puissance-commerciale-d-amazon-attire-monoprix_458603 et http://www.journaldunet.com/ebusiness/commerce/jeff-bezos-biographie-de-jef f-bezos.shtml (consultés le 01/02/2017.) et http://www.boursier.com/actualites/economie/amazon-experimente-la-livraison-par -drone-en-angleterre-26085.html et https://www.lesechos.fr/finance-marches/marches-financiers/010159042103-amazon-rejoint-lelite-de-la-tech-2104705.php et http://www.challenges.fr/entreprise/transports/20160726.CHA2122/amazon-va-tester-de-nouveaux-dro nes-livreurs-a-londres.html (consulté le 03/02/2017.)et http://www.lepetitjournal.com/londres/a-la-une-londres/132615-evasion-fiscale-le-gouvernement-britannique-durcit-le-ton.html et http://www.challenges.fr/entreprise/20140704.CHA5796/le-regime-fiscal-d-amazon-au-luxembour g-dans-le-viseur -de-bruxelles.html (consultés le 05/02/2017.)

[1] أنظر **الملحق رقم (18)**، ص 494.

Voir aussi : **Jean-Michel NORMAND**, « Premiers clients pour les drones d'Amazon et de La Poste », article publié sur le journal Le Monde, le 15.12.2016 à 14h37 - Mis à jour le 15.12.2016 à 15h22. http://www.lemonde.frla-foire-du-dronearticle20161215premiers-clients-pour-les-drones-d-amazon-et-de-la-poste_5049503_5037916.html, consulté le 04/02/2017.
Voir aussi : le site de l'entreprise(Amazon.com) : https://www.amazon.com

وعليه، فإنّ الطّائرات بدون طيّار يُمكن أن تكون عُرْضَةً لمختلف الهجمات الالكترونيّة ومحل استهداف فئات القراصنة[1]، الذين يقومون باستغلال الثّغرات الأمنيّة المتواجدة على مستوى أنظمة حماية أنظمة تشغيلها، التي تسمح لأي شخص يملك المعدّات التّقنيّة اللاّزمة لإرسال الأوامر لأجهزة الطّائرات (Un **logiciel** installé sur un **ordinateur portable** équipé d'une **antenne directionnelle**)، من التّحكّم في أنظمة تشغيلها وتغيير مسارها للاستحواذ على السّلعة المُستهدفة(Colis) التي من المفروض أن تُنقِلُها للزّبون المعني.

حيث تُعد أنظمة تشغيل الطائرات بدون طيّار سهلة للقرصنة، نظرا لاستخدامها لأنظمة اتّصال غير مشّفرة(Communications non chiffrées) ومنافذ عديدة مفتوحة (Ports ouvert)، لذا يُوصي خبراء أمن المعلومات صانعي هذه الطّائرات على ضرورة القيام بتصحيحات تقنيّة مع التّحديثات اللاّزمة على مستوى أنظمة تحكُّمها وأمنها.

1) **Bruce SNELL**, « Piratage de drones : la menace plane », Rapport McAfee Labs Prévisions 2017 en matière de menaces, Novembre 2016, pp. 40, 41, article publié à partir de l'adresse suivante: https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf, consultée le 13/12/2016.
Stéphane PLASSE, « Drones : comment lutter contre le risque de piratage ? », article publié le 15/08/2013, à 8h21, sur le site : https://www.slate.fr/story/76418/drone-France-piratge, consulté le 04/03/2016.
Kate KOCHETKOVA, « Des drones armés de pistolets, de tronçonneuses et de vulnérabilités… », article publié le 28/04/2016, sur le site : https://www.kaspersky.fr/blog/haking-armed-drones/5590/, consulté le 03/05/2016.

خلاصة الفصل الأول

من خلال ما درسناه في الفصل الأول، نصل إلى أن التّجارة الإلكترونيّة تعتمد على نظام معلوماتي مُتكامل في إطار البنية التّحتيّة لشبكات الاتّصالات، التي تُسّهل عمليات تدفّق البيانات ومعالجتها وتخزينها واستحداثها، حيث تتيح شبكة الإنترنت، باعتبارها شبكة الشّبكات، للشّركات التّجاريّة والاقتصاديّة خيارات وبدائل مُتعدّدة حسب احتياجاتها المُتغيّرة في زمن العولمة والتّطوّرات المُنبثِقة عن الثّورة الرّقميّة، حيث لَمْ يَعُدْ حاليّا على مَقْدُورِ أيّة شركة مُباشرَة نشاطاتها على النّحو التّقليدي الذي كانت تُمارس وِفْقَهُ نشاطاتها من قَبْلِ.

حيث تعتبر شبكة الإنترنت ثمرة جهود العقل البّشري التي نشأت في ظروف الحرب البّاردة بين المعسكر الشّيوعي والرّأسمالي، وتطوّرت خدماتها عبر العالم بشكل مُذهل وسريع بعد ظهور الويب، الذي ما هو إلاّ خدمة من بين الخدمات المُختلِفة المُتاحة عبر تلك الشّبكة(الإنترنت)، التي أحدثت(الخدمات) تغييرات جذريّة في نمط إدارة الشّركات ومعالجة وتداول البيانات الإلكترونيّة، ورفع قُدراتها التّسويقيّة والتّنافسيّة من خلال تلبية وفهم المُتطلبات المُتسارعة للزّبائن على السّلع والخدمات عبر مواقع التّجارة الإلكترونيّة.

تعتمد عملية إحداث مواقع التّجارة الإلكترونيّة على تقنيات الويب الحديثة، في عمليات إحداث وتصنيف وتحويل صفحات الويب من مُجرّد صفحات ثابتة إلى صفحات ديناميكيّة أو تفاعليّة، التي تستوجب من النّاحية التّقنيّة مراعاة مجموعة من الخطوات، كالتّخطيط المُسبق لمشروع المتجر الافتراضي، الذي من خلاله يقوم المعني بدراسة مُسبقة لمشروعه، أخذا بعين الاعتبار المجال والأهداف والتّكاليف المُنتظرَة من المشروع، والإمكانيات الماليّة والبشريّة والتّقنيّة المُسّخرة فيه، والإحاطة بكلّ ما يَسْتَوْجِبُهُ مُحْتَوَى المَوقِع الإلكتروني من إيواء وعِناية خاصّة، وتخطيط أو تصميم مُفصّل ومدروس بِدقّة، والتّكاليف النّاجمة عن حمايته، وصيانته، وتحديثه، الخ...، وكذا احترام دفتر الشّروط الخاص بعقد إحداث المتجر الافتراضي الذي يبرمه صاحب المشروع مع مزوّد خدمة الإنترنت، الذي من المستحسن أن يَقَعَ اِخْتِيَارِهِ على مُزوِّد يُشرف لِوَحْدِهِ على الخدمات الأساسيّة، المُتعلّقة بجميع مَرَاحِلِ إحداث واستغلال المتجر الافتراضي عبر الإنترنت، التي يتيحها سواء في إطار عقد مُوحَّد Un)

(Contrats séparés avec des conditions financières propres) أو عن طريق إبرام سلسلة من العقود الفنيّة (contrat unique) مع نفس المُزوّد.

كما يجب على صاحب مشروع إحداث المتجر الافتراضي القيام بشراء اسم النّطاق وفقا لقاعدة الأسبقيّة في تسجيل الاسم لكي يَخْدُمَهُ« premier arrivé, premier servi »، المُتبّعة في جميع إجراءات التّسجيل، والذي من المُسْتَلْزَمِ أن يُعَبِّرَ عن نَوْعِ العمل أو النّشاط، مع التّأكد من عدم استخدامه مُسبقا من قِبَلِ الأطراف الآخرين، مع إيواء الموقع الإلكتروني وتصميمه والتّرويج له في عدّة محرّكات البحث والفهارس المعلوماتيّة، وكذا احترام أحكام التّشريعات والتّنظيمات المتعلّقة بحماية المعطيات الشّخصية للأشخاص الطبيعيين، أين يتعيّن عليه الالتزام بالتّصريح لدى الهيئات المعنيّة بحماية المعطيات الشّخصية، باعتبار التّاجر الافتراضي مسؤولا على المعالجة الآلية للمعطيات الشّخصية، مع القيام بالاستغلال الفّعلي لاسم النّطاق وتأمين وصيانة المَوقِع التّجاري الإلكتروني الخ...

لضمان تقديم خدمة فعّالة ومضمونة للعملاء، يجب على المُورّد الإلكتروني احترام الشّروط القانونيّة المتعلّقة بممارسة التّجارة الإلكترونيّة، والمتطلّبات المتعلّقة سواء بالعرض الإلكتروني، والإشهار والدّفع الإلكترونيين، وكذا المتطلّبات المتعلقة بالعقد الإلكتروني الذي تترتّب عنه مجموعة من الحقوق والالتزامات لأطراف العقد.

وعليه، أصبحت مَواقِع التّجارة الإلكترونيّة بحاجة إلى تقنيات وأساليب تسويق حديثة لترويج مختلف المنتجات والخدمات، بغية جذب واستهداف فئة مُعيّنة من العملاء، على غرار التّسويق عبر محرّكات البحث(Saerch Engine Marketing)، أو برامج المشاركة التّسويقيّة(Affiliate Marketing)، والتسويق عبر شبكات التّواصل الاجتماعيSocial) (Network Marketing، حيث تُعتبر هذه التّقنيات جزءً من تطبيقات التّجارة الالكترونيّة، التي تعتمد عليها الشّركات من أجل تحقيق أهدافها التّجارية عبر مختلف أسواق العالم، كما تُوَفِّرُ تقنيات التّسويق الإلكتروني الفاعليّة في التّعامل فيما بين أطراف العملية التّسويقيّة والتّجاوب بمرونة مع عناصر المزيج التّسويقي(Mix-marketing)، المتمثّلة في كلّ من المنتوج الإلكتروني، والسّعر الإلكتروني، ومزيج التّرويج الإلكتروني، والتّوزيع الإلكتروني.

الفصل الثاني
المخاطر المهدّدة لأمن مواقع التّجارة الإلكترونيّة

بالرغم من الفوائد العديدة التي تتيحها تكنولوجيا الاتّصال والإعلام في تطبيقات التّجارة الإلكترونيّة، إلاّ أنّ المتخصّصين في هذا المجال يحذّرون أطراف المبادلة التّجاريّة من المخاطر غير المنتظرة التي تجوب محيط التّجارة الإلكترونيّة أو التي يمكن أن تترتّب عليها، وبالتّالي فإنّ الأخطار التي يمكن أن تعترض تطبيقات التّجارة الإلكترونيّة متعدّدة ومتنوّعة وتتزامن مع ظهور وتطوّر تقنيات الثّورة الرّقميّة، التي تستوجب تجاوز الآثار السّلبية المترتّبة على هذه الأخطار أو حتّى التّخفيف منها، في حالة ما إذا تزايدت أو اشتدّت درجة خطورتها، الشّيء الذي يتطلّب الوعي والإدراك والفهم السّليم لمخاطر شبكة الشّبكات (الإنترنت) ومعرفة دوافعها وطرق أو تقنيات تأثيرها **(المبحث الأول)**.

فرض التّطور الهائل والمتزايد في تكنولوجيا الاتّصال والإعلام تغييرات جذرية في نمط إدارة المؤسّسات الاقتصاديّة العامّة أو الخاصّة، وتحديث خدماتها المتاحة للعملاء، التي أصبحت تعتمد على أساليب وتقنيات حديثة أكثر فاعلية، في حين شهدت العمليات المصرفيّة خلال العشرية الأخيرة توسّعات كبيرة في استخدام التّكنولوجيا الرّقميّة في المجال المصرفي، وظهرت على أرض الواقع تطبيقات المصارف الإلكترونيّة، التي تناما دورها بفعل الوساطة وتزايد حركيّة التّدفقات النّقديّة والماليّة في مجالات التّجارة الإلكترونيّة والخدمات المصرفيّة، حيث أنّ ظهور المصارف الإلكترونيّة ساهم في اتساع نطاق التّهديدات الأمنيّة لمواقِع التّجارة الإلكترونيّة **(المبحث الثاني)**.

المبحث الأول

أهم مخاطر وتهديدات أمن مواقع التّجارة الإلكترونيّة

لقد ساهمت التّقنيّة العالية بشكل كبير في تغيير نمط إنجاز الأعمال على مستوى جميع الأصعدة التي أصبحت تتم بسرعة عالية وبدّقة متناهية، حيث تطوّرت طرق أو تقنيات معالجة البيانات الإلكترونيّة، وتضاعفت كميّة المعلومات المتداولة عبر شبكات الاتّصالات وبالخصوص الإنترنت، التي ساهمت بشكل كبير في تزايد معاملات التّجارة الإلكترونيّة وساعدت على انتشار المتاجر الافتراضيّة التي هيّئت البيئة الخصبة لتبادل المعلومات وإجراء الصّفقات التّجاريّة، مع دفع قيمة المشتريات بوسائل دفع حديثة مغايرة عن الوسائل التّقليديّة، غير أنّه بالمقابل تُشكل شبكة الإنترنت الوسط الملائم الذي تنمو وتسكن فيه الفيروسات ومختلف البرامج المعلوماتيّة الضّارة، التي باتت تُهدّد أمن واستقرار شبكات المعلومات ومدى موثوقية البيانات المخزّنة أو المتداولة فيها(**المطلب الأول**).

إنّ المشكلات الأمنيّة التي فرضتها شبكة الشّبكات(الإنترنت) في المعاملات الإلكترونيّة وبالخصوص محيط الأعمال، تستدعي الحاجة إلى تقييم مختلف التّهديدات والإحاطة بجميع المخاطر الخارجيّة والدّاخليّة، مع تحديد ما يُمكن السّيطرة عليها أو ما يخرج عن سيطرة هذه الأخطار مع تفّهم ووعي وحسن إدراك قيمة ما يُراد حمايته الذي يختلف باختلاف الموارد المُعرّضَة للتّهديد والغايات أو الأهداف المرجوة من تلك الحماية، كتحديد هويّة أطراف التّعامل الإلكتروني وضمان سريّة وسلامة البيانات الإلكترونيّة المتداولة عبر شبكة الإنترنت وضمان الوصول إلى المعلومات مع عدم إنكارها لدى أطراف التّعامل الإلكتروني(**المطلب الثاني**).

المطلب الأول
المخاطر المتعلّقة بمواقع التّجارة الإلكترونيّة

تختلف وسائل أو أساليب الاعتداء في بيئة الإنترنت باختلاف الأسباب المؤدّية إليه وشخصيّة مُتسبِّب الهجوم على الأنظمة المعلوماتيّة، لذا تحوّلت شبكة الإنترنت منذ نشأتها إلى وسيلة اتّصال فعّالة للعصابات والمجرمين لارتكاب مختلف الجرائم المعادية للقوانين والأعراف الاجتماعيّة والثّقافية السّائدة، فقد تتعلّق هذه الجرائم بقرصنة أسماء مواقع التّجارة الإلكترونيّة ممّا يثير تساؤلات قانونيّة حول العلاقة التي تربط هذه الأسماء بالعلامات التّجاريّة(**الفرع الأول**)، وأصعب التّهديدات التي تتعرّض لها المعلومات المُخزّنة في مواقع التّجارة الإلكترونيّة تلك المُنبثِقة من البرمجيات الخبيثة التي تتّخذ صور عديدة حسب الأهداف المُسطّرة لها(**الفرع الثاني**)، أو تلك النّاجمة عن عمليات الاختراق باستخدام برامج الاستطلاع والتّنصت(**الفرع الثالث**).

الفرع الأول
المخاطر المتعلّقة بأسماء مَواقِع الإنترنت

إنّ القرصنة الإلكترونية بمفهومها الواسع، ماهيّة إلاّ عملية دخول غير مصرّح به إلى نُظم شبكات الحاسوب لغرض المساس بسريّة وسلامة محتوى البيانات، وتعطيل قدرة وكفاءة الأنظمة للقيام بمهامها بشكل سَلِس، حيث يُمكن أن تتمحور تقنيات السّطو الإلكتروني حول الدّخول غير المشروع لنظم المعلومات، من خلال استعمال تقنيّة(DNS spoofing) أو IP) (Spoofing المنصبّة حول انتحال هويّة عنوان(IP)، أين يقوم أحد القراصنة على إثرها خداع مُستخدم معيّن يطلب عبر خادم اسم النّطاق غير المؤمّن Les paquets des serveurs DNS) (étant faiblement sécurisés، الدّخول إلى الموقِع الإلكتروني (http://www.mabanque.example.com)، حيث يَستبِق(Pirate) الأمور عن طريق اصطناع حُزَمْ مزوّرة(Fabriquer de faux paquets)، للرّد في نفس الوقت على طلب المستخدم وذلك قبل تَلَقي هذا الأخير الرّد من طرف الخادم(Serveur DNS)، حيث يدخل

المستخدم فيما بعد إلى موقع إلكتروني مُزوّر أو مُقلّد(Site d'hameçonnage) من دون علمه بذلك، أين يتحصّل المُجرِم(Hacker-cracker) من خلال هذه التّقنيّة (Usurpation d'adresse IP) على بياناته أو معلوماته السّريّة(المُستخدم) لاستخدامها لغرض تحقيق غايات غير مشروعة من دون أيّ ترخيص من صاحبها[1].

كما يمكن أن تنصّب القرصنة على نسخ مصنّفات فكرية بقصد الإضرار بأصحابها كنسخ برمجيات الحاسوب أو قواعد البيانات وتقليد الأسماء التّجاريّة والاستيلاء على العلامات التّجاريّة أو الخدمة(Cybersquattage)، حيث يمكن لأيّ شخص أن يقوم بتسجيل علامة تجاريّة أو صناعيّة محميّة كاسم موقع إنترنت لغرض الإضرار بمالكها، أو إعادة بيع اسم الموقِع إلى هذا المالك مرّة أخرى بثمنٍ غالي، أو لأحد مُنافسيه، قصد منع المالك من تسجيل العنوان الإلكتروني[2]، وبالتّالي فإنّ أغلب منازعات العلامات التّجارية مع أسماء المواقِع تتمحور حول الصّور التّالية:

1)– تسجيل علامة تجاريّة كاسم موقع لم يتّم تجديد تسجيله بعد:

إنّ المعمول به وفقا لأحكام اتّفاقيات تسجيل أسماء مواقع الإنترنت (Domain Name Registration Agreement)، أنّه يجب على الشّركة أو الشّخص المُسّجَل عليه اسم الموقع الإلكتروني أن يقوم بتجديد تسجيله، مع دفع رسوم التّسجيل سنويا للشّركة المعتمدة لتقديم خدمات تسجيل مواقع الإنترنت، ففي حالة إغفاله(ها) لتلك الإجراءات تقوم الشّركة المُسّجِلة بعد إخطار صاحب الموقع الإلكتروني بضرورة تجديد تسجيله، بمنح اسم الموقع لأيّ

---

1) **Hélie - SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 174- 180.

2) **Anthony PONCIER**, « La gestion de l'image de l'entreprise à l'ère du web 2.0 », Revue Internationale d'intelligence économique, 2009/1, Vol 1, pp. 85- 87.

Alexandre DEFOSSEZ, « Conflits entre noms de domaine et marques (renommées) : l'approche OMPI », Revue Internationale de droit économique, 2006/2 (t. XX, 2), pp. 175, 176.

شريف محمد غنام، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني(Domain Name)، مرجع سابق، ص ص 102، 103.

شخص آخر يطلب أو يستجيب لإجراءات التّسجيل المتّفق عليها مع تلك الشّركة(شركة التّسجيل)، حيث يمكنه بعد إتمام تلك الإجراءات، أن يَعْرِضَ على الشّركة التي أغفلت إجراءات تجديد تسجيل اسم موقعها الإلكتروني، بيع هذا الاسم بمبالغ ماليّة باهضة على مستوى إحدى مواقع المزاد العلني التي تبيع أسماء المواقع على شبكة الإنترنت[1].

فعادة ما يقوم أصحاب الاختصاص(Cybersquatters) بسرقة أسماء مواقع الإنترنت والاستيلاء عليها قبل إتمام إجراءات تسجيلها، مستغلّين في ذلك الثّغرات أو الفجوات المتواجدة في الأنظمة المعلوماتيّة لأصحاب الأولويّة في اختيار أسماء مواقعهم الإلكترونيّة، أو يتّم ذلك من خلال إحداث مواقع إلكترونية مزيّفة، يدّعون على أنها مكاتب تسجيل معتمدة يتبادلون على إثرها رسائل البريد الإلكتروني مع الرّاغبين في تسجيل أسماء مواقع الإنترنت.

2)– تسجيل اسم موقع إلكتروني يتضمّن على علامة تجاريّة غير مسّجلة:

بخلاف الحالة المذكورة أعلاه، فإنّ اسم الموقع المُسّجَل يحتوي على علامة تجاريّة غير مُسّجَلة التي اكتسبت فيما بعد، شهرة كبيرة بالنّسبة للسّلعة أو الخدمة التي تميّزها عن باقي السّلع والخدمات الأخرى، والجدير بالذّكر أنّ أغلب نزاعات أسماء المواقع تتعلّق بأسماء الممثّلين المشهورين التي من خلالها يتم تسجيل اسم موقع إلكتروني يحتوي على اسم ممثّلة أو ممثّل مشهور(ة) [2].

3)– تسجيل اسم موقع متطابق مع علامة تجاريّة:

يتمحور هذا النّوع من الاعتداءات حول قيام إحدى الشّركات بتسجيل علامة تجاريّة مشهورة، عائدة لإحدى الشّركات الاقتصاديّة الكبرى، لتطلب فيما بعد من هذه الأخيرة مبالغ ماليّة من أجل التّنازل عن أسماء المواقع المحتويّة لعلاماتها التّجاريّة والرّضوخ لمطالبها، لذا يُعدّ هذا النّمط من بين الاعتداءات الأكثر شيوعا وانتشارا فيما بين الشّركات المتنافسة وبالخصوص في فترة ظهور وانتشار شبكة الإنترنت، أين كانت فيه غالبيّة الشّركات المالكة

---

[1] من بين هذه المواقع نجد: http://www.greatdomains.com ou http://www.domains.com

[2] **فاتن حسين حوى**، مرجع سابق، ص ص 179، 180.

للعلامات التّجارية ترضخ لمطالب المحتالين أو المُضاربين بُغية استرجاع علاماتها التّجاريّة، المُسّجَلة كأسماء مواقِع، وذلك نظرا لفقدان سياسة موّحدة لتسوية منازعات أسماء المواقع.

انطلاقا من ذلك، فإنّ هذا النّوع من الاعتداءات لا يقتصر فقط على تسجيل أسماء المواقع العليا العامّة(gTLD)، بل يُمكن أن يمس أسماء المواقع المكوّنة من رموز الدّول(ccTLD) كتسجيل اسم الموقع الوطني لرمز دولة بريطانيا (www.harrodsonline.co.uk) المتطابق مع العلامة التّجاريّة(HARRODS)، وتسجيل اسم الموقع المُكوَّن من رموز دولة فرنسا(www.playstation.fr) المتطابق مع العلامة التّجاريّة(PLAYSTATION)، واسم الموقع المُسّجَل المكوّن من رموز دولة كندا (www.browne.co.ca) المتطابق مع العلامة التّجاريّة(BROWNE) الخ...[1].

4)– تسجيل اسم موقع متشابه مع علامة تجاريّة:

تتمثّل صورة هذا الاعتداء حول استخدام شخص ما بعض الحِيَل أثناء تسجيل اسم موقع شبيه، أو مماثل مع علامة تجاريّة مملوكة لإحدى الشّركات ولكن ليس متطابقا معها، حيث يقوم المحتال بإجراء تعديل طفيف على مستوى إحدى حروف العلامة التّجاريّة التي سيسّجلها كاسم موقع إنترنت، كقيامه بتسجيل اسم موقع(www.mi**s**rosoft.com) المتماثل مع العلامة التّجاريّة لشركة(Mi**c**rosoft)، أو القيام بتسجيل اسم موقع(www.am**m**azon.com) المماثل للعلامة التّجاريّة(amazon.com) العائدة لشركة(Amazon)، أو يقوم بتسجيل اسم موقع(wwwshell.com) مُمَاثِل مع العلامة التّجاريّة التي تملكها الشّركة العالميّة كاسم موقع(www.shell.com) الخ...[2]، ففي المثال الأوّل قام المُحْتَال بإدخال الحرف(S) بدلا من الحرف(C)، وفي المثال الثّاني قام بإضافة حرفا زائدا(m) إلى جانب الحرف(m)، أما في المثال الأخير فإنّ المُحتال لم يضف النّقطة(.) التي تفصل(www) عن(shell).

---

[1] **فاتن حسين حوى**، مرجع سابق، ص ص 166، 176.

[2] المرجع نفسه، ص 178.

الفرع الثاني
مخاطر البرمجيات الخبيثة ورسائل الاصطياد

يُعرَفُ عن البرامج الخبيثة(Malware) التي هي اختصارا لـ(Malicious Software) أو(Logiciels nuisibles)، على أنّها أيّ برنامج تكون كلّ مهامه أو جزء منه عمل غير مشروع أو خبيث(كالتّخريب أو الخداع أو الاستيلاء على الموارد الماليّة الخ...)، مُخصّصة للتّسلّل إلى أنظمة الحاسوب من دون معرفة مستخدمها[1]، ومن مميّزاتها نجد أنّها تسمح للمعتدي بِالتَّحَكُّمِ عن بُعد في أجهزة الحاسوب بشكل مخفي باستخدام وسيط(Proxy) أو أيّ برنامج خاص به(المعتدي)، وتسمح هذه البرمجيات باختراق بيانات سريّة خاصّة بالمستخدمين كأرقام البطاقات المصرفيّة الإلكترونيّة أو كلمات المرور أو المحادثات المكتوبة(الخ...) من دون علم أصحابها بذلك، كما تتميّز هذه البرامج على أنّها مُعَطِّلَة للخدمات أو مهدِّمة للبرامج والأجهزة.

فبِمجرّدِ تثبيت البرمجيات الخبيثة على أجهزة الحاسوب تَصْعُبُ جدًّا عملية إزالتها وتُسبّب أذى غير قابل للإصلاح يتطلّب في بعض الأحيان إعادة تهيئة القرص الصّلب المثبّت فيه نظام التّشغيل (Formatage d'un disque dur et la réinstallation d'un système informatique)، أو حتى استبداله بقرص صلب جديد مع تثبيت مرّةً أخرى برنامج نظام تشغيل جديد فيه[2].

تستخدم البرامج الخبيثة عادة فئة "الهاكرز" المشهورين بذوي القبّعات السّوداء (Black hat hackers) ضدّ الحكومات، والمواقع الإلكترونيّة للشّركات التّجاريّة لجمع المعلومات الحسّاسة المحميّة أو لتعطيل الخدمة أو تخريب البيانات وضياعها بشكل نهائي، غير أنّه يُمكِن أن

---

1) **Ali EL AZZOUZI**, La cybercriminalité au Maroc, Imprimé par Bishops Solutions, Casablanca, 2010, pp. 44, 45. http://www.cybercriminalite.ma

2) **يوسف حسن يوسف**، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، مصر، 2011، ص ص 99- 100، 101- 108، 113- 115.

تتعلّق دوافعهم من تطوير البرامج الخبيثة بالقرصنة أو التّجسّس الصّناعي والتّجاري، حيث تستعين بها الشّركات التّجارية أو الصّناعية لغرض سرقة أو الحصول على المعلومات السّريّة الخاصّة بالشّركة المنافسة، أو الانتقام من هذه الأخيرة للاستحواذ أو السّيطرة على مختلف الأسواق، وبالتّالي تقليص سمعتها التّجاريّة والميزة التّنافسيّة التي كانت تتمتّع بها.

كما يمكن أن تكون أهداف تطوير هذه البرامج (الخبيثة) متعلّقة بالابتزاز أو الاستيلاء على أموال مستخدمها، من خلال الحصول على أرقام بطاقات الائتمان أو حتّى أرقام الضّمان الاجتماعي، التي يتّم عادة تخزينها على مستوى مواقع الإنترنت، معتمدة فيها على الأوامر والتّعليمات المتواجدة في داخلها(البرامج الخبيثة) بطريقة خفيّة لا تثير انتباه مستخدمها، حيث تبقى ساكنة غير مُلفِتة للانتباه، ولا يتّم كَشْفُهَا إلاّ عن طريق الصُدْفَةِ، فغالبا ما تَنْتَشِرُ البرامج الخبيثة في برامج الأعمال[1].

من بين أخطر البرامج الخبيثة المعروفة حاليا نجد كلّ من الأحصنة الطّرواديّة(Chevaux de Troie) التي سُميت بهذه التّسمية نِسْبَةً إلى الحصان الخشبي الكبير الذي صنعه اليونانيون من أجل غزو مدينة طروادة، حيث اختبأ في داخله جنود اليونان واستطاعوا بعد إدخاله في الظّلام إلى تلك المدينة من اقتحام هذه الأخيرة(Troie) والتّغلّب على جيشها، وهكذا صُممت هذه البرمجيات الخبيثة وفقا لعمل هذه الآلية[2]، بوَصْفِهَا كبرامج

---

1) **Nicolle TORTELLO, Pascal LOINTIER**, op.cit., pp. 115- 126.

2) إنّ آلية الحصان الخشبي الكبير ماهية إلاّ حِيلَة مُبتكرة من طرف المُحارِب المُحنَّك أُلِيسْ(**Ulysse**) ملك جزيرة ايتاك(**Ithaque**) الواقعة في غرب اليونان على واجهة البحر الادرياتي(**Mer Ionienne**)، فبعد المحاولات الفاشلة التي قام بها جنود مملكة ايتاك لغزو مدينة طروادة المعروفة بتسمية إليون(**Ilion**)الواقعة في الشمال الغربي لتركيا **Asie**) (**mineure** على واجهة بحر إيجه(**Mer Égée**)، قام جنود الملك اليس(**Ulysse**) بِصُنْعِ حصان خشبي كبير لتقديمه أو تسليمه كهدية من طرفهم لجيش مدينة طروادة لغرض إيهام هؤلاء(**Troyens**) بالاستسلام ونهاية الحرب فعلا، وبالتالي التحايل عليهم وخداعهم من خلال السماح للجنود اليونانيون المختبئين بداخل الحصان الخشبي، بالخروج منه في الليل والتسلّل بكلّ سهولة إلى داخل مدينة طروادة عند إدخال ذلك الحصان من طرف الجنود الطرواديين، وهكذا تم إدخال الحصان الخشبي الكبير إلى داخل المدينة حيث استطاع الجنود اليونانيون المختبئين في داخله من الخروج في الظلام وقضوا على جميع حُرّاس مدينة طروادة وقاموا بفتح أبوابها للسماح للجنود اليونانيين بالدخول وغزو المدينة أين قاموا بحرقها وتدميرها وقتل وتشريد أهاليها، وهكذا استطاع الملك اليس(**Ulysse**) من خلال حيلة أو خُدعة الحصان الخشبي

مُخادِعة تَظهر في ظَاهِرها كبرامج عادية تُؤدّي بعض المهام المألوفة والمفيدة لمُستخدمِه، غير أنّ باطنها يخفي هدف خبيث غير مشروع، ألا وَهُوَ تحقيق غرض حقيقي من وراء تشغيله، فعادة ما تأتي هذه البرمجيات الخبيثة مع الرّسائل الإلكترونيّة المُرفق معها ملفات قابلة للتّشغيل حيث تؤدّي مهامها بمُجرّد فتح هذه الملفات، أو تأتي عند تحميل البرمجيات المُتاحة بصفة مجّانيّة عبر شبكة الإنترنت[1].

أما برامج الدّودة(Les Vers)، فهي تُصيب أجهزة الحواسيب المُوصلَة بشبكة الإنترنت بشكل أوتوماتيكي من دون تدّخل الإنسان، ممّا يجعلها تنتشر بكثرة كالبكتيريا من حاسوب إلى آخر، مُغطية شبكة بأكملها لغرض التّخريب الفّعلي للملفات والبرامج ونظم التّشغيل وبروتوكولات الاتّصال، حيث تختلف آلية عمل برامج الدودة من نوع لآخر، فبعضها يقوم بالتّناسخ داخل الجهاز إلى أعداد هائلة، بينما نجد البّعض الآخر من هذه الدّيدان تنتشر بصفة عشوائيّة من خلال إرسال نفسها عبر رسائل البريد الإلكتروني المُفّخخة، التي عادة ما تكون عناوين هذه الرسائل جذّاباً كدعوة لمُشاهدة صور أحد المشاهير أو انتحال صفة أو صلاحيات أحد الأشخاص أو المسؤولين في شركة أو هيئة معيّنة الخ...[2].

الكبير، من وضع حدّ أو نهاية لحرب شرسة دامت عشرة(10) سنوات بين اليونانيين(**Les Grecs**) والطرواديين (**Les Troyens**). للمزيد من المعلومات أنظر المواقع الإلكترونية التالية: https://fr.m.wikipedia.org/wiki/cheval_de_troie ou http://www.h-equestrianpassion.com/fr/la-legende-du-cheval-de-troie-on-dit-que-le-cheval-est-la-plus-noble-conquete-de-lhomme(consultés le 10/06/2018)

[1] **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي(النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص ص 531- 533.

محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص ص 101، 102.

محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص ص 238، 239.

سوسن زهير المهتدى، تكنولوجيا الحكومة الإلكترونية، دار أسامة للنشر والتوزيع، الأردن، عمان، 2011، ص ص 410، 411.

Philippe le TOURNEAU, op.cit., pp. 340, 355, 356.

[2] **سوسن زهير المهتدى**، مرجع سابق، ص ص 407– 410.

إلى جانب برامج أحصنة طروادة والدّيدان، يوجد نوع آخر من البرمجيات الخبيثة والمُتمثّل في القنابل الموقوتة أو المنطقيّة(Bombes logiques/ à retardement)، المُصمَّمة لكي تبقى ساكنة وغير فعّالة أو مُكتَشفَة لمدّة تصل من أشهر إلى سنوات، حيث تبدأ هذه البرامج من مباشرة مهامها الهدّامة بمُجرّد حُلول المدّة أو تحقيق شروط منطقيّة حُدّدت أو مصمّمة من قَبْلِ[1].

انطلاقا من ذلك، تعتمد البرمجيات الخبيثة على أساليب الاختفاء من خلال الاستعانة على مجموعة من البرامج الخاصّة التي تساعدها على تنفيذ مهامها بمجرد تنصيبها على جهاز الحاسوب المُستهدف ومن دون علم مُستخدِمه، وذلك على غرار برامج الرّوتكيت(RootKit) أو (Outil de dissimulation d'activité ou Maliciel furtif) التي تؤمّن الإخفاء من خلال تعديل ملفات النّظام المُضيف، ومنع ظهور البرنامج الخبيث ضمن قائمة البرامج التي تعمل مع تفادي قراءة ملفاته[2].

والمُلفت للانتباه، أنّ تقنيّة "الرّوتكيت" تُخَبِّئُ كذلك للبرنامج الخبيث راصد لوحة المفاتيح مع الأبواب الخفيّة(Backdoors) أو (Portes dérobées)، التي يتم الاستعانة بها كأسلوب لتمرير إجراءات تبدو كأنّها عادية وشرعيّة، من خلال فتح مَنْفَذْ سرّي للتّمرير الخفي في

---

[1] **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص 534.

محمد أمين أحمد الشوابكة، مرجع سابق، ص ص 239– 242.

محمود أحمد عبابنة، محمد معمر الرازقي، مرجع سابق، ص ص 103، 104.

غسان قاسم داود اللامي، أميرة شكرولي البياتي، مرجع سابق، ص ص 216– 219.

عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص ص 321– 323.

[2] لمزيد من المعلومات أنظر الموقع التالي:

http://techgenix.com/hidden_backdoors_trojan_horses_and_rootkit_tools_in_a_windows_environment/ (consulté le 04/07/2016)

Voir aussi : **Dmitry KOROLEV, Yuri GUBANOV, Oleg AFONIN**, « Comprendre RootKits : Utilisation de l'analyse de vidage de mémoire pour la détection des RootKits », article publié le 22 novembre 2013 à partir de l'adresse suivante: https://articles.forensicfocus.com/2013/11/22/understanding-rootkits/, consulté le 10/11/2016.

المستقبل في أنظمة شبكة الحواسيب المستهدفة عبر شبكة الإنترنت، فالباب الخفي يكون إمّا في هيئة برنامج منفصل أو كلمات سريّة افتراضيّة أو أيّ جهاز يتم تركيبه بشكل سرّي من خلال استغلال ثغرات نظم الحماية وتجاوز الإجراءات الأمنيّة القائمة[1].

وعليه، فإنّ برامج "الرّوتكيت(RootKit)" يتم إعدادها وكتابتها من طرف مبرمجين محترفين ذوي خبرات وكفاءات عالية في مجال أمن المعلومات، بغية إلحاق الضّرر بحاسوب أو حواسيب معيّنة، أو السّيطرة عليها وجعلها كقاعدة أساسية لتنفيذ مختلف الهجمات الإلكترونيّة، أو سرقة البيانات الإلكترونيّة الحسّاسة التي تحويها الخ...، حيث تعتبر مرحلة تثبيت "الرّوتكيت" في نظام تشغيل الجهاز المستهدف كأولى الخطوات التي يعتمد عليها القراصنة المحترفون(Crackers) أو المخادعون(Fraudeurs) أو الجواسيس(Espions)، وذلك بعد اكتشافهم واستغلالهم لبعض الثّغرات أو الهفوات الأمنيّة المتواجدة في النّظام الأمني لجهاز الحاسوب المُستهدف، كالحصول على كلمات مرور ضعيفة أو تواجد ثغرات في برمجيات الحماية من الفيروسات...الخ.

---

[1] تجدر الإشارة في هذا الشأن، أنّ وكالة الأمن القومي الأمريكية(NSA) قامت في إطار نظام الرقابة المكثفة على الإنترنت، بدفع مبلغ عشرة(10) مليون دولار أمريكي لشركة("**RSA Security**" باعتبارها كشركة فرعية(ابتداء من 2006) للشركة العملاقة(EMC) المختصة في مجال المعلوماتية وحفظ البيانات الإلكترونية، حيث تم إنشاء هذه الشركة(RSA Security) في عام 1982 على يد كلّ من (Ronald Rivest, Adi Shamir et Leonard Adleman، مُكتشفي نظام التشفير اللاتماثلي بالمفتاح العام(RSA))، التي تُقدّم الحلول الأمنية للشركات إذ تعبر حاليا الرائدة في سوق الأمن المعلوماتي، وذلك بغية إقدام هذه الشركة(**RSA Security**) على ترك منافذ أو أبواب خفيّة(Portes dérobées) في بعض برمجيات الحماية الأمنية التي تسمح لأعوان الوكالة(NSA)، القيام بعمليات الاختراق والحصول على البيانات الإلكترونية المشفرة بكلّ سهولة ومن دون أي عناء، حيث أقدمت شركة الأمن المعلوماتي(**RSA Security**) من 2004 إلى 2013 على إتاحة برنامج(BSafe) لخبراء الوكالة(NSA) لغرض النفاذ إلى البيانات الإلكترونية المشفرة للمستعملين والاستحواذ عليها، الشيء الذي أدّى بهؤلاء(العملاء أو المستخدمين) إلى فقدان المصداقية والثقة في برمجيات الحماية الأمنية المُتاحة من طرف هذه الشركة(**RSA Security**).

Laurent BLOCH, « surveillance américaine sur l'Internet », pp. 08, 09. Article disponible à partir de l'adresse : http://www.diploweb.com/Surveillance-americaine-sur-l.html, consulté le 02/10/2017.

حيث يُستخدم "الرّوتكيت" كوسيط أو واجهة خفيّة بين النّظام المستهدف والشّخص المهاجم، إذ يحتوي على عِدَّةِ عناصر نادرا ما تكون برامج قائمة بحدّ ذاتها، والتي تقوم بتغيير أو تعديل بعض هياكل نظام التّشغيل المُستهدف بطريقة سريّة، وجعلها تتجاوب وتتأقلم مع الأوامر الجديدة التي تُوَجِّهُهَا "الرّوتكيت" من دون لَفْتِ اِنتباه مستخدم الحاسوب(الضّحيّة) لذلك.

تجدر الإشارة في هذا السّياق، أنّ "الرّوتكيت(RootKit)" يتم تزويدها بِوِحْدَةِ حماية تُصعِّب أو تُعقِّد من مهام أو عمليات اكتشاف البرنامج الخبيث المصحوبة به، وتجعل جذور تعليماته الباطنيّة مخفيةً وثابتة وفي حالة نشاط دائم ومُسْتَمِرْ من دون انقطاع حتّى في حالة إعادة تشغيل نظام الحاسوب المُستهدَف، أو إعادة تثبيت نظام تشغيله مرّة أخرى في حالة اكتشافها بمجرّد الصدفة، وهذا يعني أنّ "الرّوتكيت" مزوّد بتقنيات أو قدرات أكثر مُقاوَمة في حالة كشفها حيث يُمكنِها أن تُهَدِّدَ المُستخدِم بتنفيذ هجمات أو عمليات خطيرة من بينها تكسير نظام عمل جهاز البيوس(Système BIOS) من لوحة الأم(Carte mère)[1] الخ...،

[1)] Mot **Anglais** : « **B**asic **I**nput **O**utput **S**ystem (**BIOS**) », **en français** : « système élémentaire d'entrée/sortie », est un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations élémentaires lors de sa mise sous tension, le terme(**BIOS**) est souvent utilisé pour décrire l'ensemble du micrologiciel de la carte mère. Cependant, dans la pratique, les systèmes d'exploitation modernes n'utilisent ces services(**BIOS**) que lors de l'amorçage ; ils utilisent ensuite soit leurs propres pilotes, soit les fonctions ACPI pour les opérations liées à la **carte mère**. Le **BIOS** est presque toujours développé par le **fabricant de la carte mère** à partir d'un code de référence fourni par un constructeur de BIOS (tel que AMI ou Phoenix Technologies), car il contient les paramètres spécifiques à l'initialisation de la carte mère, tels que la configuration des ports GPIO.
En effet le **BIOS** a un rôle essentiel pour le fonctionnement de la **carte mère** : - il initialise tous les composants de la carte mère, du chipset et de certains périphériques ; - il identifie tous les périphériques internes et externes qui lui sont connectés ; - si cela n'a pas déjà été fait il initialise l'ordre de priorité des périphériques d'entrée ; et il démarre le système d'exploitation présent sur le premier périphérique disponible.
Le **BIOS** est parfois appelé **firmware** lancé au démarrage, car il peut être la cible de **logiciels malveillants**, en 1999 le BIOS a connu sa première attaque d'envergure avec la propagation du virus **CIH** qui était très agressif puisqu'il effaçait l'intégralité du contenu des disques, et depuis que les mises à jour du BIOS « **Flasher le BIOS** » peuvent être réalisées à la volée via le programmateur interne de la carte mère, il est possible que ceux-ci soient la cible d'attaques de type homme du milieu.

الأمر الذي يستوجب ترك أجهزة الحواسيب المستهدفة واستبدالها بمعدّات وأجهزة حديثة مع تثبيت أنظمة تشغيلها من جديد، وعليه لا جَدْوَى أو نَفْعَ لمُضادات الفيروسات في أنظمة تشغيل(Windows) مع تقنيات "الرّوتكيت"(RootKit)، نظرا لِبِنْيَتِهَا ومِيزَتِهَا الخاصّة في الاختفاء، وما بَالُك ما إذا كانت قد دخلت مُسبقا إلى العديد من أجهزة الحواسيب، لذا فمن بين الأمور الأولى التي يجب مُراقبتها وتحديثها إلى جانب "مُضادّات الفيروسات الخاصّة بكشف وحذف الرّوتكيت(RootKit)" على غرار برنامج(TDSSKiller) الذي تّم تطويره من طرف شركة الأمن المعلوماتي الرّوسيّة(Kaspersky)، نجد الإعداد المُحكَم والدّقيق للجدران النّارية(Pare-feux) [1].

بالإضافة إلى ما سبق، فإنّ عدوى البرامج الخبيثة تنتقل من حاسوب مُصاب إلى حاسوب آخر سليم، بواسطة وسائط تخزين التي تُنْقِل الملفات والبرامج، كوِحدة التّخزين الخارجي(Flash Disk) وبطاقة الذّاكرة(Carte mémoire) الخ...، فعادة ما تنتقل البرامج الخبيثة ضمن برامج معلوماتيّة يتم تحميلها عبر شبكة الإنترنت باستخدام تقنيّة(Downloading)، أو عبر تقنيّة البريد الإلكتروني الذي يُعتبر من النّواقل الأكثر أهمّية في نقل هذه البرامج(الخبيثة) حيث تتخذ الرّسائل النّاقلة للبرامج الخبيثة عدّة أشكال، فقد تنتقل(البرامج الخبيثة) ضمن مُرْفَقَات(Attachements) لرسائل إلكترونيّة خادعة أو كاذبة((Hoax(Rumeur)[2] مبعوثة لأشخاص مستهدفة، حيث يقوم ذلك البرنامج بمهامه

Voir: **Sylvain CROUZET**, « Le BIOS - flashage et procédures de récupération », pp.4- 16. Article disponible à partir de l'adresse suivante: http://crouzet.sylvain.free.fr/files/flashbios.pdf, consultée le 12/12/2017.

[1] لمزيد من المعلومات حول الموضوع، أنظر المواقع الإلكترونية التالية:
https://www.information-security.fr/mais-cest-quoi-un-rootkit ou
http://www.valencynetworks.com/articles/rootkits-2.html / (consultés le 10/10/2017)

[2] لمعرفة المزيد عن البلاغات الكاذبة أنظر الموقع الإلكتروني التالي:
http://www.f-secure.com/virus-info/hoax/ ou http://www.hoaxbuster.com (consultés le 10/07/2018)

الإيجابية بمجرّد فتحه أو الإطّلاع على محتواه[1]، وفي نفس الوقت تُصاب أجهزة الكمبيوتر المملوكة لهؤلاء الأشخاص الذين يدّعون بأنّ ذلك البرنامج يؤدّي لهم منفعة أو فائدة معيّنة.

انطلاقا من ذلك، يُمكن لشركة تجارية معيّنة أن تستعين بمختصين لإرسال رسالة اصطياد خادعة(Phishing Scam) أو(Hameçonnage ou Filoutage) إلى شركة منافسة لها، تدّعي من خلالها(الرّسالة الإلكترونيّة) على أنّها مُرسلة بجميع المواصفات من طرف شركة(Microsoft)، التي تحثّها على ضرورة تحديث نظام تشغيل حواسيبها باستخدام رابط مُزيَّف لشركة "ميكروسوفت" لسدّ إحدى الثّغرات الأمنيّة المتواجدة في نظام التّشغيل القديم، فبمجرّد الضّغط على هذا الرّابط تتّم عملية تحديث(Mise à jour) نظام التّشغيل القديم ويبدأ برنامج التّشغيل الجديد من أداء مهامه المخفية أو الباطنيّة من دون علم الشّركة المُستهدَفة بذلك، حيث يبقى هذا البرنامج الخبيث مُتخفّيا حتّى عن برامج مكافحة الفيروسات ويُعطِّل برامج جدران الحماية ليُجرِّد فيما بعد أجهزة حاسوب الشّركة المنافسة من أية حماية ضدّ الهجمات التي يشنّها مستقبلا البرنامج الخبيث.

لذا تعتبر رسائل الاصطياد الخادعة(Phishing Scam)[2] من بين طرق الاحتيال المُستحدثة الأكثر تَفنُّنًا وإتقانا من طرف مرتكبي الجرائم المصرفيّة، إذ تبدو بالشّكل والعنوان البريدي على أنّها مُرسلة من طرف هيئة مصرفيّة حقيقيّة، حيث تُوهِم عملائها بتواجد تحديثا للبيانات أو تفيدهم بإجراءات جديدة للحماية والأمن، وتطلب منهم الدّخول مباشرة إلى المَوْقِع

---

[1] **Ivan VASSILEFF, Gérard HAAS**, « Délinquance numérique : L'attaque des STAD par les données », Revue Legicom, 1996/2, n° 12, pp. 44, 45.

[2] Le **phishing** ou **hameçonnage** est une **arnaque** consistant à envoyer un e-mail vous demandant de communiquer d'urgence des **données personnelles** : mot de passe, numéro de compte bancaire ou de carte bleue. Les organismes dont on usurpe l'identité peuvent être : une banque, - un fournisseur d'accès, - une compagnie d'électricité ou de téléphone, - une administration. Soyez donc vigilant et ne répondez jamais à ce type d'e-mail : ne cliquez pas sur le lien proposé et détruisez cet e-mail dès réception. Attention ! « Jamais votre banque, votre fournisseur d'accès ou d'autres organismes ne vous enverront d'e-mails pour vous demander des informations confidentielles sur votre compte ou votre carte bancaire… » - Pour avoir plus d'informations sur le sujet veuillez consulter le site : http://www.antiphishing.org, consulté le 04/11/2018.

الوهمي للمصرف عن طريق الرّابط(Lien hypertexte) المُزوَّد مع الرّسالة للتّأكد من أنّ برنامج متصفّح الإنترنت المعمول به مُتوافق مع التّحديثات الجديدة، وعند تصفّحهم لذلك الموقع الوهمي الذي يبدو بشكله وتصميمه وعنوانه كالموقع الأصلي أو الحقيقي للمصرف، يُطلب منهم تقديم بياناتهم الخاصّة ككلمات المرور أو معلومات سريّة عن بطاقات الائتمان[1] الخ...، وبعد الحصول على تلك المعلومات الثّمينة، يُخبر العملاء بأنّ برنامج التّصفّح متوافق مع الخدمات الجديدة، ثم يُحِيلُهُمْ فيما بَعْدْ إلى المَوقِع الحقيقي للمصرف حتّى لا تُثار شكوكهم وكأنّ شيئا لم يحدث[2]، لذا تُعد تقنيّة(Pharming) من بين تقنيات رسائل الاصطياد الخادعة الأكثر استعمالا في هذا المجال.

بالإضافة إلى ما سبق، يمكن أن تُسْتَخْدَمَ أساليب الهندسة الاجتماعيّة (Social engeneering) المعروفة، كالهاتف ورسائل البريد الالكتروني الخ...[3]، التي من خلالها يقوم المُحتال بإرساء علاقة الثّقة مع المستخدم في الشّركة حيث يستخدم تقنيّة الرّسائل الخادعة عبر الهاتف المحمول على غرار تقنيّة(Smishing)، التي تنطوي حول تلقّي صاحب الهاتف لرسالة إلكترونيّة(SMS) من متعامل هاتف نقّال يؤكّد رسميا اشتراكه في إحدى الخدمات مع استفادته من تعبئة يوميّة لرصيده، إذا لم يقم بإلغاء طلبه على مستوى الموقع الإلكتروني للشّركة، أو يقوم بإلقاء مكالمة هاتفيّة منتحلا صورة المدير إلى أحد المستخدمين في الشّركة بغية الحصول على الرّقم السّري أو رقم الهاتف الذي يسمح بالدّخول إلى النّظام المعلوماتي الدّاخلي للشّركة، الخ...[4].

---

1) **Armel BENARAB**, Commerce & Internet : comprendre les règles juridiques, L'Harmattan, Paris, 2013, pp. 79, 80.

2) أنظر **الملحق رقم (20)**، ص 495.

3) **طارق عفيفي صادق أحمد**، الجرائم الإلكترونية، جرائم الهاتف المحمول(دراسة مقارنة بين القانون المصري والإماراتي والنظام السوري)، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2015، ص ص 99، 100، 101، 104، 105، 108، 113، 131.

4) **Zouheir TRABELSI, Henri LY**, La sécurité sur Internet, Lavoisier, Paris, 2005, p. 88.

كما يمكن للمحتال أن يستعمل تقنيّة(Spear-phishing) أو(Harponnage) التي من خلالها يقوم بإرسال رسالة إلكترونيّة خادعة إلى أحد المُوظّفين في شركة معيّنة، حيث يتظاهر في متنها على أنّه زميل له في الخدمة أو رئيسه الإداري الأعلى، أو مدير الشّركة لغرض الحصول على الأرقام السّريّة وأسماء المستخدمين الأعضاء للتّسلّل أو اختراق نظام معلومات الشّركة المستهدفة، وهكذا يظل العملاء أو المستخدمين في قطاعات الاتّصالات والمصرفيّة الأكثر عرضة أو استهدافا لمخاطر أو هجمات رسائل الاصطياد الخادعة[1].

تجدر الإشارة إلى أنّ تقنيّة الرّسائل المُزعجة(Spam) عادة ما يعتمد عليها القراصنة المحترفين لنشر فيروس خبيث يسمح بتكوين شبكة الرّوبوت العملاقة(Botnet)[2] (المشتقة من كلمة(Robot Network) أو(« robot » et « réseau »))، لغرض استقطاب واختراق أكبر عدد مُمكِن من الأجهزة لغرض السّيطرة عليها والتّحكّم فيها عن بُعد بمجرّد انخراطها في تلك الشّبكة(Botnet)، حيث يسعى مُنفِّذ الهجمة بطريقة مباشرة إلى استعمال تقنيّة المسح(Scanning)، من خلال إرسال رسائل إلكترونيّة قصيرة لجهاز الضّحيّة لمعرفة إمكانية

---

1) **Didier GOBERT, Francis DERYCKERE, Paul CAMBIE**, « Le « spamming » en 24 questions & réponses », pp. 04, 05, 07, 08, 25, 26. Article publié en Janvier 2005 sur le site: https://www.droit-technologie.org, consulté le 02/09/2018.
Ali EL AZZOUZI, op.cit., pp. 48- 50.

2) - (Mot anglais (**botnet**), contraction de « robot » et « réseau » en français) : est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches, **historiquement**, un botnet désignait des réseaux de **robots IRC(Internet Relay Chat)**. Le sens de botnet s'est étendu aux réseaux de **machines zombies**, utilisés pour des usages **malveillants**, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).
La caractéristique principale des botnets est la mise en commun de plusieurs machines distinctes, parfois très nombreuses, ce qui rend l'activité souhaitée plus efficace (puisqu'on a la possibilité d'utiliser beaucoup de ressources) mais également plus difficile à stopper.
Une fois le **botnet** installé et déclaré, la **machine zombie(infectée)** peut désormais être contrôlée à distance par une, ou plusieurs machine tierce, et obéir aux ordres qui lui sont donnés pour accomplir les actions voulues par l'attaquant(avec, au besoin, l'installation d'outils complémentaires via une mise à jour distante): - Envoi de spam ; - Attaques réseau ; - Participation au service de serveur DNS dynamique, ou DDNS (fast flux) ; - Utilisation des ressources systèmes pour du calcul distribué (cassage de mot de passe), etc. http://www.shadowserver.org/wiki/pmwiki.php/Stats/ BotnetCharts, consulté le 05/12/2018.

تواجد ثغرة أو هفوة يمكن استغلالها للسّيطرة على الجهاز وتحميل برامج التّحكّم، أو يقوم بطريقة غير مباشرة على استدراج الضّحيّة لتحميل فيروس أو برامج خبيثة عن طريق الضّغط على الرّابط الذي وضعه البوت(Bot Master)[1].

وعليه، تعتبر شبكة "البوتنت"(Botnet) من أخطر التّهديدات الأمنيّة التي تُواجِهُها الشّركات والدّول حاليًّا[2]، حيث باستطاعته(Botnet) التّجسّس على الضّحيّة وإرسال رسائل

---

1) **Yashashree GUND, Ravikant TIWARI et Christiaan BEEK**, « Mirai, le botnet de l'Internet des objets », pp. 18-22. Rapport McAfee Labs sur le paysage des menaces, avril 2017, disponible sur le site : https://www.mcafee.com/fr, consulté le 29/01/2018.

2) يعتبر برنامج زوس(**Zeus**) من البرامج الخبيثة المُعدَّة لسرقة البيانات أو المعلومات المصرفية معتمدا في هجماته على لوحة المفاتيح(Keylogger) ومتصفح الموقِع الالكتروني(Browser)، إذ ينتقل هذا البرنامج بمجرد القيام بزيارة بسيطة لمَوقِع إلكتروني مُصاب أو الضغط على رابط الرسالة الخادعة أو الكاذبة(Phishing) المُرسلة عبر إحدى شبكات التواصل الاجتماعي وبالخصوص(Facebook)، ويستهدف البرنامج الخبيث أجهزة الحاسوب التي تستعمل أنظمة تشغيل وندوز(Windows) فقط دون غيرها(Mac OS et Linux)، حيث انتشر البرنامج الخبيث(**Zeus**) في حوالي 196 دولة من العالم وبالخصوص كوريا الشمالية، مصر، الولايات المتحدة الأمريكية، المكسيك، المملكة العربية السعودية وتركيا، ومسّ حوالي 2411 شركة ومنظمة من العالم باستخدام شبكة البوتنت(Botnets de Zeus) التي تضم العديد من أجهزة الحواسيب المُصابة بعدوى فيروس زوس(**Zeus**)، فحوالي 3,6 مليون جهاز حاسوب مُصاب في الولايات المتحدة الأمريكية وحوالي 1,5 مليون رسالة خادعة أو كاذبة، تم إرسالها عبر شبكة الفايس بوك(Facebook) و9 مليون رسالة إلكترونية خادعة تم إرسالها باسم شركة الاتصالات(Verizon Wireless)، لهدف نشر البرنامج الخبيث عبر العديد من أجهزة الحواسيب، وحتى الهواتف الذكية(Les téléphones BlackBerry et ceux utilisant Android)، حيث يُمكن للقراصنة أن يقوموا بتعديلات في هيئة البرنامج الخبيث لهدف سرقة بعض المعلومات أو البيانات المهمة أو الضرورية لهم، كتغيير العناوين المتعلقة بحسابات شبكات التواصل الاجتماعي (Facebook, Yahoo, Hi5, Metroflog, Sonico et Netlog.) أو البريد الالكتروني أو الحسابات المصرفية، كما أن البرنامج الخبيث(**Zeus**) تم تزويده بتقنيات الإختفاء عالية المستوى تُصعّب عملية كشفه حتى من قِبَلِ البرامج المُضادة للفيروسات التي تم تحديثها(Antivirus à jour)، ففي أكتوبر 2010 توصّل مكتب التحقيقات الفيدرالية الأمريكية(FBI) إلى تفكيك شبكة إجرامية دولية في مجال القرصنة الالكترونية مُنحدرين في كلّ من أوروبا الشرقية(90 منهم مُقيمين بالولايات المتحدة الأمريكية) والمملكة البريطانية وأوكرانيا، حيث استعملوا برنامج زوس(**Zeus**) الخبيث في اختراق العديد من أجهزة الحواسيب لسرقة البيانات السرية للبطاقات المصرفية(Les mots de passe, numéros et autres données bancaires) وارتكاب جرائم تبيض الأموال، فحوالي 70 مليون دولار من الأموال سُرقت في الولايات المتحدة الأمريكية. لمزيد من المعلومات حول البرنامج الخبيث زوس(Zeus) أنظر الموقع الالكتروني التالي: https://www.kaspersky.fr/resource-center/zeus-trojan-malware (consulté le 10/10/2018)

اصطياد خادعة(Phishing) لإبرام صفقات تجاريّة غير مشروعة، من خلال سرقة المعلومات السّرية لبطاقات الائتمان وإعادة بيعها فيما بعد لأصحابها بأثمانٍ زهيدة[1]، ويمكنه أيضا أن يَأْمُرَ الجهاز بإرسال المعلومات التي يرغب الحصول عليها أو يُغيّر الرّقم السّري لذلك الجهاز، بعد الحصول عليه بسُرعة عبر تقنيّة(Le Brute Forcing)، والإطّلاع بشكل تّام على كلّ ما يفعله الشّخص الضّحيّة على جهازه مع أخذ صورا له وما يُعْرَضُ على شاشة جهازه من دون علمه بذلك، والغريب كذلك أنّه يُمكِن "للبوتنت(Botnet)" أن يَأْمُرَ الأجهزة التّابعة له أو التي هي تحت سيطرته، بإرسال قدرٍ كبير من المعلومات إلى خادم(Serveur) مَوقِع إنترنت الجهة المُستهدفة، لغرض حجب أو منع الخدمة التي يقدّمها ذلك الموقِع الإلكتروني((Distributed Denial-of-service(DDoS)[2]، فمثلا يُمكن لأحد القراصنة المُقيم بالولايات المُتّحدة الأمريكيّة أن يَسْتَعِينَ بشبكة البوتنت(Botnet)، التي تضّم حوالي أكثر من خمسين ألف(50000) جهاز حاسوب مُتمركِز في الجزائر أو في أيّ بلد آخر، لتنفيذ هجمات منع أو حجب الخدمة(DDoS) على أحد الخوادم الرّئيسيّة لأسماء النّطاقات، ممّا يؤدّي إلى انقطاع خدماتها لعدّة ساعات أو أسابيع الخ...

لضمان ديمومة واستمراريّة خدمات البوتنت(Botnet) وجعله أكثر مقاومةً لعمليات الكّشف، يسعى منّفذي الهجمات الإلكترونية إلى إتاحة إمكانية تثبيت برامج "الرّوتكيت" التي تسمح بأداء مهامه في خِفية وسريّة تامّتين، أو يقوم بذّاته(البوتنت) بتعديل أو تغيير مُكوّنات نظام التّشغيل من خلال تعطيل برامج الحماية الأمنيّة وتغيير القواعد السّارية المفعول مع استغلال الهفوات والثّغرات الأمنيّة، المُتواجِدة أو حتى حذف وإلغاء البرامج الخبيثة التي تُعرقل حسن سير مهامه في جهاز الحاسوب المُصاب.

Voir aussi : **Louis ADAM**, « Le FBI lance l'offensive contre le malware Game over Zeus », article publié le 04 juin 2014 sur : http://www.zdnet.fr/actualités/ Le-FBI-lance-l-offensive-contre-le-malware-Gameover-Zeus -39801981.htm, consulté le 09/09/2017.

[1] أنظر **الملحق رقم (21)**، ص ص 496، 497.

[2] **Dominique BOULLIER**, « Avec Internet, un monde commun…mais pluriel. », Questions Internationales, N° 47- Janvier- février 2011, pp. 32, 33.

بالإضافة إلى تقنيات رسائل الاصطياد الخادعة المستعملة في تنفيذ الهجمات الإلكترونيّة، يمكن لمجموعة من العصابات أن تقوم بصنع ونشر برامج ديدان الحاسوب((Vers) ou (Worms)) في شبكة الإنترنت، بغية القيام بأعمال تدميرية، أو سرقة البيانات الخاصّة للمستخدمين أثناء تصفحهم للإنترنت وإلحاقهم الضّرر، حيث تمتاز هذه الدّيدان باستقلاليتها، وعدم اعتمادها على برامج أخرى تلتحق بها، ممّا يعطيها الحرّية الكاملة للانتشار بشكل سريع وأوسع مع قدرتها على المراوغة والتّناسخ فيما بينها داخل الجهاز إلى أعداد هائلة من دون تدّخل الإنسان[1]، إذْ تقوم باستهلاك موارد الجهاز واستخدام ذاكرته بشكل فضيع على نحو يؤدّي إلى بطء في حركة الاتّصال به، وبالتالي فإنّ خطورة الدّيدان تختلف في عملها بحسب نوع إلى آخر، فقد تكون مُرفقة في محتوى الرّسالة الإلكترونيّة(Vers de courrier électronique- Vers de messagerie instantanée) التي تتطلّب من المستخدم القيام بفتح الملف المرفق لكي تُصيب جهازه أو تقوم بنسخ نفسها في القنوات باستعمال روابط خارجيّة أو تضع نفسها (Vers de réseaux de partage de fichiers- Vers IRC) في مجلّدات أو ملفات المشاركة لكي تنتشر في أجهزة المستخدمين في حالة تحميل تلك الملفات[2].

كما يمكن للدّيدان(Vers Internet- Vers de réseau) أن تنتشر عبر بروتوكولات عناوين الإنترنت(IP) التّابعة لإحدى الشّركات التّجاريّة أو المصرفيّة، بغية إضعاف سرعة نقل البيانات الإلكترونيّة عبر مواقعها الإلكترونيّة وتعطيل خدماتها المتاحة، كتعطيل شبكات الصّراف الآلي أو إبطاء أنظمة التّحكّم في خطوط النّقل عبر السّكك الحديديّة أو النّقل البّحري أو الجّوي ممّا يؤدّي إلى إلغاء بعض أو جميع الرّحلات، والأدهى من ذلك أنه يمكن لهذه الدّيدان أن تنتقل بسرعة فائقة إلى الشّبكات الدّاخليّة لمحطّات الطّاقة النّوويّة، لغرض

---

1) **Dominique BOULLIER** , op.cit. , pp. 32, 33.

عايد رجا الخلايلة، المسئولية التقصيرية الإلكترونية: المسئولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص ص 112، 113.

2) **Dominique BOULLIER**, op.cit. pp. 32, 33.

تعطيل شبكات الحاسوب المركزيّة المسئولة عن مراقبة حالة المفاعلات النّوويّة (Réacteurs nucléaires) لهذه المحطّات، حتّى ولو لم تتّصل الشّبكات الدّاخليّة بشبكة الإنترنت[1].

---

[1] تعتبر دودة حاسوب ستوكسنت(**Stuxnet**) من بين البرامج الخبيثة المعقدة العالية المستوى التي تُصيب نظم تشغيل(Windows) والمُعَدّة خصّيصًا لمهاجمة أنظمة التَّحكُم الصناعية (**SCADA**(Supervision Control Data ((Acquisition، التي صممتها شركة(Siemens) الألمانية لمُراقبة الوحدات الصناعية التي تعمل بطريقة آلية، كتنظيم حركة السير وخطوط الأنابيب وإدارة المفاعلات النووية إلى غيرها من الاستخدامات المتعدّدة، حيث ينتشر البرنامج بسرعة عن طريق الإنترنت أو بواسطة أجهزة التخزين المحمولة(Clefs USB et autres disques durs portables) للإضرار بالشبكات الداخلية المغلقة، وعليه يقوم البرنامج الخبيث(Stuxnet) بشكل محدّد بدقة بعد اختراق أجهزة الحاسوب بعملية التفتيش للبحث عن علامة تجارية لأنظمة صنعتها الشركة الألمانية(Siemens)، فبمجرد العثور عليها يقوم البرنامج بتفعيل نفسه ويبدأ بالعمل على تجسّس وتخريب وتدمير المنشأة الصناعية المُستهدفة، من خلال إعادة برمجة أنظمة التحكّم المنطقي القابلة للبرمجة(API) مع إخفاء التغييرات التي قام بتنفيذها، أمّا إذا لم يجد البرنامج الخبيث تلك العلامة فيترك الحاسوب يؤدي مهامه بشكلٍ عادي، وعليه تم اكتشاف نوع من دودة(Stuxnet) لأول مرّة بصيغة فيروس(RootkitTmphider) من طرف شركة الأمن الرقمي(VirusBlokAda)(يوجد مقرها في روسيا البيضاء(Biélorussie))، الذي استغل(الفيروس) الثغرات الأمنية المتواجدة في ملفات(LNK)، ومن نفس الشهر اكتشفت شركة أمن المعلومات(Symantec) هذا الفيروس بصيغة آخرى(W32.Temphid)، كما كشفت بعض شركات الأمن الرقمي(Symantec, ESET) أنّ فروع البرنامج الخبيث(Stuxnet) استطاعت أن تسرق شهادات إلكترونية لشركات تصديق(VeriSign, JMicron Technology Corp, etc.) لاستخدامها في توقيع بعض برمجيات نظم التشغيل وذلك قبل إلغاءها من طرف هذه الشركات، فبالرغم من قيام كلّ من شركة(Microsoft) بسدّ بعض الثغرات الأمنية في نظام تشغيل(Windows)، وقيام الشركة الألمانية(Siemens) لمحاولات واسعة منذ اكتشاف الدودة لتعقب انتشارها عبر موقعها الإلكتروني، إلاّ أنّ برنامج الدودة الخبيثة(Stuxnet) مسّ العديد من أنظمة تحكّم المنشآت الصناعية التي استخدمت تكنولوجيا شركة(Siemens)، حيث أصابت حوالي 45 ألف حاسوب في أنحاء العالم، منها 60% في إيران لوحدها بما فيها حواسب العاملين بمحطتها النووية بوشهر(**Bouchehr**)**المُخطّط تشغيلها قريبا**، و18% في اندونيسيا و2% في الولايات المتحد الأمريكية وأمّا النسبة المُتبقيّة مسّت حواسيب المحطات النووية التابعة لماليزيا، اندونيسيا، الهند، ألمانيا، فرنسا. لذا وصفت شركة الأمن الرقمي الروسية(Kaspersky) برنامج(Stuxnet) على أنّه مُخِيف ومُرعِب من شأنه أن يخلق سباق تسلّح جديد في العالم، وأشارت إلى أنّ من وراءه(البرنامج) خبراء يتمتعون بقدرات وكفاءات عالية يعملون لحساب دولة معينة، كما اتفق بعض خبراء أمن المعلومات(Ralph LANGNER, etc.) أنّ برنامج دودة(Stuxnet) مصمّم بشكل كبير لتنفيذ هجوم إلكتروني على هدف صناعي محدّد، لإلحاق الضرر بأجهزة الطرد المركزي لتخصيب اليورانيوم في المنشآت النووية(البرنامج النووي الإيراني). فحسب خبراء شركة الأمن المعلوماتي(Symantec) فإنّ دودة(Stuxnet) **ستبدأ في تنفيذ مهماتها التخريبية في 24 جوان 2012**، ولولا تدابير الحماية الأمنية المُقامة والكشف المبكّر لهذا البرنامج الخبيث لحدثت كارثة نووية مماثلة لكارثة المحطة النووية لتشرنوبيل(**Tchernobyl**) الأوكرانية التي

أمّا الإنكار(Répudiation) يتمثّل في إنكار شخص مشاركته كطرف في مبادلة تجارية تمّت بطريقة إلكترونيّة، إذ يمكن لأي شخص أن ينكر دفع ثمن سلعة معيّنة لم يقم بشرائها إطلاقا عبر الموقع التّجارّي، لكون أنّ شخص معيّن انتحل هويّته عبر شبكة الإنترنت وقام باسمه بتسّلم السّلعة التي زوّدها له التّاجر، كما قد يمكن أن يحدث العكس أن يقوم الشخص بتسّلم السّلعة ويدّعي القيام بدفع ثمنها وذلك نظرا لغياب الوسائل المبرّرة لذلك، وفي كلتا الحالتين يتعرّض صاحب الموقع التّجاري(التّاجر) لأضرار فادحة لكونه أبرم صفقة تجاريّة مع شخص مجهول الهويّة.

انطلاقا من ذلك، يمكن القول أنّ البرمجيات الخبيثة تؤثر تأثيرا سلبيا على شبكات الاتّصالات بشكل مباشر أو غير مباشر، حيث تصل مهامها في بعض الأحيان إلى تعطيل أو إحداث شلل كبير في شبكات معلومات الشّركات الاقتصاديّة، كالشّركات المصرفيّة والطّيران والنّقل البّحري إلى غيرها من الشّركات الكبرى المنتشرة حول العالم، حيث أنّ التّوقّف القصير لهذه الشّبكات من شأنه أن يُكَبِّدَ أصحاب هذه الشّركات، أو المُستفيدين من خدماتها خسائر ماليّة فادحة تؤدّي في كثير من الأحيان إلى الإفلاس، وانخفاض مستوى الخدمات المتاحة للمستهلكين وإرباك الشّبكات الأخرى المتّصلة بالشّبكات المُعطَّلَة، وبالتّالي

انفجر مفاعلها النووي في 26 أفريل 1986، حيث **يُعتقد** أنّ البرنامج الخبيث(**CIH**) الذي يشير اختصارا إلى صانعه التايواني(**Cheng Ing-Hau**) كان السبب في انفجار ذلك المفاعل، حيث اكتشفته لأوّل مرّة شركة الأمن الرقمي-(**F-Secure (Créée en 1988 sous le nom de Data Fellows.)**) في جوان 1998، التي أثبتت أنّ ذلك البرنامج الخبيث مُصمّم لأداء مهامه التخريبية بالضبط عند حُلُولِ تاريخ "**26 أفريل**" الذي يتزامن مع تاريخ انفجار المحطة النووية لتشرنوبيل(**Tchernobyl**)، في حين أَلحَقَ الفيروس الخبيث(**CIH**) الأضرار للعديد من أجهزة الحواسيب في قارتي أوروبا وأسيا في **26 أفريل 1999**، والجدير بالذكر أنّ البرنامج الخبيث ينتشر فقط في أنظمة تشغيل شركة(Microsoft) مثل(Windows 95, Windows 98 et Windows ME.).

Alix DESFORGES, « Le cyberespace : un nouveau théâtre de conflits géopolitiques. », Questions internationales, n° 47- janvier- février 2011, pp. 50- 52.

لمزيد أكثر من المعلومات حول هذا الموضوع أنظر المواقع الإلكترونية التالية:

http://www.xmco.fr/actualite-securite-vulnerabilite-fr.html ou http://www.xmco.fr ou http://cert.xmco.fr (consultés le 15/05/2016.) ou http://www.secuser.com/alertes/1999/tchernobyl.htm ou http://www.sophos.fr/virusinfo/analyses/ w95cih.html (consultés le 17/05/2016.)

فإنّ جودة ونجاح الأعمال يرتكزان على جودة وأداء شبكات الاتّصال واستمراريّة عمل قواعد البيانات المحميّة.

الفرع الثالث

مخاطر برامج الاستطلاع والتصنّت ومنع تقديم الخدمة

يُقصد بالاستطلاع(Reconnaissance) جمع المعلومات من دون إذن أو تخويل من صاحبها لغرض استكشاف شبكة شركة معيّنة، ورسم مخطّطها ومعرفة الخدمات المُستخدمة فيها واستنتاج نقاط ضعفها، فمن خلالها يقوم القراصنة في المرحلة الأولى استخدام أدوات(Whois, NSLookUp, Ping) لكشف وتحديد عناوين البروتوكولات المسّجلة للشّركة الضّحية، وفي المرحلة الثّانية يقومون بمسح جميع المنافذ المؤدّية إلى الشّبكة لاستنتاج المنافذ المفتوحة والخدمات العاملة في العناوين المستنتجة، التي على إثرها يتوّصلون إلى معرفة أنواع التّطبيقات المستخدمة وأسماء أنظمة التّشغيل التي تشغل حاسبات الشّركة المستهدفة، حيث يعتمد القراصنة فيما بعد على هذه النتائج ليقرّروا ما إذا كانت نقاط الضّعف المستخلصة قابلة للاستغلال أم لا[1].

أمّا التصنّت(Eavesdropping) أو(Écoute du réseau) يعمل بدروه على استطلاع الشّبكات واكتشاف الهجمات على هذه الأخيرة، حيث تستخدم من خلالها أدوات تحليل الشّبكات وبروتوكولاتها وأدوات تحسّس والتقاط الحُزم(Paquets)، على شبكات الحاسب الآلي لجمع معلومات ثمينة حول مُعدّات الشّبكة وتقنيات إعداد كلّ منها، وبالتالي يعتمد القراصنة من خلال هذه الأدوات على البرتوكولات التي تقبل التصنّت كـ(SNMP, TCP/IP etc.) التي من خلالها تتّم عمليات مراقبة الحُزم والتقاط كلمات المرور وأسماء المستخدمين أثناء عبورها

---

[1] **علاء حسين الحمامي، علاء الدين جواد الراضي**، الإصدار السادس لبروتوكول الإنترنتIPv6 (العمود الفقري لإنترنت الأجيال القادمة)، دار الراية للنشر والتوزيع، عمان، الأردن، 2015، ص ص 176، 177، 178، 179، 180.

على شبكة الإنترنت[1]، وتُسّهل عملية الوصول إلى شبكة الشّركة المُستهدفة والدّخول إلى أجهزة خوادم الويب التّابعة لها، التي تمّكنهم من جمع البيانات السّريّة لبطاقات الائتمان والمعلومات الشّخصيّة لأصحابها وحتى البيانات الإلكترونيّة الحسّاسة التي تخدم الاقتصاد الوطني لبلد معيّن.

وتجدر الإشارة في هذا السّياق، أنّ معظم حالات الاستطلاع والتصنّت يقف من ورائها قراصنة مُحترفين ينّفذون مهامهم لحساب دولة أو دول معيّنة، بغية الحصول على البيانات أو المعلومات الحسّاسة المتداولة عبر شبكة الإنترنت، التي تساعدها على ترصّد وكشف الهجمات الالكترونيّة أو حتّى القيام بعمليات التّجسّس والقرصنة لأهداف الأمن والاقتصاد الوطنيين[2].

وعليه، تعتبر هجمة رفض تقديم الخدمة(Déni de service) أو (Denial of Service (DoS)) من بين أخطر أشكال التّهديدات الحديثة على نظم المعلومات، حيث يقوم من خلالها المعتدي في نفس الوقت بإرسال عدد هائل من الخدمات أو الحزم من الشّبكة الخارجيّة(الإنترنت) إلى إحدى أجهزة الشّبكة الدّاخليّة للمؤسّسة، لإيقاف أو إبطال الخدمة المعلوماتيّة المتاحة للمشتركين فيها (La saturation ou le blocage des systèmes informatiques)، فغالبا ما يستخدم القراصنة المحترفين عدد كبير من أجهزة الحاسوب المُصابة بالبرامج الخبيثة المتواجدة في مواقع جغرافيّة مختلفة، لإرسال كمّ هائل من طلبات

---

1) **Fabrice HARROUET**, « Écoute du réseau et usurpation d'identité ("Les aventures de SNIFF et SPOOF . . . ") », pp. 16-22. Article disponible à partir de l'adresse: http://www.enib.fr/~harrouet/, consultée le 20/12/2018.
Hélie - SOLANGE GHERNAOUTI, Sécurité Internet : Stratégies et technologies, op.cit., pp. 170, 171.

2) **Denis C. ETTIGHOFFER**, « L'économique numérique sera-t-elle sous domination américaine ? », Revue Géoéconomie, 2010/2 (n° 53), pp. 96- 99.
Zygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON et R. B. J. (ROB) WALKER, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », Revue Cultures & Conflits, 2015/02 (n° 98), pp. 134- 136, 141- 143.

تقديم الخدمة في نفس الوقت إلى خوادم الويب لتعطيل خدماتها، وطَمْسِ مَصدَر الهجمات حيث تسمى هجمة رفض الخدمة في هذه الحالة بـ (Distributed Denial-of-service(DDoS))، أو يقوم أحد هؤلاء استخدام تقنيّة الإغراق (Dépassement de la mémoire tampon أو Buffer Overflow)، التي تنطوي على إرسال رسالة إلكترونيّة ذي حجم كبير تفوق قُدرات خادم أو موزّع الويب على استقبالها أو استيعابها[1].

انطلاقا من ذلك، فإنّ "الهاكرز" يستطيع أن يُنفّذَ هجمات الحرمان من الخدمة عن طريق تقنيّة(Distributed Denial-of-service(DDoS)) أو (Denial of Service (DoS))، حيث يقوم من خلالها بإرسال سَيْلٍ من الطّلبات والأوامر أو البيانات غير اللاّئقة، إلى المَوقِع الإلكتروني المُستهدَف عن طريق أجهزة حواسيب مُتعدّدة، مصابة في إطار شبكة "البوتنت(Botnet)" بعدوى إحدى البرمجيات الخطيرة الخبيثة (Chevaux de Troie, Vers, etc.)، وذلك بشكل كثيف ومُتزايد تفوق بكثير قدرة الجهاز المُزوّد على المعالجة، ممّا يُسبب في بطء الخدمات المتاحة وصعوبة وصول المستخدمين إلى هذا الموقِع، نظرا لاكتظاظ وتزاحم الطّلبات المُوجَّهة إليه.

حيث يتّم تنفيذ هذه الهجمات بسهولة، ومن دون كسر ملفات كلمات السّر أو سرقة البيانات السّرية أو الاستعانة بأحدث المعدّات، وإنّما يَسْتَغِلُّونَ في بعض الأحيان الثّغرات الأمنيّة المتواجدة في نظم حماية الشّبكات، كأن يقوم أحد المهاجمين إتّباع أسلوب هجمة الدّمعة(Teardrop)، من خلال إرسال حُزَمًا مُشوَّهة(Paquets IP falsifiés) إلى الخادم، ممّا يؤدي إلى انهيار عمليات معالجة عناوين(IP) على الجهاز المُزوّد، أو يَنْتَهِج أسلوب إغراق عملية المعالجة نفسها في نظام التّشغيل، من خلال إرسال أوامر معالجة أو إدخال

---

[1] Document du club de la sécurité des systèmes d'information Français(**CLUSIF**), « Gérer la sécurité d'un site de commerce électronique », Mai 2001, version 1.0, pp. 18,19. Disponible sur le site : https://www.clusif.asso.fr/, consulté le 10/09/2018.
Hélie - SOLANGE GHERNAOUTI, Sécurité Internet : Stratégies et technologies, op.cit., pp. 180, 181.

طويلة(Buffer Overflow)، حيث لا تَصُدُّهَا عمليات معالجة المُدخَّلات ضمن نظام التّشغيل مما يؤدّي إلى انهياره، وهذا ما استغله(الثّغرة) واضعو فيروس "الشّيفرة الحمراء(Code Red)" في خوادم ونُظم تشغيل شركة(Microsoft) الخ....

وعليه، أصبحت هجمات رفض الخدمة من نوع (Distributed Denial-of-service(DDoS)) تزداد شدّتها التّخريبيّة عاما بعد الآخر، واستهدفت بشكل واسع مبيعات وخدمات الشّركات التّجارية عبر شبكة الإنترنت، حيث تعرّضت في عام 2000 مواقع الإنترنت لكلّ من(Yahoo !, Amazon.com, Buy.com, CNN.com, eBay.com, etc.) إلى هذا النّوع من الهجمات، ممّا كبّدها خسائر مالية فادحة ولو لبضع ساعات فقط[1].

تتجسّد تطبيقات البرمجيات الخبيثة من خلال استخدام برامج التّجسّس(Spyware) أو (Espiogiciels)[2]، لمُراقبة سلوكيات مستخدم جهاز الحاسوب وتسجيل جميع التّحركات والأفعال التي تتّم على ذلك الجهاز، بُغية الحصول على معلومات سريّة ذات صلة بكلمات المرور وأرقام الحسابات المصرفيّة الخ...، أو لتحقيق أهداف تجارية بحتة كمعرفة أنماط المستخدم الاستهلاكية أو محرّكات البحث الأكثر استخداما أو المواقع التّجاريّة الأكثر تسوّقا.

انطلاقا من ذلك، فإنّ برامج التّجسّس تتمكّن من النّزول إلى أجهزة الحواسيب ضمن البرامج المجّانيّة أو المشبوهة التي يتّم تحميلها عبر شبكة الإنترنت، أو تقوم هذه البرامج استغلال الثّغرات الأمنيّة المُتواجِدة في أنظمة حماية الحاسوب للوصول إليه، فبعد تثبيت البرنامج على جهاز الحاسوب، يقوم بإخفاء نفسه(برنامج التّجسّس) في نظام التّشغيل على نحو يصعب على المستخدم من اكتشاف مكان وجوده، فعادة ما يتّم ربط برامج التّجسّس

[1] أنظر **الملحق رقم (22)**، ص 498.

[2] للتعرف أكثر على برامج التجسس أنظر الموقع التالي:(consulté le 19/05/2016) http://www.lavasoft.com

بالبرامج التي تتعقّب المعلومات الشّخصيّة أو الحسّاسة، أو بالبرامج التي تعرض مختلف الإعلانات عبر شبكة الإنترنت[1].

من بين تقنيات التّجسّس الأشد خطورة والأكثر استخداما عبر مواقع التّجارة الإلكترونيّة نجد برنامج "راصد لوحة المفاتيح(Key logger)"، أو(Enregistreur des frappes) الذي يعمل على تسجيل ونسخ كلّ ما يُكْتَبُ على صَفحةِ هذه اللّوحة، من رسائل بريدية إلكترونيّة كلمات مرور ودردشة أو أرقام البطاقات المصرفيّة الإلكترونيّة وعناوين المواقع الإلكترونيّة التي تمّت زيارتها الخ...، حيث لا تكتشفها عادة البرامج المضّادة للفيروسات والبرامج الضّارة، فمن المَعمولِ على هذه البرامج أنّها تُسوَّق كبرامج مُراقَبَة، لكن في الوقت نفسه تُستخدم استخداما غير مشروع أو خبيث، إذ تُرسل تلك البرامج بشكل مُستمر إلى الغَيْرِ جميع البيانات المكتوبة على لوحة المفاتيح من دون علم أصحابها[2]، وبالتّالي فإنّ برامج مراقبة الإنترنت(Internet monitoring software)، تقوم بترصّد كل ما يفعله المستخدم عبر شبكة الإنترنت كمراقبة البرامج التي تم تنزيلها، وتسجيل كل من رسائل البريد الإلكتروني وأسماء وعناوين المواقع التي تمّت زيارتها، والوقت الذي قَضَاهُ المستخدم عند تَصفّحِه لهذه المواقِع[3].

فإلى جانب هذه البرامج، نجد برامج الإعلانات(Adware) التي تُستخدم للتّسويق التّجاري غير المرغوب فيه أو الإجباري، عن طريق تحويل المستهلك إلى مواقع تجاريّة من دون إذنه بذلك أو تقوم بتعطيل محرّك البحث القائم وتُعوِّضُه بمحرك بحث آخر مقلّد أو مزوّر، ليقوم بمهام الجّهة الإعلاميّة لبرنامج الإعلانات[4]، حيث يُتيح إعلانات لمنتجات معيّنة بمجرّد البحث عن مثيلاتها في ذلك المحرّك، أو تُستخدم تقنيّة(Spamming) لإرسال عدد كبير من

---

[1] **سوسن زهير المهتدى**، مرجع سابق، ص 414.

[2] **Ali EL AZZOUZI,** op.cit., pp. 64- 65.

[3] **سوسن زهير المهتدى**، مرجع سابق، ص ص 416، 417، 418.

[4] المرجع نفسه.

الرّسائل البريديّة الإشهاريّة غير المرغوب فيها، والتي تُزعج الكثير من العملاء، وهذا ما يؤدّي إلى تشويه السُّمعة التّجاريّة للمؤسّسة، كما تُستخدم كذلك البرامج الانبثاقيّة أو الفُقاعيّة(Pop-up) التي تُنشر إعلانات تتضمّن صُور إباحيّة، إلى جانب صور السّلع والخدمات المروّج بها، وذلك أثناء القيام بتصفّح الموقع التّجاري عبر شبكة الإنترنت، حيث تؤدّي هذه البرامج في غالب الأحيان إلى مشاكل أمنيّة في أنظمة التّشغيل من جرّاء الإخفاق في سدّ ثغرات الحماية فيها.

انطلاقا من ذلك، فإنّ طرق التّعرف على الإصابة ببرامج التّجسّس والمراقبة تتجّلى من خلال كثرة الصّفحات الانبثاقية، التي تُنشِر صور منافية للآداب والأعراف السّائدة في المجتمع، وليس لها صلة بالسّلع والخدمات المروَّج لها في الموقع التّجاري، حيث تجعل جهاز الحاسوب في الكثير من الأحيان بطيء الحركة أو يستجيب لدرجة ملحوظة، كما أنّه في حالة ما إذا قام المستهلك بعملية البحث فإنّ متصفّح الإنترنت يستخدم محرّكاً للبحث مغاير للمحرّك الذي حدّده ذلك المستخدم، فغالبا ما يجد هذا المستهلك أنّ قائمة المواقع المُفضّلة في برنامج متصفّح الإنترنت تحتوي على مواقع إلكترونيّة لم يقم بإضافتها من قَبْلِ، أو تظهر له(المستهلك) صفحة ويب بداية بصفة مُتكرّرة تُحيله إلى موقِع إلكتروني آخر لم يقم باختياره كصفحة بداية، كما أنّه في الكثير من الأحيان، نجد أنّ العديد من الحواسيب المصابة بعَدوى برامج التّجسّس، تَستعمِلُ أرقام هواتف مُسّجلة باسم أصحابها من دون إذنِهِم، للاتصال بخطوط أرقام هواتف أجنبيّة غير معروفة، وبتكاليف باهظة وذلك من دون تعرّف أصحابها عن مصدر الاتّصال[1].

[1] **سوسن زهير المهتدى**، مرجع سابق، ص ص 416، 417، 418.

المطلب الثاني
تهديدات أمن مواقع التّجارة الإلكترونيّة

إنّ تكريس الأمان في بيئة الإنترنت بصورة أكيدة وشاملة ومضمونة بصفة نهائيّة لا وجود له في الواقع، فقُوّة أيّ نظام معلوماتي حديث تُقاس بِأَضْعَفِ نُقطة فيه، حيث أنّ لكلّ شبكة من شبكات الاتّصال مَواطِن ضُعف خاصّة بها تجعل من المعلومات والبيانات الإلكترونيّة المتداولة عبرها، عُرضَةً لمختلف التّهديدات الرّئيسيّة التي تختلف باختلاف مصادرها(**الفرع الأول**)، وتعدّد الدّوافع والمنهجيات التي يرصدها أصحاب الاختصاص الذين يستحوذون في الكثير من الأحيان على معلومات متقدّمة وَجِدُّ مُتطوّرة، تجعل مُهمّة اختراق أنظمة مواقِع التّجارة الإلكترونيّة أكثر سهولة من الدِّفاعِ عنها(**الفرع الثاني**)، ولعلّ أنّ اعتماد أطراف المعاملة التّجاريّة على تطبيقات شبكة الإنترنت تُثير العديد من المسائل المتعلّقة بتحديد هويّة الأشخاص وضمان سلامة وسرية التّبادل الإلكتروني مع عدم إنكاره(**الفرع الثالث**).

الفرع الأول
التّهديدات الرّئيسيّة لأمن مواقع التّجارة الإلكترونيّة

لتحديد وتقييم الأخطار التي تشّكل تهديدا لمختلف أنظمة حماية شبكات الحاسوب والإنترنت، يستوجب الأمر التّعرف على المصادر الرّئيسيّة المُهدّدة لهذه الشّبكات حيث يمكن حصرها في العناصر التّالية: التّهديدات غير المنظّمة (**أولا**)، والتّهديدات المنظّمة (**ثانيا**)، والتّهديدات الدّاخليّة (**ثالثا**)، والتّهديدات الخارجيّة (**رابعا**).

أولا– التّهديدات غير المنظّمة.

إنّ عملية إعداد الفيروسات المختلفة أصبحت في وقتنا الحالي كثقافة في أوساط أفراد المجتمعات كطلاّب المدارس الابتدائية وطلاب الثّانوية الخ...، حيث أنّ تقنيّة برمجتها سهلة ولا تستدعي بالضّرورة الاستعانة بأصحاب الخبرات والكفاءات العالية في ميدان تكنولوجيا الاتّصال والإعلام، إذْ تُتيح شبكة الإنترنت العديد من البرمجيات (Programmes générateurs de virus) التي تُساعِد على برمجة العديد من الفيروسات حسب الأهداف

والغايات المرجوّة، كما أنّ العديد من مواقع الإنترنت تُتيح تقنيات القرصنة المجّانيّة لتنفيذ التّهديدات الإلكترونيّة غير المنظّمة، كبرنامج كسر كلمات المرور الضّعيفة (Advanced ZIP Password Recovery(AZPR)) الذي يتيح إمكانية تصديع كلمات مرور الملفات المضغوطة بصيغة(ZIP)، الذي يتميّز بسرعة محاولات اكتشاف كلمات المرور الضّعيفة التي قد تصل إلى ملايين المحاولات في الثّانية الواحدة[1].

فكلّما كانت كلمة المرور أطول(أي تحتوى على تشكيلة من الحروف والأرقام والرّموز) كان وقت تصديع أطول وقد يصل إلى سنين متعدّدة، وفي هذا السّياق يتّم الاستعانة بمُصدّع كلمات العبور(Passwords Cracker) يعتمد على أي برنامج تطبيقي، يمتلك القدرة على تجاوز عقبة الشّفرة المستخدمة في نظم الحماية وإحباط آليتها، حيث يعتمد مُسبقا على خوارزميات مُماثلة للخوارزميات الأصليّة المُستخدمة في التّشفير، التي تعمل بدورها على توليد شفرات حديثة تُناظر الشّفرات المعتمدة في صياغة كلمات العبور الأصليّة.

كما يُمكِن تنصيب برنامج صغير لمراقبة سلوكيات مستخدمي موقع تجاري معيّن واستغلال الهفوات والثّغرات التي يتركها هؤلاء على مستوى الشّبكة[2]، حيث يجرأ الكثير منهم على تخزين أرقام البطاقات المصرفيّة أو كلمات المرور على أنظمة تشغيل الحاسوب، التي تظل مصدر خطر، يمكن أن يؤذي شبكة الموقع التّجاري بأضرار خطيرة تزيد بازدياد مهارة القراصنة وقوّة التقنيات المستخدمة فيها، مما يؤدّي إلى فقدان مصداقيّة ذلك الموقِع.

ثانيا– التّهديدات المُنظّمة.

إنّ مصدر هذه التّهديدات تنبثق من قراصنة مختصّين في عمليات اختراق المواقع الإلكترونيّة، حيث يعرفون جيّدا نظم التّشغيل المعلوماتيّة، ويتقنون استخدام لغات النّصوص

---

[1] يمكن تنزيل البرنامج على الموقع الالكتروني التالي: http://www.elcomsoft.com

[2] **دلال صادق الجواد، حميد ناصر الفتال**، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2008، ص ص 16 ،17.

البرمجيّة ويحسنون التّأقلم مع تقنيات التّشفير وفكّها، ويطوّرون ويبدعون تقنيات قرصنة حديثة ومعقّدة، لاختراق المواقع الإلكترونيّة وبالخصوص مواقع الشّركات التّجاريّة والمؤسّسات المصرفيّة التي تدّعي على أنّها محميّة، فغالبا ما يتورّطون(القراصنة) في قضايا التّجسّس أو الاحتيال أو سرقة وتحويل الأموال من حسابات العملاء إلى حساباتهم بطرق سريّة لا تُلفت الانتباه إلاّ عن طريق الصدفة[1].

انطلاقا من ذلك، برزت ظاهرة القرصنة الإلكترونيّة كسلاح العصر الرّقمي الحديث الذي يُستخدم لتنفيذ الهجمات الإلكترونيّة المُنظّمة، حيث يُهدّد المنشآت الحيويّة كالمفاعلات النّوويّة وشبكات الطّاقة الكهربائيّة والميّاه والنّقل وأنظمة التّحكّم الصّناعيّة والمواصلات وأنظمة الطّائرات، والأمن الوطني ويُدمّر المخزونات الماليّة للمصارف وانتهاك الأسرار الخ...[2]، لذا تُعدّ القرصنة الإلكترونيّة شكل من أشكال حرب المعلومات التي يمكن أن

---

[1] **Hélie- SOLANGE GHERNAOUTI**, « Menaces, conflits dans le cyberespace et cyberpouvoir », Revue Sécurité et stratégie, 2011/3 (n°7), pp. 63- 66.

[2] أكدّ مُجمّع ياهو للإنترنت(**Le groupe internet Yahoo!**) بأنّه تعرض من 2012 حتى 2014 إلى أكبر عملية قرصنة إلكترونية إلى حدّ الآن، التي سمحت للقراصنة باختراق النظام الأمني والحصول على مليار من الحسابات الإلكترونية المُتواجدة في قواعد البيانات التابعة للمُجمّع، حيث استحوذوا من خلالها على جميع المعطيات الشخصية المتعلقة بالعملاء أو الزبائن كأسماء وتواريخ الميلاد، العناوين الإلكترونية وأرقام الهواتف والكلمات السرية، حيث أكدّ المُجمّع بأنّ عملية الاختراق لم تمس البيانات الإلكترونية المتعلقة بالبطاقات المصرفية الذكية وأنّه اتخذ جميع الإجراءات اللازمة لتأمينها، والجدير بالذكر أنّ هاكر ظهر تحت غطاء تسمية(Peace) قد عرض في أوت 2012 حوالي 200 مليون لأسماء المستعملين وكلمات المرور المتعلقة بمجمع ياهو! بمقابل دفع 1.900 دولار أمريكي، حيث استعمل نفس التقنية مع البيانات الإلكترونية لعملاء شركتي كلّ من(Myspace et Linkedin)، وعليه أكدّ خبير الأمن المعلوماتي(Graham CLULEY) أنّ عملية القرصنة قد تم تنفيذها من طرف جماعة من الهاكرز تحت رعاية دولة معينة(Hakers sponsorisés par un État)، وكنتيجة لذلك أوصى مجمع ياهو! عملائه بضرورة تغيير كلمات المرور وعدم النقر على الروابط وتحميل أو تنزيل أيّ برمجية، مع اتخاذ اليقظة والحذر من الرسائل الإلكترونية الخادعة التي تطلب منهم بياناتهم الشخصية الخ...

Florian REYNAUD, « Plus d'un milliard de comptes d'utilisateurs Yahoo ! ont été piratés », article de journal Le Monde, publié le 14/12/2016 à 23h23 sur le site : http://www.lemonde.fr/pixels/article/2016/12/14/, consulté le 17/12/2016.

Benjamin FERRAN, « Yahoo ! confirme le piratage de 500 millions de comptes », article de journal Le Figaro, publié le 22/09/2016 à 10 h 35 sur le site :

تكون السّبب الحقيقي لنشوب الحروب(بمفهومها التّقليدي) فيما بين الدّول[1]، أو استغلالها في مجال السّياسة لتغيير مجرى المسار الانتخابي لمرشّح حزب معيّن على غرار الحزب الديمقراطي للولايات المتّحدة الأمريكيّة[2].

---

http://www.lefigaro.fr/secteur/high-tech/2016/09/22/, consulté le 09/10/2016.

1) **François-BERNARD HUYGHE,** « Des armes à la stratégie », Revue Internationale et stratégique 2012/3 (n° 87), pp. 59-61.

2) قامت مجموعة من القراصنة المحترفين باختراق نظام الحماية الأمنية لشبكة اللجنة الوطنية الديمقراطية باعتبارها كأعلى هيئة في الحزب الديمقراطي الأمريكي((Democratic National Committee(DNC)، أين استطاعوا أن يتحصلوا على الآلاف من رسائل البريد الإلكتروني لمُرشّحة ذلك الحزب هيلاري كلينتون(**Hillary CLINTON**)، وكان ذلك في الوقت الذي كانت تشغل منصب كاتبة الدولة للشؤون الخارجية، حيث قاموا بنشر محتوياتها(E-mails) عبر الموقع الإلكتروني لويكيليكس(Wikileaks) المشهور بنشر الوثائق السرية الرسمية، وكنتيجة لذلك أُسْتُغِلَّتْ هذه التسريبات كذريعة سياسية من طرف خصمِها في الحزب الجمهوري دونالد ترامب(**Donald TRUMP**) أثناء الحملة الانتخابية لتقليص شعبية مُرشّحة الحزب الديمقراطي(**Hillary CLINTON**) واستهداف وجذب العديد من الجماهير للانتخاب عليه، وهذا ما حصل إذ فاز في الإنتخابات الرئاسية على حساب مرشحة الحزب الديمقراطي، ونظرا لفقدان أدّلة ثابتة وموثوقة في تورّط جهاز المخابرات الروسية في عملية التسريبات وجَّه أعضاء الحزب الديمقراطي الحَاكِم أصابع الاتهام إلى جماعة من الهاكر الرُّوس المُدعمين من قِبلِ حكومتهم، وفي انتظار تولّي مُمثّل الحزب الجمهوري(**Donald TRUMP**) الفائز في الانتخابات الرئاسية منصبه بصفة رسمية، قام الرئيس(**44 للولايات المتحدة الأمريكية**) الأمريكي باراك أوباما(**BARACK Obama**) قبل النهاية الرسمية لعهدته الرئاسية، بطردِ مُمَثِّلِي السفارة الروسية من أراضي الولايات المتحدة الأمريكية غير أنّ روسيا الفيدرالية التزمت بعدم الردّ بالمِثْلِ(...).

كما تعرضت في 08 و09 أفريل 2015 قناة التلفزيون الفرانكفونية العالمية(**TV5 Monde**) المنشأة في عام 1984 بصفة مشتركة من طرف الشركات السمعية البصرية(الفرنسية، السويسرية، البلجيكية، الكندية، والكيبكية) لعملية القرصنة(Cyberattaque)، أدّت إلى شلّ وتعطيل خدماتها لمدّة ساعات مع نشر شعار ورسالة دعم للدولة الإسلامية(État islamique) على شبكات التواصل الاجتماعية الخاصة بها (les comptes Twitter et Facebook de la chaîne) باللغة العربية والإنجليزية والفرنسية التي من خلالها هدّدوا السلطات الفرنسية، وذلك بالرغم من تحذيرات الوكالة الفرنسية لأمن أنظمة المعلومات (Agence nationale de la sécurité des systèmes d'information (ANSSI)) في أواخر شهر مارس 2015، من تعرّض أحد خوادمها الغير المؤمنة (L'un de ses serveurs non protégé) لعملية الاختراق، حيث توصلت فيما بعد القناة(**TV5 Monde**) إلى استعادة عافيتها ومُباشَرة نشاطاتها بعد تدخّل خبراء تلك الوكالة(ANSSI)، فبعد التحرّيات والتحقيقات القضائية الابتدائية التي باشرها هؤلاء الخبراء توصلوا إلى أنّ القراصنة اعتمدوا على تقنية الرسائل الخادعة(Hameçonnage) أو(Phishing) التي من خلالها قاموا بإرسال رسائل إلكترونية كاذبة إلى كافة صَحَفِيِي القناة حيث استجاب إليها ثلاثة منهم فقط، الأمر الذي سمح للقراصنة باختراق شبكة

وعليه، فإنّ عمليات الاختراق المنظّمة تكون عادة موجّهة من طرف دولة معيّنة لغرض التّجسّس على شبكة حواسيب هيئة رسميّة أو شركات اقتصاديّة كبرى في دول أخرى، أو تخريب وتعطيل تلك الشّبكات وما يرتبط بها من أجهزة، حيث يقوم بتنفيذ هذه العمليات قرصان أو جماعة "هاكر" التي غالبا ما تكون مدعومة من طرف حكومة معينة[1]، حيث تملك معرفة "دقيقة" و"عميقة" بالحواسيب وشبكاتها وتتمتّع بخِبرات ومهارات عالية في لغات البرمجة وأنظمة التّشغيل، ويُحسنون استغلال تقنيّة الهجوم من دون انتظار (Vulnérabilité Zero day) التي من خلالها يقومون باكتشاف نقاط الضّعف المتواجِدة في برمجيات الحاسوب والثّغرات الأمنيّة في الشبكات غير المعروفة، مع استغلالها في أقرب وقت مُمكِن وفي الظّرف والمكان المناسبين لغرض نشر برمجياتهم الخبيثة وتنفيذ الهجمات الإلكترونيّة، وذلك قبل أن يكتشفها مُطوّري البرمجيات أو خبراء الأمن المعلوماتي الذين يقومون في حالة ما إذا تحقّق ذلك بسّد هذه الثّغرات، مع نشر برمجيات تصحيحيّة[2].

القناة مع نشر البرنامج الخبيث(Cheval de Troie)، وكنتيجة لذلك توصلت كلّ من وكالة الأمن(ANSSI) ووكالة الأمن المعلوماتي الأمريكية(FireEye)، أنّ جماعة من الهاكر المعروفين تحت تسمية **(APT28 ou Pawn Storm, Tsar Team, Fancy Bear, Sednit)** كانت من وراء تنفيذ الهجمة الإلكترونية على تلك القناة معتمدين في ذلك على الآثار التي تركها هؤلاء القراصنة، حيث يُعتقد أنّ هذه الجماعة تُباشِر مهامها بدعمٍ من حكومة معيّنة(روسيا)، ولعلّ أنّ هذه الهجمة كانت كردّ حول إلغاء السلطات الفرنسية على خلفيات الأزمة الأوكرانية للصفقة المُبرمة مع روسيا الفيدرالية حول الناقلتين البحريتين العسكريتين(Deux navires Mistral)، كما يُعتقد أنّ تلك الجماعة (APT28 ou Pawn Storm, etc.) هي التي نفّذت كذلك عملية القرصنة على الحزب الديمقراطي الأمريكي. لمزيد من المعلومات أنظر:

Damien LELOUP et Martin UNTERSINGER, « Piratage de TV5 Monde : l'enquête s'oriente vers la piste russe », article de journal Le Monde, publié le 09/06/2015 à 18h43 sur le site : http://www.lemonde.fr/pixels/article/2015/06/09/, consulté le 02/10/2016.

Gilles PARIS, « Le parti démocrate voit la main de la russie derrière la publication d'e-mails par Wikileaks », article de journal Le Monde, publié le 25/07/2016 à 18h34 sur le site : http://www.lemonde.fr/elections-americaines/article/2016/07/25/, consulté le 28/08/2016.

[1] **Myriam QUÉMÉNER**, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Revue Sécurité et stratégie, 2011/1 (n°5), p.60.

[2] تُعتبر دودة اللَّهَبْ**(Flame)** أو فَلاَمُرْ**(Flamer)** بالإنجليزية المعروفة كذلك تحت تسمية**(Worm.Win32.Flame)** أو**(sKyWIper)**، من بين برامج التجسّس الخبيثة المعقّدة التي تُهاجم أنظمة تشغيل(Windows) للشركة الأمريكية(Microsoft)، تم الإعلان عن اكتشافها في سنة 2012 من طرف كلّ من مركز

ثالثا– التّهديدات الدّاخليّة.

يُقصد من مرتكبي التّهديدات الدّاخليّة الأشخاص الذين ينتمون إلى الجهة المستهدفة، إذ يشّكلون المصدر الحقيقي للخطر الذي من شأنه أن يؤدّي إلى تعطيل شبكة الشّركة بأكملها وإلحاق أضرارا بسريّة المعلومات أو سلامتها، أو حتّى منع الوصول إليها في بعض

الأمن المعلوماتي الإيراني(MAHER Center, Iran National CERT) وشركة الأمن المعلوماتي الروسية(Kaspersky Lab) ومخبر التشفير وأمن الأنظمة لجامعة التكنولوجيا والاقتصاد ببودابست، حيث استطاع الفيروس أن يُصِيبَ حوالي ألف(1000) جهاز حاسوب يعمل بنظام تشغيل(Windows) وقادر على الانتشار إلى حواسيب جديدة عن طريق الشبكات المحلية وأجهزة التخزين الإلكترونية المحمولة، واستخدام الشهادات الإلكترونية المُزوّرة كغطاء خفي لتحديث أنظمة تشغيلها(il se fait passer pour une mise à jour de Windows)، حيث لا ينتشر(**Flamer**) بصفة آلية أو أوتوماتيكية عبر مختلف الأجهزة إلاّ بأمرٍ من مركز تَحَكُّمِهِ أو تشغيله (Centre de commande)، ويسمح كذلك لمشغليه بإرسال أمر يُزِيل آثار البرنامج الخبيث تمامًا من الحاسوب المُصاب وذلك لتفادي الانتشار العشوائي الذي من شأنه أن يُزيدَ من احتمالات اكتشافه، وعليه فإنّ البرنامج الخبيث(Flamer) قادر على التقاط رسائل البريد الإلكتروني(e-mails) والبيانات المشفرة بصغة(PDF) ومُشاهدة ما يَحدُث على شاشة الحاسوب المُصاب، بل وحتى تشغيل ميكروفون ذلك الحاسوب(Activer le micro de l'ordinateur) لتسجيل الأصوات والمُحادثات في عين المكان وكذا تسجيل كلٍّ من المكالمات عبر خدمة سكايب(Skype) ونشاط لوحة المفاتيح والبيانات المرسلة عبر الشبكة(Mémoriser chaque frappe sur le clavier)، كما يمكن أن يُحوّلَ الحاسوب المُصاب إلى محطة البلوتوث(Déclencher l'émetteur-récepteur sans fil Bluetooth) لالتقاط المعلومات الشخصية من أجهزة البلوتوث القريبة مع إرسالها إلى خوادم التحكّم الخ...، وبالتالي فإنّ برنامج التجسّس فَلامُر(Flamer) صُمّم لغرض الحصول على المعلومات الحسّاسة التي تُساعد أو تفتح الطريق لتنفيذ الهجمات الإلكترونية في المستقبل، فمن بين الدول المُستهدفة نجد دول الشرق الأوسط على غرار كلّ من لبنان، سوريا، السودان، مصر، فلسطين، المملكة العربية السعودية، و"**إيران خاصّة**"، فحسب خبراء شركة الأمن المعلوماتي(Kaspersky) فإنّ البرنامج الخبيث مُصمّم من قِبَلِ أخصائيّين ذي قدرات عالية في مجال تكنولوجيا الاتصال والإعلام، بدعمٍ من إحدى الحكومات لغرض جمع المعلومات الحسّاسة حول أنظمة التحكّم الصناعي للمنشآت الصناعية، حيث أنّ الجماعة التي وقفت من وراء تصميمه كانت نفس الجماعة التي صَمَّمَتْ البرامج الخبيثة التي استهدفت البرنامج النووي الإيراني (Centrifugeuses d'enrichissement d'uranium de l'Iran) على غِرَارِ دودة(Stuxnet) ودودة(Duqu) الخ...

Benjamin FERRAN, « Israël et les États-Unis accusés d'avoir créée le virus Flame », Article de journal Le Figaro, publié le 20/06/2012 à 16:07 sur le site : http://www.lefigaro.fr/secteur/high-tech/2012/06/20/ consulté le 03/01/2016.

Voir aussi : l'**Alerte** de propagation « Flamer », Une menace extrêmement complexe et discrète cible le Moyen-Orient, article publié par Norton by Symantec sur : https://fr.norton.com/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east/article, consulté le 05/01/2016.

الحالات[1]، وبالتّالي فإنّ حجم التّهديد من الدّاخل يزداد سوءًا في حالة ما إذا كان مرتكبه شخصا ماهرا يتمتّع بمزية لا يتمتّع بها المهاجمون من الخارج، إذ يمتلك دراية شاملة حول تقنيات تكنولوجيا الاتّصال والإعلام ويُتقِن أو يُحْسِنُ التّعامل مع أساليب أو طرق طمس آثار الجريمة الإلكترونيّة المرتكبة من طرفه، على مستوى الشّبكة الدّاخليّة للمؤسّسة، كما أنّه لا يكون عُرضة للكثير من الاحترازات الأمنيّة التي يتعرّض لها المهاجمون من الخارج.

وعليه، يمكن للشّخص المُهدِّد من الدّاخل أن يقوم بأعمال يصعب على غيره القيام بها من الخارج، كمهاجمة الشّبكة الدّاخليّة للمؤسّسة التي يعمل فيها، لخلق منافذ أو نقاط عبور خفيّة في بروتوكول اتّصال الجهاز المستهدف، وفتح ثغرات في أنظمة الحماية التي وضعتها المؤسّسة لتحصين المعلومات المخزّنة، أو يقوم بمهاجمة المعلومات بالسّرقة أو التّغيير أو الحذف أو نقل المعلومات الحسّاسة المخزّنة على مستوى الشّبكة الدّاخليّة للمؤسّسة إلى الشّبكة الخارجيّة المتّصلة بالإنترنت[2]، أو يقوم بنقل البرمجيات الخبيثة من شبكة الإنترنت إلى الشّبكة الدّاخليّة للمؤسّسة بالتّواطؤ مع المؤسّسة المنافِسة لها، مُهَيِّأً بذلك أرضية الجّسر الذي يَعبُر منه المهاجمون من الخارج إلى أنظمة المعلومات التي تحاول المؤسّسة حمايَتُها، كما يمكن أن يتعلّق الهدف من تنفيذ التّهديدات الدّاخلية، تحقيق مكاسب ماليّة من خلال قيام المهاجم بسرقة البيانات السّريّة الحسّاسة للجهة التي يعمل فيها مع استخدامها لاحقا لطلب الفِدية منها، الخ...

رابعا– التّهديدات الخارجيّة.

تتمثل هذه التّهديدات في تلك التي يتسبّب في حدوثها أشخاص يعملون من خارج المؤسّسات أو الشّركات الصّناعيّة المستهدفة، إذ يستغلون الفجوات أو الثّغرات المتواجدة في

---

1) **Aglietta MICHEL et Scialom LAURENCE,** « Les défis de la monnaie électronique pour les banques centrales », p. 89. Article publié à partir de l'adresse suivante: http://www.sceco.univ-poitiers.fr/franc-euro/articles/MAgliettaLScialom.PDF, consultée le 14/04/2018.

2) **محمد عبد حسين الطائي، ينال محمود الكيلاني،** إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015، ص ص 120– 122.

أنظمة حماية شبكة الإنترنت للتّسلّل إلى المعلومات الحسّاسة، أو إقامة جسر مزيّف مع الشّبكة الدّاخليّة للمؤسّسة المستهدفة لغرض التّجسّس والسّيطرة على أنظمة التّحكّم الصّناعي التي تسمح بتنفيذ الهجمات الإلكترونية في المستقبل[1]، أو تعديل وتخريب أنظمة التّشغيل الخاصّة بها التي تُعدّ بمثابة الشّرايين والأوردة التي تتدّفق من خلالها البيانات والأوامر المعلوماتيّة لمُختلف الأجهزة، وبالتّالي فإنّ خطورة الهجمات الإلكترونيّة الخارجيّة تختلف باختلاف شخصيّة ودوافع مرتكبيها[2]، حيث قسّم خبراء تكنولوجيا الإعلام والاتّصال قراصنة الإنترنت إلى ثلاث فئات، فالأولى تتضمّن على أصحاب القبّعات البيض (White hat hackers ou Les chapeaux blancs) الذي يعملون في المؤسّسات الحكوميّة وشركات أمن

---

[1] يعتبر البرنامج الخبيث لدودة دوكو(**Duqu**) الجيل الأحدث من البرنامج الخبيث لدودة ستوكسنت(**Stuxnet**)، تم اكتشافه في سبتمبر 2011 من طرف مخبر التشفير وأمن الأنظمة لجامعة التكنولوجيا والاقتصاد ببودابست (Laboratoire de Cryptographie et de Sécurité Système (**CrySyS Lab**) de l'université polytechnique et économique.)، حيث اختلفت تحاليل ودراسات شركات وخبراء الأمن المعلوماتي حول درجة خطورة دودة(Duqu) على الأنظمة المعلوماتية، فحسب شركة الأمن المعلوماتي(Symantec) فإنّ دودة(Duqu) تحتوي على نفس التقنيات والمواصفات التي بُرمجت من أجلها دودة ستوكسنت(**Stuxnet**)، وأنّ الهدف من تصميم برنامج دودة(Duqu) يتعلق هو الأخر بمهام تخريبية أو هدّامة حيث يسعى على جمع أو الحصول على المعلومات الحسّاسة التي تسمح فيما بعد بتنفيذ الهجمات الإلكترونية الخطيرة، وأمّا دراسات شركتي الأمن المعلوماتي(F-Secure) و(McAfee) تؤكد أنّ برنامج دودة(Duqu) قادر على سرقة الشهادات الإلكترونية الأمنية لبرامج الحاسوب المُستهدفة التي تسمح باستحداث وخلق برامج خبيثة لتنفيذ الهجمات الإلكترونية في المُستقبل، وعليه اتفقت هذه الشركات حول الغاية التي صُمّم من أجلها البرنامج الخبيث لدودة(Duqu) والمتعلقة بجمع المعلومات الاستخبارية والحصول على معلومات ذات صلة بالشركات المُصنّعة، التي تسمح بتنفيذ الهجمات الإلكترونية الخطيرة على أنظمة التحكّم الصناعي (Les systèmes de contrôle industriels) وأنّ هذه الدودة(Duqu) تستهدِف برامج أنظمة تشغيل الحاسوب(Windows)، حيث تم تصميمها(Duqu) من طرف نفس الجماعة التي كانت من وراء تصميم البرنامج الخبيث لدودة(Stuxnet) المُستخدمة لإحداث الفوضى داخل البرنامج النووي الإيراني، والغريب في برنامج دودة(Duqu) أنّه صُمّم بأن يقوم بنفسه بمباشرة إجراءات تنحيته(le malware se désinstalle automatiquement) بصفة آلية بعد مرور 36 يوم ممّا يُعقّد أو يُقلّص من احتمالات كشف آثاره، وبالتالي فإنّ الجماعة التي وقفت من وراء هجوم دودة(Duqu) كانت تبحث عن المعلومات الحسّاسة كوثائق التصميم التي تُساعدها في المُستقبل على شنّ الهجمات الإلكترونية على منشآت التحكم الصناعي، وعليه فمن المُحتمل أنّ هجمات أخرى لجمع المعلومات قد بدأت بالفعل ولم يتم اكتشافها بعد[...].

Source : https://fr.wikipedia.org/wiki/Duqu/(consulté le 04/02/2016)

[2] **محمد عبد حسين الطائي، ينال محمود الكيلاني**، مرجع سابق، ص ص 123، 125.

المعلومات، أو حتّى بصفتهم منفردين لاكتشاف ثغرات البرامج والأجهزة والشّبكات للإبلاغ عنها من أجل سدّها ومنع استغلالها من قِبل المخترقين، حيث يقومون بتنفيذ هجماتهم المخطّطة بطريقة شرعيّة عندما يُطلب منهم ذلك وبأوامر من السّلطة.

من بين هؤلاء القراصنة، نجد كلّ من المخترع الأمريكي ستيفن غاري وزنياك (Stephen Gary WOZNIAK) باعتباره مهندس إلكتروني ومبرمج ورجل أعمال، ومن مؤسّسي شركة(APPLE) الشّهيرة[1]، والعالم الفيزيائي البريطاني "تيموتي جون بيرنر لي (Timothy John BERNERS-LEE) "الذي يعتبر العقل المُبدع وراء تطوير الشّبكة العنكبوتيّة العالميّة، ومُؤسّس مَوقِع "ويكيليكس(WikiLeaks)" الأسترالي "جوليان أسانج"(Julian ASSANGE) كمُطوّر للبرمجيات(Programmeur et développeur de logiciels libres)، كما يمكن أن يكون أصحاب القبّعات البيض مُجرمِي حاسوب تحوّلوا إلى قراصنة أخلاقيين على غرار الأمريكي "كيفين ميتنيك"(Kevin MITNICK)، المُلقب بالنّسر الأمريكي(Condor) الذي يعتبر كأكبر "هاكرز" في العالم وأحد أشهر مُخترقي أنظمة شبكات الحاسوب والهواتف، حيث أُعتقِل وسُجِن أكثر من مرّة، قَبْلَ أن يتحوّل إلى هاكر(Hacker) أخلاقي ويصبح مُستشارا في أمن تقنيات الدّفع الإلكتروني ومُتحدّثًا عاما في أمن الحاسوب، وصاحب العديد من المؤلفات في هذا الاختصاص من أهمها فنّ الاختراق (L’art de l’intrusion) وفنّ الاحتيال(L’art de la supercherie)، وصاحب نظرية كاملة في تحديد وسائل التّصدي للقراصنة تُدعى "الهندسة الاجتماعيّة"(social engeneering) أو(L'ingénierie sociale) حيث بات الآن (Kevin MITNICK) واحد من أصحاب كِبريات الشّركات المنتجة لبرمجيات الحماية الأمنيّة للشّبكات والحاسوب[2].

---

[1] **Rodrigo NIETO GÓMEZ**, « Cybergéopolitique : de l'utilité des cybermenaces », Revue Hérodote, 2014/1 (n° 152-153), pp. 110, 111.

[2] أنظر الموقع الإلكتروني التالي: https://fr.wikipedia.org/wiki/Kevin_Mitnick/(consulté le 02/03/2017)

فإلى جانب العالم(Kevin MITNICK) نجد كذلك الأمريكي "أدريان لامو" (Adrian LAMO) الذي يستخدم المقاهي والمكتبات ومقاهي الإنترنت لتنفيذ هجماته الإلكترونيّة(Pirate informatique de type grey hat)، من خلال اختراق مواقع إلكترونيّة لشركات شهيرة مثل "نيويورك تايمز"(New York Times) و"مايكروسوفت"(Microsoft) و"ياهو"(Yahoo!)، وذلك قبل أن يتحوّل إلى "هاكر" أخلاقي، حيث يعمل مستشارًا في أمن الحاسوب وساعد السّلطات الفيدراليّة الأمريكيّة في الكشف عن المتّهم (Bradley MANNING) في تسريب الآلاف من الوثائق الحسّاسة للحكومة الفيدراليّة في موْقِع(WikiLeaks)[1].

أمّا النّوع الثّاني من القراصنة، يتمثّل في أصحاب القبّعات السّود (Black hat hackers ou Les chapeaux noirs) الذين يخترقون أنظمة أمن الحواسيب لغرض تحقيق مكاسب شخصيّة، كسرقة بيانات بطاقة الائتمان أو البيانات الشّخصيّة لهدف بيعها، أو لتحقيق المنفعة الذّاتية كصنع ربوتات برمجية(BotNet) التي تُستخدم فيما بعد لشن هجمات إلكترونية ضدّ مواقع إلكترونيّة معيّنة، فمن بين أشهر هؤلاء القراصنة نجد كل من البريطاني "غاري مكينون(Gary MCKINNON)" المُتّهم بتنفيذ أكبر عمليات اختراق ضّد شبكات حواسيب حكومة الولايات المتّحدة الأمريكيّة، مثل أنظمة حواسيب الجّيش الأمريكي(القوّات البريّة والجويّة والبحريّة) ووكالة الأبحاث الفضائيّة(NASA) حيث تسبّب في وقوع أضرار بالغة، كما نجد كذلك "الهاكر" الأميركي "ألبرت غونزاليس"(Albert GONZALEZ) المتّهم على أنّه العقل المُدبّر لأكبر سرقة في التّاريخ لأجهزة الصّراف الآلي وبطاقات الائتمان، حيث يُعتقد أنّه، وجماعته من القراصنة، باعوا خلال الفترة من 2005 إلى 2007 الملايين من أرقام بطاقات الصّراف الآلي وبطاقات الائتمان ...الخ[2].

---

[1] أنظر الموقع الإلكتروني التالي : https://fr.wikipedia.org/wiki/Adrian_Lamo/(consulté le 03/03/2017)

[2] أنظر الموقع الإلكتروني التالي : https://fr.wikipedia.org/wiki/Albert_Gonzalez/(consulté le 06/03/2017)

تتمثّل الفئة الأخيرة من القراصنة في أصحاب القبّعات الرّمادية (Grey hat hackers ou Les chapeaux gris) التي تحتوي على مزيج من القراصنة ذوي القبّعات البيض وذوي القبّعات السّود، حيث يقومون تارةً بأعمال قانونيّة بمُساعدة أمنيّة لهدف تأمين الأجهزة والشّبكات ومعرفة نقاط الضّعف واستقطاب المزيد من إجراءات الأمن والوقاية، وتارةً أخرى يقومون بأعمالهم كقراصنة أشرار أين ينفّذون عمليات الاختراق لأغراض خبيثة أو لمصلحتهم الشّخصيّة حسب ما يَمْلِيهِ ضَمِيرُهُمْ الشّخصي[1].

الفرع الثاني
تنفيذ الهجمات الإلكترونيّة

عادة ما تتوافر لدى مرتكبي الهجمات الإلكترونيّة على أنظمة حماية الشّبكات التي تُخزّن وتنتقل عبرها المعلومات، ثلاثة عناصر أساسيّة تدفعهم لارتكابها والمتمثّلة في: وجود الدّافع **(أولا)**، الطّريقة المستخدمة في تنفيذ الهجمات الالكترونيّة **(ثانيا)**، وجود الثّغرات أو الفجوات **(ثالثا)**.

أولا– وجود الدّافع.

لا بدّ على كلّ شخص يُريد فعل شيء ما أن يكون لديه ما يدفعه لفعل ذلك، وعليه فإنّ دوافع مهاجم أنظمة أمن المعلومات تتعدّد وتختلف بحسب شخصية القائم بالهجوم والمجال المستهدف، فقد يكون الدّافع منه استكشاف كيفية عمل الأنظمة وطرق تقديم الخدمات، أو الرّغبة في إثبات قدراته الفكريّة أو مهاراته التّقنيّة أو مراقبة ورصد واعتراض الاتّصالات وحركة سير وانتقال المعلومات، أو استخدام بروتوكولات التّعريف بعناوين الإنترنت واستغلال نقاط الضّعف فيها لتخطيط الهجوم[2].

---

[1] **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص ص 550، 551.

[2] **سمير دنون**، العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية، شركة المؤسسة الحديثة للكتاب، لبنان، 2012. ص ص 215، 217، 218، 219.

كما يمكن أن يكون الدّافع من شنّ الهجمات الإلكترونيّة على مواقع التّجارة الالكترونيّة الحصول على الأموال، أو الرّغبة في الانتقام من الجهة المستهدفة وإبعاد أكبر عدد ممكن من الزّائرين لموقعها التّجاري، وهذا ما يحدث فيما بين الشّركات المنافسة، إذ تستعين إحداها بأحد المحترفين لاختراق أنظمة حماية معلومات الموقّع التّجاري التّابع للشّركة المنافسة لها، من أجل تعطيله أو تنفيذ هجمات رفض الخدمة فيه، لمنع وصول الزّبائن لموقعها وبالتّالي تقليص ميزتها التّنافسيّة وتشويه سمعتها التّجاريّة والشّهرة التي كانت تتمتّع بها في الأسواق[1].

ففي كلّ الظّروف، تكون الدّوافع من تنفيذ الهجمات الإلكترونيّة بحسب الأهداف المُسّطرة والمصلحة أو النّتيجة المرغوب تحقيقها، حيث يكون الدّافع ايجابيا في حالة ما إذا كانت نيّة مُنفّذ الهجمة الإلكترونيّة لا تهدف إلى إلحاق أيّ أذى بالغير[2]، من خلال التّلاعب أو إبراز

---

[1] **يوسف حسن يوسف**، الجرائم الدولية للإنترنت، مرجع سابق، ص ص 252– 256.

[2] استطاع الباحث في شأن الأمن المعلوماتي(**Chris ROBERTS**) أن يُسيطرَ على نظام الإنذار الخاص بشركة الطيران(Compagnie United Airlines) كالتّحكّم في درجة الحرارة لبعض أجهزة الطائرة ومستوى الوقود والزيت الخ...، حيث قام عدّة مرّات عبر شبكة التواصل الاجتماعي(Twitter) إخطار أعوان المكتب الفيدرالي للتّحريات الدّاخليّة(FBI) للولايات المتحدة الأمريكية عن الثغرات الأمنية المتواجدة في نظام((**IFE**)In-Flight Entertainment)، الذي يسمح بمشاهدة الفيديو واللّعب الخ... على متن الطائرة وذلك نظرا لضعفه وهشاشته، في حين تتم عملية الدخول إلى النظام باستخدام كابل إيترنت مع بعض التعديلات فيه(Câble Ethernet modifié) بعد فتح العُلبَة (Le boitier(**SEB**) **S**eat **E**lectronic **B**ox) المُتواجدة من تحت كلّ مقعد طائرة، حيث يمكنه فيما بعد التحكّم بصفة كليّة في نظام(**Thrust Management Computer**) الذي يُشرف على إدارة مخططات الرحلات ومحركات الطائرة(**Réacteurs de l'avion**) ووحدة(**CLB**) التي تتحكّم في عملية رفع الطائرة، وعليه أكّد الباحث للأعوان الفيدراليين بعد إيقافه أنّه كان بمقدوره خلال سنتي 2011 و2014 أن يُنفّذَ العديد من الهجمات الإلكترونية على متن 20 طائرة، وحتى تعديل قوّة دَفْع محرّكاتها أثناء تحليقها وما بالك بالأجهزة الأخرى، وهكذا أثارت القضية عدّة انشغالات وتساؤلات بشأن أمن الرّحلات الجويّة خاصة وأنّ الطائرات قامت بتعميم خدمات شبكات الويفي(**Réseaux Wi-Fi**) على متنها، حيث يُمكِن أن يُعوِّلَ عليها القراصنة لتنفيذ مختلف الهجمات الإلكترونية على مستوى أنظمتها.

Tanguy ANDRILLON, « Un hacker aurait réussi à prendre le contrôle d'un réacteur d'avion en plein vol. » Article de journal La Ruche, publié le 18 mai 2015 à 15 H 56 sur le site : http://www.laruche.it/, consulté le 15/03/2017.

مهارات أو قدرات تقنيّة أو الإزعاج أو محاولة اكتشاف ثغرات أمنيّة لسدّها فيما بعد أو الحصول على معلومات لتفادي الجريمة الخ...، أمّا إذا كان الدّافع سلبي، فتتجه نيّة المهاجم، في هذه الحالة إلى تحقيق مهام تخريبيّة، أو هدّامة، من شأنها أن تُلحق أضرارا فادحة للغير، والتي من شأنها أن تتسبّب في نشوب حروب فيما بين الدّول، كالتّجسّس السّياسي أو الصّناعي أو تدمير المواقع الإلكترونيّة أو اختراق قواعد البيانات بغية الحصول على معلومات حسّاسة للحكومات أو الشّركات الاقتصاديّة أو أيّ هيئة معيّنة[1].

كما يمكن أن يتعلّق الدّافع السّلبي بالانتقام، حيث يمكن أن يقوم أيّ مُبرمِج أو مدير على وشك أن يُطرد من عمله في شركة معيّنة بترك منافذ خلفيّة للنّظام(Backdoor)، أو تنصيب إحدى البرمجيات الخبيثة "كالقنبلة الموقوتة" تسمح له بتخريب أو تدمير نظام صاحب الشّركة بأكمله من دون علم هذا الأخير[2].

تجدر الإشارة إلى أنّه ظهرت فئة معيّنة من القراصنة(Hackers) المجهولين نظّموا أنفسهم في مجموعات صغيرة منعزلة، تعمل في نطاق مصطلح النّضال الالكتروني(Hacktivisme) الذي يشير اختصار إلى كلمتي(Hacker) و(Activisme)، حيث تختلف دوافعهم النّضالية وفقا لاتجاهات سياسيّة أو عسكريّة أو دينيّة وثقافيّة أو اقتصاديّة أو اجتماعيّة الخ...، من خلال القيام بعمليات الاختراق للعديد من شبكات الحاسوب والمواقع الإلكترونيّة التّابعة للحكومات، وشركات الحماية ومواقع الجيوش النّظامية والهيئات الرّياضيّة الدّوليّة(الخ...) للتّعبير عن مواقفهم واحتجاجاتهم، حيث يُسَخِّرُونَ خبراتهم

---

1) **Philippe LE TOUREAU**, op.cit., p. 357.
Rodrigo NIETO GÓMEZ, op.cit., pp. 102, 103.
عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية(الحاسب الآلي وشبكة المعلومات(الإنترنت))، دار الوراق للطباعة والنشر والتوزيع، بيروت، لبنان، 2004، ص ص 288–292.

2) **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص ص 166، 178.
جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة الحديثة)، درا البداية، عمان، الأردن، 2007، ص ص 166– 168.

وقدراتهم التّقنيّة في مجال تكنولوجيا الاتّصال والإعلام، لتنفيذ الهجمات الالكترونيّة في سبيل نُصرَة قضايا سياسيّة أو اجتماعيّة أو فكريّة أو دينيّة الخ...، في حين تعدّدت المواقف بشأن هذا النّوع من القراصنة المجهولين، حيث يرى البّعض أنّهم مناضلين إلكترونيين، ويعتبرهم الآخرون كمقاتلين إلكترونيين أو فوضويين، والبّعض الآخر وصف تصرّفاتهم بالإرهاب الإلكتروني الخ...[1]

فمن بين أبرز المجموعات المعروفة عن هؤلاء القراصنة نجد كلّ من مجموعة(Anonymous) أو القراصنة المجهولون، المنتشرين عبر العالم في مجموعات غير مركزية الذين يرتدون نمط معيّن من الأقنعة المُمَثِّلَة لشخصيّة(Guy Fawkes)، حيث نفذّت العديد من الهجمات الإلكترونية، كتسريب العديد من رسائل البريد الإلكتروني لرؤساء الدّول والكثير من الملفات الحسّاسة، التي يُدَّعَى على أنّها محميّة ومواقع الشّركات التّجاريّة والمصرفيّة العالميّة، الخ... [2]، كما نجد كذلك نادي فوضى الحاسوب (Chaos Computer Club) الذي يعتبر كأكبر تجمّع للقراصنة المجهولين، وكذلك مجموعات(Lulz security) و(Telecomix)[3] الخ...

ثانيا– طريقة تنفيذ الهجمات الإلكترونيّة.

يكمن سرّ نجاح الهجمات الإلكترونيّة المرتكبة على حساب أنظمة أمن المعلومات في الطّريقة المستخدمة في تنفيذ هذه الهجمات، والتي ينفرد بها المهاجمين المحترفين، حيث تكون لديهم خبرات وتصّورات واضحة وخطط واستراتيجيات مدروسة بدقّة وإحكام لتحقيق

---

1) **Julien PASTEUR**, « La faille et l'exploit : l'activisme informatique », Revue Cités, 2004/1 (n° 17), pp. 66, 67.

2) **Olivier HASSID**, « Edito », Revue Sécurité et stratégie, 2012/4 (n°11), p. 02.

أنظر كذلك الموقع الإلكتروني التالي: https://fr.wikipedia.org/wiki/Anonymous_(collectif)/ (consulté le 14/09/2018.)

3) انظر المواقع الالكترونية التالية: https://fr.wikipedia.org/wiki/Chaos_Computer_Club/(consulté le 16/09/2018.) ou https://fr.wikipedia.org/wiki/Telecomix/ ou https://fr.wikipedia.org/wiki/LulzSec/(consultés le 18/09/2018.)

الهدف المنشود، فلصّد هذه الهجمات أو التّخفيف في الأضرار التي تُلحقها، يجب معرفة طرق أو تقنيات تنفيذ الهجمات واستراتيجياته ودواعي أو متطلّبات نجاحها، فغالبا ما يتّم الاستعانة بخبرات القراصنة المحترفين لكشف مصدر وطرق تنفيذ الهجمات الإلكترونيّة، من أجل صدّها أو التّقليل من الأضرار المتسبّبة أو اعتراض الهجمات المستقبليّة[1].

فكثيرا ما يتم الاعتماد على تقنيّة البرمجيات الخبيثة(Malware) كالفيروسات والدّيدان وأحصنة طروادة والقنابل الموقوتة الخ...[2]، لتنفيذ الهجمات الإلكترونية حيث يتّم تضمينها أو إدراجها عمدًا في أنظمة الحواسيب لأغراض تكون عادة ضّارة، فقد تُستخدم لعرقلة تشغيل أنظمة حواسيب شركة معيّنة وجمع المعلومات الحسّاسة لها أو الوصول إلى الأنظمة الخاصّة لشبكاتها، أو تعطيل حركة سير موارد شبكات الحاسوب أو حتى تدمير أجهزتها أو تخريب نظام ملفات البيانات المتواجدة على مستوى القرص الصّلب(Disque dur)، حيث تتراوح درجة خطورة هذه البرمجيات من أذى بسيط إلى أذى غير قابل للإصلاح، يتطلّب إعادة تهيئة نظام التّشغيل وتركيب الأجهزة، نظرا إلى صعوبة إزالتها بشتى التّقنيات المتاحة[3].

وعليه، برزت في الآونة الأخيرة فئة معيّنة من برمجيات التّجسّس يكون الغرض منها تحقيق الأرباح، من خلال مراقبة متصفّحي شبكة الإنترنت وعرض إعلانات غير مرغوب فيها(Adware) أو(Publiciels)، أو إعادة توجيه إعلانات برنامج التّسويق إلى صانع برنامج التّجسّس لهدف الحصول على دعم هذه الإعلانات، أو الحصول على معلومات حسّاسة متعلّقة بمنتوج أو خدمة معيّنة(Spyware) من دون علم صاحبها، أو الاحتيال على مُستخدمي الإنترنت من خلال إقناعهم على تواجد برنامج خبيث في حواسيبهم وحثّهم

---

[1] **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص ص 589، 590.

[2] **جعفر حسن جاسم الطائي**، مرجع سابق، ص ص 200، 201.

[3] **Marie- Pierre FENOLL- TROUSSEAU, Gérard HASS**, La cybersurveillance dans l'entreprise et le droit, édition Litec, Paris, 2012, pp. 156, 157, 160, 161.

بالمقابل على ضرورة تحميل برنامج مُكافحة البرمجيات الضّارة (Antivirus ou Antispyware) الذي هو في الحقيقة برنامج مُزيّف(Scareware-Riskware أو (Rogue(escroc))[1].

كما يمكن أن يقوم القراصنة باستخدام إحدى برمجيات الفدية الخبيثة(Ransomwares) أو(Logiciels de Rançon-Rançongiciels)، التي تعتمد بدورها على نفس الحيل التّقنيّة المستخدمة في البرمجيات الخبيثة لاختراق أنظمة التّشغيل المعلوماتيّة من خلال استغلال الثّغرات الأمنيّة(Web Exploit) المتواجدة في أنظمة الحماية الأمنيّة، أو الاعتماد على رسائل الاصطياد الخادعة التي على إثرها يُقيّد برنامج الفدية الخبيث الوصول إلى نظام الحاسوب المُصاب، ويُطالِب بدفع فدية لصانع ذلك البرنامج(Hacker) مُقابل السّماح للضّحيّة(La victime) بالوصول إلى ملفاته أو المعطيات الشّخصيّة المُحْتَجَزَة كرهائن.

حيث أنّ بعض أنواع هذه البرمجيات الخبيثة(Rançongiciels) تقوم بتشفير جميع الملفات أو البيانات الالكترونية على مستوى القرص الصّلب(Disque dur) للنظام المعلوماتي، وتَعْرِض رسالة على شاشة الحاسوب تَطْلُبُ من مَالِكِه أو مستخدمه(الضّحيّة) دفع الفِدْيَةَ(Rançon) بمُقابل تسليم المفتاح الخاص بفك التّشفير المُسْتَحْوَذْ من طرف صانع ذلك البرنامج(Ransomware)[2].

---

[1] **Rogue (logiciel malveillant), Source :** https://fr.wikipedia.org/wiki/Rogue_(logiciel_malveillant)/ (consulté le 20/09/2018)

[2] يعود تاريخ ظهور برنامج الفدية الخبيث إلى عام 1989 أين يُعتبر برنامج(PC Cyborg Trojan) الذي أحدثه جوزيف بوب(**Joseph POPP**)، كأوّل برنامج فدية يستخدم تقنية التشفير المُماثل(Cryptographie symétrique) للملفات على مستوى القرص الصلب لجهاز الحاسوب، حيث يقوم البرنامج في بداية الأمر بتحذير المستخدم بشأن انتهاء مدة صلاحية بعض الرخص المتعلقة بالبرمجيات ليقوم فيما بعد بتشفير الملفات باستخدام نفس مفتاح التشفير على مستوى القرص الصلب(Le disque dur) لجهاز الحاسوب، ويطلب من مُستخدمه ضرورة دفع قيمة 189 دولار لشركة (PC Cyborg Corporation) بغية فك الشفرة المُستخدمة بنفس مفتاح التشفير، في حين تعود فكرة استخدام تقنية التشفير اللاتماثلي(Cryptographie asymétrique) في هجمات برنامج الفدية إلى عام 1996، التي أحدثها كلّ من **Adam**)

وعليه ازداد في الآونة الأخيرة استخدام برنامج الفدية الخبيث(Ransomware) من قِبَلِ القراصنة في تنفيذ الهجمات الإلكترونيّة للحصول على الأموال بطريقة سهلة عبر شبكة الإنترنت، التي من خلالها تتم عملية الدّفع سواء عن طريق التحويل إلى حساب مصرفي(Virement bancaire) أو بفرض رسوم إضافية على رسالة إلكترونيّة SMS) (surtaxés أو باستخدام العملات الافتراضية المُشّفرة كالبِتْكُويْن (Monnaie virtuelle comme le bitcoin)، والدّليل على ذلك تلك الهجمة الإلكترونيّة الأخيرة لبرنامج الفدية الخبيث(**WannaCry**) التي مسّت العديد من المرافق الحيويّة التّابعة لمختلف دول العالم[1].

(**L.Young**) و(**Moti Yung**) ضد أنظمة تشغيل(Macintosh SE/30)، وذلك باستخدام خوارزميات التشفير اللاتماثلي(Les algorithmes RSA ou TEA) التي اعتمد عليها القراصنة فيما بعد في تنفيذ هجمات برامج الفدية الأخرى، على غرار كلّ من (GPcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip ou MayArchive, etc.). لمزيد من المعلومات أنظر:

Christiaan BEEK, « Déclin des logiciels de demande de rançon au 2e semestre 2017 », pp. 32-34, Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre 2016. Disponible sur le site : https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf. , consulté le 27/01/2018.

[1] أنظر **الملحق رقم (23)**، ص 499.

يعتبر برنامج وناكراي(**WannaCry**) المعروف تحت تسمية(**WannaCrypt**) أو (**WanaCrypt0r 2.0**) من بين أحد برامج الفدية الخبيثة الذي أُستخدِم في تنفيذ الهجمات الإلكترونية المكثفة عبر العالم في ماي 2017، التي مسّت حوالي أكثر من ثلاثمائة ألف(300000) جهاز حاسوب عبر مائة وخمسون(150) دولة من العالم، وبالخصوص الهند، الولايات المتحدة الأمريكية وروسيا الفيدرالية، اسبانيا وبريطانيا، سويسرا، الخ...، التي تعتمد أجهزة حواسيبها على أنظمة تشغيل وِنْدَوْزْ اِكْسَبِي(Windows XP) وكذا وِنْدَوْزْ10(Windows10) التي لم يتم بَعْدُ تحديث أنظمة أمنها (Mises à jour de sécurité). وعليه تعتبر هجمات برنامج الفدية الخبيث(**WannaCry**) كأكبر عملية قرصنة إلكترونية لم يشهدها عالم الإنترنت من قَبْلِ، التي مسّت العديد من الشركات على غرار شركة الاتصالات الاسبانية(Telefónica)، والشركة الأمريكية للتوزيع(FedEx) ومُتعاملي الهاتف النقال(Vodafone, etc.) وهيئة خدمات الإغاثة (Le National Health Service) ووزارة الداخلية الروسية، وشركة صناعة السيارات الفرنسية رونو(Renault)، وكذا نظام المعالجة الآلية للبيانات الصحية التابع للمستشفيات الوطنية البريطانية((**NHS**) Système national de santé britannique) الذي يعتبر من بين أكبر ضحايا برنامج الفدية الخبيث(**WannaCry**)، الذي يعتمد من خلال تنفيذ هجماته الإلكترونية على استغلال الثغرات الأمنية(« MS17-010 » La vulnérabilité) المُستعملة من طرف البرنامج الخبيث(EternalBlue) لوكالة الأمن القومي الأمريكية(NSA)، التي اكتشفتها واستغلتها جماعة من الهاكر في أفريل

ثالثا– وجود الثّغرات أو الفجوات(Vulnérabilités ou Failles).

يُقصد بها تواجد نقاط أو مواطن ضعف في تصميم أو إعداد أو تهيئة البرمجيات المعلوماتية، أو الأجهزة التي تُحفظ أو تُخزن فيها المعلومات، أو معدات أو برامج تشغيل الشّبكات أو بروتوكولات الاتّصال التي تنتقل عبرها المعلومات، والنّقص في توثيق سياسات الحماية الخ...، والمُلفت للانتباه، أنّ كلّ مكوّنات شبكات الاتّصال تحتوي على مواطن ضعف قابلة للاستغلال من طرف منّفذي الهجمات الإلكترونيّة[1]، فعادة ما يقوم المُخترق

2017 يُطلق عليها تسمية(The Shadow Brokers et Equation Group)، وذلك بالرغم من قيام شركة ميكروسوفت بتحديث نظام التشغيل في شهر قبل 14 مارس 2017. فبمجرد اختراق البرنامج الخبيث جهاز الحاسوب المُستهدَف يقوم ذلك البرنامج بتشفير جميع الملفات والبيانات الالكترونية المعنية مع إعلان أو إظهار على شاشة الحاسوب المُصاب صفحة تتضمن على طلب تقديم الفدية لمُستخدم ذلك الحاسوب، مقابل الحصول على مفتاح التشفير الخاص بالملفات أو البيانات الالكترونية المحتجزة، ليقوم فيما بعد برنامج الفدية الخبيث بنفس العملية عبر شبكة الحواسيب المُصابة عبر دول العالم في ظرف سريع ووجيز، حيث يجب على الضحية منذ البداية(وقت ظهور الطلب على شاشة حاسوبه) الالتزام بدفع مبلغ الفدية بعملة البِتْكُويْنْ الإفتراضية(Bitcoin) عبر شبكة الإنترنت، التي يُعادل مبلغها 300 دولار أمريكي ليرتفع إلى 600 دولار في حالة ما إذا لم يقم المُستخدِم(الضحية) بدفع مبلغ الفدية الأول(300 دولار) في غضون الثلاثة أيام من ظهور الإعلان على شاشة حاسوبه، فإذا لم يقم بدفع قيمة الفدية للمرّة الثانية تتعرض ملفاته أو بياناته الإلكترونية المُحتجزة من قِبَلِ طَالِب الفدية(Hacker) إلى الإتلاف أو التدمير كجزاء لعدم دفع الفدية، كما أنّه في الحالة العكسية لا يوجد ما يضمن للمُستخدِم(الضحيّة) الحصول حقًّا على مفتاح التشفير الذي يسمح له باسترجاع ملفاته أو بياناته الالكترونية المحتجزة وذلك في حالة ما إذا قام بدفع قيمة الفدية، فحسب خبراء الأمن المعلوماتي فإنّ جماعة الهاكر التي كانت من وراء برنامج الفدية الخبيث استطاعت أن تتحصل على أكثر من 91000 دولار أمريكي، ولإيقاف أو الحدّ من سرعة انتشار برنامج الفدية الخبيث عبر أنظمة تشغيل الحواسيب، قام الباحث البريطاني في مجال أمن المعلوماتي بتسجيل اسم النطاق(**killswitch**) الذي أعدّه مُطوّري(Développeurs) برنامج الفدية الخبيث لضمان أداء مهام هذا الأخير عبر أجهزة الحواسيب المُصابة، حيث ينتشر ذلك البرنامج بسرعة في حالة عدم تسجيل اسم النطاق(**killswitch**) الذي يعتمد عليه أثناء أداء مهامه. للمزيد من المعلومات أنظر:

Nathalie GUIBERT, Damien LELOUP et Philippe BERNARD, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », article de journal Le Monde, publié le 13/05/2017 sur: http://www.lemonde.fr/international/article/2017/05/13/une-cyberattaque-massive-bloque-des-ordinateurs-dans-des-dizaines-de-pays_5127158_3210.html, consulté le 20/05/2017.

1) **Géraldine VACHE MARCONATO**, « Évaluation quantitative de la sécurité informatique : approche par les vulnérabilités », Thèse de Doctorat, Spécialité : Système Informatiques, École Doctorale Systèmes, Université de Toulouse, 2009, pp.34- 45.

Guillaume HARRY, « Failles de sécurité des applications Web », pp. 08- 30. Article disponible sur : http://www.cnrs.fr, consulté le 18/08/2018.

بالاستعانة على مجموعة من البرمجيات الخبيثة المُصّممة خصّيصا لكشف واستغلال الثّغرات المتواجدة على مستوى أنظمة الحماية الأمنيّة لشبكات الحاسوب، حيث تمّكنه فيما بعد في التّحكّم عن بُعد في الجهاز الذي تّم اختراقه من دون مُنازِع[1].

كما يمكن أن يقوم بعض مزوّدي خدمات الإنترنت (Google, Facebook, Microsof, Paltalk, Youtube, Skype, AOL, Société RSA, etc.) أو متعاملي الهواتف المحمولة (Orange, BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel et Interroute, etc.) بتقديم يد المساعدة لبعض شركات الأمن الوطنيّة(NSA, le GCHQ, le SPETSSVIAZ, etc.)، من خلال السّماح لها باستغلال الهفوات أو الثّغرات المتروكة عمدا في أنظمة الحماية الأمنيّة (يكون ذلك مجّانا أو بمقابل)، لهدف الحصول على البيانات الإلكترونيّة وجمع المعلومات اللاّزمة لترصّد مختلف التّهديدات الإلكترونيّة، وتفادي ارتكاب الجرائم الماسّة بالأمن والاقتصاد الوطنيين(الإرهاب، تبييض الأموال، الخ...)[2].

علاوة على ما سبق، فإنّ الثّغرات الأمنيّة يمكن أن يكتشفها مُطوّري برامج الحاسوب(Développeurs)، أو من طرف فئة الهاكرز(Hackers) الذين عادة ما يستعينون بتقنيات برنامج حاسوب إكسبلويت(Exploit)، الذي يسمح لأيّ شخص أو برنامج خبيث استغلال الثّغرات أو الهفوات في أنظمة الحماية الأمنيّة لنظام التّشغيل أو لأيّ برنامج

محمد عبد حسين الطائي، ينال محمود الكيلاني، مرجع سابق، ص ص 143- 146.

[1] **Fernand LONE SANG**, « Protection des systèmes informatiques contre les attaques par entrées- sorties », thèse de doctorat, spécialité : Réseaux, télécommunications, Systèmes et Architecture, École Doctorale Mathématique Informatique Télécommunication de Toulouse(EDMITT), Université de Toulouse, 2012, pp. 15, 16, 17.
Jonathan BROSSARD, « Sécurité : 15 ans d'échec », Revue Sécurité et stratégie, 2012/4 (n°11), pp. 09- 11, 13, 14.

[2] أنظر **الملحق رقم (24)**، ص 500.

Jean-MARC MANACH, « En attendant la « Cryptocalypse » », Revue Vacarme, 2014/4 (n° 69), pp. 103- 107.

حاسوب[1]، سواء تّم ذلك من خلال الاتّصال عن بُعد بالشّبكة أو البرنامج المُعرَّض للاختراق(Remote exploit) أو على مستوى الجهاز الذي يتطلّب اختراقه مُسبقا (Local exploit)، حيث يتسّبب ذلك البرنامج في إحداث سلوكيات غير مُتوّقعة أو غير مقصودة، من أجل الاستفادة من الأخطاء البرمجيّة والسّماح للبرنامج الخبيث، من بسط سيطرته على الشّبكة أو جهاز الحاسوب وتنفيذ هجمات الحرمان من الخدمة(Déni de service(DoS)).

فعن طريق تلك الثّغرات، يستطيع المعتدين إمّا بتطوير برامج معلوماتيّة خبيثة لاختراق نظم التّشغيل المعلوماتيّة، أو تسعى الشّركات المكتشفة لها(الثّغرات) إلى تطوير برامج وقائيّة لاستباق الهجمات وسّد أو ردم الفجوات أو الثّغرات القائمة على مستوى أنظمة حماية الشّبكات الدّاخليّة أو الخارجيّة[2].

---

[1] بما أنّ الأمن بصفة كلية ينعدم في مجال الأمن المعلوماتي استطاع كلّ من(Nitesh Dhanjan) و(Rujith) في 07 أفريل 2007، من اكتشاف ثغرة أمنية على مستوى أنظمة الحماية لموقع(Twitter) التي من خلالها أثبتوا أنّ التعرّف على رقم الهاتف المرتبط بحساب المستخدم، يكفي لوحده القيام بعملية انتحال هوية المستخدم وإرسال الرسائل الإلكترونية باسمه عبر تقنية(FakeMyText)، حيث قامت شركة تويتر فيما بعد بإتاحة تقنية كلمات المرور للمستخدمين التي تسمح بتحديد هوية أصحاب الحسابات، فبالرغم من ذلك الإجراء فإنّ مَوقِع شركة(Twitter) تعرّض في 2009 و2018 إلى عملية القرصنة أين تم اختراق العديد من حسابات المستخدمين بما فيهم رؤساء البلدان والشخصيات المشهورة، أين استحوذوا من خلالها على البيانات السرية لأصحاب هذه الحسابات، كما قِيلَ أنّ عدد من الأشخاص أو الشركات في مجال أمن المعلومات استطاعت أن تقوم بانتحال هوية مستخدمي موقع(Twitter)، لإبداء أراء(Points de vue) مُغايِرة وغير مُتطابِقة مع الآراء الحقيقية لأصحابها للتأثير حول موضوع أو مجرى أحداث معينة، وهذا ما حدث(حسب بعض الخبراء) في خلال حملة الانتخابات الرئاسية للولايات المتحدة الأمريكية لعام 2016. – لمزيد من المعلومات أنظر المواقع الإلكترونية التالية:

http://www.strategies.fr/actualites/medias/1030643W/ce_matin.htm et http://www.washingtontimes.com/news/2009/jan/05/obamas-twitter-site-hacked/(consultés le 02/11/2016) et http://www.techcrunch.com/2009/01/05/either-fox-news-had-their-twitter-account-hacked-or-bill-oreilly-is-gay-or-both/ et http://mashable.france24.com/medias-sociaux/20160719-twitter-compte-certification-badge-bleu/(consultés le 20/11/2018)

Voir aussi : **William AUDUREAU**, « Pour les djihadistes, la dynamique est plutôt d'abandonner Twitter », article de journal Le Monde, publié le 22 mars 2017 sur : http://www.lemonde.fr/pixels/article/2017/03/22/pour-les-djihadistes-la-dynamique-est-plutot-d-abandonner-twitter_5099068_4408996.html, consulté le 02/04/2017.

[2] مصطلح(**Aircrack-ng**) عبارة عن سلسلة من برمجيات مراقبة الشبكات اللاسلكية المُستخدمة لكسر مفاتيح (WEP et WPA) لشبكات الويفي(Réseaux WIFI)، وتُعتبر كتكملة لبرنامج(Aircrack) الذي تم إحداثه من

تجدر الإشارة، إلى أنّ بعض الشّركات التّجارية(amazon.com, etc.) تُصّرح بأساليب الأمان التي تعتمدها في إطار علاقتها المباشرة مع العملاء، لكسب الثّقة معهم ومنحِهم الضّمان بشأن المعلومات وخصوصيتها، إلاّ أنّ مثل هذه الأساليب من شأنها أن تَقَعَ تحت سيطرة القراصنة التي تُشّكل لهم حافزا ودافعا للتّجريب والاختراق في آنٍ واحد[1].

طرف(Christophe DEVINE) كمستشار في مجال أمن المعلومات، وتم تغيير تسميته فيما بعد من طرف (Thomas D'OTREPPE) إلى مصطلح(Aircrack-ng)، وعليه فإنّ الغاية الرئيسية من تلك البرمجيات تكمن في كشف الثغرات الأمنية المتواجدة في شبكة الاتصال اللاسلكية، وتتواجد في أنظمة تشغيل كل من(Windows, Linux et FreeBSD)، وبالمقابل يمكن لفئة القراصنة المحترفين(Crackers) استخدام إحدى هذه البرمجيات لاختراق شبكة الاتصال اللاسلكية المحلية من دون الحصول على أيّ ترخيص، وهذا ما حصل خلال الأسابيع الماضية لشهر أكتوبر 2017 أين قام أحد القراصنة بتنفيذ هجمة إلكترونية (Krack -Key Réinstallation(AttaCKs « attaque en أُطلق عليها تسمية((« réinstallation de clé، من خلال استغلاله لإحدى الثغرات الأمنية المتواجدة في شبكة الاتصال اللاسلكية الويفي واخترق جميع البيانات والمعطيات الشخصية المتداولة فيما بين المستخدمين، حيث بمقدوره القيام بتغيير أو تعديل تركيبة البيانات الإلكترونية الحساسة المُتداولة مع نشر إحدى البرمجيات الخبيثة الخطيرة ضمن شبكة الاتصال اللاسلكية الويفي، حيث اكتشف تلك الهجمة الباحث الجامعي(Mathy VANHOEF) من جامعة(Louvain) البلجيكية، وتم تأكيد ذلك فيما بعد المركز الحكومي الأمريكي للإخطار حول أمن المعلومات(US-CERT) وكذا المركز الفرنسي-(FR CERT)، حيث قرر الباحث(Mathy VANHOEF) عدم نشر مقاله عبر شبكة الانترنت الذي يُوضّح التقنيات التي استخدمها في كشف الثغرة المتواجدة، وذلك لتفادي استخدام هذه التقنيات من طرف القراصنة بأنفسهم في إحداث معداتهم الخاصة، وعليه مسّت تلك الهجمة جميع الأجهزة المتصلة بشبكة الويفي(Smartphone, ordinateur portable, etc.) ولتفادي تلك الهجمة أكدّ ذلك الباحث أنّ تغيير كلمة السّر الخاصّة ببروتوكول الاتصال بشبكة الويفي(WPA2) لا تجدي نفعا، وأنّ الوسيلة الوحيدة لتجنّب أثار الهجمة تكمن في تثبيت تحديثات أنظمة تشغيل أجهزة الحاسوب والهواتف الذكية، أين يصعب للمستخدمين تطبيق ذلك الإجراء لسبب أنّ بعض أجهزة الاتصال بشبكة الويفي لا تتوافر على تحديثات أنظمة تشغيلها، وكذا يوصى باستخدام الشبكات الإفتراضية الخاصة(VPN) في الاتصال وبروتوكولات الاتصال المؤمنة(https) لتبادل البيانات الإلكترونية فيما بين المستخدمين الخ... لمزيد من المعلومات أنظر:

Martin UNTERSINGUR, « Une grave vulnérabilité découverte dans les réseaux Wi-fi », article de journal Le Monde, publié le 16/10/2017 sur : http://www.mobile.lemonde.fr/pixels/2017/10/16/une-grave-vulnérabilité-découverte-dans-les-réseaux-Wi-fi_5201770_4408996.html, consulté le 20/10/2017.

Guillaume BONVOISIN, « Faille Krack Wi-Fi : 5 mesures à prendre pour se protéger du piratage », article de journal CNETFrance.fr, publié le 17/10/2017 sur : http://www.cnetfrance.fr/news/wifi-mesures-securité-piratage-39858764.htm, consulté le 25/10/2017.

[1] **Vincent WEAFER**, « Partage de cyberveille sur les menaces : le danger de l'inconnu », pp. 09, 12, 14 , 15, Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre

الفرع الثالث
أهداف تأمين مواقع التّجارة الإلكترونيّة

أصبحت شبكة الانترنت منذ نشأتها عُرضة لمختلف المخاطر والتّهديدات التي تمّس بالأنظمة المعلوماتيّة، وأمن البنية التّحتيّة للشّبكات وما عليها من نقاط الدّخول والخروج والتّخزين واعتراض المعلومات، وكشف نقاط الضّعف التي تفسح المجال للقيام بعمليات الاختراق والتّخريب والتّدمير أو التّعطيل لمواقع التّجارة الإلكترونيّة، وحتّى كشف أسرار البيانات الإلكترونيّة الحسّاسة للشّركات والأفراد سواء الشّخصيّة منها أو الصّناعيّة والتّجاريّة والمهنيّة، ومما لا شّك فيه أنّ اهتمامات سياسات أمن شبكات الاتّصالات تتمحور بالخصوص إلى تحقيق الغايات أو الأهداف التّالية: التّعريف بهويّة أطراف التّعامل الالكتروني **(أولا)**، سريّة البيانات المتداولة **(ثانيا)**، سلامة محتوى التّصرف الالكتروني **(ثالثا)**، ضمان الوصول إلى المعلومات **(رابعا)**، عدم إنكار التّبادل الالكتروني **(خامسا)**.

أولا– التّعريف بهويّة أطراف التّعامل الإلكتروني(Identification):

إنّ تنامي إجراءات اختراق أنظمة حماية المعلومات وانتشار عمليات انتحال الهويّة والقرصنة وظهور مواقع إلكترونية مزّيفة تنتحل هويّة مواقع إلكترونيّة حقيقيّة، كل ذلك يستوجب ضرورة إتّباع حلول تقنيّة تضمن تحديد هويّة أطراف التّعامل الإلكتروني باستعمال الأرقام السّريّة ووسائل التّشفير التّماثلي واللاّتماثلي، وتقنيات التّعريف البيولوجيّة للمستخدم ومدى الاستعانة بخدمات وسيط محايد عن أطراف التّعامل الإلكتروني الخ... [1].

2016. https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf. , consulté le 29/01/2018.

[1] تعرضت الخدمات المتاحة من طرف شركة فيس بوك في الآونة الأخيرة إلى الكثير من الانتقادات نظرا لفقدان معايير السلامة والأمن والخصوصية بشأن البيانات والمعطيات الشخصية المتداولة، واحترام حُرمة الحياة الخاصة للمستخدمين التي تستوجب الحماية، حيث اضطرت العديد من الدول إلى اتخاذ إجراءات الرقابة على كلّ ما يتم تداوله على مستوى موقع فيس بوك وحظره في بعض الأحيان لدواعي السلم والأمن القوميين (République populaire de Chine , le Viet Nam , l'Iran , l'Ouzbékistan , le Pakistan , la Syrie, le Bangladesh, etc.)، لتفادي تنظيم حركات

ثانيا– سريّة أو موثوقيّة البيانات المتداولة(Confidentialité):

ينصّب هذا العنصر حول حماية خصوصيّة وسريّة المعلومات الإلكترونيّة المتداولة بين صاحب الموقع التّجاري والعملاء، لتوفير أعلى درجة من الأمان في التّعامل، مع ضمان قدر معقول من الخصوصيّة للبيانات الإلكترونيّة التي يتّم تخزينها أو تداولها عبر شبكة الإنترنت[1]، لكن يبدو أنّ مسألة تأمين البيانات الإلكترونيّة المتداولة مرتبطة بالمركز المالي للشّركة التّجاريّة، فكلّما كانت قدرتها الماليّة عالية تزداد قدراتها على تَحَمُّلِ التّكاليف الخاصّة بتأمين المعلومات عبر شبكاتها[2].

وعليه، ينبغي على المؤسّسة وضع ترتيبات تقنيّة موثوقة ومؤمّنة لمنع الاستخدام أو الإطّلاع غير المرّخص على المعلومات الحسّاسة أو السّريّة، بما فيها المعلومات الشّخصيّة وأرقام البطاقات المصرفيّة الإلكترونيّة والكلمات السّريّة المتعلّقة بالعملاء أو الأسرار

المعارضة أو التحريض على شنّ هجمات إرهابية أو القيام بأعمال الشغب ضد السلطة الخ...، وبالمقابل قامت شركة فايس بوك بوضع بعض إجراءات السلامة كإرسال رسالة بريدية تحذيرية إلى كلّ مُستخدم تعرّض حسابه إلى عملية الاختراق أو الانتهاك، مع إتاحتهم إجراءات تغيير أو تعديل كلمات المرور الخاصة بهم أو إلغاء الحساب أو إيقاف التعامل أو الاتصال مع مُستخدم أخر الخ...، كما قامت الشركة في 15 جوان 2017 بتوظيف حوالي 150 خبير في مجال مكافحة الإرهاب حيث كان ذلك بمبادرة من رئيسة الوزراء البريطانية(Theresa May) تزامنا مع الأحداث الإرهابية التي وقعت في لندن ومانشستر(Londres et Manchester)، مع حثّ دول المجموعة السبعة(G7) على سنّ تشريعات وتنظيمات لإرغام الشركات المسؤولة عن خدمات شبكات التواصل الاجتماعي على اتخاذ المزيد من إجراءات الوقاية والسلامة.

للمزيد من المعلومات أنظر المواقع الالكترونية التالية:

http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia(consulté le 10/09/2017) et http://www.forbes.com/2006/09/11/facebook-opens-up-cx_rr_0911facebook.html(consulté le 12/09/2017) et http://fr.techcrunch.com/2007/08/13/le-code-source-de-facebook-pirate-et-publie/), TechCrunch.com(consulté le 14/09/2017) et http://www.lepoint.fr/high-tech-internet/facebook-3-000-personnes-de-plus-pour-filtrer-les-images-violentes-03-05-2 017-2124539_47.php(consulté le 10/05/2017.)

[1] **أمير فرج يوسف**، عالمية التجارة الإلكترونية وعقودها وأساليب مكافحة الغش التجاري الإلكتروني، المكتب الجامعي الحديث، الاسكندرية، 2009، ص ص 112، 113.

[2] **عبد الفتاح بيومي حجازي**، التجارة الالكترونية وحمايتها القانونية: نظام التجارة الإلكترونية وحمايتها المدنية، الكتاب الأول، دار الكتب القانونية، مصر، 2007، ص ص 273– 276.

المعلوماتيّة المملوكة للمؤسّسة، وهو ما يتطلّب تحليلا دقيقا لمتطلّبات الأمن حتّى يقع الاختيار المناسب لوسيلة التّأمين التي تحقّق الأمن والموثوقيّة الملائمين[1].

فغالبا ما تكون الأخطاء البشريّة السّبب الحقيقي في تلف أو سرقة المعلومات الشّخصيّة للعملاء أو لتنفيذ الهجمات المنظّمة من داخل المؤسّسة، فمن المفروض على أعوان هذه الأخيرة أن يلتزموا بالمحافظة على سريّة المعلومات التي عُهِدَتْ إليهم ولا يجوز لهم القيام بإفشائها للغير[2]، حيث يجب على المؤسّسة التّجاريّة أن تلتزم بمعايير توظيف الأشخاص المؤتمنين، عن طريق حُسن اختيارها لأشخاص مؤّهلة وكفوءة، جديرة بالثّقة للقيام بمسؤولياتهم وواجباتهم المهنيّة وتتمتّع بخبرات عالية في تقنيات تكنولوجيا الاتّصال والإعلام، وأن تكون لديهم دراية ومعرفة شاملتين بأحكام القوانين والتّنظيمات الخاصّة بالمعاملات الإلكترونيّة وبالخصوص معاملات التّجارة الإلكترونيّة والمصرفيّة[3].

ثالثا– سلامة محتوى التّصرف الإلكتروني(Intégrité):

إنّ معاملات التّجارة الإلكترونيّة تتّم في بيئة إلكترونيّة إفتراضيّة مملوءة بالمخاطر المتعلّقة بسرقة المعلومات الخاصّة بأطراف التّعامل التّجاري، والوصول غير المرّخص من طرف القراصنة إلى المعلومات الإلكترونيّة المتبادلة، والانتشار الهائل للبرمجيات الخبيثة التي تُؤدي خدمات عن بعد لأصحابها كتجسّس كلمات العبور وتوقيع المحرّرات الإلكترونيّة بدلا من أصحابها، تخريب أو تدمير الملفات الإلكترونيّة وإتلافها وتحويل الأموال بطرق غير

---

[1] **عبد الفتاح بيومي حجازي**، مرجع سابق، ص ص 273– 276.

عبد الرحمن بن عبد الله السند، مرجع سابق، ص ص 46– 51.

Voir aussi : **Fernand LONE SANG**, op.cit., pp. 09, 10.

[2] **علاء عبد الرزاق السالمي**، مرجع سابق، ص ص 374– 376.

Fernand LONE SANG, op.cit. 09, 08.

[3] **Didier CARRÉ**, « L'entreprise : nouveaux défis cyber », Revue Sécurité et stratégie, 2014/4 (n°19), pp. 92, 93.

مشروعة فيما بين الحسابات المصرفيّة الخ...[1]، كل ذلك يتطلّب إعداد تصميم محكم ودقيق لأجهزة حماية مواقع التّجارة الإلكترونيّة، من حيث ضبط صلاحيات النفاذ والوصول إلى عتادها، مع توثيق جميع العمليات والتّصرفات، التي تجرى على مكوّنات شبكة الاتّصال الدّاخليّة والخارجيّة(الإنترنت)، والمراقبة الدّورية للتّأكد من بقاء الشّبكات محميّة، مع تحديد نقاط الضّعف واختيار المعايير والتّخطيط لتنفيذ الضوابط الأمنيّة اللاّزمة[2].

رابعا– ضمان الوصول إلى المعلومات(Disponibilité):

إنّ التّطور المذهل والسّريع في تقنيات تكنولوجيا الاتصال والإعلام زاد من أهمّية تشغيل أنظمة المعلومات وبقاءها بصورة مستمرّة، حيث أنّ أيّ توّقف لها يكبّد المؤسّسات الاقتصاديّة خسائر ماديّة ومعنويّة فادحة، في حين يجب أن تكون جميع مكوّنات النّظام المعلوماتي متوّفرة، وتتضمّن على تطبيقات وقواعد بيانات وخادم ومعدّات التّخزين وحماية حدود شبكة الاتّصال من بدايتها إلى نهايتها الخ...، حتى يتمكّن من له الحق في الاطّلاع على المعلومات في الوصول إليها بكلّ ثقة وأمان[3].

خامسا– عدم إنكار التّبادل الإلكتروني(Non- répudiation):

تعتبر العقود المبرمة عبر مواقع التّجارة الإلكترونيّة الأكثر انتشارا واستخدما في مجال إبرام مختلف صفقات التّجارة الإلكترونيّة عبر شبكة الإنترنت، حيث تتّم من خلالها عمليات تبادل الوثائق والبيانات الإلكترونيّة في بيئة إلكترونيّة افتراضيّة مملوءة بالمخاطر، وعليه تُثير معاملات التّجارة الإلكترونيّة العديد من المسائل التّقنيّة والقانونيّة حول موثوقيّة وسائل إثبات التّصرفات الإلكترونيّة وضمان عدم إنكار محتواها، ومدى التّأكد أو الوثوق من صّحة العقود الإلكترونيّة، وسلامة صفة الأطراف المبرمة لها عبر شبكة الإنترنت، التي تستوجب إرساء

---

[1] **عمرو عيسى الفقى**، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، مصر، 2006، ص ص 107– 109.

[2] **Stéphane LOHIER, Dominique PRÉSENT**, Internet : Services et réseaux, Dunod, Paris, France, 2004, p. 159.

[3] **Stéphane LOHIER, Dominique PRÉSENT**, op.cit., p. 159.

منظومة قانونيّة تنص صراحة على الاعتراف بطرق الإثبات الإلكترونيّة الحديثة الموثوق بها من طرف الجهات الرّسميّة، حيث يتمكّن من خلالها أطراف التّعامل الإلكتروني من إثبات محتوى تصّرفاتهم الإلكترونيّة، مع عدم إنكارها[1].

المبحث الثاني

توسّع تهديدات أمن مواقع التّجارة الإلكترونيّة بظهور المصارف الالكترونيّة وتَطوُّر تقنيات الدّفع الإلكتروني

عرفت المنظومة المصرفيّة العالمية في مجال الاقتصاد الرّقمي عدة تحوّلات وتطوّرات جعلتها تتماشى مع الخيارات الاقتصاديّة الرّاهنة التي فرضتها تكنولوجيا الثّورة الرّقمية في مجال الخدمات المصرفيّة، كلّ ذلك دفع بمختلف المؤسّسات المصرفيّة إلى إعادة النّظر في سياساتها المصرفيّة، وانتهاج هندسة ماليّة رقميّة حديثة من شأنها أن تساهم في تطوير الخدمات المصرفيّة وجذب الكثير من المتعاملين لإنعاش ميدان التّجارة عبر شبكة الإنترنت**(المطلب الأول)**.

شهدت الأنظمة والتّطبيقات الماليّة التّقليديّة تطوّرات مذهلة وسريعة من حيث أدوات وتقنيات الدّفع الإلكتروني التي أصبحت تتم عبر شبكة الإنترنت، وذلك تزامنا مع توسّع وانتشار تطبيقات التّجارة الإلكترونيّة، التي وضعتها الشّركات أو المؤسّسات في صميم اهتماماتها، وتسابقت على الاستفادة من التّسهيلات التي تتيحها خدماتها، بُغية الحصول على الإيرادات من العملاء بطريقة آمنة وكفوءة، مع تمكين هؤلاء من الحصول على ما يريدون من سلع أو خدمات بطريقة موثوقة عبر شبكة الإنترنت **(المطلب الثاني)**.

---

[1] **Stéphane LOHIER, Dominique PRÉSENT**, op.cit., p. 159.

يونس عرب، "أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها"، مرجع سابق، ص ص 2، 3.

المطلب الأول

توسّع تهديدات أمن مواقع التّجارة الإلكترونيّة بظهور المصارف الالكترونيّة

يعتبر القطاع المصرفي من بين أهم القطاعات الاقتصاديّة الأكثر حساسيّة وتأثّرا بثورة تكنولوجيات الاتّصال والإعلام، التي ساهمت في تنويع وتطوير الخدمات المصرفيّة الإلكترونيّة عبر شبكة الإنترنت، في ظل المنافسة المتنامية فيما بين المصارف، وقد جاء مفهوم المصارف الإلكترونيّة كمَسار جديد ضمن تطبيقات التّجارة الإلكترونيّة التي أثّرت على السّياسات المصرفيّة، وذلك بوصفها تنفرد في تقديم خدمات مصرفيّة خاصّة ومتميّزة للمتعاملين معها(**الفرع الأول**)، كما أنّ مهام المصارف الإلكترونيّة متنوّعة ومتعدّدة بحسب الأهداف المرجوة من كل خدمة(**الفرع الثاني**)، التي من خلالها تُتيح المصارف الإلكترونيّة مجموعة من المزايا لأطراف التّعامل الإلكتروني عبر شبكة الإنترنت(**الفرع الثالث**).

الفرع الأول

مفهوم المصارف الإلكترونيّة

ساهمت الثّورة الرّقميّة في تطوير المعاملات المصرفيّة وتجريدها من مادياتها إلى دعامات إلكترونيّة، حيث ظهرت مصارف افتراضيّة عبر شبكة الإنترنت تتيح كافّة المتطلّبات اللاّزمة للخدمات الإلكترونيّة المصرفيّة(**أولا**)، التي جعلت المصارف الإلكترونيّة تنفرد بمجموعة من الخصائص التي تُميّزها عن المصارف التّقليديّة(**ثانيا**).

أولا– تعريف المصارف الإلكترونيّة:

تعتمد العمليات المصرفيّة في وقتنا الحالي على الاتّصالات والمعلومات سواء فيما بين المصارف أو مع العملاء، إذ تطوّر مفهوم الخدمات الماليّة من مجرّد تنفيذ أعمال عبر الخط، إلى مصرف له وجود كامل عبر شبكة الإنترنت يحتوي على موقع إلكتروني خاص به يتضمّن على كافّة المتطلّبات اللاّزمة لأداء العمليات المصرفيّة الإلكترونيّة، التي ساهمت بظهور الفكرة المبدئيّة للمصارف المتقدّمة أو المتطوّرة التي يُطلق عليها العديد من

المصطلحات، كالبنوك الإلكترونيّة(Electronic Banking)، بنوك الإنترنت (Banking Internet)، بنوك الويب(Web Banking)، بنوك الخدمة الذّاتية(Self Service Banking)، البنك المنزلي(Home Banking)، البنك على الخط(Online Banking)، البنوك الإلكترونيّة عن بُعد(Remote Electronic Banking)[1].

فبالرّغم من تعدّد هذه المصطلحات إلاّ أنّ جوهرها يُؤدّي إلى نفس المعنى، وذلك بالنّظر إلى أنّ المصارف الإلكترونيّة تُتيح خدمات إداريّة وماليّة عن بُعد، عبر قنوات مصرفيّة إلكترونيّة، تسمح للعملاء بإدارة حساباتهم أو القيام بالاستشارات الماليّة والإداريّة وخدمات الاستثمار والتّجارة وغيرها، في أيّ مكان أو وقت يريدونه[2].

وقد تزامن ظهور فكرة المصارف الإلكترونيّة مع ظهور فكرة النّقود الإلكترونيّة في بداية الثّمانينات، التي أتاحت الفرصة فيما بعد للمؤسّسات الماليّة والمصرفيّة باستخدام تقنيات دفع إلكترونيّة حديثة ومتطوّرة، لتمكين المتعاملين من إجراء معاملاتهم المصرفيّة بشكل إلكتروني، وذلك باعتباره اتجاها حديثا مغايرا عن ما هو معروف في المصارف التّقليديّة، في حين يعتبر "نت بانك"(Net.B@nk) كأوّل مصرف إلكتروني ظهر في منتصف التّسعينيات بالولايات المتّحدة الأمريكيّة سنة 1995[3].

---

[1] **مصطفى كمال طه، وائل أنور بندق**، الأوراق التجارية (الكمبيالة– السند الإذني– الشيك– النقود الإلكترونية– الأوراق التجارية الإلكترونية– بطاقات الوفاء والائتمان)، دار الفكر الجامعي، الإسكندرية، 2005، ص ص 330، 331.

محمد البنان، العقود الإلكترونية، منشورات المنظمة العربية للتنمية الإدارية(أعمال المؤتمرات)، مصر، 2007، ص ص 10–13.

يوسف حسن يوسف، البنوك الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص ص 11–13، 37، 38.

[2] **Michel AGLIETTA et Laurence SCIALOM**, op.cit., p 85.

يونس عرب، "العقود الإلكترونية– أنظمة الدفع والسداد الإلكتروني"، ص ص 122، 123، 124، مقال منشور عبر الموقع التالي: http://www.arablaw.org

[3] **Source:** https://en.wikipedia.org/wiki/NetBank/(consulté le 19/05/2017)

محمد البنان، مرجع سابق، ص 10.

انطلاقا من ذلك، يُمكن تعريف المصارف الإلكترونيّة على أنّها:" **عبارة عن مواقع إلكترونيّة مصرفيّة عبر شبكة الإنترنت، تتيح تسهيلات عن بُعد لانجاز العديد من الخدمات المصرفية بشكل إلكتروني.**"

وبذلك استطاعت شبكة الإنترنت أن تغيّر من وجه الأعمال وفي نمط أداءها، فعن طريقها يمكن أن يتحقّق على أرض الواقع بناء مصرف من دون جدران أو مباني ومكاتب وموظّفون يتّصلون مباشرة بالعملاء[1]، فتكلفة إحداث موقع مصرفي عبر شبكة الإنترنت قليلة بكثير مُقارنة مع التّكاليف التي تتطلّبها عملية تشييد وبناء فرع مصرفي واحد، كما أن عملية جذب العملاء من عدّة أنحاء أو مناطق من العالم لا تستدعي حاليا التّنقل إليهم أو حتى اللّجوء إلى فتح فروع مصرفيّة قائمة تابعة للمصارف الرّئيسيّة.

بالإضافة إلى ذلك، تتيح المواقع الإلكترونيّة المصرفيّة عدّة منافذ للعملاء التي تقودهم أو تُوّجههم مباشرة إلى قواعد بيانات تابعة لمواقع إلكترونيّة حليفة مُكَمِّلَة للخدمات المصرفيّة المتاحة من قِبَلِ المصرف، كمواقع مقدّمي خدمات التّصديق الإلكتروني المعتمدين ومواقِع بورصات تداول الأسهم والسّندات، ومواقع إصدار وإدارة البطاقات الماليّة، وأيّ موقِع من شأنه أن يتيح نوع من الخدمات المصرفية أو الاستشارية عبر الموقع الإلكتروني للمصرف.

ثانيا– خصائص المصارف الإلكترونيّة:

تتمتّع المصارف الإلكترونيّة بمجموعة من الخصائص والمتمثّلة فيما يلي:

أ)– تتميّز بأنّها مصارف افتراضيّة تتيح للعملاء خدمات مصرفيّة تقليديّة(سحب ودفع وتحويل الخ...)، بطرق إلكترونيّة حديثة عبر شبكة الإنترنت، من دون تنقلهم إلى المَوقِع الجغرافي للمصرف.

يونس عرب، "العقود الإلكترونية– أنظمة الدفع والسداد الإلكتروني"، مرجع سابق، ص 121.

[1] **منير محمد الجنبيهي، ممدوح محمد الجنبيهي**، البنوك الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2004، ص 18.

ب)– يسمح المَوقِع الإلكتروني للمصرف للمتعاملين معه بالدّخول مباشرة إلى قاعدة بياناته لإجراء مختلف العمليات المصرفيّة، مع تزويد حواسيبهم الشّخصية بمجموعة من البرامج المعلوماتيّة ذات صلة بمعاملاتهم المصرفيّة الشّخصيّة (Personal Financial Management(PME), Microsoft's Mony, Meca's Managing your mony, etc.) .

ج)– تُمكّن المصارف من تسويق الخدمات المصرفيّة عبر شبكة الإنترنت من أجل تعزيز مكانتها التّنافسيّة لجذب أكبر عدد ممكِن من المتعاملين، والرّقي إلى مستوى المعاملات التّجاريّة العالميّة[1].

د)– تستطيع المصارف عن طريق مواقع الويب تقديم جميع المعلومات المتعلّقة ببرامجها ومنتجاتها وخدماتها المصرفيّة، وتتيح الاتّصال والتّبادل بينها(المصارف) وبين المتعاملين، وإثارة التّفاعل معهم لإنجاز معاملاتهم بطرق إلكترونيّة عبر شبكة الإنترنت[2].

هـ)– تُقدم المصارف الافتراضيّة العديد من الفوائد لأطراف العملية المصرفيّة، بحيث تمكّن من استقطاب أو جذب أكبر عدد ممكن من العملاء، وإتاحة خدمات مصرفيّة حديثة ذات نوعيّة وجودة عاليتين، كما تساهم على تخفيض التّكاليف النّاجمة عن الخدمة وتختصر من وقت ومكان أداء الصّفقات التّجاريّة، وتزيد من معنويات وقدرات وكفاءة المصارف الإلكترونيّة.

الفرع الثاني
أهمّية المصارف الإلكترونيّة ومزاياها

أفرزت الثّورة الرّقميّة مجوعة من الأساليب والتّقنيات التّكنولوجيّة الحديثة التي استخدمت في المجال المصرفي، لهدف عصرنة الخدمات المصرفيّة وتحويلها من طابعها المادّي إلى دعامات إلكترونيّة(**أوّلا**)، كما أنّ التّوسّع الهائل في اقتصاد المعلومات والانتشار السّريع

---

[1] **Thierry DISSAUX,** « Paiements, monnaie, banque électroniques : quelle évolution pour la banque ? », Revue d'Économie financière, n°53, 1999. La monnaie électronique. pp. 122- 126.

[2] **محمد عبد حسين الطائي**، مرجع سابق، ص 229.

للشّبكات المعلوماتيّة أعطى دفعا جديدا لنمط إدارة المصارف الإلكترونيّة، التي أصبحت تتيح خدماتها وفقا لمستويات من الجودة تتناسب مع إدراك وتوقّعات عملائها(**ثانيا**).

أولا– أهمّية الخدمات المصرفيّة الإلكترونيّة:

تكمن أهمّية الخدمات المصرفيّة الإلكترونيّة في النّقاط التّالية:

أ)– تحسين نمط أداء المصارف الإلكترونيّة: إنّ التطوّرات التي عرفتها الثّورة الرّقميّة والانتشار السّريع وغير المسبوق للتّطبيقات البرمجيّة، ساهم بشكل كبير في عولمة أعمال المصارف وغيّرت من نمط إدارة وتسيير الخدمات المصرفيّة[1]، من خلال توسيع قاعدة المتعاملين معها وتحسين كفاءة أداء المصارف وزيادة مستوى ومردوديّة الخدمات المتاحة عبر شبكة الإنترنت باعتبارها شبكة الشّبكات.

ب)– تحسين جودة الخدمات مع تخفيض التّكاليف: إنّ تحسين جودة الخدمات المصرفيّة مرهون بمدى تجاوب المصارف مع التّقنيات التّكنولوجية الحديثة وتنويع قنوات التّوزيع الإلكتروني لغرض جذب ولاء العملاء، كما أنّ الاعتماد على الشّبكات المعلوماتيّة يساهم بشكل كبير في تخفيض النّفقات وتوفير فرص نقل المعلومات بأقل التّكاليف مع الاقتصاد في الوقت.

ج)– التّأثير على سلوك العملاء: إنّ تصميم جودة الخدمة المصرفيّة الإلكترونيّة يحتاج إلى دراسة توقّعات العملاء حول مستوى الخدمات المتاحة ومدى إشباعها لرغباتهم وحاجياتهم، حيث يعتبر الرّضا بمثابة الأداء المُدرِك للتّوقعات أين تبادر المصارف في تقديم الأداء

---

[1] **شيروف فضيلة**، "أثر التسويق الإلكتروني عل جودة الخدمات المصرفية(دراسة حالة بعض البنوك في الجزائر)"، مذكرة الماجستير، تخصص: تسويق، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري– قسنطينة، 2009، ص ص 48–52.

المناسب الذي يفوق كل التّوقعات المحتملة للعملاء، بغية جذب واستقطاب عملاء جدد والاحتفاظ بهم[1].

د)– تعزيز الثّقة مع العملاء: تعتبر الثّقة والأمان من بين الضّمانات التي يستوجب توافرها في العمليات المصرفيّة الإلكترونيّة، حيث تسعى المصارف إلى تعزيز علاقتها مع العملاء من خلال اعتماد قنوات اتصال متعدّدة ومؤمّنة تضمن توثيق وسلامة البيانات الالكترونيّة المُتداولة، مع عدم إنكارها من جانب أطراف التّعامل الإلكتروني.

هـ)– توسيع وتنويع نطاق الخدمات المتاحة: إنّ تعويل المصارف على التّقنيات التّكنولوجيّة الحديثة ساهم في تطوير وتنويع الخدمات المصرفيّة المتاحة، مع توسيع نطاقها على نحو أوسع عبر شبكة الإنترنت، لتلبية حاجيات ومتطلّبات العملاء والحفاظ على ولائهم مع رفع مستوى رضائهم تجاه الخدمات المصرفيّة المقدّمة إليهم[2].

ثانيا– مزايا المصارف الإلكترونيّة:

ترتبط فكرة المصارف الإلكترونيّة بالأسباب والغايات التي أدّت أو ساهمت في ظهورها على أرض الواقِع، كما قد يعود ذلك إلى المزايا التي تُتِيحُهَا عبر شبكة الإنترنت، والمتمثّلة فيما يلي:

أ)– تعزيز الميزة التّنافسيّة: تُمكِّن المصارف من تعزيز مكانتها في الأسواق وتحقيق الميزة التّنافسيّة لخدماتها الماليّة التي تؤهّلها إلى مستوى الخدمات العصريّة التي تتيحها المصارف العالميّة المشهورة أو السّباقة في عصرنة العمليات المصرفيّة؛

---

[1] **تيسير العجارمة**، التسويق المصرفي، دار حامد للنشر والتوزيع، عمان، الأردن، 2005، ص ص 354– 358.

[2] **ليث محمود أحمد الحاج**، "نظام الخدمات المصرفية الإلكترونية عبر(SMS) ودوره في تحقيق ولاء العملاء في البنوك التجارية الأردنية"، رسالة الماجستير، قسم إدارة الأعمال، كلية الأعمال، جامعة الشرق الأوسط، 2012، ص ص 16، 17.

ب)– تحسين كفاءة وجودة الخدمات المصرفيّة: إن تَوَجُّهَ مختلف المصارف إلى تطبيقات شبكة الإنترنت يزيد من كفاءتها ويُحسِّن من جودة ونوعية الخدمات المصرفيّة المتاحة للعملاء، فأصبح بمقدور أي عميل الاتّصال مباشرة بالمصرف عبر الإنترنت للقيام بعملياته الماليّة في وقت وجيز مع أداء وكفاءة عاليّتين وذلك من دون انتقال العميل شخصيا إلى مقرّ المصرف، وما ينتظره هناك من عناء وانتظار في حالة تواجد متعاملين آخرين يزاحمونه لغرض الحصول على نفس الخدمة[1]؛

ج)– توفير الثّقة والأمان: تتيح المصارف لعملائها تقنيات أو أساليب دفع إلكترونيّة حديثة تمكّنهم من إجراء معاملاتهم التّجاريّة عبر شبكة الإنترنت بكل ثقة وأمان، سواء كان ذلك في إطار أوامر الدّفع المصرفيّة الإلكترونيّة وخدمات المقاصة الإلكترونيّة، أو في إطار خدمات الصّرافات الإلكترونيّة كجهاز الصّراف الآلي (Automatic Teller Machine(A.T.M)) أو الموزّع الآلي للأوراق النّقديّة (Distributeur Automatique de Billets (D.A.B))، أو الشّباك الآلي للمصرف (Guichet Automatique de Banque(G.A.B))، أو الأجهزة المتواجدة في المحلاّت التّجاريّة (Terminal de Paiement Électronique(TPE))، أو البطاقات المصرفيّة الذّكية(Carte à puce) التي تعتبر من بين أبرز أدوات المدفوعات الالكترونيّة في عصر العولمة والذّكاء الاصطناعي[2]؛

د)– تنويع الخدمات المصرفيّة: توفّر المصارف الإلكترونيّة خيارات وتسهيلات واسعة ومتعدّدة للمتعاملين معها، بحيث تتيح كافة الخدمات المصرفيّة التي تقدّمها المصارف التّقليديّة في صيغ إلكترونيّة عبر شبكة الإنترنت، كأشكال النّشرات الإعلانيّة الإلكترونيّة

---

[1] **مصطفى كمال طه، وائل أنور بندق،** مرجع سابق، ص ص 332، 333.

[2] للمزيد من المعلومات في هذا الموضوع، أنظر: **محمد مدحت عزمي،** مرجع سابق، ص ص 354–361.

عن الخدمات المصرفيّة، طرق تسديد السّفتجات والفواتير، تحويل الأموال بين الحسابات المختلفة، تسهيل مهمّة التّأكد من الأرصدة، وكيفية إدارة المَحافِظ الماليّة من أسهم وسندات تابعة للعملاء الخ...[1]؛

هـ)- **الاقتصاد في التّكاليف والنّفقات:** تساهم المصارف الإلكترونيّة من تقليص التّكاليف أو النّفقات النّاجمة عن تقديم الخدمات المصرفية بشكل إلكتروني، فتكلفة الخدمات المصرفيّة المتاحة عبر شبكة الإنترنت تكون أقل إذا ما قارناها مع تكلفة الخدمات المتاحة من طرف المصارف العادية[2]، كما أنّ تكلفة إنشاء موقع إلكتروني للمصرف عبر الشّبكة تكون منخفضة إذا ما قارناها مع تكلفة إحداث فروع جديدة للمصرف عبر أنحاء العالم، وما تتطلّبه من مباني وأجهزة وموارد ماليّة وبشريّة ضخمة، كما تساهم المصارف الإلكترونيّة من تقليص مختلف التّكاليف على عاتق العملاء، وهذا ما يعزّز من نوعية وجودة الخدمات المتاحة والسّعي على استقطاب وجذب المتعاملين[3]؛

و)- **ترويج الخدمات المصرفيّة:** يستطيع المصرف، بفضل تطبيقات شبكة الإنترنت، من الولوج أو الوصول إلى قاعدة عريضة من العملاء المرتقبين، من دون التّقيّد بمكان أو زمان معيّن، فعن طريق موقعه الإلكتروني يتم التّعريف بجميع المعلومات المتعلّقة بالمصرف، والتّرويج لخدماته المصرفيّة المتاحة في شكل إعلانات إلكترونيّة لجذب أكبر عدد ممكن من العملاء[4].

---

[1] **يوسف حسن يوسف**، البنوك الالكترونية، مرجع سابق، ص ص 15-17.

[2] **محمد عبد حسين الطائي**، مرجع سابق، ص ص 231، 232.

[3] **Ali ELIDRISSI**, « Les sites Web bancaires. Un outil de communication et de distribution au service du client », Revue des Sciences de gestion, 2005/4 (n°214-215), pp. 167, 168.

[4] Ibid., pp. 170, 171.

الفرع الثالث
نظم التّسوية والمقاصة الإلكترونيّة

تساهم العمليات المصرفيّة في توفير السّيولة وتحريك عجلة الاقتصاد الوطني لأيّ بلد معيّن من العالم، حيث شهدت هذه العمليات في الآونة الأخيرة تطوّرا ملموسا في ظل الاقتصاد الرّقمي والتّطوّر الهائل والمستمر في مجال التّقنيات المصرفيّة، التي من خلالها تم تجريد العمليات المصرفيّة التّقليديّة من مادياتها وتحويلها إلى دعامات إلكترونيّة، وذلك نظرا لارتفاع تكلفة تداول الشّيكات وأوامر الدّفع والتّحويلات، مع طول فترة عمليات التّسوية **(أولا)** والمقاصة فيما بين المصارف **(ثانيا)**.

أولا– نظام التّسوية الإجماليّة الفوريّة للمدفوعات (Real Time Gross Settlement system (RTGS)).

إنّ تحقيق الفعاليّة الماليّة وتشجيع معاملات التّجارة الإلكترونيّة في أي بلد مرهون بمدى عصرنة المنظومة المصرفيّة، وتطوير أنظمة الدّفع الإلكترونيّة التي تعتمد على نظام التّسوية الإجماليّة الفوريّة للمدفوعات(**1**)، والذي يُعرف في الجزائر بنظام "الجزائر للتّسوية الفوريّة" (ARTS) (**2**).

1)– المقصود بنظام التّسوية الإجماليّة الفوريّة للمدفوعات(RTGS):

يعتبر نظام التّسوية الإجماليّة الفوريّة من أهمّ أدوات الحدّ من مخاطر المدفوعات، ومن تأثيرات مشاكل السّيولة على النّظام المالي والمصرفي كَكُلْ، حيث يتم من خلاله تسوية المبالغ الإجماليّة في وقت حقيقي مع سير التّحويلات بصفة مستمرة وعلى الفور بصفة إجماليّة من دُونِ أيّ تأجيل، ويحق لأيّة مؤسّسة(مصرفيّة وماليّة أو مراكز الصّكوك البريديّة أو الخزينة العموميّة) لها حساب تسوية في المصرف المركزي، المشاركة في نظام التّسوية الإجماليّة الفوريّة للمدفوعات، حيث يعالج هذا النّظام(RTGS) التّحويلات الماليّة التي تتم سواء فيما بين المصارف أو حسابات الزّبائن، وتكون فيها المبالغ الماليّة مُستعجلة أو ذات أهمّية، وكذا تسوية المبالغ المَدينة(Débits) والدّائِنة(Créances) النّاتجة عن طريق المقاصة

الإلكترونيّة تعالج بهذا النّظام قَرْضاً ودَيْناً في نفس الوقت، وفي حالة استحالة تطبيق العملية ترفض من قبل غرفة المقاصة الإلكترونيّة وعلى الرّاغب أن يعيد العملية وفي وقت لاحق[1].

2)- نظام الجزائر للتّسوية الفوريّة(ARTS):

دفعت التّطوّرات التي شهدها العصر الرّقمي بالمشّرع الجزائري إلى عصرنة المنظومة المصرفيّة، من خلال وضع نظام التّسوية الإجماليّة الفوريّة للمبالغ الكبيرة والدّفع المستعجل(أ)، الذي يسعى منه المصرف المركزي إلى تحقيق مجموعة من الأهداف(ب)، حيث يُعدّ الانخراط في هذا النّظام حُرّاً ومفتوحاً للمشاركين في مجال الخدمات المصرفيّة(ج)، حيث لا تُقبل إلاّ العمليات المصرفيّة المنصوص عليها في هذا النّظام(د).

أ)- التّعريف بنظام الجزائر للتّسوية الفوريّة(ARTS):

انتهج المصرف المركزي الجزائري نظام التّسوية الإجماليّة الفوريّة للمبالغ الكبيرة والدّفع المستعجل "أرتس"((ARTS(Algeria Real Time Settlement)[2]، كنظام تسوية فيما بين

---

[1] **بوعافية رشيد**، "الصيرفة الإلكترونية والنظام المصرفي الجزائري– الآفاق والتحديات"، مذكرة الماجستير في العلوم الاقتصادية، تخصص: نقود، مالية وبنوك، جامعة سعد دحلب– البليدة، 2006، ص ص 170–171–170.

[2] نظام المصرف المركزي(الجزائري) رقم 05–04 مؤرخ في 13 أكتوبر 2005، يتضمن نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل، ج ر عدد 02، الصادر في 15 جانفي 2006.

تنص **المادة 01** من هذا النظام، على ما يلي:" يهدف هذا النظام إلى تعريف ووضع نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل. وبالإضافة إلى هذا، فإنّه يحدد مسؤوليات المتعامل والمشاركين في هذا النظام وكذا قواعد اشتغاله."

وتنص **المادة 02** منه، على ما يلي:" يعتبر نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل، الذي وضعه بنك الجزائر، والمسمى بنظام الجزائر للتسوية الفورية((ARTS(Algeria Real Time Settlement) "أرتس" نظاما للتسوية بين البنوك لأوامر الدفع عن طريق التحويلات المصرفية أو البريدية للمبالغ الكبيرة أو الدفع المستعجل التي يقوم بها المشاركون في هذا النظام."

وتنص **المادة 03** منه، على ما يلي:" تتم عملية الدفع في نظام "أرتس**ARTS**" على أساس إجمالي(دون الخضوع للمقاصة) وفي الوقت الحقيقي على حسابات التسوية المفتوحة في هذا النظام لصالح المشاركين ويخضع فتح حسابات التسوية لاتفاقية بين بنك الجزائر والمشاركين المعنيين."

المصارف لأوامر الدّفع عن طريق التّحويلات المصرفيّة أو البريديّة للمبالغ الكبيرة والدّفع المستعجل التي يقوم بها المشاركون في هذا النّظام، وتتم عمليات الدّفع فيما بين المصارف على أساس إجمالي "من دون الخضوع للمقاصة" وفي الوقت الحقيقي على حسابات التّسوية المفتوحة في هذا النّظام لصالح المشاركين(Participants)، حيث تخضع عملية فتح حسابات التّسوية لاتّفاقية بين المصرف المركزي بصفته "صاحب النّظام(مَالِكاً لَهُ) ومُتَعَامِلاً فِيهِ"، والمُشاركِين المعنيين، وبالتّالي يستوجب على كل مصرف أن يكون لديه حساب تسوية واحد لدى المصرف المركزي الذي يقوم بدوره بالتّصديق على أمر الدّفع وإجراء عملية التّسوية فقط في حالة وجود حساب كافي لدى المصرف المسحوب عليه، ففي حال تسوية أمر الدّفع تصبح عملية الدّفع نهائيّة وغير قابلة للرّجوع فيها.

ب)– أهداف نظام الجزائر للتّسوية الفوريّة(ARTS):

يسعى المصرف المركزي الجزائري من إقامة نظام التّسوية الإجماليّة الفوريّة إلى تحقيق الأهداف التّالية:

- التّسوية الإجماليّة الفوريّة لأوامر الدّفع التي يعادل أو يفوق قيمتها المليون دينار جزائري، وكذا أوامر الدّفع المستعجلة التي تصدر عن المشاركين حيث تقلّ قيمتُها عن هذا الحدّ الأدنى[1]؛
- تبادل أوامر الدّفع فيما بين المصارف مع إعلام المصرف المركزي عن مختلف المعلومات المتعلّقة بالدّفع أو اشتغال النّظام(تنفيذ الأوامر، بيان حسابات التّسوية، تسيير السّيولة)؛
- تلبية احتياجات المستعملين من خلال عصرنة الخدمات المصرفيّة والحصول عليها في ظرف وجيز وفي الوقت المحدّد؛

[1] تنص **المادة 25** من النظام رقم 05–04، سالف الذكر، على ما يلي: "إنّ أوامر الدفع، التي أصدرها المشاركون والمصادق عليها والمقبولة من طرف نظام "أرتس**ARTS**" غير قابلة للإلغاء."
راجع كذلك نص المادة 26 من نفس النظام.

- تقليص آجال التّسوية لأوامر الدّفع حيث تتم التّحويلات بصفة مستمرة وعلى الفور بدون تأجيل وعلى أساس إجمالي؛
- تخفيض التّكاليف الإجماليّة المترتّبة عن عمليات المعالجة لأوامر الدّفع؛
- توفير السّيولة من خلال تشجيع وجذب الاستثمارات الأجنبيّة في الجزائر، وكذا الاشتراكات التي يدفعها المشاركون للمصرف المركزي الجزائري باعتباره كمالك لنظام أرتس وكمشارك فيه(ARTS)[1]؛
- مواجهة مخاطر التّسوية التي يُواجِهُهَا المشتركون في نظام الدّفع الناجمة عن تراكم الالتزامات غير القابلة للتّسوية في أرصدة المصارف المشاركة، أو عدم قدرة أحد المشاركين على الوفاء بالتزاماته الماليّة تجاه الزّبائن أو المصرف المركزي، مما يؤثّر سلبا على المشاركين الآخرين، فكلّما ازدادت مخاطر التّسوية ازدادت فرص التّأثير السّلبي على النّظام المالي ككل.

ج)– الانخراط في نظام أرتس(ARTS):

يعتبر المصرف المركزي كمشارك في نظام أرتس(ARTS) حيث يُعدّ الانخراط في هذا الأخير حُرّاً ومفتوحا للمصارف، والمؤسّسات الماليّة، الخزينة العموميّة، بريد الجزائر، والمتعاملون المُكلّفون بأنظمة الدّفع الأخرى، ويتطلّب الانخراط في هذا النّظام(ARTS) تقديم طلب الانخراط مع موافقة المصرف المركزي، حيث يتحصّل كل مشارك عند الانخراط على الرّموز السّريّة التي تُمكّنه من إجراء عمليات الدّفع، وبالتّالي يُمكِن للمُنخرط عند تقديمه لطلب الانخراط في نظام أرتس(ARTS) أن يختار إمَّا وضعية مشارك مباشر (Participant direct) أو مشارك غير مباشر(Participant indirect)، فعندما ينصّب الاختيار حول

---

[1] تنص المادة 55 من النظام رقم 05–04، سالف الذكر، على ما يلي: " يجب على المشاركين في نظام "أرتس**ARTS**" أن يسددوا المصاريف الناجمة عن معالجة أوامر الدفع."

تنص المادة 56 من نفس النظام، على ما يلي:" [...]. يمثل جزء من مصاريف الاستغلال الثابتة لنظام "أرتس**ARTS**" رسما سنويا يدفعه المشاركون."

راجع كذلك نص المادة 57 من نفس النظام.

الوضعيّة الأولى(المشارك المباشر)، فَإِنَّ المُنْخَرِطَ يَخْضَعُ للتّحقيقات والإجراءات المعمول بها التي تبنّاها المصرف المركزي الجزائري، فالمُشارِك المباشر يُعْتَبَرُ "مُشَارِكاً" عندما يحوز على حساب تسوية في نظام أرتس(ARTS) وترتبط أرضيته بهذا الأخير، بينما المشارك غير المباشر يعتبر "مشاركا" يحوز بدوره على حساب تسوية في نظام أرتس(ARTS)، غير أنّه لا يُمْكِنُهُ الاتّصال بهذا النّظام(ARTS) إلاّ عن طريق أرضية "مشارك" خاصّة بمُشارك مُباشر[1].

يُمكِن للمُشاركِين أن يُغَيِّرُوا وَضعِياتِهم مع إعلامهم للمصرف المركزي بذلك في غضون شهر واحد(01) قبل التّاريخ الفّعلي للتّغيير، ففي حال ما إذا رغب المشارك غير المباشر في تغيير وضعيته إلى مشارك مباشر، فَعَلَيْهِ(Participant indirect) أن يخضع للتّحقيقات وإجراءات الفحص العاديّة عبر أرضيّته، بينما المشارك المباشر الذي يرغب في تغيير وضعيته إلى مشارك غير مباشر، يجب عليه(Participant direct) أن يقترح حلا يضمن استمرارية الخدمة لصالح المشاركين غير المباشرين الذين يُشكّل بالنسبة لهم الوسيط التّقني، وفي جميع الظّروف، يجب على المشاركين في نظام "أرتس(ARTS)" التّقيُّد بقواعد اشتغال هذا الأخير وبمُرشد استعماله وبشروط الأمن التي يحدّدها المصرف المركزي، حيث يتكفّل هذا الأخير بصفته صاحب النّظام ومُتعامِلاً فيه(ARTS)، بضمان الاشتغال الحسن لهذا النظام(ARTS)، حيث لا يضمن(المصرف المركزي) تحقيق عمليات الدّفع ولا يُعتبر المدين الأخير بموجب الالتزامات المُرتبطة بالدّفع إلاّ في حالة قروض اللّيلة الواحدة التي تم مَنحُها[2].

---

[1] تنص المادة 12 من النظام رقم 05–04، سالف الذكر، على ما يلي: "يعد المشارك المباشر مشاركا يحوز حساب تسوية في نظام "أرتسARTS" وترتبط أرضيته المسماة بأرضية "مشارك" بهذا الأخير."

وتنص المادة 13 من نفس النظام، على ما يلي:" يعتبر المشارك غير المباشر مشاركا يحوز حساب تسوية في نظام "أرتسARTS" غير أنّه لا يمكنه الاتصال بهذا النظام إلا عن طريق أرضية "مشارك" خاصة بمشارك مباشر."

راجع كذلك أحكام المواد 09 و10 و11 من نفس النظام.

[2] تنص المادة 07 من النظام رقم 05–04، سالف الذكر، على ما يلي: "يجب على المشاركين التقيّد بقواعد اشتغال النظام المنصوص عليها في هذا النظام وفي مرشد استعمال نظام "أرتسARTS"."

د) – العمليات المقبولة في نظام أرتس(ARTS):

وفقا لأحكام المادة 22 من نظام المصرف المركزي رقم 04/05 المؤرخ في 13 أكتوبر 2005، الذي يتضمّن نظام التّسوية الإجماليّة الفوريّة للمبالغ الكبيرة والدّفع المستعجل، فإنّ نظام أرتس(ARTS) لا يقبل إلاّ العمليات المصرفيّة البِينيّة للحساب الخاص ولحساب الزّبائن، والعمليات على النّقد الورقي مع المصرف المركزي والعمليات المرتبطة بالسّياسة النّقديّة أو كل عملية أخرى رخص بها المصرف المركزي، وكذا العمليات المتعلّقة بصافي أرصدة مقاصة التّسديدات المسمّى "بنظام التّسديدات للجمهور العريض أو التّسديدات بالتّجزئة"، وصافي نظام تسوية النّقد مقابل تسليم السّندات.

ولا يمكن إصدار أوامر الدّفع إلاّ من طرف المشاركين في نظام "أرتس"(ARTS) والمُصدرة بالدّنانير، حيث يجب معالجة أوامر الدّفع عن طريق تحويل كل مبلغ يعادل أو يفوق المليون دينار جزائري، وكذا أوامر الدّفع المستعجلة التي تقل عن هذا الحدّ الأدنى والتي تصدر عن المشاركين، في حين يقبل النّظام(ARTS) عمليات الدّفع المتضمّنة لتاريخ قيمة اليّوم والتي يجب إدخالها في النّظام في نفس التّاريخ، فبالنّسبة لعمليات التّحويل نحو الخارج التي توافق تاريخ قيمتها تاريخ قيمة يوم الجمعة أو يوم السّبت، فيتم حتما تحويل مقابل القيمة بالدّينار داخل نظام "أرتس" يوم العمل الأخير من الأسبوع، وتتم معالجة عمليات تحويل القيمة المقابلة بالدّينار لعمليات التّرحيل التي يوافق تاريخ قيمتها يوم الجمعة، حسب قيمة يوم العمل الأوّل للأسبوع الموالي[1].

وتنص المادة 16 من نفس النظام، على ما يلي:" يجب على المشاركين في نظام "أرتسARTS" أن يتقيّدوا بشروط الأمن التي يحدّدها بنك الجزائر."

راجع كذلك أحكام نص المواد 05 و06 و14 من نفس النظام.

[1] تنص المادة 21 من النظام رقم 05–04، سالف ذكر، على ما يلي: "يجب معالجة أوامر الدفع عن طريق تحويل لكل مبلغ يعادل أو يفوق المليون دينار وهذا، على مستوى نظام "أرتس**ARTS**". ويقبل هذا الأخير أوامر الدفع المستعجلة التي تقل عن هذا الحد الأدنى والتي تصدر عن المشاركين."

راجع كذلك أحكام المادتين 19 و20، من نفس النظام.

يتم إرسال أوامر الدّفع في هذا النّظام(ARTS) حسب طبيعتها والوقت المحدّد لافتتاح أو ختام يوم التّبادل، ويجب على المشاركين التّأكد من توفر الأموال الكافية قصد تصفية عملياتهم، حيث تتم عملية تسوية أوامر الدّفع بصفة نهائيّة(بشرط توفّر الأموال) بمُجرّد أن يتم قيد الجانب الدائن لحساب تسوية الآمر وفي الوقت ذاته تُقيّدُ القروض المُطابقة في حساب تسوية المشارك المُستفيد، في حين يُوجِّه النّظام(ARTS) بشكل مُوَازٍ للمُشاركين الآمرين والمُستفيدين تبليغا، يتضمن تنفيذ الأوامر المُصْدَرَةِ، ففي حال تعدّد الأوامر لا تصبح التّسوية نهائيّة إلاّ بعد القيام بقيد الجانب المَدين والجانب الدَّائن للحسابات[1].

وفي جميع الظّروف، تخضع أوامر الدّفع التي يُرسِلُهَا المُشَارِكُونَ إلى نظام "أرتسARTS"، لمراقبة قصد التّصديق من طرف ذلك النّظام، ففي حالة إثبات مخالفة في الأمر بالدّفع، فإنّه يُرفض تلقائياً من خلال إرسال رسالة للمُشارِك فوراً، وفي حالة المُصادقة على الأمر بالدّفع، يشرع النّظام(ARTS) في تسويته أو ترتيبه في قائمة الانتظار في حالة عدم كفاية المؤن في حساب التّسوية[2].

ثانيا– نظام المقاصة الإلكترونيّة:

يعتبر نظام المقاصة الإلكترونيّة جزءً من نظام المدفوعات، حيث تتنوّع نُظم المقاصة بحسب الخدمات المصرفيّة المتاحة، كمقاصة الشّيكات، مقاصة الأوراق الماليّة، مقاصة

---

[1] تنص المادة 23 من النظام رقم 05–04، سالف الذكر، على ما يلي: "يجب أن يتأكد المشاركون من توفر الأموال الكافية قصد تصفية عملياتهم."

– راجع كذلك أحكام المادتين 26 و27 من نفس النظام.

[2] تنص المادة 36 من النظام رقم 05–04، سالف الذكر، على ما يلي: "إنّ أوامر الدفع التي يرسلها المشاركون إلى نظام "أرتسARTS"، تخضع لمراقبة قصد التصديق من طرف النظام. في حالة ما يبرز الأمر بالدفع مخالفة، فإنّه يُرفض تلقائيا ببعث رسالة للمشارك على الفور.

في حالة المصادقة على الأمر بالدفع، يشرع النظام في تسويته أو ترتيبه في قائمة الإنتظار في حالة عدم كفاية المؤن في حساب التسوية."

تنص المادة 28 من نظام"المصرف المركزي" رقم 05–04، سالف الذكر، على ما يلي:" يمكن لأمر الدفع أن يكون محل رفض من طرف النظام لأسباب فنية. يعود هذا الرفض لعدم تقيّد المشارك الآمر بالقواعد المتعلقة بإرسال أوامر الدفع."

بطاقات الدّفع الإلكترونيّة، وغيرها من الخدمات، وفي جميع الظّروف يكون لكل دولة نظام دفع وطني واحد فقط.

1)– مفهوم المقاصة الإلكترونيّة:

كانت عملية مقاصة الشّيكات تتم عن طريق المُناولة اليدويّة التي من خلالها يتم تبادلها في وقت ومكان واحد من طرف مندوبي المصارف الأعضاء في مكتب أو غرفة المقاصة، فبالرّغم من الدّور الفعّال الذي تلعبه هذه الأخيرة في تنفيذ الإجراءات اللاّزمة لضمان السّير الحسن لعمليات المقاصة اليدويّة للشّيكات، إلاّ أنّ هذه الأخيرة تعتبر في عصرنا الحالي إحدى العوائق التي تَقِفُ أمام تَطَوُّرِ القطاع المصرفي، نظرا لِطُولِ فَتْرَةِ تحصيل وتبادل قيمة الشّيكات وارتفاع التّكاليف اللاّزمة لإجراء عمليات المقاصة وازدياد مخاطر الضّياع والسّرقة والإتلاف للشّيكات المترتّبة عن النّقل المادّي لها إلى غُرَفِ المقاصة، حيث يؤدّي كل ذلك إلى استياء العملاء وتأخير معاملاتهم مع فقدان مصداقيّة التّعامل بالشّيك كأداة وفاء رئيسيّة لتسويّة المعاملات الماليّة والتّجاريّة، ولتفادي كل ذلك بات على المصارف المركزية التّفكير والبحث عن وسيلة أحسن تضمن عملية المقاصة لوسائل الدّفع في ظل الاقتصاد الرّقمي وتطوّر تكنولوجيات الاتّصال والإعلام.

لذا أصبحت تكنولوجيا الثّورة الرّقميّة في عصرنا الحديث تُستخدم بشكل كبير وفي نطاق واسع في مجال الخدمات المصرفيّة، حيث يعتبر نظام المقاصة الإلكترونيّة لوسائل الدّفع من أحدث الأنظمة المصرفيّة وأكثرها تطوّرا في مجال الخدمات المصرفيّة، حيث يقوم هذا النّظام بعملية التّقاص لأوامر الدّفع اعتمادا على الصّور والمعلومات المُتَدَاوَلَةِ عبر شبكة اتّصالات سريعة وآمنة، تربط المصارف المُشاركة فيها بمركز التّقاص الرئيسي في المصرف المركزي[1].

---

[1] **أسماء بنت لشهب، باسم محمد ملحم**،"التنظيم القانوني للمقاصة الإلكترونية للشيكات وللعلاقات القانونية الناشئة عنها في القانون الأردني"، مجلة دراسات، علوم الشريعة والقانون، كلية الحقوق، الجامعة الأردنية، عدد 2013/02، ، ص ص 456، 457.

وعليه، يمكن تعريف المقاصة المصرفيّة الإلكترونيّة على أنّها عبارة عن نظام لتسويّة مدفوعات وسائل الدّفع(الشّيكات، السّفتجات، البطاقات المصرفيّة، الحوّالات، إلى غيرها)، فيما بين المصارف بطريقة إلكترونيّة، الذي من خلاله(النّظام) يتم تحصيل وتبادل قِيم المدفوعات من حساب عميل أحد المصارف إلى حساب عميل أخر في وقت مُحدّد، عبر وسيط مُفوَّض من قِبَلِ المصرف المركزي باعتباره كمالك ومشارك في هذا النّظام.

2)– واقع المقاصة الإلكترونيّة في الجزائر:

لعصرنة الخدمات المصرفيّة في الجزائر، قام المصرف المركزي بإصدار نظام رقم 05–06 مؤرخ في 15 ديسمبر 2005، يتعلق بمقاصة الصّكوك وأدوات الدّفع الخاصّة بالجمهور العريض الأخرى، الذي من خلاله وضع نظام ما بين المصارف للمقاصة الإلكترونيّة للصّكوك والسّندات والتّحويلات والاقتطاعات الأوتوماتيكيّة، السّحب والدّفع باستعمال البطاقة المصرفيّة، يُدعى بنظام الجزائر للمقاصة المسافيّة ما بين البنوك–أتكي(Algérie Telé Compensation Interbancaire(ATCI))، الذي يشتغل وفقا لمبدأ المقاصة المتعدّدة الأطراف لأوامر الدّفع التي يقدّمها المشاركون في هذا النّظام، حيث لا يقبل هذا الأخير(ATCI) سوى التّحويلات التي تقل عن مليون(01) دينار، في حين يجب أن تنفّذ أوامر التّحويل التي تفوق أو تساوي قيمتها الاسميّة هذا المبلغ عن طريق نظام التّسوية الإجماليّة الفوريّة للمبالغ الكبيرة والدّفع المُستعجل"أرتس**ARTS**"[1].

---

[1] **نظام(المصرف المركزي الجزائري) رقم 05–06** مؤرخ في 15 ديسمبر 2005، يتعلق بمقاصة الصكوك وأدوات الدفع الخاصة بالجمهور العريض الأخرى، ج ر عدد 26، الصادر في 23 أبريل 2006.

تنص المادة 02 منه على ما يلي:" ينجز بنك الجزائر نظام المقاصة الإلكترونية الذي يدعى "نظام الجزائر للمقاصة المسافية ما بين البنوك–أتكي"(ATCI). ويتعلق الأمر بنظام ما بين البنوك للمقاصة الإلكترونية للصكوك والسندات والتحويلات والاقتطاعات الأتوماتيكية السحب والدفع باستعمال البطاقة المصرفية.

لا يقبل هذا النظام إلا التحويلات التي تقل التي تقل عن مليون(1) دينار، يجب أن تنفذ أوامر التحويل، التي تفوق أو تساوي قيمتها الاسمية هذا المبلغ، ضمن نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المُستعجل.

يشتغل نظام أتكي(ATCI) وفقا لمبدأ المقاصة المتعددة الأطراف لأوامر الدفع التي يقدمها المشاركون في هذا النظام."

وعليه، فَوَّضَ المصرف المركزي الجزائري مُهِمَّةَ تسيير نظام أتكي(ATCI) لمركز المقاصة المُسبقة المصرفية(CPI)، الذي يقوم بتسيير عمليات الدّفع التي تُرسل في النّظام(ATCI) ويعتبر كفرع تابع للمصرف المركزي، في هيئة شركة مُساهمة(المركز (CPI)) رأس مالها مفتوح لكل المشاركين في نظام أتكي(ATCI)[1]، الذي يكون الانخراط فيه مفتوح لكلّ من المصارف والخزينة العموميّة وبريد الجزائر أو أي مشارك أخر جديد، حيث تخضع المشاركة في هذا النّظام لموافقة مُسبقة من طرف المركز (CPI)، في إطار اتّفاقية السّاحة التي تُحدّد حقوق وواجبات المشاركين فيما بينهم وتجاه المركز باعتباره كمسيّر لنظام أتكي(ATCI)، والتي تُرسل نسخة منها(الاتّفاقية) إلى المديريّة العامّة للشّبكة وأنظمة الدّفع التّابعة للمصرف المركزي، فبمجرّد الانخراط في النّظام يتحصّل كمشارك على رموز تعريف تسمح له بإرسال أوامر الدفع عبر النظام(ATCI)، كما يمكن لكل مشارك أن يختار وضعية مشارك مباشر أو مشارك غير مباشر مع إمكانية تغيير هذه الوضعيّة من خلال تبليغ يُوّجه إلى مركز المقاصة المسبقة المصرفيّة في غضون شهر واحد قبل التّاريخ الفّعلي للتّغيير، حيث يتم إرسال نُسخة من التّبليغ إلى المديريّة العامّة للشّبكة وأنظمة الدّفع لمصرف الجزائر[2].

وتنص المادة 03 على ما يلي:" يتم حساب أرصدة المقاصة المتعددة الأطراف من قبل نظام أتكي(ATCI)، ثم تدفق، بغرض تسويتها، في نظام التسوية الإجمالية الفورية للمبالغ الكبيرة والدفع المستعجل المسمى أرتسARTS."

[1] تنص المادة 04 من النظام رقم 05–06، سالف الذكر، على ما يلي:" يفوض بنك الجزائر مهمة تسيير نظام أتكي(ATCI) لمركز المقاصة المسبقة المصرفية(CPI) وهي شركة أسهم وفرع تابع لبنك الجزائر."

[2] تنص المادة 04 من النظام رقم 05–06، سالف الذكر، على ما يلي:" يفوض بنك الجزائر مهمة تسيير نظام أتكي(ATCI) لمركز المقاصة المسبقة المصرفية(CPI) وهي شركة أسهم وفرع تابع لبنك الجزائر."

وتنص المادة 17 من النظام رقم 05–06، على ما يلي:" فضلا عن بنك الجزائر، إنّ الانخراط في نظام أتكي(ATCI) مفتوح لكل من البنوك والخزينة وبريد الجزائر."

وتنص المادة 18 من النظام رقم 05–06، على ما يلي:" يفوِض المشاركون في نظام أتكي(ATCI) لمركز المقاصة المسبقة المصرفية قبولهم بأي مشارك جديد في النظام."

راجع كذلك نصوص المواد من 19 إلى 23 من النظام رقم 05–06، سالف الذكر.

تجدر الإشارة في هذا السّياق، أنّ عملية تقديم السّفتجات والسّندات لأمر في أتكي(ATCI)، تتم بطريقة إلكترونيّة في شكل غير مادّي، على أن يحوز مسبقا المشارك المقدّم الشّكل الورقي لأدوات الدّفع بعد أن يحقّق من صحتها القانونيّة، مع ضمان مطابقة المعلومات الواردة في أدوات الدّفع الإلكترونيّة.

3)– واقع المقاصة الإلكترونيّة في تونس:

قام المصرف المركزي التّونسي في إطار المشاورات الواسعة التي أطلقها في سنة 1996 لغرض عصرنة المنظومة المصرفيّة التّونسية، بإحداث المنظومة التّونسية الالكترونيّة للمقاصة فيما بين البنوك(Système tunisien de télécompensation interbancaire) تُشْرِفُ عليه شركة المصرفية المُشتركة للمقاصة الالكترونيّة Société Interbancaire de) Télécompensation(**SIBTEL**))، التي تم تأسيسها في نوفمبر 1999 من طرف 14 مؤسسة مصرفيّة(البنك المركزي، الشّركة التّونسية للبنك، بنك تونس العربي الدّولي، البنك الوطني الفلاحي، البنك التّونسي، التّجاري بنك، الاتّحاد البنكي للتّجارة والصّناعة، بنك الأمان، الاتّحاد الدّولي للبنوك، البنك العربي لتونس، الديوان الوطني للبريد، بنك الإسكان، اتّصالات تونس، سيتي بنك.)، حيث انخرط فيها حوالي 25 مؤسسة مصرفيّة(البنك المركزي التّونسي، 23 بنكا، الدّيوان الوطني للبريد.)[1].

انطلاقا من ذلك، فإنّ الهدف من إحداث المنظومة التّونسية الالكترونيّة للمقاصة بين البنوك يتعلق بإرساء ثقافة جديدة للمعاملات فيما بين المصارف، تقوم على التّعاون الفنّي والحريّة التّجاريّة، وكذا تحديث وسائل التّبادل فيما بين المصارف للقضاء نهائيا على التّبادل المادّي للأوراق الماليّة، مع تسوية عمليات المقاصة للبيانات الإلكترونيّة والصّور الضّوئيّة (المُصوَّرة بالسّكانير) المتبادلة في وقت محدّد من كل يوم(في ظرف 24 ساعة).

[1] أنظر الموقع الإلكتروني التّالي: http://www.sibtel.com.tn (consulté le 12/04/2017.)

وعليه، اكتسبت المصرفية المشتركة للمقاصة(SIBTEL) صفة مكتب خدمات "سويفت" (SWIFT)، لاستضافة منظومة(SWIFT Alliance Gateway) عبر منصّة إلكترونيّة موثوقة تُمكِّن المصارف التّونسية من الاتّصال بشبكة(SWIFT NET) بكل ثقة وأمان، وضمان تبادل البيانات المعلوماتية المتعلّقة بالأوراق الماليّة المُزمَع مقاصتها، وكذا الصّور الضّوئيّة للصّكوك والسّفتجات بطريقة إلكترونيّة عبر شبكة تراسل البيانات ونقلها، حيث تقوم المصارف بالتّوقيع إلكترونيا على صور الصّكوك والقّيم المُراد تعويضها للتّعريف بهذه المصارف وضمان صحة المعاملة المصرفيّة التي تم القيام بها، مع توثيق وحفظ الأوراق الماليّة المتداولة بطريقة إلكترونيّة لغرض الاطّلاع عليها عبر شبكة الانترانت[1].

الفرع الرابع
مخاطر المصارف الإلكترونيّة

تسعى المصارف الإلكترونيّة من وراء استخدام تطبيقات شبكة الإنترنت إلى تكريس وجودها الفّعلي مع تعزيز فاعلية وكفاءة الخدمات المقدّمة للعملاء، وبالتّالي فبالرّغم من الفوائد التي تقدّمها المصارف الإلكترونيّة، إلاّ أنّ تطبيقات التّجارة الإلكترونيّة والبيئة الافتراضيّة التي تُمارس فيها العمليات المصرفيّة تفرض على المصارف الإلكترونيّة مواجهة مجموعة من العوائق أو المخاطر التي تعترض العمليات المصرفيّة، والمتمثّلة في المخاطر الأمنيّة **(أولا)**، والمخاطر المتعلّقة بالصّرف المزدوج **(ثانيا)**، والمخاطر المتعلّقة بالسّيولة **(ثالثا)**، ومخاطر السّمعة **(رابعا)**، والمخاطر القانونيّة **(خامسا)**، والمخاطر المتعلّقة باستخدام العملات الافتراضيّة **(سادسا)**، وتلك المتعلّقة بانتهاك حقوق الملكيّة الفكريّة **(سابعا)**، والمخاطر المتعلّقة بالتّطوّرات التّكنولوجيّة الحديثة **(ثامنا)**.

[1] للمزيد من المعلومات حول الموضوع، اطّلع على الموقع الإلكتروني التّالي: http://www.sibtel.com.tn

أولا– المخاطر الأمنيّة:

إنّ تطوّر وتنامي تطبيقات التّجارة والعمليات المصرفيّة الإلكترونيّة صاحب معه ظهور وانتشار تقنيات اختراق شبكات أنظمة المعلومات من طرف القراصنة المحترفين، بحسب الغايات والأهداف المُسطّرة منهم، فقد يتعلّق الأمر باختراق نظم المعلومات والقيام بعمليات الاحتيال على العملاء وسرقة بياناتهم الإلكترونيّة السّريّة واستغلالها، أو إيجاد وتهيئة الثّغرات المُتواجدة في النّظام الأمني للشّبكة المعلوماتيّة لغرض القيام بأعمال التّخريب وتعطيل نظام التّشغيل[1]، حيث تُثير هذه المخاطر تحدّيات جديدة للمصارف الإلكترونيّة في مجال سلامة وسرية أنظمة الدّفع الإلكتروني ومدى صّحة وموثوقيّة العقود المصرفيّة الإلكترونيّة المُبرمة عبر شبكة الإنترنت، الأمر الذي يتطلّب إرساء بِنية أمنيّة تحتيّة موثوقة لضمان سلامة جميع الاتّصالات الالكترونية، والتّأقلم والتّفاعل مع المستجدّات الحديثة للثّورة الرّقميّة.

ثانيا– المخاطر المتعلّقة بالصّرف المُزدوج (Double dépenses de monnaies électronique):

إنّ عدم التّأمين الكافي للأنظمة المعلوماتيّة المصرفيّة من شأنه أن يُشَجِّعَ عمليات الاحتيال والتّدليس عبر الشّبكة الافتراضيّة المصرفيّة، من خلال قيام أطراف التّبادل الالكتروني بتزييف ونسخ العملات الإلكترونيّة وطرحها للتّداول من جديد لعدّة مرّات عبر المنصّة الإلكترونيّة المصرفيّة، حيث يمكن للقراصنة المحترفين استغلال الثّغرات الأمنيّة المتواجدة في نظام تشغيل المصرف والقيام برفع قيمة وحدات النّقد الإلكتروني التي تم حفظها أو تخزينها على مستوى المحفظة الإلكترونيّة أو أداة الدّفع الإلكتروني.

فمن الصَّعْبِ على التّاجر الافتراضي كشف وحدات العملات الالكترونيّة المُزوّرة التي تم تَدَاوُلِهَا من طَرَفِ المُستهلك الإلكتروني، حيث يمكن لهذا الأخير أن يقوم بعد عملية الشّراء

[1] **طارق محمد حمزة**، النقود الإلكترونية كإحدى وسائل الدفع، تنظيمها القانوني والمسائل الناشئة عن استعمالها، منشورات زين الحقوقية، بيروت، لبنان، 2011، ص 446.

بتحويل نسخة من قيم العملات الإلكترونيّة المُزوّرة إلى التّاجر والاحتفاظ بالوحدات الأصليّة في المحفظة الإلكترونيّة للمُستهلك[1].

ولتفادي كلّ ذلك، تستعين المصارف الإلكترونيّة والمؤسّسات الماليّة بتقنيات التّصديق الإلكتروني باعتبارها كوسيلة أمان حديثة، تضمن إثبات هويّة أطراف الصّفقات التّجاريّة وتؤكّد سلامة وسريّة مُحتوى التّبادل الإلكتروني مع عدم إنكاره، حيث تلعب آليات التّشفير دوراً حيوياً في تأمين قِيم وَحدات الدّفع الإلكتروني سواء في تأمين وسائل أو أدوات الدّفع الإلكتروني أو لِتَجَنُّبِ عمليات الإنفاق المُزدوج غير المشروع[2].

ثالثا– المخاطر المتعلّقة بالسّيولة:

ينطوي العمل المصرفي الإلكتروني بدوره على مخاطر تقليديّة، تتطلّب معرفة مُسبقة ووعيا كافيا على النّحو الذي يُمكّنُ المصرف على مراقبتها والحيطة منها، حيث تعتبر مخاطر السّيولة من بين المخاطر التّقليديّة المترتّبة عند تقديم المصرف للخدمات المصرفيّة للعملاء، كمنح القروض والأزمات الماليّة العالميّة والمنافسة الشّديدة في الأسواق، ومخاطر تبديل العملات...إلى غير ذلك، في حين تزداد شّدة هذه المخاطر عبر شبكة الإنترنت التي تُتِيح للمصرف فرص أو خيارات أوسع لتسويق خدماته المصرفيّة والمُخاطرة بأمواله التي يقوم بتوظيفها عبر أسواق دول العالم، حيث يُعْتَبَرُ المصرف المُمَوِّلُ الرَّئِيسِي لأنشطة الاستثمار، وأحد الدّعامات الأساسيّة لضمان سلامة حركة دخول الأموال من الخارج إلى الدّاخل أو العكس وكذا سلامة أسواق الأوراق الماليّة.

رابعا– مخاطر السُّمعة:

إنّ انتشار وتزايد مخاطر البيئة الافتراضيّة من شأنها أن تُؤَثِّرَ على كفاءة وجودة الخدمات المصرفيّة الإلكترونيّة المتاحة للعملاء، وبالتّالي فإنّ اختراق وانتهاك أمن وسريّة

---

[1] **طوني عيسى**، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2001، ص 200.

[2] المرجع نفسه.

البيانات السّريّة للمعاملات المصرفيّة ينعكس سلبا على سمعة المصرف ومدى قدرته على الحفاظ على العلاقات القائمة مع عملائه أو حتى استحداث علاقات جديدة مع عملاء جدد، بسبب عدم قدرة وكفاءة المصرف على استيعاب التّقنيات التّكنولوجيّة الحديثة، التي تُؤمِّن حركة نقل وسير وتدفّق المعلومات والبيانات الالكترونيّة المتداولة عبر مسالك أو قنوات اتّصال موثوقة ومؤمّنة، تضمن الحماية الأمنيّة الكافية للعملاء مع رفع مستوى رضائهم تجاه الخدمات المصرفيّة المقدّمة إليهم، وهذا ما ينعكس إيجابا على سمعة المصرف.

خامسا– المخاطر القانونيّة:

تكمن المخاطر القانونيّة للمصرف الإلكتروني في انتهاكه للأحكام التّشريعيّة والتّنظيميّة السّارية المفعول في البلد المعني، وبالخصوص تلك المتعلّقة بحماية المُستهلك والتّجارة الإلكترونيّة والعمليات المصرفيّة وتبييض الأموال وتمويل الإرهاب، وكذا حماية المعطيات الشّخصيّة... إلى غير ذلك من التّشريعات والتّنظيمات، التي من شأنها أن تُعرِّضه إلى جزاءات عقابيّة، كما أنّ عدم الاستقرار التّشريعي للدّول يُزيد أكثر من حدّة المخاطر القانونيّة للمصارف، نتيجة عدم المعرفة القانونيّة الكافية لها، أو جَهْلِهَا لبعض الاتّفاقيات الدّولية المُبرمة من طرف الدّول المعنيّة.

سادسا– المخاطر المتعلّقة بالتّطوّرات التّكنولوجيّة الحديثة:

يجب على المصارف أن تسعى على إحاطة مُوظّفيها بالمخاطر النّاجمة عن استعمال تكنولوجيا الاتّصال والإعلام، وتطوير نوعية تدريباتهم بما يتواكب مع مستجدّات العصر الرّقمي، عن طريق الاستعانة بخبراء تكنولوجيا المعلومات لتكوينهم وتهيئتهم على الاستخدام اللاّئق والأمثل لمختلف التّقنيات التّكنولوجيّة الحديثة المستخدمة، في مجال العمليات المصرفيّة والحفاظ على سريّة وخصوصيّة المبادلات الإلكترونيّة المتداولة فيما بين أطراف التّعامل الإلكتروني[1].

---

[1] **Michel AGLIETTA, Laurence SCIALOM**, op.cit., pp. 87- 92.

ثامنا– المخاطر المتعلّقة بانتهاك حقوق الملكيّة الفكريّة:

تُواجه المصارف الإلكترونيّة تحدّيات خاصّة بالمسائل المتعلّقة بحماية الملكيّة الفكريّة، للبرمجيات المعلوماتيّة وقواعد البيانات التي تتضمّن على معلومات المصرف أو تلك المستخدمة انطلاقا من موقعه الإلكتروني، كتقليد برامج الحاسوب أو تقليد معلوماتها الخ...، في حين تفرض هذه التّحدّيات على المصارف تهيئة البيئة القانونيّة اللاّزمة وعصرنتها مع مستجدّات تكنولوجيا الاتّصال والإعلام التي تُمثّل أهمّ ضمانات نجاح العمليات المصرفيّة الإلكترونيّة[1]، لذا يجب على مشّرعي الدّول الرّاغبة في عصرنة العمليات المصرفيّة السّعي على سنّ نصوص تشريعيّة وتنظيميّة خاصّة بها لغرض حفظ حقوق أطراف العملية المصرفيّة(المصرف والعملاء)، كما أنّ للمصارف المركزية مكانة ودور مهم في توجيه نوايا المؤسّسة التّشريعيّة نحو تبنّي تشريعات متوائمة مع المفاهيم الحديثة للعصر الرّقمي لمواجهة التّحدّيات القانونيّة والتّقنيّة التي تعترض المصارف الإلكترونيّة.

تاسعا– المخاطر المتعلّقة باستخدام العملات الافتراضيّة:

ظهرت في الآونة الأخيرة العملات الافتراضيّة المشّفرة(Crypto- monnaies) باعتبارها عملات الكترونيّة حرّة وكوسيط حديث للتّبادل الافتراضي، يُعوّل عليها أطراف التّعامل الإلكتروني في إجراء المعاملات التّجاريّة والماليّة عبر شبكة الإنترنت، حيث لا تُشرف الدّول أو المصارف المركزيّة على عمليات إحداث وحداتها، بل تُنشئ(Crypto- monnaies) على الإنترنت بواسطة مجموعة من الأشخاص معروفة أو مجهولة الهويّة، وكذا تسمح بتبادل ونقل الأموال فيما بين الأرصدة بسرعة وبسهولة، من دون الاستعانة بأيّ وسيط، أو إجراء المقاصة مع استبدالها بالعملات الماديّة الرّسميّة للدّول، وبالتّالي تفادي الرّسوم المفروضة على عمليات التّحويل، ممّا يشجّع بالمقابل تزايد أنشطة التّهرّب الضّريبي وغسيل الأموال والغش التّجاري والمُضاربة على حساب العملات الرّسميّة للدّول، الخ...

---

[1] **يونس عرب**، "العقود الإلكترونية– أنظمة الدفع والسداد الإلكتروني"، مرجع سابق، ص 128.
يوسف حسن يوسف، البنوك الإلكترونية، مرجع سابق، ص ص 272– 274، 276، 277.

وفي غياب الإطار القانوني المُنظّم للعملات الافتراضيّة اكتفت معظم الدّول(الأجنبيّة والعربيّة) بتوجيه تحذيرات للمستهلكين والمستثمرين (Des mises en garde à l'intention des consommateurs et des investisseurs potentiels.) من مخاطر وعواقب التّعامل بالعملات الافتراضيّة، حيث تُشكّل حاليّا هذه العملات، باعتبارها وسيلة دفع حديثة عبر الإنترنت، تحدّيا كبيرا لجميع الدّول والمصارف المركزيّة التي تستوجب إرساء آليات قانونيّة وتقنيّة، لرقابة عمليات تداول هذه العملات وتفادي الأنشطة غير المشروعة[1].

المطلب الثاني

توسّع تهديدات أمن مواقع التّجارة الإلكترونيّة بتَطوُّر تقنيات الدّفع الإلكتروني

يعتبر القطاع المصرفي من بين القطاعات الحسّاسة في اقتصاد أيّة دولة من العالم، بغض النّظر عن المنهج الإيديولوجي(اشتراكي أم رأسمالي) المتّبع في ذلك، فدوام واستمرارية السّيولة الماليّة في اقتصاد الدّول هو بمثابة سريان الدّم في عروق جسم الإنسان الذي يضمن صّحته، حيث شهدت البيئة المصرفية ثورة حقيقيّة في تقنيات الإعلام والاتّصال، التي سيطر فيها العقل الُمبدِع على نمط تقديم الخدمات المصرفيّة، وطرق إدارة الحسابات الماليّة الخاصّة بالعملاء، التي تطوّرت مع ظهور وشيوع مواقع التّجارة الإلكترونيّة، وما تُوفّرُه من خدمات إلكترونيّة وتسهيلات لأطراف التّبادل التّجاري من حيث تقنيات الدّفع الإلكتروني

---

1) Voir l'avertissement de l'Autorité bancaire européenne(**ABE**) à l'attention des consommateurs concernant les monnaies virtuelles, du 12 décembre 2013, pp. 02-03. Publié sur : https://www.eba.europa.eu...EBA_2013_01030000_F....pdf ou http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014 08+Opinion+on+Virtual+Currencies.pdf ou http://www.mf-ctrf.gov.dzpressebultin%252042.pdf ou http://www.conseiller.ca/nouvelles/lautorite-bancaire-europeenne-deconseillelusage-du-bitcoin-2-48736, consultés le 27/06/2018.

Focus de la Banque de France, sur l'émergence du bitcoin et autres crypto-actifs: enjeux, risques et perspectives, n° 16 - 5 mars 2018, pp. 03, 04. https://www.publications.banque-france.fr/liste-chronologique/focus/,consulté le 08/04/2018.

Rapport d´information (Sénat Français) fait au nom de la commission des finances(1) sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles, du 23 juillet 2014, op.cit., pp. 09- 18. http://www.senat.frrapr13-767r13-7671.pdf, consulté le 25/06/2018.

عبر الإنترنت، على غرار النّقود الإلكترونيّة(**الفرع الأول**)، الشّيك الالكتروني(**الفرع الثاني**)، البطاقات الذّكية(**الفرع الثالث**)، الدّفع عن طريق الهاتف الذّكي (**الفرع الرابع**).

الفرع الأول

النّقود الإلكترونيّة(Monnaies électroniques)

يُشْبِهُ التّعامل بتقنيّة النّقود الإلكترونيّة(E-Cash- E-money) من النّاحية العملية التّعامل بالنّقود التّقليديّة في معظم خصائصها، إذ لا تختلف النّقود الإلكترونيّة عن النّقود التّقليديّة إلاّ في الوسيلة المستعملة للدّفع، فهي مخزّنة على وسيط الكتروني (**أولا**)، كما ظهرت في الآونة الأخيرة عملات افتراضية مُشّفرة، غير رسميّة، لا تُصدِرها المصارف المركزيّة (**ثانيا**).

أولا – مفهوم النّقود الالكترونيّة(Monnaies électroniques):

أتاحت الثورة الرقمية تقنيات متعّددة في بيئة التّجارة الالكترونيّة على غرار النّقود الإلكترونيّة(**1**)، التي تنفرد بمجموعة من الخصائص التي تميّزها عن العملات الماديّة(**2**).

1 – تعريف النّقود الالكترونيّة(Monnaies électroniques):

تتضمّن العملات الإلكترونيّة على سلسلة من البّتات(Bits) التي تُمثّل وحدة أو قيمة نقديّة مكافئة للقيمة المُحدّدة بالعملة الماديّة الرّسميّة، إذ تُشرِف على عملية إصدارها مؤسّسة ماليّة مُقابل إيداع مبلغ مالي في حساب مصرفي، حيث تحتوي كلّ وحدة نقود رقميّة على رقم مرجعي(Numéro de référence) خاص وفريد بها يُميِّزها عن باقي العملات الرّقميّة الأخرى، مع التّوقيع الرّقمي للجهة المُصدِرة لها(المؤسّسة الماليّة) والمُلتزِمة بصفة "قانونيّة" أو "اتّفاقا" بتحويل وِحدة العملة إلى القيمة التي تكافئها من العملة الرّسميّة.

وعليه، يعتبر مصطلح النّقود الالكترونيّة حديث لدى مختلف التّشريعات، حيث عرّفها المشّرع الفيدرالي الأوروبي بموجب المادة 2/02 من التّوجيه الأوروبي رقم 110/2009 المؤرخ في 16 سبتمبر 2009، المتعلّق بالنّفاذ إلى خدمات مؤسّسات النّقود الإلكترونيّة

ورقابتها، المعدِّل للتّوجيهات الأوروبية رقم 60/2005 و48/2006 والملغي للتّوجيه الأوروبي رقم 46/2000[1]، على أنّها قيمة نقديّة مخزّنة في شكل إلكتروني أو مغناطيسي تُمثِّل دَيْنْ على عَاتِقِ الجهة المُصدِرة لها مقابل إيداع مبلغ مالي من المعني، يسمح له بتنفيذ العمليات النّقديّة المحدّدة بموجب المادة 5/04 من التّوجيه الأوروبي رقم 64/2007 المؤرخ في 13 نوفمبر 2007 المتعلّق بخدمات الدّفع في السّوق الدّاخلي[2]،(الذي سيُلغَى ابتداء من تاريخ دخول حيّز التّنفيذ التّوجيه الأوروبي رقم 2366/2015 المؤرخ في 25 نوفمبر 2015 أي "في 13 جانفي 2018"، الذي نقل حرفيا نص هذه المادة "5/04")[3]، حيث تكون مقبولة كوسيلة دفع من قِبَلِ الأشخاص(الطبيعيّة والمعنويّة) غَيْرَ الشّركة المُصدرة لها(النّقود الإلكترونيّة).

---

1) **Directive 2009/110/CE** du parlement européen et du conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, **modifiant** les directives 2005/60/CE et 2006/48/CE et **abrogeant la directive 2000/46/CE**, JOUE, n° L 267/7 du 10/10/2009.

Art. 02/2 : « **monnaie électronique**: une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique. »

2) **Directive 2007/64/CE** du parlement européen et du conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, JOUE, n° L 319/1 du 5/12/2007.

3) **Directive(UE) 2015/2366** du parlement européen et du conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et **abrogeant la directive 2007/64/CE**, JOUE, n° L 337/35 du 23/12/2015.

Art.04/5 : « «opération de paiement», une action, initiée par le payeur ou pour son compte ou par le bénéficiaire, consistant à verser, à transférer ou à retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire. »

Art.114 : « La directive **2007/64/CE** est **abrogée avec effet** à compter du **13 janvier 2018**. Toute référence faite à la directive abrogée s'entend comme faite à la présente directive et est à lire selon le tableau de correspondance figurant à **l'annexe II** de la présente directive. »

حيث طبّق المشّرع الفرنسي أحكام التّوجيه الأوروبي رقم 110/2009 وبالخصوص نص المادة 2/02 منه حرفيا بموجب المادة(**L315-1**) من التّقنين المتعلّق بالنّقد والقرض[1].

كما طبّق المشّرع الفيدرالي البلجيكي أحكام التّوجيه الأوروبي رقم 110/2009 وبالخصوص المادة 2/02 منه في أحكام قانون 17 نوفمبر 2012 المعدّل لقانون 21 ديسمبر 2009[2].

---

1) **Loi n° 2013-100** du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière, JORF n°0024 du 29 janvier 2013.

Code monétaire et financier - Dernière modification le 16 novembre 2019 - Document généré le 15 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr

Art. L315-1 : « **I.**- La **monnaie électronique** est une **valeur** monétaire qui est **stockée** sous une forme **électronique**, y compris **magnétique**, représentant une **créance** sur **l'émetteur**, qui est émise **contre la remise de fonds** aux fins d'opérations de paiement définies à l'article **L.133-3** et qui est acceptée par une personne physique ou morale **autre que l'émetteur** de monnaie électronique.

II.- Les unités de monnaie électronique sont dites unités de valeur, chacune constituant une créance incorporée dans un titre. »

Art. L133-3 : « **I.** Une opération de paiement est une action consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire, ordonnée par le payeur ou le bénéficiaire.

II. L'opération de paiement peut être ordonnée : **a) -** Par le payeur, qui donne un ordre de paiement à son prestataire de services de paiement ;

b) - Par le payeur, qui donne un ordre de paiement par l'intermédiaire du bénéficiaire qui, après avoir recueilli l'ordre de paiement du payeur, le transmet au prestataire de services de paiement du payeur, le cas échéant, par l'intermédiaire de son propre prestataire de services de paiement ;

c) - Par le bénéficiaire, qui donne un ordre de paiement au prestataire de services de paiement du payeur, fondé sur le consentement donné par le payeur au bénéficiaire et, le cas échéant, par l'intermédiaire de son propre prestataire de services de paiement. »

Art. L315-2 : « Chacune des **unités** de monnaie électronique est émise sans délai contre la remise de fonds. »

Art. L315-3 : « Chacune des **unités** de monnaie électronique ne peut être émise que pour une valeur nominale **égale** à celle des fonds collectés en contrepartie. »

2) **Loi du 21 décembre 2009** relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement, MB n° 2199 du 19/01/2009. https://www.moniteur.be

Loi du 27 novembre 2012 modifiant la loi du 21 décembre 2009, relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement et d'autres législations dans la mesure où elles sont relatives au statut des établissements de paiement et des établissements de monnaie électronique et des

انطلاقا من ذلك، فإنّ المشّرع الفيدرالي للإتّحاد الأوروبي قدّم مفهوما خاصا للنّقود الإلكترونيّة، على نحو يجعلها تتماشى مع التّطوّرات التّكنولوجيّة المستقبليّة (Les produits de monnaie électronique qui pourraient être développés à l'avenir.) مع إخضاع عملية إصدارها لرقابة الدّولة أو المصارف المركزيّة لها، حيث اعتبر النّقود التي يتم تخزينها على أيّ وسيط إلكتروني مُقابِل مبلغ مالي مُودَع في الحساب المصرفي، الوحيدة التي تستهِل أو تُكيّف على أنّها نقودا إلكترونيّة تُستعمل كوسيلة للدّفع الإلكتروني، وبالتّالي فإنّ عملية تجريد النّقود من ماديتها تتم بمُجرّد تخزينها على أيّ وسيط أو ذاكرة إلكترونيّة (Supports ou mémoires électroniques) على سبيل محفظة النّقود الإلكترونيّة أو بطاقة تعبئة أو الدّفع المُسبق، هاتف نقّال ذكّي الخ...، تضمن توثيق هويّة صاحب الحساب وتُثبِت رصيده النّقدي حيث تسمح بالقيام بجميع التّصرفات النّقديّة المعروفة في صورتها الماديّة[1].

2 – خصائص النّقود الإلكترونيّة(Monnaies électroniques):

من خلال أحكام المادة 2/02 من التّوجيه الأوروبي رقم 110/2009 المذكور أعلاه، يتبيّن لنا أنّ النّقود الإلكترونيّة تتضمّن على ثلاثة خصائص أساسيّة تُميّزُها عن العملات الماديّة والإلكترونيّة الأخرى، وتتمثّل فيما يلي:

– إنّها قيمة نقديّة مخزّنة في شكل إلكتروني أو مغناطيسي على أيّ وسيط إلكتروني.

– تُمثّل إيداعا ماليّا في حساب مصرفي حيث لا تقل قيمة العملات الالكترونية عن القيمة المودعة من الأوراق الماليّة أو النّقود المعدنيّة.

– تكون النّقود الإلكترونية مقبولة كوسيلة دفع من قِبل الأشخاص الطبيعيّة والمعنويّة غير الشّركة الماليّة أو المصرفيّة المُصدِرة لها.

---

associations de crédit du réseau du Crédit professionnel, MB n° 76567 du 30/11/2012. https://www.moniteur.be

1) **Chiheb GHAZOUANI**, Le commerce électronique international, Latrach édition (1ère édition), Tunis, 2011, pp. 153, 154, 155.

وعليه، فإنّ النّقود الإلكترونيّة تتميّز على أنّها مُجرّد كيانات افتراضيّة غير ماديّة تتضمّن على ملفات إلكترونيّة صغيرة، ذات صلة بحساب مصرفي أو بطاقة ممغنطة أو دفع مُسبق(Prépaiement) باستخدام النّقود الماديّة، وقابلة للتّحويل في أيّ وقت إلى النّقود الرّسميّة وإمكانية تبادلها مع مختلف السّلع والخدمات المتاحة عبر شبكة الإنترنت، كما تتميّز كذلك النّقود الإلكترونيّة بأنّها سهلة الاستخدام والتّخزين والنّقل، حيث يمكن وضعها على القرص الصّلب أو في ذاكرة جهاز الحاسوب أو شحنها في البطاقات البلاستيكيّة الممغنطة أو البطاقات الذّكيّة، التي بدورها تتطلّب توافُر معدّات مدعومة ببرمجيات معلوماتية خاصّة لتأمين وحماية القيّم النّقديّة المحفوظة لتفادي العبث فيه أو سرقتها أو تزويرها[1].

بالإضافة إلى ذلك، نجد أنّ التّوقيع الرّقمي للجهة المُصدِرة للنّقود الإلكترونيّة يُمكّن من تحديد وتوثيق هويّتها ويُوفّر ضمانا كافيا بتحويل النّقود الإلكترونيّة إلى نقود ماديّة عند طلبها، وذلك من دون أن يضطّر الأفراد بالتّعريف بأنفسهم إلى البائعين أو أيّ مؤسّسة ماليّة ما دام أنّهم يقدّمون نقود ماديّة، وما يميّز كذلك وحدة النّقود الرّقميّة عدم صلاحيتها لإبرام أكثر من صفقة واحدة، ممّا يستدعي الأمر الاتّصال من جديد بالمؤسّسة الماليّة لإصدار وحدة نقدية رقميّة وفقا لمرجع تسلسلي جديد لم يسبق استخدامه من قَبْلْ، وذلك على غرار النّقود الماديّة التي تستمر في عملية الانتقال والتّداول من يد إلى يد من دون الرّجوع إلى السّلطة المُصدرة لها، وذلك باستثناء الظّروف التي تستدعي سحبها من التّداول كإتلافها أو تمزيقها أو تعرّضها للتّبليل، وبالتّالي تعتبر شركة(PayPal) من بين الشّركات العاملة بنُظم العملات الرّقميّة(Digital Cash) عبر أسواق العالم، حيث تُمكِّن أطراف التّبادل الإلكتروني من إجراء المبادلات التّجاريّة بسرعة مع ضمان عمليات الدّفع الإلكتروني[2].

---

1) **Jean-Claude PAILLÈS**, « Les systèmes de paiement électronique sur internet », Revue Les Cahiers du numérique, 2003/1 - Vol. 4, pp. 59, 60.
2) Ibid.

ثانيا – العملات الافتراضيّة(Crypto-monnaies):

تُعدّ النُّقود الإلكترونيّة إحدى الوسائل الحديثة المُستخدمة في التّعاملات التّجاريّة، حيث تنقسم إلى نقود إلكترونيّة اسميّة التي من خلالها تتضمّن وحدة النّقد الإلكتروني على معلومات تتعلّق بهويّة الأشخاص الذين تَدَاوَلُوهَا، وهذا ما يسري أو ينطبق على البطاقات الذّكيّة(Cartes à puces)، بينما النُّقود الرّقميّة غير الاسميّة أو الافتراضيّة هي نوع من النّقود الرّقمية غير المُنظَّمَة(Non régulée) غير المُصدَرة من طرف المصارف المركزيّة، حيث يُمكِن استخدامها كوسيلة دفع عبر الإنترنت لقيمة السّلع والخدمات، مع تحويلها مُقابل العملات الرّسميّة التّقليديّة للدّول أو العكس في إطار أسواق التّبادل الخاصّة بالعملات الافتراضيّة(Plates-formes de marché) [1]، وللتّعرّف أكثر حول العملات الافتراضيّة يستوجب التّطرّق إلى تقنيّة عملها **(1)** والتّسهيلات التي تُتيحها **(2)**، وطبيعتها القانونيّة **(3)** ومخاطرها **(4)**.

1)– تقنيّة عمل العملات الافتراضيّة(Crypto-monnaies):

تعتمد تقنيّة العملات الرّقميّة الافتراضيّة على أسلوب النّد للنّد(Pair à Pair) وآليات التّشفير اللاّتماثلي(مفتاح عام وخاص) لغرض تأمين المعاملات الماليّة الإلكترونيّة، حيث تُمثّل وحدات أو قيم نقديّة إلكترونيّة مخزّنة على القرص الصّلب(Disque dur)، أو خادم جهاز الحاسوب(Serveur) أو الهاتف الذّكي(Smartphone)، الخ...، تكون مُتكافِئة مع قِيَمِ العملات التّقليديّة لمختلف الدّول، في حين يتم إنشائها عبر الإنترنت عن طريق نظام تقني متكامل وأساسي يرتكز على مجموعة من الخوارزميات الرّياضيّة المعقّدة(Algorithmes)، يُشرف عليها مجموعة أو شخص معيّن مُعرّف الهويّة أو بدونها ولا تستدعي تواجد سلطة مركزيّة تشرف على عملية إصدارها، ويتم تداولها فيما بين أرصدة(Comptes) أطراف

---

[1] **أحمد سفر**، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2008، ص 49.

للمزيد من المعلومات حول استخدام العملات الإلكترونية الافتراضية في العديد من دول العالم أنظر الموقع الإلكتروني التالي : http://www.coinmap.org/ et https://getaddr.bitnodes.io/ et http://bitcoincharts.com/markets/localbtcCHF.html(consultés le 12/04/2016)

التّعامل الإلكتروني بسهولة، ومن دون دفع أيّ رسوم أو إجراء عمليات المقاصة ما دام أنّها لا تخضع لرقابة المصارف المركزيّة[1].

وعليه، يعتبر البِتْكُويْنْ(Bitcoin)(يشير اختصارا إلى كلمتي(Bit) التي تُمثّل وحدة معلومات عدديّة و(Coin) التي تعني قطعة نقود)، كأوّل عُمْلَة رقمية افتراضيّة مشّفرة تم إنشائها في 2008 من طرف شخص أو مجموعة غير معروفة الهوية تُطلق على نفسها الاسم الرّمزي لـ(Satoshi NAKAMOTO)، طُرحت لأوّل مرّة للتّداول عبر الإنترنت في عام 2009 تحت شعار(« ฿ »، **BTC**, **XBT**)، حيث ظهرت فيما بعد إلى جانبها العديد من العملات الافتراضيّة المُنافِسة لها (Namecoin- Litecoin, Swisscoin, Peercoin- Monero- Ethereum- Nxten, etc.)[2].

تعتمد عملة البتكوين في المعاملات الماليّة على مبدأ النّد للنّد(Peer-to-Peer) الذي يستعين بدوره على مبادئ التّشفير اللاّتماثلي والخوارزميات، التي تسمح للمُستخدمين(Usagers) والمُعْدِنِينْ أو المُنْقِبِينَ((Miners(Mineurs) (يعتمدون على مُعدّات وبرامج لتكوين وإنتاج البِتْكُويْنْ وضمان حسن سير معاملاته، فعملية تعدين البِتْكُوينْ تُشبه من النّاحية العمليّة تقنيات وطرق استخراج الذّهب(Or) من باطن الأرض، الذي يَتطلّب جُهد كبير من جانب المَوارِد البّشريّة ومُعِدَّات معيّنة مُخصّصة لذلك الغرض.)، بالتّعامل بطريقة مباشرة فيما بينهم من دون تَدخُّل أيّ وسيط أو سلطة مركزيّة رسميّة(المصارف المركزيّة)، حيث يملك كلّ مُستخدم مُسجَّل عبر الشّبكة محفظة أو عدّة محافظ نقود إلكترونيّة(Wallets)، تتضمّن على واحد أو أكثر من العناوين الإلكترونية للبِتْكُوينْ(Bitcoin)

---

[1] **Gerald STUBER**, « Le bitcoin : une monnaie virtuelle sans émetteur central », Revue de la Banque du Canada- printemps, 2014, p. 16. https://www.revue-bdc-printemps14-fung.pdf

أنظر كذلك الموقع الإلكتروني التالي : http://www.coinmap.org/(consulté le 12/04/2016)

[2] **Y. POULLET et H. JACQUEMIN**, op.cit., pp. 804, 805, 813, 814.

للمزيد من المعلومات حول الموضوع، أنظر المواقع الإلكترونية التالية: http://coinmap.org/ et http://bitcoincharts.com/markets/localbtcCHF.html et https://getaddr.bitnodes.io/(consulté le 15/04/2016.)

التّابعة للمستخدمين تُمثّل أرقام حسابات مصرفيّة لأرصدتهم(Des numéros de compte) عبر الإنترنت، التي من خلالها يتم تبادل عُملة البِتْكُويْنْ ونَقلها فيما بين الأرصدة بكلّ سهولة ومن دون أيّ رسوم تحويل أو ضريبة أخرى، حيث يُزوّد كل مُستخدم بمفتاحين، أحدهما خاص(Clé privée) يسمح له بالتّوقيع على معاملات بيع وشراء البِتْكُويْنْ، الذي يستوجب الحفاظ عليه بطريقة مؤمّنة ففي حالة فقدانه له(المفتاح الخاص)، يَفقِد مَعَهُ جميع عملات البِتْكُويْنْ المُتَحَصَّلِ عليها ولا يستطيع تَعْوِيضُهَا[1].

ففي حالة ما إذا تحصّل مُستخدم آخر على المفتاح الخاص الضّائع فيستغِّل بالتّالي فُرَص استخدام عملات البِتْكُويْنْ لمصلحته من دون علم صاحبها، وأمّا المفتاح الأخر يكون عام(Clé publique) يُتيح لبرمجيات الشّبكة بفحص والتّحقّق من صحة التّوقيع الإلكتروني لصاحب المعاملة، في حين تُسجّل جميع عمليات شراء عملة البِتْكُوينْ في السّجل المركزي للشّبكة((La chaine de Blocs(La blockchain) في شكل سلسلة من الكُتَلِ، تحتوي على جميع عناوين ومعاملات المشاركين في الشّبكة على النّحو الذي يُمكّن من معرفة الرّصيد الذي يملكه كلّ عنوان، حيث ترتبط كلّ كتلة(Bloc) بدالة هاش الكتلة السّابقة لها وهكذا إلى غاية الوصول إلى كتلة التّكْوِينْ(Genesis block)، فَتَغْيِيرِ أيّ كتلة يتطلّب تغيير جميع الكُتل مع تحديث دالة الهاش الرّئيسيّة من جديد[2].

وعليه، فإنّ عمليات بيع وشراء البِتْكُوينْ تتمتّع بقدرٍ عالٍ من المجهولية(Anonymat) حيث تعتمد فقط على عناوين المستخدمين(Utilisateurs) التي تتغيّر من حين لأخر لتعقيد فرص كشف والتعرّف على هويّتهم، كما أنّ عملة البِتْكُويْنْ لا تتضمّن على أرقام تسلسليّة

---

[1] للمزيد من المعلومات حول الموضوع، أنظر كذلك المواقع الإلكترونية التالية: https://bitcoin.fr/obtenir-des-bitcoins et https://bitcoin.frpaypal-adopte-bitcoin.html et http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (consultés le 22/04/2016.)

[2] **Y. POULLET et H. JACQUEMIN**, op.cit., pp. 803- 808.

للمزيد من المعلومات حول الموضوع، أنظر المواقع الإلكترونية التالية: http://coinmap.org/ et http://bitcoincharts.com/markets/localbtcCHF.html et https://getaddr.bitnodes.io/(consulté le 15/04/2016)

تسمح بِتَتَبُّعِ العُملات التي تمّ إنفاقها للوصول إلى البائع أو المشتري وهذا ما يجعلها كعملة لا مركزيّة وغير مُنظمّة قُانُونِيًّا[1].

بالإضافة إلى ذلك، نجد أنّ سِعر عُملة البِتْكُويْنْ منذ إنشائها في تذبذب(صعودا ونزولا) حيث يفوق في بعض الأحيان قيمة الذّهب والدّولار الأمريكي أو الأورو أو اليّان الياباني حيث اختلفت المواقف والآراء بشأنه، فهناك من يرى بأنّ هذا السّعر مُبالَغ فيه بينما يرى البّعض الأخر أنّ هذا السّعر لا يتناسب مع القيمة الحقيقيّة للبِتْكُوينْ كسلعة، تتطلّب عملية إنتاجها إلى بذل مجهودات كبيرة وتكاليف باهظة جرّاء استغلال الطّاقة الكهربائيّة أثناء قيام المُنْقِبِينَ(Miners) بعمليات التّعدين(Minage)، التي تستعين ببرمجيات خاصّة لفكّ الشّفرات والقيام بالعمليات الحسابيّة المُعقّدة لضمان السّير الحسن لعمليات البيع والشّراء.

2)– التّسهيلات التي تتيحها العملات الافتراضيّة(Crypto-monnaies):

من بين التّسهيلات التي تُتيحها العملات الافتراضيّة المشّفرة(Crypto-monnaies) نجد أنّها أُنشئت خصّيصا لإجراء المعاملات التّجاريّة والماليّة عبر شبكة الإنترنت من دون تدخّل أي وسيط أو مصرف مركزي، حيث تعتمد هذه المعاملات على مبادئ التّشفير اللاّتماثلي التي تضمن السّير الحسن لها ولا تستدعي إثبات هويّة أطراف التّعامل الإلكتروني بل ترتكز فقط على العناوين الالكترونيّة لهم، كما تتم عملية نقل وتحويل الأموال فيما بين الأرصدة في أيّ مكان من العالم بكلّ سهولة وفي أقرب وقت مُمكِن من دون اشتراط أيّ سقف معيّن للتّحويل، أو دفع رسوم تحويل أو إجراءات عمليات المقاصة فيما بين المصارف أو المرور عبر وسطاء.

فحسب التّقرير الذي أصدره المجلس الفيدرالي السّويسري في 25 جوان 2014 حول العملات الافتراضيّة[1]، فإنّ معظم المتعاملين في مجال التّجارة والخدمات في سويسرا قَبِلوا

---

[1] **Sylvain MIGNOT**, « Le Bitcoin : nature et fonctionnement », Revue Banque & Droit, nº 159 janvier- février 2015, pp. 10- 11.
Jean-Paul DELAHAYE, op.cit., pp. 76, 77, 81, et suiv.

التّعامل بالعملات الافتراضيّة وبالخصوص عملة البِتْكُويْنْ كوسيلة دفع عبر الإنترنت على غرار الفنادق والمطاعم ومحلاّت البيع بالتّجزئة، كما أنّ معظم مواقع التّجارة الإلكترونيّة قَبِلَتْ التّعامل بالعملات الافتراضيّة وبالخصوص البِتْكُويْنْ، كوسيلة دفع إلكترونيّة حديثة عبر الإنترنت مُقابل أو لِقاء منتجاتها، وذلك على غرار مواقع شبكات التّواصل الاجتماعي ومواقع الفيديو والموسيقى ومواقع حجز أسماء النّطاقات وبيع خدمات الإيواء أو الاستضافة إلى غيرها من المواقع المتنوّعة التي تُتيح خدمات بيع منتجاتها عبر شبكة الإنترنت، حيث تُصنَّف سويسرا في المرتبة الثّالثة عشرة(13) عالميًّا حسب الدّول التي تُستخدَم فيها العملات الافتراضيّة، بينما تتربّص الولايات المتّحدة الأمريكيّة(USA) على المرتبة الأولى عالميًّا أين تُستخدم فيها كثيرا هذه العملات(Crypto-monnaies).

انطلاقا من ذلك، تستعمل العملات الافتراضيّة سواء "كوسيلة دفع إلكتروني" لقيمة مستحقات مختلف السّلع والخدمات أو "كسلعة" تبادل فيما بينها في إطار منصّات الأسواق الماليّة الإلكترونيّة الخاصّة بها((Plates-formes d'échange(de négoce) [2]، حيث يستطيع من خلالها المتعاملين عبر شبكة التّسويق تبديل العملات الافتراضيّة مقابل العملات الرّسميّة للدّول من خلال بيع العملات الافتراضيّة مقابل شراء العملات الرّسميّة أو العكس، في حين تتم عملية تحديد السّعر الخاص لهذه العملات الافتراضيّة بطريقة آلية، إذ أنّ قيمتها تفوق في بعض الأحيان قيمة الذّهب أو حتّى العملات الرّسميّة كالدّولار واليّان والأورو الخ...

فوفقا للدّراسات التي قامت بها المدرسة الفيدرالية(زيوريخ السّويسريّة) للتّكنولوجيا (École polytechnique fédérale de Zurich (EPFZ)) بناءً على أمرٍ من المجلس الفيدرالي للكُنْفِيدِرَالِيَّة السّويسرية، فإنّ أوّل منصّة إلكترونيّة عبر الإنترنت(Plate-forme de négoce)

---

1) **Rapport** du Conseil fédéral (Confédération suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab(13.3687) et Weibel(13.4070), du 25 juin 2014, p. 10. Disponible sur : https://www.news.admin.chNSBSubscribermessageattachments35353.pdf, consulté le 12/03/2016.

2) **Rapport** du Conseil fédéral (Confédération suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab(13.3687) et Weibel(13.4070), du 25 juin 2014, op.cit., pp. 10, 11.

تسمح ببيع وشراء عملة البِتْكُويْنْ مقابل الفرنك السّويسري تتعلّق بـ(LocalBitcoins.com) المُتواجدة بهلسنكي(Helsinki) الفنلنديّة، حيث تُتيح للمستخدمين إمكانية تبديل أو تحويل عملات البتكوين إلى العملات الرّسميّة للدّول كالدّولار والفرنك السّويسري الخ...، عبر أجهزة صَرَّافْ آلية خاصّة بها(Bitcoins Teller Machines(BTM))، فأوّل صرّاف آلي للبِتْكُوينْ ظهر في مدينة فانكوفر(Vancouver) الكنديّة الذي دخل حيّز الخدمة في 29 أكتوبر 2013، لتنتشر فيما بعد عبر العديد من دول العالم على غرار سويسرا وكندا وفرنسا، وبعض الدول العربيّة كالإمارات(دبي) وفلسطين[1] الخ...

تتيح تقنيّة التّعامل بالعملات الافتراضيّة لبعض الدّول إمكانية اللّجوء إليها خلال الأزمات الاقتصاديّة والتّضخّم النّقدي، جرّاء انهيار قيمة العملة الوطنيّة الرّسميّة أو تراجعها وارتفاع الأسعار ونقص السّيولة الخ...، وذلك تزامنا مع استقرار أو ارتفاع قيمة العملات

---

[1] أنظر **الملحق رقم (25)**، ص 500.

Riccardo SANSONETTI, « Le bitcoin: opportunités et risques d'une monnaie virtuelle ». Article publié le 01/09/2014 à partir de l'adresse suivante: http://dievolkswirtschaft.ch/fr/2014/09/sansonetti-4/, consultée le 12/02/2016.

Adeline RAYNAL, « Le premier distributeur automatique de bitcoins débarque au Canada », article de journal La Tribune, publié le 29/10/2013 à 14:29 sur le site: http://www.latribune.frentreprises-financebanques-finance20131029trib000793018le-premier-distributeur-automatique-de-bitcoins-debarque-a.html, consulté le 14/02/2016.

Adrien SCHWYTER, « Le premier distributeur de Bitcoins arrive à Paris », article de journal Les Echos, publié le 15/05/14 à 17H40 sur le site: http://www.lesechos.fr/15/05/2014/lesechos.fr/0203500349838_le-premier-distributeur-de-bitcoins-arrive-a-paris.htm, consulté le 17/02/2016.

Jean LUC, « Un distributeur de bitcoins à Paris ». Article publié le jeudi 15 mai 2014 à 0:14, à partir de l'adresse: https://bitcoin.fr/un-distributeur-de-bitcoins-a-paris/, consultée le 22/02/2016.

– **دارين العمري**، "افتتاح أوّل صرّاف لعملة "بتكوين" الافتراضية في دبي"، مقال منشور في 29 ابريل 2014، التوقيت 12:42(أخر تحديث له تم في 01 ماي 2014، التوقيت 06:32)، على الموقِع التّالي:http://arabic.cnn.com/business/2014/04/29/bitcoin-sergey-yusopov-interview (تم الاطّلاع عليه في 2016/02/25.)

– **أضافه عباس**، "شركة حوسب الفلسطينية تبدأ التعامل بالبتكوين"، مقال منشور في 2014/05/04؛ التوقيت18:16، على الموقع التالي: http://arabicbitcoin.net/news/hawsib-starts-accepting-bitcoin (تم الاطّلاع عليه في 2016/02/27.)

الافتراضيّة الأمر الذي يدفع بهذه الدّول إلى حتمية استخدامها كبديل وحيد للعملة الرّسميّة المنهارة لهدف التّخفيف من آثار الأزمة الاقتصاديّة أو الماليّة أو حتّى القضاء عليها[1].

3)– الطبيعة القانونيّة للعملات الافتراضيّة (Crypto-monnaies):

إنّ وضع العملات الافتراضيّة حاليا لا يزال محل نقاش ولم يتم الاعتراف بها رسميا كعملة لغياب الإطار التّشريعي أو التّنظيمي الخاص بها، كما أنّ طبيعتها لا تتوافق من النّاحية القانونيّة مع ما وُرِدَ في نص المادة 2/02 من التّوجيه الأوروبي رقم 110/2009 المؤرخ في 16 سبتمبر 2009 المتعلّق بالنّفاذ إلى خدمات مؤسّسات النّقود الإلكترونيّة ورقابتها، حيث أنّ هذه العملات لا تُصْدَرُ من طرف المؤسّسات الماليّة والمصرفيّة التي تحصّلت على ترخيص بمزاولة نشاطاتها، ولا تخضع لرقابة المصارف المركزيّة بمفهوم أحكام المادة 3،1/02 من نفس التّوجيه، كما أنّ المبلغ المالي الذي يتّم إيداعُه لا يُمثّل دين(Créance) على عاتق هذه الجّهات، ما دام أنّه يُدفع لجهات(معروفة أو مجهولة الهويّة)

---

[1] تعتبر **فنزويلا** أوّل دولة في العالم قامت بإحداث **عملة افتراضية سيادية** تدعى بترو(**Petro**) قابلة للتداول مقابل سعر البترول الواحد، وذلك لهدف مُواجهة الأزمات والاضطرابات في السياسة النقدية والاقتصادية في البلاد(التّضخم النّقدي، المديونية الخارجية، عجز ميزان المدفوعات، اضطرابات اجتماعية، الخ...)، وكذا العقوبات المالية التي فرضتها الولايات المتحدة الأمريكية على فنزويلا في ظل انخفاض أسعار البترول، حيث طَرحت بصفة رسمية في 20 فيفري 2018 مبلغ يُقدّر بـ 38,4 مليون من قيم العملة الافتراضية(**Petro**) للتداول(البيع) أي ما يُعادل 60 دولار من سعر البرميل الواحد من احتياط البترول الفنزويلي، الذي من خلاله استطاعت الحكومة من تحصيل مبلغ يقدر بحوالي 735 مليون دولار من الأرباح على حدّ تعبير الرئيس الفنزويلي نيكولاس مادورو(NICOLAS Maduro) خلال اللقاء الصحفي، أين أكدّ من خلاله أنّه سيتم طرح قيمة 100 مليون من العملة الافتراضية(**Petro**) للتداول خلال الأشهر المقبِلة التي تسمح للحكومة الفنزويلية من تحصيل خمسة مليار دولار، عِلْمًا أنّ الدُيون الخارجية لدولة فنزرويلا تُقدّر بمبلغ 150 مليار دولار، وبالمقابل قامت الولايات المتحدة الأمريكية بمنع شركاتها وأفرادها من شراء قِيم العملة الافتراضية(**Petro**) المطروحة للتداول من طرف المُجمَّع البترولي الفنزويلي(PDVSA)، الذي يستحوذ على أكبر مخزون من احتياط البترول عالميا، أين تستقطب منه(البترول) دولة فنزويلا حوالي 96% من العائدات الخارجية من العملة الصعبة.

لمزيد من المعلومات أنظر:

Luc LENOIR, « Cryptomonnaie : Le petro vénézuélien en vente », article de journal Le Figaro, publié le 20/02/2018, à 07 :19 sur: http://www.lefigaro.fr/flash-econ/2018/02/20/97002-20180220FILWWW00034-cryptomonnaie-le-petro-vénézuélien-en-vente.php, consulté le 13/03/2018.

تباشِر نشاطاتها خارج الرّقابة القانونيّة، وبالتّالي فإنّ العملات الافتراضيّة لا تُعتبر كعملة من النّاحية القانونيّة وأنّ التّعامل بها يُثير مسائل قانونيّة أخرى حول تكييف وتطبيق أحكام التّشريعات الضّريبيّة، وكذا القانون الواجب التّطبيق في حالة النّزاع فيما بين أطراف المعاملة التّجاريّة الخ...[1].

اعترف المشّرع الجزائري لأوّل مرّة باستخدام التّقنيات الإلكترونيّة الحديثة في مجال المعاملات المصرفيّة، بموجب المادة 69 من الأمر رقم 03–11 المؤرخ في 26 أوت 2003 المتعلّق بالنّقد والقرض[2]، التي من خلالها اعتبر جميع الأدوات التي تُمكّن الأشخاص من القيام بتحويل الأموال مهما كان "السّند" أو "الأسلوب التّقني" المُستعمل فيها كوسائل دفع حديثة في الميدان المصرفي، حيث لم يتطرّق في هذا الأمر إلى تعريف النّقود الإلكترونية ولا العملات الافتراضيّة ولم يُنظِّم خدمات الشّركات الماليّة والمؤسّسات المُصدرة للنّقود الإلكترونيّة ورقابتها، بل اكتفى فقط بالكشف عن إرادته ونِيّته في استخدام تقنيات الدّفع الإلكتروني الحديثة في العمليات المصرفيّة، كحتمية فرضتها مستجدّات الثّورة الرّقميّة، لكن بصدور القانون رقم 17–11 المؤرخ في 27 ديسمبر 2017 المتضمّن لقانون الماليّة لسنة 2018، قام المشّرع الجزائري بموجب أحكام المادة 117 منه[3]، بِمَنْعِ جميع التّعاملات

---

[1] **David DESCÔTEAUX**, « Quel cadre réglementaire pour Bitcoin? », pp. 1- 4, article publié à partir de l'adresse suivante: http://www.iedm.orgfilesnote0514_fr.pdf, consultée le 09/05/2016.
Murielle CAHEN, « Traitement civil et pénal du bitcoin », pp. 01- 03. Article juridique publié le 17/04/2015, à partir de l'adresse suivante: http://www.legavox.frblogmurielle-cahentraitement-civil-penal-bitcoin-17601.pdf, consultée le 03/02/2016.
Pierre STORRER, « Droit des moyens et services de paiement : Les monnaies virtuelles dans tous leurs états », Revue Banque n° 775- septembre 2014, pp. 86-89.
Hubert de VAUPLANE, « l'analyse juridique du Bitcoin », pp. 353- 359. Article publié à partir de l'adresse suivante: http://www.kramerlevin.comfilesPublication26eb1df1-847a-40f0-bad1-5d839880ddd3PresentationPublicationAttachmentc8021100-5, consultée le 15/04/2016.
Myriam ROUSSILLE, « Le Bitcoin : objet juridique non identifié », Revue Banque & Droit nº 159 janvier- février 2015, pp.27- 29.

[2] أمر رقم 03–11 مؤرخ في 26 أوت 2003، يتعلق بالنقد والقرض، ج ر عدد 52 الصادر في 27 أوت 2003، معدل ومتمم.

[3] **قانون رقم 17–11** مؤرخ في 27 ديسمبر 2017 يتضمن قانون المالية لسنة 2018، ج ر عدد 76، الصادر في 28 ديسمبر 2017.

الإلكترونيّة المتعلّقة بشراء وبيع واستعمال وحيازة العملات الافتراضيّة، التي تَفْتَقِدُ للدّعامة الماديّة كالقطع والأوراق النّقديّة وعمليات الدّفع بالصّك أو بالبطاقة المصرفيّة.

وعليه، فإنّ مواقف الدّول الأجنبيّة، تفاوتت بشأن طبيعة التّعامل بالعملات الافتراضيّة، حيث اعتبرتها ألمانيا كنقود من نوع خاص(Argent privé) تُستعمل كوسيلة دفع بين أطراف التّعامل الإلكتروني[1]، بينما تُمثّل لدى بعض الدّول الإِسْكُنْدِنَافِيَّة كالنّرويج وفنلندا والسّويد بمثابة سلع(Marchandises) للتّداول فقط وليست كوسيلة دفع[2]، أمّا الولايات المتّحدة الأمريكيّة، بريطانيا، كندا، البرازيل تَعْتَبِرُهَا كوسيلة بسيطة للتّبادل والدّفع فقط وليست نقود بحدّ ذاتها[3]، في حين منعت بعض الدّول مؤسّساتها الماليّة التّعامل بهذه العملات على غرار كلٍّ من روسيا الفيدرالية، الصّين، تايلاند، اليابان، الجزائر، الخ...[4]، كما منعت بعض الدّول على غرار فرنسا والولايات المتّحدة الأمريكيّة وسويسرا وألمانيا من بيع وشراء العملات الافتراضيّة(Plate-forme de négoce de monnaies virtuelles) على أراضيها، من دون أيّ ترخيص من جانب السّلطات الرّسميّة المعنيّة[5]، في حين تسعى بعض الدّول

تنص **المادة 117** من نفس القانون، على ما يلي: "يمنع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها. العملة الافتراضية هي تلك التي يستعملها مستخدمو الإنترنت عبر شبكة الإنترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو بالبطاقة البنكية. يعاقب على كلّ مخالفة لهذا الحكم، طبقا للقوانين والتنظيمات المعمول بها."

1) **Rapport** du Conseil fédéral(Suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, op.cit. p. 24. https://www.news.admin.chNSBSubscribermessageattachments35353.pdf

2) Ibid.

3) **Rapport** du Conseil fédéral(Suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, op.cit. p. 24. https://www.news.admin.chNSBSubscribermessageattachments35353.pdf

4) Ibid., pp. 25, 26.

5) **Rapport** d´information (Sénat Français) fait au nom de la commission des finances(1) sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles(Par MM. Philippe MARINI et François MARC, Sénateurs), du 23 juillet 2014, op.cit., pp. 31, 48, 49. Disponible sur le site: https://www.senat.frrapr13-767r13-7671/, consulté le 25/06/2018.

كأُستراليا مثلا إلى التّفكير منذ 2015 حول كيفية تنظيم التّعامل بالعملات الإفتراضيّة، حيث لا تُصنّف المعاملات التي تتّم بعملة البتكوين(Bitcoin) ضمن جرائم تبيض الأموال[1].

4)– مخاطر التّعامل بالعملات الافتراضيّة (Crypto-monnaies):

بالرّغم من المزايا التي تُتيحها العملات الافتراضيّة في مجالات التّجارة الإلكترونيّة باعتبارها كوسيلة دفع إلكتروني حديثة عبر الإنترنت، إلاّ أنّ المخاطر المحيطة بها تجعل المُتعاملين يفقدون الثّقة والأمان في تعاملاتها، فمن بين عيوب التّعامل بهذه العملات نجد أنّه يُشجّع عمليات تبيض الأموال والتّهرّب الضّريبي وغسيل الأموال وانتحال الهويات، وكذا مُمارسة الأنشطة غير المشروعة كتجارة المخدّرات والغّش التّجاري وتمويل الإرهاب، الخ...، كما أنّ نظام التّعامل بالعملات الافتراضيّة يكون عُرضة لمختلف التّهديدات الإلكترونيّة عبر الإنترنت التي تؤدّي إلى مَحوِ العملات الافتراضيّة بالكامل في خوادم أجهزة الحواسيب أو التّعرض إلى خطر الانخفاض المفاجئ لسعرها أو قيمتها وهذا ما يؤثّر على استقرار حجم وقيمة الاستثمارات المستقطبة[2].

---

[1] **Rapport** du Conseil fédéral(Suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, op.cit., p.25.

[2] تعرضت أغلبية أجهزة الحواسيب خلال السداسي الثاني من سنة 2017 إلى هجمة إلكترونية واسعة النطاق أُطْلِقَ عليها تسمية(Adylkuzz)، التي من خلالها استغل القراصنة نفس الثغرات أو الهفوات الأمنية المتواجدة على مستوى نظام تشغيل(Windows) التي اعتمد عليها القراصنة في برنامج الفدية الخبيث(WannaCry)، إلاّ أنّ البرنامج الخبيث(Adylkuzz) لا يطلب الفدية من مُستعمِل جهاز الحاسوب المُصاب، أو حتى العمل على توقيف خدمة جهاز الحاسوب، بل يقوم بعملية تعدين وشراء العملات الافتراضية المشفرة بسرية تامة من خلال استغلال جميع مصادر الطاقة والقدرات الحسابية لأجهزة الحواسيب المُصابة، مع خلق قيمة عملة افتراضية مشفرة(Monero) التي تسمح لهم بتحقيق الأرباح في افتراضية تامّة، وذلك أمام مرأى مُستخدميها ومن دون علمهم بما يجري في داخل حواسيبهم أو حتى اكتشاف أثاره، فحسب خبير أمن المعلومات(Robert Holmes) فإنّ هجمة(Adylkuzz) مسّت أكثر من مائتي ألف(200.000) جهاز حاسوب التي من خلالها استطاع القراصنة من كسب مبلغ أكثر من مليون دولار أمريكي(1.000.000 دولار).

للمزيد من المعلومات أنظر:

وعليه، فإنّ عمليات إصدار النّقود الرّقميّة الافتراضيّة مُستقبلاً من قِبَلِ الأفراد أو المؤسّسات غير المصرفية تؤثر بشكلٍ كبير على نُظُم تسوية المدفوعات فيما بين الدّول، وعدم التّحكّم في قِيَمِ الفوائد وأسعار صرف العملات وفقدان الثّقة لدى المستهلكين بالتّعامل بالعملات الماديّة الرّسميّة للدّول الخ...، ممّا يُثِير مخاوف تتطلّب ضرورة إخضاع مسألة إصدار العملات الافتراضيّة تحت إشراف الدّولة ورقابة المصارف المركزيّة[1]، التي تُسنِدها إلى مصارف ومؤسّسات ماليّة معتمدة(المصارف التّجاريّة أو المؤسّسات الماليّة غير المصرفيّة)، الشّيء الذي يمنح للدّولة السّيطرة على حجم النّقود الإلكترونيّة، وتجنّب أيّ اضطراب في السّياسة النّقديّة والاقتصاديّة والتّقليل من فُرص التّهرّب الضّريبي، وغسيل الأموال والقضاء على المشاكل القانونيّة التي يُمكِن أن تُثيرها العملات الافتراضيّة[2].

Sarah SERMONDADAZ, « Après WannaCry, voici le virus qui génère de la crypto-monnaie à votre insu », article de journal Sciences et Avenir, publié le 18/05/2017 à 13h03, sur: https://www.sciencesetavenir.frhigh-techinformatiqueapres-wannacry-voici-le-virus-qui-genere-de-la-crypto-monnaie-a-votre-insu_113056.html, consulté le 03/06/2017.

1) Directive 2009/110/CE du parlement européen et du conseil du 16 septembre 2009, […].
Art.2/1-3 : « 1- **Établissement de monnaie électronique**: une personne morale qui a obtenu, en vertu du titre II, un **agrément** l'autorisant à émettre de la monnaie électronique ;
3- **Émetteur de monnaie électronique**: les entités visées à l'article 1er, paragraphe 1, les établissements qui bénéficient de l'exemption au titre de l'article 1er, paragraphe 3, et les personnes morales qui bénéficient d'une exemption au titre de l'article 9. »
David BOUNIE, « Quelques incidences bancaires et monétaires des systèmes de paiement électronique », Revue Économique, 2001/7 Vol. 52, pp. 318, 319, 325- 326.

2) **محمود أحمد إبراهيم الشرقاوي**، "مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها"، (ص ص 37– 39)، **محمد إبراهيم محمود الشافعي**، "الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية"، (ص ص 167– 171)، بحثان مقدمان في مؤتمر "الأعمال المصرفية بين الشريعة والقانون" الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، المجلد الأول.
Michel AGLIETTA et Laurence SCIALOM, op.cit., pp. 18- 23.

الفرع الثاني

الشّيك الإلكتروني(Chèque électronique)

قامت المؤسّسات الماليّة بتطوير وتحويل آليات الدّفع من دعاماتها التّقليديّة إلى دعامات إلكترونيّة حديثة وجعلها تتواكب مع مستجدّات ومتطلّبات تطبيقات التّجارة الإلكترونيّة، في حين يعتبر الشّيك الإلكتروني في جوهره كبديل إلكتروني للشّيك الورقي وكالتزام قانوني بوفاء مبلغ مالي معيّن في مكان وتاريخ محدّدين لصالح فرد أو جهة معيّنة، إذ يحتوي بدوره على جميع البيانات الإلزاميّة الواردة في الشّيك الورقي[1]، كتسمية السّند(ذكر كلمة الشّيك) وتحديد المبلغ والمكان الذي يجب الدّفع فيه، وتاريخ إنشاء الشّيك، اسم السّاحب مع توقيعه، اسم المسحوب عليه، واسم المستفيد عند الاقتضاء لأن عدم ذكر اسم هذا الأخير(المستفيد) يجعل الشّيك صادرا لحامله ويكون قابلا للتّداول بمجرد التّسليم أو الإطّلاع عليه، وعلى العموم يمكن تعريف الشّيك الإلكتروني على أنّه: "**ورقة مصرفية إلكترونية مكتوبة وفقا للأوضاع التي استقر عليها القانون تحمل على متنها، أمرا من جانب السّاحب(Tireur) إلى المسحوب عليه(Tiré) الذي يكون في هيئة مصرف أو مؤسّسة ماليّة مؤهّلة قانونا، لدفع مبلغ محدّد لشخص يدعى المستفيد(Bénéficiaire) أو حامل الشّيك(Porteur)**".

انطلاقا من ذلك، يعتبر الشّيك الإلكتروني كأداة وفاء بالدّيون تسير مسار النّقود في التّعامل ولا تؤدّي وظيفة الائتمان، حيث يستعمل إمّا لسحب مبالغ ماليّة مودعة في مصرف أو الوفاء بدين على عاتق ذمّة السّاحب أو لكي يُضاف إلى رصيد حساب جاري، وعليه تُعد الشّيكات الإلكترونيّة كأدوات مفضّلة لدى أطراف معاملات التّجارة الإلكترونيّة وبالخصوص المستهلكين الذين وصولوا إلى سقف الائتمان المتاح لهم، أو لا يستحوذون على تقنيات

---

[1] **مصطفى كمال طه، وائل أنور بندق**، مرجع سابق، ص ص 350، 351.

محمود محمد أبو فروة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص 50.

بشير العلاق، التسويق الإلكتروني، مرجع سابق، ص ص 148، 149.

الدّفع الإلكتروني الأخرى كبطاقات الائتمان الخ...، كما أنها تعتبر الأكثر استعمالا من جهة المصارف والمؤسّسات الماليّة، وذلك بالنّظر إلى سهولة وبساطة تقنياتها وانخفاض تكاليف معالجة الشّيكات الإلكترونيّة بالمقارنة مع التّكاليف النّاجمة عن معالجة الشّيكات الورقيّة[1].

تستوجب تقنية الدّفع بالشّيك الإلكتروني على المصارف أو المؤسّسات الماليّة أو المتاجر الاستعانة بمزوّد خدمة المعالجة الآلية للشّيكات الإلكترونيّة، الذي يستعين بدوره بإحدى الشّبكات الخاصّة التي تتيح خدمات المقاصة الإلكترونيّة فيما بين المصارف، من أكثرها استخداما نجد شبكة مركز المقاصة الآلية(Automated Clearing House(ACH))، المستخدمة من طرف المصارف الأمريكيّة لغرض تسوية وتوثيق الشّيكات الإلكترونيّة المتداولة، لكونها تتيح لأطراف التّعامل الإلكتروني مستويات عالية من الثّقة والأمان وتُقلّل من مخاطر قبول الشّيكات بأنواعها[2].

ففي حالة ما إذا قام العميل أو المستهلك بزيارة المَوقِع الإلكتروني الخاص بالتّاجر ويطلب شراء بعض المنتجات المروّجة فيه، فسيتّم تحويله مباشرة بطريقة أوتوماتيكيّة إلى مزوّد خدمة الشّيكات الإلكترونيّة الذي تحصّل مسبقا على المعلومات الخاصّة بإجمالي قيمة الصّفقة المطلوب سِدادها واسم العميل وعنوانه، التي يقوم بعرضها في نموذج الشّيك المُبيّن على الشّاشة، من خلاله(النّموذج) يقوم العميل بإضافة رقم هويّته وحسابه والبيانات المتعلّقة بالمصرف، وبعدها يقوم مزوّد الخدمة بالاتصال بمصرف العميل لغرض التّأكد من سلامة

---

[1] **نبيل صلاح محمود العربي**، "الشيك الإلكتروني والنقود الرقمية(دراسة مقارنة)"، المجلّد الأول، بحث مقدم في مؤتمر "الأعمال المصرفية بين الشريعة والقانون" الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، ص ص 67– 69.

محمود محمد أبو فروة، مرجع سابق، ص 50.

[2] **أحمد سفر**، مرجع سابق، ص ص 43– 45.

وصّحة البيانات المتضمّنة في الشّيك الإلكتروني، وضمان التّاجر بتوفّر الرّصيد عند حلول وقت الوفاء به وذلك قبل إيداعه لدى مركز التّسوية الآلية(مثل الشّيك الورقي) [1].

إنّ التّطوّرات التّكنولوجيّة الحديثة التي شهدتها مجالات الثّورة الرّقميّة وتزايد استخدام تقنيات الدّفع الإلكترونيّة الجديدة، دفع بالمشّرع الجزائري إلى إجراء بعض التّعديلات في أحكام التّقنين التّجاري بغية منه التّأقلم ومسايرة التّطوّرات التّكنولوجيّة المستقبليّة في مجالات المعاملات التّجاريّة والمصرفيّة، من خلال تجريد التّبادل المادّي للأوراق التّجاريّة والسّماح بالتّعامل بها على أيّة وسيلة أو دعامة إلكترونيّة حديثة محدّدة بموجب التّشريع والتّنظيم المعمول بهما، حيث نص بموجب المواد 3/414 و3/467 و2/502 من التّقنين التّجاري، على إمكانية التّعامل بإحدى الأوراق التّجاريّة كالسّفتجة أو السّند لأمر أو الشّيك، بأيّة وسيلة تبادل إلكترونيّة مُعترف بها بموجب التّشريع والتّنظيم المعمول بهما[2].

---

[1] **الياس ناصيف**، العقود الدولية: العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص ص 168، 169.

[2] أمر رقم 75–59 مؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، المعدل والمتمم بموجب القانون رقم 05–02 المؤرخ في 06 فيفري 2005، ج ر عدد 11 الصادر في 09 فيفري 2005.

تنص **المادة 414** على ما يلي: "يجب على حامل السفتجة الواجبة الدفع في يوم محدد أو في أجل ما من تاريخ معين أو بعد الإطلاع، أن يقدم السفتجة للدفع إمّا في يوم وجوب دفعها أو في أحد يومي العمل المواليين له.

ويعتبر التقديم المادي للسفتجة لغرفة المقاصة بمثابة تقديم للوفاء.

يمكن أن يتم هذا التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما."

تنص **المادة 3/467** على ما يلي:" تطبق على السند لأمر الأحكام المتعلقة بالسفتجة فيما لا يتعارض مع طبيعته وذلك في الأحوال الآتية: – التظهير(المادة من 396 إلى 402)؛ – الاستحقاق(المادة من 410 إلى 413)؛

– **الوفاء**(المادة من **414** إلى 425)؛ [...]."

تنص **المادة 502** على ما يلي:" يعد التقديم المادي للشيك إلى إحدى غرف المقاصة بمثابة تقديم للوفاء.

يمكن أن يتم هذا التقديم أيضا، بأيّة وسيلة تبادل إلكترونية مُحدّدة في التشريع والتنظيم المعمول بهما."

الفرع الثالث

البطاقات الذّكيّة(Cartes à puces)

يُعْرَفُ عن البطاقة الذّكيّة(Smart Card) أو(Carte à puce) على أنّها بطاقة بلاستيكية أو ورقيّة(Voire en papier ou en carton) تحتوي على شريحة ذاكرة إلكترونيّة (Circuit intégré) أو(Puce) تسمح بتخزين بيانات ووحدات إلكترونيّة مع استرجاعها بطريقة منتظمة عند الحاجة إليها، حيث تُزوّد(La puce) بمُعالِج تحكُّم دقيق مُدمج(Microprocesseur)[1] يُشبه من النّاحية التّقنيّة الشّرائح الموجودة على مستوى أجهزة الحاسوب، مُزوَّد ببرنامج صغير مُتعلّق بنظام تشغيل(Système d'exploitation pour carte à puce) يسمح بالتّحكُّم في البطاقة مع إدارة ملفات البيانات وتنفيذ العمليات الحسابيّة الخاصّة كالتّشفير والتّوقيعات الرّقميّة والتّفاعل بذكاء مع أجهزة القراءة في مختلف التّطبيقات.

ويعود ظهور البطاقة الذّكيّة لأوّل مرّة إلى عام 1974 أين اكتشفها العَالِم الفرنسي رولاند مورينو(Roland MORENO) الذي قام بتسجيل براءة اختراعه في نفس السّنة، في حين أُستخدمت هذه البطاقة(Smart Card) أكثر في عام 1983 في قطاع الاتّصالات(Télécarte) عبر أجهزة الهاتف العموميّة، غير أنّه انتشرت فيما بعد استخداماتها في التّسعينيات، وذلك تزامنا مع ظهور وتطوّر البطاقات الذّكيّة التي تحتوي على شريحة الخّط(Subscriber Identity Module(SIM)) المُستعملة في الهواتف المحمولة الشّائعة آنذاك في أوروبا، التي تسمح بتحديد هويّة صاحبها وتلقّي المكالمات الهاتفيّة والرّسائل

---

[1] **Microprocesseur** en informatique: Circuit intégré fait d'une plaque de silicium sur laquelle sont gravés des transistors et capable de réaliser des opérations arithmétiques et logiques. Synonyme: puce. https://www.wiképidia.fr ou https://www.larousse.fr/, consultés le 10/02/2016.
Aude PLATEAUX, « Solutions opérationnelles d'une transaction électronique sécurisée et respectueuse de la vie privée », Thèse de Doctorat de l'Université de Caen Basse-Normandie (école doctorale SIMEM), spécialité : Informatique et Applications, 2013, pp. 48- 50.

وشحن قِيَمْ أو وحدات ماليّة معيّنة وتخزين المعلومات الشّخصيّة للمستخدم وتحويل الوحدات الرّقميّة فيما بين الأرصدة، مع القيام بتعبئة الرّصيد وبعمليات الاتّصالات عبر الإنترنت[1].

كما شهدت تلك الفترة وبالخصوص في عام 1994 ظهور معايير جديدة لمؤسّسات ماليّة عالميّة(Europay, Master Card et Visa(EMV)) لاستخدام بطاقات الإئتمان، التي زوّدتها بتطبيقات تكنولوجيّة حديثة كالتّجاوب مع تقنيات مرافق المفاتيح العموميّة(PKI) وتزويدها بالآليات المؤمّنة لإحداث وفحص التّواقيع الإلكترونيّة الموصوفة وحفظ الشّهادات الإلكترونيّة، مع تمكين حامل البطاقة الذّكيّة من إجراء عمليات الدّفع والشّراء في أيّ منطقة من العالم عبر الإنترنت بكلّ ثقة وأمان[2].

انطلاقا من ذلك، تعتبر البطاقة الذّكيّة(Carte à puce) كمحفظة نقود إلكترونيّة (Porte monnaie électronique)[3]، حيث تتعدّد مجالات استخدامها بحسب الخدمات المتاحة للعملاء أو المستهلكين، كالتّطبيقات المتعلّقة بالتّعريف بهويّة الأشخاص (Passeport et carte d'identité biométriques, badge d'accès aux bâtiment, etc.)، وكذا في قطاع الصّحة(Carte de santé) والضّمان الاجتماعي(Carte d'assurance maladie) والاتّصالات(Carte SIM)، والعمليات الماليّة والمصرفيّة(Carte bancaire) الخ...، وبالتّالي فإنّ كلّ نوع من البطاقات المصرفيّة الذّكيّة(بطاقات السّحب والدّفع على الحساب، وبطاقات الصّراف الآلي ونهائيات الدّفع(TPE) وبطاقات الائتمان الذّكيّة الخ...)، يتميّز بصيغة تعاقدية مستقلة تتناسب مع وظيفتها.

---

1) **Laetitia CHAIX**, « Le paiement mobile : modèles économiques et régulation financière », Revue d'Économie financière, 2013/4 (N° 112), pp. 278-280, 293.

2) **Étienne WÉRY,** Facture, Monnaie et paiement électroniques, édition du Juris-Classeur, Litec, France, 2003, pp. 61- 64.

Arnaud-F. FAUSSE, La signature électronique : transaction et confiance sur Internet, DUNOD, Paris, 2001, pp. 203- 207.

3) **شريف محمد غنام**، "محفظة النقود الرقمية(رؤية مستقبلية)"، بحث مقدم في مؤتمر "الأعمال المصرفية بين الشريعة والقانون"، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، المجلد الأول، ص ص 110– 113.

تجدر الإشارة في هذا السيّاق، أنّ المشّرع الجزائري قد سمح بموجب أحكام المادتين 543 مكرر23، و543 مكرر24، من التّقنين التّجاري، بإمكانية التّعامل تجاريا ببطاقات الدّفع والسَّحْب الإلكترونيّة التي تُصدِرها المصارف والمؤسّسات الماليّة المؤهّلة قانونا لأصحابها، حيث يُمكِن لمالك البطاقة المصرفيّة القيام بعمليات سحب أو تحويل الأموال، ولا يجوز له الرّجوع عن عملية الدّفع في حالة تواجد أمر أو الالتزام بالدّفع، ولا يمكن الاعتراض على عملية الدّفع إلاّ في حالة ضياع أو سرقة البطاقة المُصَرَّحِ بها قانونا أو تواجد تسوية قضائيّة أو إفلاس المستفيد، بينما تُتيح "بطاقة السّحب" لصاحبها سحب الأموال فقط[1].

لذا ألزم المشّرع الجزائري بموجب أحكام المادة 111 من القانون رقم 17–11 المؤرخ في 27 ديسمبر 2017 المتضمّن لقانون الماليّة لسنة 2018، كلّ مُتعامِل اقتصادي يُقدِّم سِلَعاً أو خدمات للمستهلكين أن تكون لديه وسائل دفع إلكتروني، تسمح للمستهلكين بدفع ثمن مُشترياتهم باستعمال بطاقات الدّفع الإلكتروني بناء على طلبهم، حيث يتعيّن على المتعاملين الاقتصاديين الامتثال لأحكام هذه المادة(111) في أجل أقصاه سنة واحدة(01) ابتداء من تاريخ نشر قانون الماليّة لسنة 2018 في الجريدة الرّسميّة أي (في 28 ديسمبر 2017)، وكل مخالفة له يعاقب عليها بغرامة قَدْرُهَا خمسون ألف دينار(50.000 دج)[2].

---

[1] أمر رقم 75–59 مؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، معدل ومتمم.

تنص المادة 543 مكرر23 على ما يلي:" تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال. تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب الأموال."

تنص المادة 543 مكرر24 على ما يلي:" الأمر أو الالتزام بالدفع المعطى بموجب بطاقة الدفع غير قابل للرجوع فيه، ولا يمكن الاعتراض على الدفع إلاّ في حالة ضياع أو سرقة البطاقة المصرح بهما قانونا، أو تسوية قضائية أو إفلاس المستفيد."

[2] تنص المادة 111 من القانون رقم 17–11 المؤرخ في 27 ديسمبر 2017، الذي يتضمن قانون المالية لسنة 2018، على ما يلي:" يتعين على كلّ متعامل اقتصادي بمفهوم القانون رقم 04–02 المؤرخ في 23 يونيو سنة 2004، الذي يحدد القواعد المطبقة على الممارسات التجارية، المعدل والمتمم، يقدم سلعا و/أو خدمات للمستهلكين، أن يضع في متناولهم وسائل دفع إلكتروني تسمح لهم بدفع مشترياتهم باستعمال بطاقات الدفع الإلكتروني، بناء على طلبهم.

تعتبر بطاقة الائتمان الذّكيّة وسيلة دفع إلكتروني حديثة تقوم على فكرتي "الوفاء والائتمان" في نفس الوقت، حيث تُصْدَرُ بمعرفة مؤسّسة ماليّة أو مصرف باسم حاملها التي تُعْطِي له الحق في الحصول على تسهيل ائتماني، للوفاء بقيمة مشترياته من سلع أو خدمات لدى أصحاب المواقع التّجاريّة الإلكترونية(التّجار)، الذين تربطهم علاقة عقديّة خاصّة بالمُصدِر(المؤسّسة الماليّة أو المصرف)[1] حول قبول بطاقات الائتمان الذّكيّة كوسيلة وفاء عبر الإنترنت، وبالتّالي فإنّ بطاقة الائتمان الذّكيّة تتشابه من حيث الحجم والشّكل مع البطاقة البلاستيكيّة الممغنطة(Carte magnétique)، إلاّ أنّها تختلف مع هذه الأخيرة من حيث التّقنيات التّكنولوجيّة الحديثة المستخدمة في تسجيل واستعادة المعلومات المخزّنة، حيث تحتوي بطاقة الائتمان الذّكيّة على شريحة ذاكرة إلكترونيّة(Puce) تُشبه قرص صلب صغير محمي وفقا لسمات أمنيّة اختياريّة، حيث تسمح بتخزين كميّة هائلة من البيانات الإلكترونيّة واسترجاعها بطريقة آلية عند الضّرورة، وكذا شحن وتخزين وحدات إلكترونيّة لاستخدامها في عمليات الوفاء بقيمة المشتريات من سلع وخدمات.

لكي تتّم عملية الدّفع باستعمال البطاقة المصرفيّة الذّكيّة، يجب أن تربط بين مُصدِر البطاقة وحاملها علاقة عقديّة مُلزمة للجانبين(Contrat synallagmatique)، من خلالها يوافق المُصدر(المصرف) على منح طالب البطاقة(الحامل) تسهيل ائتماني، بمبلغ مُعيّن محدّد المدّة يستخدمه للوفاء بمشترياته لدى التّجار الذين قبلوا الوفاء بالبطاقة عبر مواقعهم التّجاريّة، كما يجب على المُصدِر أن تكون بَيْنَهُ وبين صاحب المتجر الافتراضي علاقة

كل إخلال بهذا الالتزام يشكل مخالفة لأحكام هذه المادة ويعاقب عليها بغرامة قدرها خمسون ألف دينار(50,000 دج).[...].

يتعين على المتعاملين الاقتصاديين أن يمتثلوا لأحكام هذه المادة في أجل أقصاه سنة واحدة(01)، ابتداء من تاريخ نشر هذا الحكم في الجريدة الرسمية."

[1] **سعد محمد سعد**، "المسائل القانونية التي تثيرها العلاقة الناشئة عن استخدام بطاقة الائتمان بين الجهة مصدرة البطاقة والتاجر"، بحث مقدم إلى مؤتمر "الأعمال المصرفية بين الشريعة والقانون"، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الثاني، ص ص 801، 805.

عقديّة(Contrat de fournisseur)، يلتزم من خلالها التّاجر بقبول البطاقة في الوفاء عن بُعد، وذلك مُقابل إلتزام مُصدِر البطاقة بإتاحة جميع المعدّات والبرمجيات الضّروريّة لإجراء الصّفقات وضمان الوفاء للتّاجر بقيمة مشتريات حامِل البطاقة المصرفيّة، مع إخطاره(التّاجر) بصفة دوريّة ومنتظمة بجميع البطاقات المصرفية الذّكيّة المُنتهيّة صَلاحيتُها أو المُلغَاة أو المَسروقَة أو الضَّائعَة وذلك لتفادي الاستخدام غير المشروع لها[1].

إنّ بطاقة الإئتمان الذّكية تُحقّق الكثير من المزايا لأطراف التّعامل الإلكتروني(مُصدِر البطاقة، حامِلها، التّاجر)، إذ يتم تداولها في جميع أنحاء العالم ويتم قبولها كأداة وفاء وائتمان في نفس الوقت، باعتبارها وسيلة مرنة تُسهِّل للعميل عمليات سِداد تكاليف السّفر والسّياحة والصّحة وإتمام الصّفقات التّجارية في الخارج الخ...، وذلك من دُونِ المُخاطرة بحمل النّقود المعدنيّة أو الأوراق الماليّة مَعَهُ عبر الحدود، إذْ يُمْكِنُ للمُستهلك أن يقومَ عبر الإنترنت في ظرف وجيز بشراء ودفع وطبع تذكرة السّفر عبر المنصّة الإلكترونيّة لإحدى شركات الطّيران، مع كِراء سيّارة لَهُ مُسبقاً عِنْدَ الوصول إلى مطار بلد النُّزول، وحجز شقّة عبر المنصّة الإلكترونيّة لأحد فنادق بلد الوصول، وكذا يقوم بدفع مُستحقات الخدمات المُتعلّقة بفاتورة الاتّصالات، الغاز والكهرباء، الماء، النّقل الخ...، من دون التَّنقُّل إلى عين المكان أو بذل أيّ جهد أخر، حيث تُوَفِّرُ هذه البطاقة لحاملها عنصري الثّقة والأمان كضمانات رئيسيّة في معاملاته الإلكترونيّة، ففي حال ضياعها أو الشّك في سرقة المفتاح الخاص لحاملها، يجب على هذا الأخير إخطار مُصدِر البطاقة لإيقاف التّعامل بها فوراً[2].

---

1) **Etienne WÉRY**, « Comment rédiger en pratique un contrat de commerce électronique? », op.cit., pp. 32- 35.
Chiheb GHAZOUANI, op.cit., pp. 150, 151, 152.

2) **عصام حنفي محمود موسي**، "الطبيعة القانونية لبطاقات الائتمان"، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الثاني، ص ص 859–861.

وعليه، فإنّ البطاقة المصرفيّة الذّكيّة تُصْدَرُ أصلاً من طرف إحدى المؤسّسات الماليّة العالميّة المُحتكِرة لَهَا(Master Card et Visa, etc.)، أو من طرف إحدى المصارف الأعضاء في هذه المؤسّسات، وكاستثناء يمكن لأيّ مصرف أو هيئة ماليّة استثماريّة أخرى أن تقوم بإصدار هذا النّوع من البطاقات، باعتبارهم كوسطاء أو وكلاء بالعمولة لفائدة المؤسّسة المَالِكة للبطاقة شريطة الحصول على إذن مُسبق من الشّركة المُحتكرة، حيث يتحقّق ذلك من النّاحية العمليّة بموجب إتفاقيات إصدار البطاقة المصرفيّة الذّكيّة[1].

الفرع الرابع
الدّفع عن طريق الهاتف الذّكي

تعتبر تقنيّة الدّفع عن طريق الهاتف الذّكي من بين الوسائل الإلكترونيّة الحديثة المستخدمة في دفع ثمن مختلف السّلع والخدمات، وكبديل لطرق الدّفع عن طريق النّقود أو الشّيكات أو بطاقات الائتمان، حيث يمكن تمييز ثلاثة نماذج لتقنيات الدّفع بواسطة الهاتف الذّكي: الدّفع عن بُعد عبر الإنترنت(Paiement à distance) **(أولا)**، والدّفع عن طريق الاتّصال القريب(Paiements de proximité) **(ثانيا)**، وتحويل الأموال من هاتف ذكّي إلى هاتف ذكّي آخر(Transfert d'argent de mobile à mobile) **(ثالثا)**.

أولا)– الدّفع عن بُعد عبر الإنترنت(Paiement à distance):

تعتمد هذه التّقنيّة على تطبيقات التّسوّق والشّراء والدّفع الخاصّة بالهواتف الذّكيّة(AliExpress, AmazonShopping, eBay, Souq, Alibaba.com, Jumia, etc.)، التي تتيح للمستهلك سهولة وسرعة البحث عن المنتجات والمقارنة فيما بين الأسعار، فبمجرّد

---

[1] **موسى رزيق**، "رضا حامل البطاقة الائتمانية بالعقد والحماية التي يقررها المشرع له، دراسة في ضوء تشريع المعاملات المدنية الاتحادي"، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الثالث، ص ص 1040– 1042.

دخوله إلى إحدى هذه التّطبيقات، يقوم المستهلك بالتّسجيل ثم يكتب اسم السّلعة المطلوبة في خانة البحث، وبعدها يَتَّبِعُ الخطوات المشروحة بتلك المواقِع لإتمام عملية الشّراء والدّفع، بشرط توافر الرّصيد الكافي لتلك العمليّة التي من خلالها يتّم خصم رصيد التّعبئة أو حساب بطاقته المصرفيّة الذّكيّة، ولضمان الاستخدام المؤمّن لهذه التّطبيقات عبر شبكة الإنترنت يجب على المستهلك أن يقوم بإدماج رقم هاتفه الذّكي ببطاقته الالكترونيّة المصرفيّة لدى الهيئة المُصدِرة لها، وذلك لتسهيل عمليات الشّراء والدّفع في آن واحد، من دون إرسال البيانات السّريّة الخاصّة ببطاقته المصرفيّة الإلكترونيّة إلى الغير[1].

وعليه، فإنّ معظم أنظمة الدّفع الإلكتروني لا تشترط على المستهلك الإلكتروني، أثناء قيامه بالدفع عبر الإنترنت تقديم البيانات السّريّة المتعلّقة ببطاقة الائتمان، كما هو الحال مع شركة(Buyster) التي تشترط فقط رقم الهاتف مع الرّقم السّري للمستهلك، أو شركة(PayPal) التي تشترط البريد الإلكتروني مع الرّقم السّري للمستهلك من دون إرسال بيانات بطاقته المصرفيّة للمستفيدين[2]، كما أنّ بعض المتاجر الافتراضيّة لا تقوم مباشرة بشحن جميع السّلع إلى دول العالم، فمن الأفضل على المستهلك الاستعانة ببعض شركات الشّحن الوسيطة (Shop & Ship, MyUS, DHL ACT, FedEx Mobil, UPS Mobil, USPS Mobil, etc.) التي تقوم بإيصال السّلعة إلى أي مكان في العالم، حيث تتشابه هذه الشّركات في مبدأ عملها، لكنّها تختلف في أسعار الخدمة وسرعة التّوصيل[3].

---

[1] **Thibault VERBIEST, Etienne WÉRY**, « Commerce électronique par téléphonie mobile (m-commerce): un cadre juridique mal défini », Recueil DALLOZ, n° 41, 2004, pp. 03, 04, 05, 06.

[2] للمزيد من المعلومات حول الخدمات التي تتيحها هذه الشركات، أنظر المواقع الإلكترونية التالية:
https://www.buyster.fr/ ou https://www.paypal.com/ (consultés le 20/03/2018)
Voir aussi : **Romain V.GOLA,** op.cit., pp. 343- 346.

[3] للتعرف أكثر على الخدمات التي تتيحها هذه الشركات، أنظر المواقع الإلكترونية التالية:
https://www.myus.com/ ou https://www.dhl.com/ ou https://www.shopandShip.com/ ou https://www.fedex.com/ ou https://www.ups.com/ ou https://www.usps.com/

ثانيا)– الدّفع عن طريق الاتّصال القريب(Paiements de proximité):

يُطلق على هذه التّقنيّة كذلك الاتّصال القريب المدى أو الدّفع اللاّتلامسي (Paiement sans contact) التي تعتمد على تكنولوجيا(Near Field Communication (NFC)) أو (La communication en champ proche (CCP))، التي ماهيّة إلاّ رقاقة يتّم إدماجها على بطاقة(SIM) التي من خلالها يتم نقل وتحويل كميّة صغيرة نسبيا من البيانات عبر مسافات قصيرة لا تتعدّى بضعة سنتيمترات[1]، إذ يكتفي أي مستهلك في المحلاّت التّجاريّة برفع هاتفه الذّكي وتقريبه إلى أحد نقاط البيع الطّرفية(طاولة حساب، قارئ بطاقة مصرفيّة، أجهزة الدّفع) من دون لمسها، ويتّم الدّفع فوري من خلال السّحب هاتفيا من حساب المستهلك المصرفي من دون الحاجة لإدخال رقم سرّي أو التّوقيع إلكترونيا، حيث لا يمكن أن تتجاوز قيمة المبلغ المسحوب الحدّ الأقصى المسموح به، فإذا تجاوزت قيمة المشتريات هذا الحدّ، يتعيّن على المُستهلك وضع الرّقم السّري على هاتفه الذّكي مع تقريب هذا الأخير مرّة أخرى نحو نقطة البيع الطّرفية لدفع مستحقات الشّراء[2].

بالإضافة إلى تقنيّة(NFC)، توجد تقنيات تكنولوجيا أخرى مُستخدمة في الدّفع اللاّتلامسي عن طريق الهاتف الذّكي، على غرار تقنيّة(iBeacon) التي استحدثتها شركة "آبل" للهواتف الذّكيّة تعتمد على تكنولوجيا البلوتوث(Bluetooth Low Energy (BLE)) التي تسمح بنقل وتحويل البيانات على مسافة 50 متر(عكس تقنيّة(NFC))، كما توجد كذلك تقنيّة الرّقم السّري المخفي(Code QR(Quick Response))، التي تُتيح للمستهلك إمكانية إجراء عملية الدّفع عن طريق تصوير الرّقم السّري بهاتفه الذّكي الذي يقوم مباشرة بفكّ تشفيره(Code QR) مع إتمام عملية تحويل المبلغ من حساب المستهلك نحو حساب التّاجر،

---

1) **Jean-Marc DÉCAUDIN, Jacques DIGOUT**, e-Publicité(Les fondamentaux), Dunod, France, 2011, p. 196.

2) **Romain MEGEMONT**, « Paiement mobile sur smartphone : présentation, fonctionnement et sécurité », article publié sur FrAndroid , le 28-04-2018. https://www.frandroid.com/android/application/500871_ Paiement-mobile-sur-smartphone-présentation-fonctionnement-sécurité, consulté le 01/05/2018.

في حين تتوافر هذه التّقنيّة على مستوى جميع الهواتف الذّكيّة[1]، حيث تتنافس الشّركات من كافة الاختصاصات على تطوير هذه التّقنيات بما فيها المصارف وشركات الهاتف النّقال ومواقع الدّفع الإلكتروني عبر الإنترنت، كشركة "غوغل" التي طوّرت نظام تشغيل أندرويد(Android)، وشركة "آبل(Apple)" التي طوّرت نظام تشغيل(IOS)، الخ...[2].

ثالثا)– تحويل الأموال فيما بين الهواتف الذّكيّة (Transfert de mobile à mobile):

انتشرت في الآونة الأخيرة تطبيقات الهواتف الذّكيّة الخاصّة بتحويل الأموال عبر الإنترنت من حساب إلى حساب آخر(مصرفي أو بريدي)، من دون التّنقّل إلى المراكز المعنيّة للدّفع أو سحب الأموال، حيث تسمح للمستخدمين بتحويل الأموال عبر الإنترنت فيما بين حساباتهم مع دفع فواتير الغاز والكهرباء والماء أو اشتراكات الهاتف أو الإنترنت الخ...، حيث قامت مؤسّسة بريد الجزائر بإصدار تطبيق(BaridiMob)، موجّه لأصحاب البطاقات الذّهبيّة وأجهزة الهواتف الذّكيّة(Smartphone) التي تعمل بنظام تشغيل(Android) أو (أيفون بنظام(IOS) قريبا)[3]، الذي يسمح لهم بإجراء المعاملات التي تتيحها البطاقة كإرسال واستقبال الأموال والاطّلاع على الرّصيد، شحن الرّصيد الهاتفي ودفع فواتير الماء والغاز والكهرباء والهاتف والإنترنت، الخ...

---

1) **Christophe COQUIS**, « NFC, QR Codes, iBeacon, RI : tout savoir sur les technologies sans contact », article publié sur Softonic International S.A, le 29/09/2014. https://www.fr.softonic.com/articles/nfc-qr-codes-ibeacon-ri-technologies-sans-contact, consulté le 25/02/2016.

2) **Laetitia Chaix**, « Le paiement mobile : perspectives économiques, modèles d'affaire et enjeux concurrentiels », Thèse de Doctorat en Sciences Économiques, Université Nice Sophia Antipolis, 2013, pp. 51, 52, 56-58.

أنظر كذلك: **حوالف عبد الصمد**، "النظام القانوني لوسائل الدفع الإلكتروني"، رسالة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد– تلمسان، 2014، ص ص 297– 301.

3) للتعرف على شروط وإجراءات الانضمام والتسجيل واستعمال تطبيق "بريدي موب" أنظر النموذج المتوافر في الموقع الإلكتروني التالي: https://www.edcarte.poste.dz/fr/mode_operatoire.html (تم الاطّلاع عليه في 2018/03/14.)
للإطلاع على القواعد العامة لاستعمال تطبيق "بريدي موب"، أنظر الموقع الإلكتروني التالي: https://www.epay.post.dz/mobilebank/service/policy?lang=fr (تم الاطّلاع عليه في 2018/03/14.)

خلاصة الفصل الثاني

من خلال ما سبق، نصل إلى أنّ الثّورة الرّقميّة دفعت بمختلف المؤسّسات المصرفيّة العالميّة إلى إعادة النّظر في سياساتها المصرفيّة وانتهاج هندسة ماليّة رقميّة حديثة، تتماشى مع مستجدّات الخيارات الاقتصاديّة التي فرضتها تطبيقات الاقتصاد الرّقمي في مجالات الخدمات المصرفيّة، حيث تنامت تطبيقات المصارف الإلكترونيّة التي تزايد دورها بِفِعْلِ تزايد حركيّة التّدفقات النّقديّة والماليّة في مجالات التّجارة الإلكترونيّة، كما أنّ مفهوم المصارف الإلكترونيّة جاء كمسار جديد ضمن تطبيقات التّجارة الإلكترونيّة، التي أثّرت على السّياسات المصرفيّة وساهمت في توفير السّيولة وتطوير تقنيات الدّفع الإلكتروني التي تعتمد على نُظم التّسوية والمقاصة الإلكترونيّة، حيث تّم تجريد تقنيات الدّفع التّقليديّة من مادياتها وتحويلها إلى دعامات إلكترونيّة، نظرا لارتفاع تكلفة تداول الشّيكات وأوامر الدّفع والتّحويلات الماليّة الخ...، مع طُولِ فترة عمليات التّسوية والمقاصة فيما بين المصارف.

وعليه، تعتبر العملات الافتراضيّة المشّفرة(Crypto- monnaies) من بين تقنيات الدّفع الإلكتروني الحديثة، التي يُعوّل عليها أطراف التّعامل الإلكتروني في إجراء المعاملات التّجارية والماليّة عبر الإنترنت، وذلك باعتبارها كعملات الكترونيّة حرّة لا تُشرف الدّول أو المصارف المركزيّة على عمليات إحداثها، بل تُنشئ عبر الإنترنت عن طريق مجموعة من الأشخاص معروفة أو مجهولة الهويّة، حيث تسمح بتبادل الأموال فيما بين الأرصدة بسرعة وسهولة من دون الاستعانة على أيّ وسيط أو إجراء المقاصة مع استبدالها بالعملات الماديّة الرّسميّة للدّول، وبالتّالي تفادي الرّسوم المفروضة على عمليات التّحويل ممّا يشجّع بالمقابل أنشطة التّهرّب الضّريبي وغسيل الأموال والغّش التّجاري والمُضاربة على حساب العملات الرّسميّة للدّول الخ...، وفي غياب الإطار القانوني المُنّظم لهذه العملات، اكتفت الدّول بتوجيه تحذيرات للمستهلكين من مخاطر وعواقب التّعامل بهذه العملات، التي تستوجب إرساء آليات قانونيّة وتقنيّة، لرقابة عمليات تداولها وتفادي الأنشطة غير المشروعة.

تُشّكل شبكة الإنترنت الوسط الملائم الذي تنمو وتسكن فيه الفيروسات ومختلف البرامج المعلوماتية الضّارة، التي تُهيّئ البيئة الخصبة للعصابات والمجرمين لارتكاب مختلف الجرائم المعادية للقوانين والأعراف الاجتماعيّة والثّقافيّة السّائدة، والتي تُثير العديد من المسائل المتعلّقة بتحديد هويّة الأشخاص وضمان سلامة وسرية التّبادل الإلكتروني مع عدم إنكاره، فقد تتعلّق هذه الجرائم بقرصنة مواقع التّجارة الإلكترونيّة، وما تُثيره من نِزاعات قانونيّة مع أصحاب حقوق الملكيّة الفكريّة، كنسخ برمجيات الحاسوب أو قواعد البيانات وتقليد الأسماء التّجاريّة والاستيلاء على العلامات التّجاريّة أو الخدمة(Cybersquattage)، حيث يمكن لأيّ شخص أن يقوم بتسجيل علامة تّجاريّة أو صناعيّة محميّة، كاسم نطاق على شبكة الإنترنت لغرض الإضرار بمالكها، أو إعادة بيع اسم النّطاق إلى هذا المالك مرّة أخرى بثمنٍ غالي، أو لأحد منافسيه قصد منع المالك من تسجيل العنوان الإلكتروني.

كما تُعتبر البرمجيات الخبيثة حاليا (Chevaux de Troie, Les Vers, Bombes logiques/ à retardement, etc.) من أصعب التّهديدات التي تتعرّض لها مواقع التّجارة الإلكترونيّة، التي تتّخذ صُوَر عديدة حسب الأهداف المُسّطرة لها، حيث تتميّز هذه البرامج على أنّها مُعَطِّلَةٌ للخدمات أو مهدِّمة للبرامج والأجهزة، فبِمجرّدِ تثبيتها على أجهزة الحاسوب تصعب جدًّا عملية إزالتها وتُسبّب أذَى غير قابل للإصلاح يتطلّب في بعض الأحيان إعادة تهيئة القُرص الصّلب المثبّت فيه نظام التّشغيل، أو حتى استبداله بقرص صُلب جديد.

إنّ تكريس الثّقة والأمان في بيئة الإنترنت بصورة أكيدة وشاملة ومضمونة بصفة نهائيّة لا يتحقّق من النّاحية التّقنيّة والعمليّة، ذلك لأنّ لمواقع التّجارة الإلكترونيّة مَواطِن ضُعف خاصّة بها تجعل من البيانات الإلكترونيّة المتداولة عَبرها، عُرضَةً لمختلف التّهديدات الرّئيسيّة التي تختلف باختلاف مصادرها، وتعدّد الدّوافع والمنهجيّات التي يَرْصُدُهَا القراصنة الذين يستحوذون على معلومات حسّاسة تجعل مُهمّة اختراق أنظمة الحماية أكثر سهولة من الدِّفاعِ عَنْهَا، حيث تفرض على أرض الواقع حتميّة إرساء سياسة أمنيّة موثوقة، وإجراءات تشريعيّة وتنظيميّة لحماية مواقع التّجارة الإلكترونيّة من مختلف التّهديدات.

البـــاب الـثانـــي

الـحمـــايــة التّقنيّـة والـقانونيّــة

لـمواقـع الـتّجـارة الإلـكترونيّة

تُشّكل شبكة الإنترنت ميدانا حديثا لإجراء الحروب الإلكترونيّة، تتسابق من خلالها عن بُعد الجّيوش العصريّة ومراكز البحوث، لتطوير تقنيات وأساليب الدّفاع الإلكترونيّة العالية المستوى لتفادي أيّ هجوم معلوماتي افتراضي مباغت، إذ لا يمرّ يوم إلا ونسمع بظهور فيروسات وبرمجيات ضارّة جديدة، أو تظهر برمجيات معلوماتية وتختفي الأخرى، نتيجة المنافسة الشّديدة وعدم قدرة منتجيها في تحديثها أو ترقية تجهيزاتها، لذا تُعدّ مجالات التّجارة الإلكترونيّة المحيط الأكثر تعرّضا لمختلف المخاطر التي تُهدّد سلامة وأمن البيانات الإلكترونيّة المتداولة، واستقرار واستمراريّة عمل شبكات مواقع التّجارة الإلكترونيّة، حيث وصل الأمر إلى أنّ أيّ تَوقُّف أو تعطيل ولو كان بسيط في مُكوّنات هذه الشّبكات، من شأنه أن يُؤدّي بالشّركات الصّناعيّة والتّجاريّة أو المصرفيّة، إلى تحمّل خسائر ماليّة ضّخمة تُؤدّي في بعض الأحيان إلى حدوث أزمات اقتصاديّة أو ماليّة عالميّة، وعليه تعتبر أنظمة المعلومات بمثابة الشّبكة العصبيّة لمواقع التّجارة الإلكترونيّة، حيث تُبنى فيها قواعد المعلومات المتكاملة وتتبادل فيها البيانات الإلكترونيّة السّريّة والحسّاسة، التي تستوجب وضع إجراءات أمنيّة موثوقة، لحماية جميع مُكوّنات ومَوارِد شبكات المعلومات(**الفصل الأول**).

إنّ التّهديدات الأمنيّة لا تنطوي فقط على الجانب التّقني المُرتبط بمُكوّنات الشّبكات المعلوماتيّة ومَوَارِدِهَا، بل تَمسّ بحقوق أخرى محميّة بموجب الأحكام التّشريعيّة والتّنظيميّة المتعلّقة سواء بحقوق الملكيّة الرّقميّة لصاحب المَوقِع التّجاري، بجانبيها الأدبيّة والفنيّة(حقوق المؤلف والحقوق المجاورة) أو الملكيّة الصّناعيّة والتّجاريّة، كما أنّه عادة ما تكيّف الهجمات الإلكترونيّة المرتكبة من طرف العصابات والمجرمين والمخالفين للقوانين والتّقاليد والأعراف السّائدة في المجتمعات، على أنّها جرائم إلكترونيّة مخالفة للنّظام العام، كسرقة المعلومات السّريّة للشّركات وترويج برامج التّخريب والتّجسّس والقرصنة، والغش التّجاري وغسيل الأموال والجرائم المنظّمة، والمساس بالمعطيات الشّخصيّة والحياة الخاصّة الخ...، التي تستجوب التّحقيق والتّحري لجمع الأدّلة الجنائية، حيث يعاقب عليها بموجب أحكام قوانين العقوبات (**الفصل الثاني**).

الفصل الأول
الحماية التّقنيّة لمواقع التّجارة الإلكترونيّة

إنّ انتشار شبكة الإنترنت وتَحوُّلِها إلى وسيلة مالية مُربحة في مجال الأعمال، ساهمت بشكلٍ كبير في انتشار ونمّو تطبيقات التّجارة الإلكترونيّة، وتطوّر المعدّات والبرامج المعلوماتيّة، وتطوّرت نُظم وتقنيات تشغيل الشّبكات، التي سمحت للمتعاملين الاقتصاديين بترويج مختلف السّلع والخدمات عبر مواقع إلكترونيّة افتراضيّة، مملوءة بمختلف المخاطر المتعلّقة بالقرصنة والتّجسّس الصّناعي وتدمير المواقع الإلكترونيّة، وإساءة أو تعطيل موارد الشّبكات وانتحال الهوّيات الخ...، ولعلّ أنّ أهمّ المشكلات الأمنيّة المطروحة حاليّا على مستوى شبكات الاتّصالات التّجاريّة هي تلك المتعلّقة بالخصوصيّة والحماية، ومِصداقيّة وإنكار المعلومات التي يتّم تداولها وتحويلها فيما بين أطراف التّعاقد الإلكتروني عبر مواقع التّجارة الإلكترونيّة، ولتفادي تلك التّهديدات يتعيّن على مُتّخذي القرار إرساء الضّمانات التّقنيّة اللاّزمة لحماية مكوّنات وموارد شبكات مواقع التّجارة الإلكترونيّة(**المبحث الأول**).

تعتبر الثّقة والأمان من بين الضّمانات الرّئيسيّة التي يجب توافرها في المعاملات التي تتّم عبر مواقع التّجارة الإلكترونيّة، وذلك بالنّظر إلى المشاكل التّقنيّة والقانونيّة المتوّلدة عن البيئة الإلكترونيّة الافتراضيّة، المُنصّبة بالخصوص حول إثبات الهويّة وسريّة وسلامة المراسلات الإلكترونيّة، ومن عدم تعرّضها لأيّ تغيير أو تعديل أو تزوير فيها، مع عدم إنكارها من جانب أطراف التّعامل الإلكتروني، الأمر الذي يستوجب البحث عن تقنيات حديثة لتوثيق أو تصديق التّصرفات الإلكترونيّة تحت إشراف أطراف ثالثة محايدة ومعتمدة من طرف الجهات الرّسميّة(**المبحث الثاني**).

المبحث الأول

الحماية الأمنيّة والوقائيّة لمواقع التّجارة الإلكترونيّة

تزداد أخطار شبكة الإنترنت بازدياد ضخامة المعاملات الإلكترونيّة والانتشار الهائل لمواقع التّجارة الإلكترونيّة التي تشّكل الهدف الرّئيسي للعديد من العصابات والمجرمين الذين يقومون بتنفيذ هجماتهم الإلكترونيّة، لغرض التّجسّس الصّناعي أو الاستيلاء أو الاستحواذ على الأموال، أو التّرويج ببرامج القرصنة وسرقة المعلومات المتداولة أو المخزّنة أو القيام بعمليات التّسلّل والاختراق إلى الشّبكات الخ...، في حين أصبحت شبكة الإنترنت أداة اتصال فعّالة لهؤلاء، للنّفوذ أو التّغلغل إلى داخل الشّبكات الدّاخليّة لمواقع الشّركات التّجاريّة أو الصّناعيّة، إذ أنّ معظمهم ينّفذون تهديداتهم الخارجيّة انطلاقا من شبكة الإنترنت، مستغلّين في ذلك الهفوات أو الثّغرات الأمنيّة المتواجدة في أجهزة أو معدّات حماية الشّبكة، ومن هنا تبرز أهمّية الحاجة إلى وضع سياسة أمنيّة ناجعة للحماية العالية لشبكات مواقع التّجارة الإلكترونيّة **(المطلب الأول)**.

إنّ حماية وتأمين شبكات الحاسب الآلي لا تكمن فقط في توريد وتثبيت(Installer) الأجهزة ومختلف برمجيات الوقاية من مختلف الفيروسات، وإنّما تكمن كذلك في إعداد وتوعية المستهلك أو المشتري عن مختلف التّهديدات أو الأخطار المنبثقة، من حين لآخر من شبكة الإنترنت، والاستخدام الأمثل لتقنيات الحماية الأمنيّة المتطلّبة في مواقع التّجارة الإلكترونيّة أثناء أو قبل القيام بتصرّفاته التّجاريّة، كالتّسوّق الآمن عبر الإنترنت وحماية مكوّنات شبكة الحاسب الآلي والاستعانة ببرامج الحماية من الفيروسات، وبخدمات مُشّغل الدّفع الإلكتروني الآمن الذي يشرف عليه طرف ثالث موثوق ومعتمد من طرف الجهات الرّسميّة **(المطلب الثاني)**.

المطلب الأول
الحماية الأمنيّة لمواقع التّجارة الإلكترونيّة

ترتبط معاملات التّجارة الإلكترونيّة بشكل وثيق بأمن معلومات الشّبكات، وذلك نظرا لانتشار وازدياد مخاطر الجرائم الإلكترونيّة، نتيجة التّداخل فيما بين الأنظمة المعلوماتيّة لشبكات الحاسوب في بيئة التّجارة الإلكترونيّة، حيث ينبغي الإلمام بجميع التّهديدات عند إعداد سياسات الحماية الضّروريّة المنطوية حول نشاطات وأهداف الشّركة أو المؤسّسة(**الفرع الأول**)، وعليه فإنّ شبكة الإنترنت ماهيّة إلاّ شبكة ما بين الشّبكات التي تُدار كلّ واحدة منها بمعزل عن الأخرى، حيث لا تعتمد أيّا منها، أثناء تشغيلها، على الشّبكات الأخرى إذ يُستخدم في كلّ شبكة تقنيات داخليّة مختلفة تسمح بالاتّصال فيما بين الشّبكات عن طريق بوابات أو منافذ مشتركة ومحميّة (**الفرع الثاني**)، وبما أنّ التّهديدات الالكترونيّة تمسّ المصالح الحيويّة للدّول، فإنّ معاملات التّجارة الإلكترونيّة تتطلّب الاستعانة بخدمات جهات الرّقابة على الإنترنت (**الفرع الثالث**)، كما أنّ عملية المعالجة الآلية للمعطيات الشّخصيّة للأشخاص الطبيعيين تتطلّب إرساء تدابير حماية أمنيّة لها (**الفرع الرابع**).

الفرع الأول
الإحاطة بالأخطار المهدّدة بأمن شبكات المعلومات

إنّ إعداد سياسة الحماية الأمنيّة للشّبكات (Établissement d'une politique de sécurité) لا تتمحور فقط حول وضع إجراءات تقنيّة وتثبيت معدّات وفقا لمواصفات هندسيّة معيّنة[1]، بل تستوجب الأخذ بعين الاعتبار أهداف الحماية، والوعي وحسن إدراك مختلف الأخطار الإلكترونيّة الدّاخليّة(Menaces internes) والخارجيّة(Menaces externes) التي تمّس بمكوّنات الشّبكات ومواردها، والتّنبؤ بها لمنع حدوثها أو تحقيقها مستقبلا مع جعل

1) **Hélie - Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 49, 50, 51.

العصابات والمجرمين يحجمون عن مواصلة أو تنفيذ خطّتهم[1]، وعليه فإنّ التّطور الهائل لتكنولوجيا الاتّصال والإعلام وتشّعب ونمّو وازدياد استخدامات تطبيقات شبكة الإنترنت في أوساط الأفراد والمجتمعات، وتوسّع نطاق المشكلات الأمنيّة لشبكات الحاسوب، وضخامة حجم مخاطرها التي تزداد بازدياد مُستخدمي الشّبكات وظهور ثقافة جديدة في صناعة البرامج المعلوماتيّة الخبيثة أو الضّارة وانتشارها في أوساط الأفراد، أصبح من غير المُمكِن تصوّر تحقيق الأمن المعلوماتي للشّبكات المحميّة بصفة نهائيّة ومضمونة أو أكيدة، ممّا يؤدّي إلى ضرورة وضع خطّة أمنيّة ديناميكيّة تتلاءم وتتجاوب مع عوامل ومستجدّات البيئة الالكترونيّة الافتراضيّة، مع ضمان حدّ مقبول من المخاطر المتوّقع حدوثها أو السّعي لتجنّب انتشارها في حالة ما إذا مسّت بالأنظمة المعلوماتيّة للشّبكات[2].

انطلاقا من ذلك، فإنّ عملية تقييم الأخطار الدّاخليّة والخارجيّة للشّبكات، وتحديد قيمة ما يُراد حمايته فيها وما يُمكِن السّيطرة عَليهِ وإدارتهِ وما يَخرجُ عن السّيطرة عليهِ، وضمان متابعة كلّ ما يُمكِن أن يحدثَ من جديد، والإحاطة بكل التّهديدات والثّغرات الأمنيّة المستجدّة أو المستقبليّة التي من شأنها أن تمّس بأنظمة أمن الشّبكات ومواردها، تأتي من الأولويات الأساسيّة والضّروريّة لدى إقرار سياسة الحماية الأمنيّة للشّبكات[3].

ولعلّ أنّ ما يجب إثارته في هذا السّياق، المسائل الهامّة المتعلّقة بتحديد وتوثيق هويّة أطراف التّعامل الإلكتروني، وضمان سريّة وسلامة البيانات الإلكترونيّة المتداولة وعدم

---

1) **Christophe CAMBORDE**, Sécuriser vos applications Internet (Messageries, Intranet, sites web, e-commerce), Dunod, Paris, France, 2004, pp. 88, 89.

علاء حسين الحمامي، سعد عبد العزيز العاني، مرجع سابق، ص ص 433– 436.

2) **Hélie- Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 61, 62.

Christophe CAMBORDE, op.cit., pp. 90- 96.

3) **Hélie- Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp.68, 182, 183, 184.

إنكارها، مع ضمان استمراريّة عمل الأنظمة المعلوماتيّة والوصول إلى البيانات الإلكترونيّة المُرّخص بها عبر الشّبكات[1].

بالإضافة إلى ذلك، فإنّ سياسة الحماية الأمنيّة لشبكات مواقع التّجارة الإلكترونيّة تتطلّب تخصيص الوقت الكافي، لبذل الجّهود اللاّزمة لإعدادها وتطويرها(Politique de sécurité) بما يتوافق مع أهداف وإجراءات تطبيق وتنفيذ سياسة الحماية الأمنيّة المُسّطرة، وكذا التّعرف على مشاكل الهياكل التّنظيميّة في إدارة تقنيّة المعلومات، ومدى توافقها مع سياسة الحماية وإعداد وتحديث مختلف الأجهزة، والبرامج المعلوماتيّة الحديثة المستخدمة لحماية الشّبكات وترصّد أو تدارك نقاط الضّعف في الشّبكات، التي يستغلّها أصحاب الاختصاص لاختراق شبكات المعلومات، وتحديد إجراءات العمل المعتمدة لتحقيق حماية عالية لهذه الشّبكات، مع حصر التّدابير الوقائيّة الفعليّة والاحتياطيّة اللاّزمة لمنع حدوث المخاطر أو تجنّب تنفيذ الهجمات الإلكترونيّة على مستوى الشّبكات الدّاخليّة أو الخارجيّة[2].

الفرع الثاني

الحماية الأمنيّة لحدود شبكات المعلومات ونظم تشغيلها

إنّ الإحاطة بمختلف مخاطر أمن شبكات المعلومات تستدعي فَهْماً وَاسِعاً ورُؤية جديدة لمناهج وتقنيات حماية حدود هذه الشّبكات من مختلف التّهديدات الإلكترونيّة(**أولا**)، كما أنّه من الخَطَأِ أن تُترك البيانات الإلكترونيّة تتداول عبر شبكة الإنترنت من دون حماية أمنيّة موثوقة لنُظم تشغيل الشّبكات(**ثانيا**).

---

1) **Hélie - Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 64- 67.

2) أنظر **الملحق رقم (26)**، ص 500.

Voir aussi: **Géraldine VACHE MARCONATO**, op.cit., pp. 118-120.

أنظر كذلك: **علاء حسين الحمامي، سعد عبد العزيز العاني**، مرجع سابق، ص ص 437– 441.

أولا– الحماية الأمنيّة لحدود شبكات المعلومات.

تحتوي الشّبكات المعلوماتيّة على معدّات وأجهزة ماديّة ساكنة وبرامج معلوماتيّة فاعلة تبّث الحركة والنّشاط في هذه الأجهزة والمعدّات، التي تشتمل على الموزّعات(Switchs) والموجّهات(Routers) وجدران الحماية((Pare-feux(Firewalls)، وأجهزة الخادم(Servers) التي تتضمّن على خوادم قواعد البيانات(Data Base)، وخوادم ترجمة عناوين الإنترنت(DNS) وخوادم توزيع هذه العناوين ومُوزّعي الويب، وخوادم الحماية بأشكالها المختلفة التي تستعين ببرمجيات الحماية لتقوم بوظيفة جدار حماية أو مضّاد للفيروسات أو كخادم كشف الثّغرات وتثبيت التّحديثات الخ...

لذا يُعتبر جدار الحماية الجهاز الأكثر شهرة واستخداما في أمن بيئة الشّبكات، حيث يحتوي على خليط من البرمجيات والأجهزة، التي تمنع الوصول غير المُصّرح به للشّبكة من مُستخدمي شبكة الإنترنت، مِمَّا يُوفّر حماية عالية للشّبكة ضّد عمليات الاختراق غير المشروع[1]، في حين يمكن أن تُستخدم هذه الجدران من طرف الأفراد أو الشّركات التّجاريّة والصّناعيّة أو الحكوميّة، ففي بداية الأمر صُمِّمَت جدران الحماية للقيام بمهام التّصفية(Filtering) حيث تطوّرت في الآونة الأخيرة لتصبح أجهزة حماية متعدّدة الخصائص ضمن صندوق أو جهاز واحد((Unified Threat Management(UTM)، وذلك بعدما أُلحقت بها وظائف مختلفة، مثل كشف محاولات الاختراق والتّجسّس Instruction) ((Detection System(IDS، وكشف محاولات الاختراق والتّصدي لها Intrusion) ((Protection System(IPS وكشف ومكافحة الفيروسات والبرمجيات الضّارة كأحصنة طروادة والدّيدان الخ...، وتصفية كلّ من مواقع الإنترنت غير المرغوبة(Web Filtering)، والبريد الإلكتروني الدّعائي(Spam) ومحتوى صفحات الويب[2]، فبالإضافة إلى وظائف

---

[1] **رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية(دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي)، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2008، ص 145. **ناصر خليل**، مرجع سابق، ص ص 226– 228.

[2] **عامر إبراهيم قنديلجي، إيمان فاضل السامرائي**، مرجع سابق، ص ص 215– 217.

الحجب والتّصفية نجد أن هذا النّوع من جدران الحماية تقوم بتأمين الشّبكات الافتراضيّة الخاصّة(VPN) أو(RPV) التي تستخدم قنوات مشّفرة لنقل المعلومات الخاصّة أو السّريّة عبر شبكة الإنترنت، كما تقوم(Firewalls) بوظيفة تسجيل حركات الدّخول والخروج من كلّ الواجهات(Interfaces) أو المنافذ(Ports) الخ...[1]

تقوم جدران الحماية الحديثة من الناحية العمليّة بتقسيم الشّبكات إلى مناطق رئيسيّة مزوّدة بمنافذ حسب حجم الشّبكة واحتياجات أو متطلّبات الحماية الأمنيّة فيها، فالمنطقة الآمنة تمثّل عادة الشّبكة الدّاخليّة التي تتضمّن على أجهزة حاسوب المستفيدين، ومعدّات الحماية من الفيروسات وأجهزة الخادم التي تؤمّن عمليات التّحقق من صّحة هويّة المستفيدين الخ...، في حين تُمثّل المنطقة غير الآمنة لشبكة الإنترنت منطقة عامّة خارجيّة غير موثوق بها، أمّا المنطقة المعزولة (Zone démilitarisée(DeMilitarized Zone(DMZ) ou ((Périmètre de sécurité) تفصل بين الشّبكة الدّاخليّة(المنطقة الآمنة) وشبكة الإنترنت(المنطقة غير الآمنة)، حيث يمكِن أن يحتوي التّصميم على عدّة مناطق معزولة بحسب الحاجة إليها، إذ تحتوي على أجهزة خوادم تربط بين مستخدمي الشّبكة المعزولة وبين مستخدمي الشّبكة الدّاخليّة والشّبكة الخارجيّة المعروفة بالإنترنت[2].

وعليه، تقوم أجهزة الجدران النّارية بحماية العناوين الإلكترونيّة على مستوى الشّبكة الدّاخليّة، مع تسجيل جميع حركات الدّخول إلى البيانات والخروج منها عبر جميع المنافذ أو الواجهات، في خادم مُخصّص لتخزين وتحليل كلّ هذه التّصرفات لهدف اتخاذ تدابير الوقاية اللاّزمة لمنع حدوثها أو انتشارها[3]، وبالتّالي فإنّ أفضل جدران الحماية هي التي تُتيح إمكانيات تنفيذ احتياجات سياسات الحماية الأمنيّة، كحماية الشّبكات الدّاخليّة من عمليات

---

1) **Jean-François PILLOU, Fabrice LEMAINQUE**, op.cit., pp. 214- 218.

2) Ibid.

Hélie- SOLANGE GHERNAOUTI, Sécurité Internet : Stratégies et technologies, op.cit., pp. 216, 217.

3) **علاء حسين الحمامي، سعد عبد العزيز العاني**، مرجع سابق، ص 329– 331.

الاختراق وحماية الشّبكات الافتراضيّة من مختلف التّهديدات، والمحافظة على سرعة الأداء والوصول إلى مختلف المعلومات بطريقة محميّة، فعادة ما يتّم الاستعانة بجدار الحماية الاحتياطي الذي يتّم تشغيله مباشرة بطريقة آلية في حالة ما إذا تعطّل جدار الحماية الرّئيسي وذلك من دون أيّ انتظار[1].

لتمكين جدران الحماية من أداء وظائفها الأمنيّة من جهاز واحد، يجب أن تُوضَعَ على حدود شبكة الشّركة أي في بوّابة الاتّصال بشبكة الإنترنت، حيث تتطلّب عملية إعدادها الاستعانة بخبراء ذوي مهارات عالية في إعداد سياسة أمن المعلومات، للقيام بدراسة شاملة للمواضيع المعرّضة للهجمات الإلكترونيّة، ومن ثمّ تركيبها(Firewalls) بالطّريقة اللاّئقة والمناسبة، حيث تصبح عديم الجَدْوَى في حالة ما إذا لم يتّم استخدامها بطريقة صحيحة وفعّالة ممّا يؤدّي إلى عواقب وخيمة جدّا، في حين يجب العِلم بأنّ الغاية من تركيب جدران الحماية تَكْمُنُ من الدّرجة الأولى في "تأمين حدود الشّبكة فقط"، ولا فائدة تُرجَى منها في حالة تواجُد أبواب أو منافذ خلفية((Backdoors(Portes dérobées) في الشّبكة غير مُتّصلة أو مُرتبطة بجدران الحماية، كالاتّصال عن طريق المُودم(Modem non restrictif) أو تحميل برمجيات خبيثة عبر الإنترنت، كما أنّها(Pare-feux) لا تمنع المستخدم الدّاخلي في الشّبكة من نسخ البيانات المحميّة على أيّ وسيط إلكتروني محمول الخ...[2]

انطلاقا من ذلك، يجب القيام باختبارات تجريبيّة لعمل جدران الحماية عن طريق محاولة اختراقها من خارج الشّركة بصورة دوريّة، من أجل التّأكد من سلامة وظائفها أو تجربة التّحديثات أو التّعديلات قبل تثبيتها أو تركيبها ضمن مُكوّنات الشّبكة، مع تشغيل الخدمات

---

[1] أنظر **الملحق رقم (27)**، ص 501.

Voir aussi : **Hélie - SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., p. 220.

[2] **Nadia NOUALI-TABOUDJEMAT, «** Les firewalls comme solution aux problèmes de sécurité », p. 7. Article disponible sur le site: http://www.webreview.dz, consulté le 05/12/2018.

علاء حسين الحمامي، سعد عبد العزيز العاني، مرجع سابق، ص 332.

Jean-François PILLOU, Fabrice LEMAINQUE, op.cit., pp. 219, 220.

المطلوبة وإيقاف الخدمات غير المعمول بها، وتحديث نظام التّشغيل عند الحاجة إلى ذلك بطريقة موثوقة(أي بنصحٍ من الشّركة الأصليّة المُورِّدة لنظام التّشغيل)، وتفّحص التّطبيقات وقواعد البيانات وكلمات المرور المستعملة خلف جدران الحماية، مع كشف الثّغرات الأمنيّة المحتملة فيها وسدّها باتّخاذ الإجراءات الملائمة، الخ...[1]

ثانيا– الحماية الأمنيّة لنظم تشغيل شبكات المعلومات.

يشكل نظام التّشغيل(Système d'Exploitation(SE))[2] حَلَقَة وَصْلْ رئيسيّة بين مُكوِّنات جهاز الحاسوب(الماديّة والبرامج المعلوماتيّة) ومُستخدمه(الحاسوب)، حيث تصنّف هذه النّظم بِحَسَبِ الجهاز أو الميدان الذي تُشّغله، فقد يكون الخادم أو يكون نظام التّشغيل مخصّصا للأعمال أو الاستخدام المنزلي أو معالجة بيانات التّجارة الإلكترونيّة أو المجال الصّناعي، القضايا العسكريّة الخ...، ومن بين أهّم برامج نظم التّشغيل المعمول بها حاليًا نجد كلّ من(Windows, Mac OS, UNIX et Linux).

في حين تعتبر نظم تشغيل موارد الشّبكات الأكثر عُرضة لمختلف الهجمات الإلكترونيّة، التي يستغّل منّفذيها الثّغرات الأمنيّة المتواجدة في هذه النّظم للتّسلّل غير المصّرح به إلى المعلومات، أو الحصول على كلمات المرور السّريّة أو زرع البرمجيات الخبيثة لغرض الحصول على المعلومات المتداولة الخ...، وبالتّالي تُعتبر الحماية الأمنيّة لنظم التّشغيل من بين المسائل الحيويّة لأيّ نظام معلوماتي شاغل داخل الشّبكة الواحدة، التي تستوجب الاستعانة بخدمات برامج الحماية من البرامج الخبيثة الضّارة, Kasper Sky, E-Trust)

---

1) **Hélie - SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 218, 219, 230, 231.

2) En anglais (**Operating System(OS)**) : est un ensemble cohérent de programmes qui remplissent **deux grandes fonctions** :

– assurer un ensemble de services en présentant aux utilisateurs une interface adaptée à leurs besoins ;

– effectuer un certain nombre d'opérations préparatoires pour assurer les échanges entre les différents éléments qui composent un ordinateur (l'unité centrale, la mémoire et les périphériques d'entrée / sortie). Il gère le pilotage de ces derniers à travers les gestionnaires de périphériques, plus communément appelés pilotes (drivers) qui lui sont intégrés ou ajoutés. http://fr.www.wikipedia.org/wiki/système d'exploitation/, consulté le 10/01/2019.

(Norton, Sophos, Anti-Malware, E-trust, MacAfee, etc.، التي تقوم بفحوصات دوريّة لجميع حواسب الشّبكة والقيام بتثبيت تحديثات(Mises à jour) نظم التّشغيل المصّرح بها من طرف الشّركة الأصليّة المورّدة لها، مع الاستعانة بمُكمِّلات وظائف جدران الحماية وتطبيق سياسة الحماية باستخدام كلمات المرور القويّة بدلا من الكلمات الافتراضيّة التي قد تكون مُسبقة الإعداد حيث تُستَغَّلُ للوصول إلى قواعد البيانات الخ... [1].

وعليه، تُعتبر قواعد البيانات(Bases de données) كجزء من مُكوّنات جهاز الحاسوب تحتوي على مجموعة متكاملة من البيانات التي يشرف عليها عادة نظام التّشغيل، حيث تمكّن المستفيدين في الشّركة من التّعامل معها، والقيام بعمليات البحث وتسجيل ومعالجة وتخزين واسترجاع المعلومات الخ...، وبالتّالي فإنّ الاعتماد كليّا على إعدادات الحماية الخاصّة بجدران الحماية وخط دفاع نظم التّشغيل، وحتّى لو بلغت هذه الأخيرة أعلى درجات الحماية، فإنّ قواعد البيانات تكون عُرضة لمختلف العصابات والمجرمين المحترفين الذين يستغلّون الثّغرات الأمنيّة المتواجدة في أنظمة الحماية، من أجل القيام بمختلف الهجمات الإلكترونيّة التي تكون في بعض الأحيان أشّد خطورة، ولتفادي كل ذلك يُوصي خبراء أمن المعلومات بضرورة الاعتماد على تقنيّة التّشفير، التي تُعوّل على خوارزميات إخفاء المعلومات، وجعلها غير قابلة للقراءة بتحويلها إلى رموز أو حروف أو أرقام أو أشكال، حيث يمكن عَكسها لاحقا إلى هيئتها الأصليّة باستخدام مفاتيح التّشفير المستعملة في ذلك.

إنّ تقنيّة التّشفير كانت تُطبّق لغرض إخفاء النّص الواضح مع جعله غير قابل للقراءة، لكن تطوّرت استخدامات هذه التّقنيّة لتحقيق غايات أو أغراض أخرى ككشف المعلومات المُدخلة بطريقة غير شرعية أو التي تم حذفها أو تعديلها، كما يُمكن أن تُستخدم لحماية قنوات ربط أجهزة حاسوب المستفيدين(المكتبيّة أو المحمولة) مع أجهزة الخادم(التي تَحتضِن

---

[1] Document du Club de la sécurité des systèmes d'information Français(**CLUSIF**), « Sécurité des applications Web : comment maîtriser les risques liés à la sécurité des applications Web », septembre 2009, pp. 08-11, 14- 16. Disponible sur le site : https://www.clusif.asso.fr/, consulté le 12/09/2018.

المواقع الإلكترونيّة)، ومُعدّات شبكة الاتّصال كالموجّهات(Routers) والمبدّلات(Switchs) وجدران الحماية، وحماية قنوات الانتقال التي تربط فيما بين الأجهزة الطّرفية مع الحواسب المُضيفة، كما يُستخدم التّشفير عند تَوقُّع فَشَلِ طرق التّحكّم المختلفة في توفير الحماية الأمنيّة التّامة للبيانات الإلكترونيّة، كالتّحكّم في الدّخول باستعمال كلمات المرور، والتّحكّم في تدفّق البيانات لمنع تسّرب المعلومات، والتّحكّم في محاولات الاستنتاج لمنع القراصنة من تنفيذ عمليات الاستفسار، واستخلاص بعض المعلومات السّريّة.

الفرع الثالث

دور وكالات الأمن المعلوماتي في حماية أمن مواقع التّجارة الالكترونيّة وفقا لكل تشريع

يُعتبر القطاع المصرفي وميدان التّجارة الإلكترونيّة أكثر عُرضة وتهديدا من طرف القراصنة، الذين يتقنون استخدام تقنيات التّجسّس والنّصب والاحتيال ونهب أو سرقة الأموال، وقرصنة البيانات الشّخصيّة والسّريّة لأصحاب البطاقات المصرفية الذّكيّة والتّنصت على الاتّصالات الخ...، الأمر الذي أدّى بأصحاب مواقع التّجارة الإلكترونيّة إلى الاستعانة بخدمات شركات الأمن المعلوماتي التي تستعين بكفاءات بشريّة متميّزة، يتمتّعون بخبرات واسعة في مجال تكنولوجيا الاتّصال والإعلام، وتستخدم أحدث التّقنيات التّكنولوجيّة في كشف الفيروسات والبرمجيات الخبيثة المعقدّة بشتى أنواعها، وكذلك تقوم بإخطار عملائها بمستجدّات التّهديدات المكتشفة مع اتخاذ التّوصيات أو الاحتياطات اللاّزمة لتفاديها.

وعليه، تسمح التّقنيات المعتمدة من طرف شركات الأمن المعلوماتي بالتّفتيش العميق في صفحات المواقع وأنظمة الشّبكات، بُغية البحث عن عمليات الاختراق أو رصد والكشف عن الثّغرات الأمنيّة المتواجدة على مستوى أنظمة الحماية الأمنيّة للشّبكات المُتسبّبة من طرف أنواع معيّنة من الدّيدان أو الفيروسات وأحصنة طروادة، حيث تقوم هذه الشّركات بإتاحة أحدث برمجيات الوقاية من مختلف الفيروسات والبرمجيات الضّارة وفقا لمُستويات عالية من الأمان المتطلّبة، فمن بين أهمّ شركات الأمن المعلوماتي التي يُعوَّل عليها في كشف وترصّد ومكافحة مختلف الجرائم والتّهديدات الإلكترونيّة نجد كلّ من (Kasper Sky, F-Secure, ESET, Symantec, Virus Blok Ada, E-trust, MacAfee, etc.) .

وباتت مخاطر أمن المعلومات ترقى إلى مستوى تهديد الأمن الوطني للدّول، الأمر الذي دفع بهذه الأخيرة إلى إحداث وكالات أمن وطنيّة تُشرف على عمليات رقابة وأمن مختلف شبكات الاتّصالات، والتّنبؤ من مختلف التّهديدات الخارجيّة والدّاخليّة التي من شأنها أن تمسّ بأمنها واقتصادها الوطنيين واستقرار مؤسّساتها ومصالحها الحيويّة، حيث سنتطرّق إلى بعض التّشريعات الأجنبيّة **(أولا)** والوطنيّة **(ثانيا)** المنشئة لهذه الوكالات على النّحو التّالي:

أولا– التّشريعات الأجنبيّة.

قامت معظم الدول الأجنبية بإرساء منظومات أمنية موثوقة شاملة تُشرف عليها وكالات أمنية وطنية، بغية التنبؤ من مختلف التهديدات عبر شبكات الاتصالات، ونذكر من بين هذه التشريعات الأجنبية ما يلي:

1)– القانون الفيدرالي للولايات المتّحدة الأمريكيّة:

قامت الولايات المتّحدة الأمريكيّة أثناء الحرب العالميّة الثّانية(1945/1939) بإحداث وِحدة((Communications Intelligence (COMINT تحت وصاية الجّيش الأمريكي، مُكلّفة بفّك الشّفرات والتّنصت على اتّصالات العدّو للحصول على المعلومات العسكريّة الحسّاسة، التي تساعد الدّولة الفيدراليّة(USA) وحُلفائِها على تغيير موازين القِوَى وتَرجِيح كفّة الحرب لصالحهم، حيث تغيّرت تسمية تلك الوِحدة في زمن الحرب البّادرة بالخصوص أثناء العُهدة الرّئاسيّة للرّئيس(33) للولايات المتّحدة الأمريكيّة هَارِي تَرُومَانْ (Harry TRUMAN(1945- 1953))، إلى وكالة الأمن القومي(NSA) التي تعتبر كأكبر وكالة استعلامات أمريكيّة مُكلّفة بمُراقبة الاتّصالات الإلكترونيّة بمفهومها الواسع، والتّنبؤ من مختلف التّهديدات الإلكترونيّة الدّاخليّة والخارجيّة التي تستهدف الأمن الوطني للدّولة الفيدراليّة(USA)[1]، حيث تُمارس مهامها في إطار رقابة المحكمة الفيدراليّة الأمريكيّة للرّقابة

1) **Pierre MAGNAN**, « La NSA, le big brother américain, is watching you depuis 1952 », article publié le 14/06/2013 à 16H24 sur le site : http://geopolis.francetvinfo.fr/la-nsa-le-big-brother-americain-is-watching-you-depuis-1952-17641, consulté le 26/12/2018.

على الاستعلامات الخارجيّة (United States Foreign Intelligence Surveillance Cour(**FISC**) ou(**FISA Cour**))، التي أُستحدِثت بموجب قانون الكونجرس الأمريكي المؤرخ في 25 أكتوبر 1978 المتعلّق بمُراقبة الاستعلامات الخارجيّة (Foreign Intelligence Surveillance Act (**FISA**))، الذي حدّد إجراءات الرّقابة الماديّة والإلكترونيّة وكذا تنظيم عمليات جمع المعلومات الخارجيّة سواء بصفة مباشرة أو في إطار تبادل المعلومات مع الهيئات الأجنبيّة[1].

وعليه، تعرّضت أحكام هذا القانون(FISA) بعد أحداث11 سبتمبر2001 إلى عدّة تعديلات منحت لوكالة الأمن القومي(NSA) صلاحيات واسعة في مجال الرّقابة على الاتّصالات الإلكترونيّة من دون الحصول على ترخيص أو أمر قضائي(FISC)، حيث قام الرّئيس الأمريكي آنذاك (**George Walker Bush-** 43e président des États-Unis(2001-2009)) بعد موافقة الكونجرس، بالتّوقيع على قانون مكافحة الإرهاب (USA PATRIOT Act) في 26 أكتوبر2001[2]، الذي قام بتسهيل إجراءات التّحريات والتّحقيقات والوسائل

---

1) Public law 95-511, Foreign Intelligence Surveillance Act(**FISA**) of Oct. 25, 1978. https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

2) Public law 107–56, Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (**USA patriot act**) act of 2001. https://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf

تعرضت بعض أحكام هذا القانون(**USA PATRIOT Act**) إلى التعديل بموجب أحكام القانون الفيدرالي المتعلق بالحريات(**Freedom Act USA**) الذي أصدره الرئيس الأمريكي باراك أوباما(Barak OBAMA) في 02 جوان 2015 بعد موافقة الكونجرس عليه، وذلك على إثر تسريبات إيدوارد سنودن(Edward SNOWDEN) في جوان 2013 حول نظام الرقابة المكثفة الذي انتهجته الحكومة الفيدرالية الأمريكية على الاتصالات الإلكترونية، حيث فرض بعض القيود على عمليات المراقبة على الاتصالات الإلكترونية والحصول على المعطيات بشكلٍ مُكثّف (La collecte en vrac ou massive)، التي تُباشرها السلطات الفيدرالية عن طريق وكالة الأمن القومي(NSA) في داخل الولايات المتحدة الأمريكية وذلك من دونِ أن تشمل تلك القيود على الاتصالات الخارجية، وكذا إضفاء الشرعية القانونية على المحكمة الفيدرالية(FISC) المُستحدثة بموجب القانون الفيدرالي حول الاستعلامات الخارجية(FISA)، حيث لا يجوز على السلطات الأمنية الفيدرالية في أقاليم الولايات الفيدرالية استعمال المعطيات المُتحصل عليها عن طريق عمليات المراقبة على الاتصالات الإلكترونية، إلاّ بعد الحصول على أمر قضائي مع التحديد الدقيق لهوية الفرد المشتبه فيه في ارتكاب الأعمال الإرهابية الخ...،

اللاّزمة لمكافحة الإرهاب ومنح الجهات الأمنيّة الفيدراليّة(FBI, CIA, NSA.) صلاحيات واسعة للاطّلاع والحصول على المعطيات الشّخصيّة للأشخاص، ومُراقبة الاتّصالات الإلكترونيّة والتّنصت على المكالمات لغرض جَمْعِ المعلومات الضّروريّة التي تُساعد على كشف المُخطّطات الإرهابيّة، كما تّم تعديل هذا القانون(**FISA**) في 2007 بموجب قانون(Protect America Act) وفي 2008 بأحكام قانون (FISA Amendments Act of 2008)[1] الذي وسّع من صلاحيات الرّقابة على الاتّصالات الالكترونيّة الخارجيّة، حيث وافق مجلس الشّيوخ الأمريكي(Le Sénat) في 2012 على تمديد صلاحية العمل بأحكام هذا القانون لمدّة خمسة(05) سنوات إضافيّة(إلى غاية 31 ديسمبر 2017).

انطلاقا من ذلك، فإنّ وكالة الأمن الوطني مُكلّفة بالمهام المتعلّقة بحماية جميع الاتّصالات الإلكترونيّة للحكومة الفيدراليّة الأمريكيّة وأنظمة معلوماتها ضدّ عمليات الاختراق والقرصنة الإلكترونيّة، مع ضمان المراقبة الوقائيّة للاتّصالات الإلكترونيّة لهدف ترصّد وكشف التّهديدات الإلكترونيّة المتعلّقة بالأعمال الإرهابيّة والتّخريبية والمساس بأمن الدّولة والاقتصاد الوطني[2]، من خلال جمع وتسجيل وحِفظ المُعطيات الرّقميّة مع تحديد مَسَارِهَا ومَصْدَرُهَا سواء على المستوى الدّاخلي أو الخارجي، وكذا تطوير وتنسيق عمليات تبادل المعلومات مع نظيراتها الأجنبيّة وبالخصوص تلك التّابعة للدّول الحليفة الأقرب للولايات المتّحدة الأمريكيّة على غرار كلّ من أستراليا، بريطانيا، كندا ونيوزلندة الجديدة، فإلى جانب

لمزيد من المعلومات أنظر :

Martin UNTERSINGER, Damien LELOUP, « Qu'est- ce que le USA Freedom Act ? », article de journal Le Monde, publié le 01/06/20015 à 11h08 sur le site : http://www.lemonde.fr/pixels/article/2015/06/01/, consulté le 03/10/2016.

Public law 114–23, Uniting and strengthening America by fulfilling rights and ensuring effective discipline over monitoring act of June 2, 2015, or the ''**USA Freedom Act of 2015**''. https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

1) Public law 110–55, Protect America Act of Aug 5, 2007.
https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf

FISA Amendments Act of Jul 9, 2008(Passed Congress/Enrolled Bill).
https://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf

2) **Karl WASS**, « Treillis et cravate - sécurité, le point de vue des managers », Revue Vacarme, 1999/1 (n° 7), p. 22.

ذلك تُشرف الوكالة(NSA) على المهام المتعلّقة بخدمات التّصديق من خلال اعتماد مراكز تقييم معدّات أمن تكنولوجيا المعلومات، في إطار مخطّطات التّقييم والتّصديق التي تقوم بإعدادها مُسبقا، وتساهم في إعداد المعايير ومشاريع القوانين المتعلّقة بمجال تكنولوجيا المعلومات[1] الخ...

2)– القانون الفيدرالي للاتّحاد الأوروبي:

قام المشّرع الفيدرالي للإتّحاد الأوروبي، بموجب المادة الأولى فقرة واحد(1/01) من التّنظيم الإداري رقم 460/2004 المؤرخ في 10 مارس 2004، المُتعلّق بإنشاء وكالة أوروبية مُكلّفة بأمن الشّبكات والمعلومات[2]، باستحداث وكالة أوروبيّة تُشرف على سلامة أمن الشّبكات والمعلومات (Agence Européenne chargée de la Sécurité des Réseaux et de l'Information(AESRI)) أو "(ENISA) بالإنجليزيّة"، تُشرف وفقا للمادة الثالثة(03) من نفس التّنظيم على المهام المتعلّقة بجمع واستغلال المعلومات المفيدة، التي تسمح بالتّنبؤ والكّشف عن مختلف التّهديدات أو الجرائم الإلكترونيّة التي تمّس بأمن الإتّحاد الأوروبي والإحاطة بجميع المخاطر بغية توحيد استراتيجيات السّياسة الأمنيّة، مع تنظيم عمليات التّوعية لمُسْتَخدِمِي الشّبكات والمعلومات وتزويدهم بالمستجدّات الطّارئة حول مخاطر استعمال التّقنيات التّكنولوجيّة الحديثة، وكذا توحيد المعايير في المعدّات والبرمجيات المُستخدمة في مجال أمن الشّبكات والمعلومات، مع تكثيف وتنسيق التّعاون فيما بين دول الإتّحاد الأوروبي أو مع الدّول الأجنبيّة بشأن أمن الشّبكات والمخاطر المتعلّقة بها.

---

1) **Arnaud-F. FAUSSE**, op.cit., pp. 64, 65.
Pour avoir plus d'informations sur les missions de la NSA, consultez le site : https://www.nsa.gov/about/mission/index.shtml

2) **Règlement (CE) n° 460/2004** du parlement européen et du conseil du 10 mars 2004 instituant l'agence européenne chargée de la sécurité des réseaux et de l'information, JOUE, n° L 77/1 du 13/3/2004.
Art.1 : « 1- Aux fins d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur, il est institué une **Agence européenne chargée de la sécurité des réseaux et de l'information**, ci-après dénommée (**Agence**). »

3)– القانون الفرنسي:

قام المشّرع الفرنسي بإحداث الوكالة الوطنيّة لأمن أنظمة المعلومات(ANSSI) لدى الوزير الأول والملحقة بالأمين العام للدّفاع والأمن الوطنيين، بموجب المادة الأولى(01) من المرسوم رقم 834/2009 المؤرخ في 07 جويلية 2009 المتعلّق بإنشاء مصلحة ذات اختصاص وطني تُدعى بـ"الوكالة الوطنيّة لأمن أنظمة المعلومات"[1]، التي تُشرف وفقا للمادة 03 من نفس المرسوم على مجموعة من المهام، كالمساهمة في اقتراح القواعد القانونيّة المتعلّقة بحماية أنظمة المعلومات والتّحقّق من مدى تطبيق إجراءاتها، وضمان المراقبة الوقائيّة للاتّصالات الإلكترونيّة لغرض الكّشف عن الجرائم الإلكترونيّة التي تمّس بأمن الدّولة ومؤسّساتها والاقتصاد الوطني، مع القيام بعمليات التّنسيق والتّوعية للوقاية من الجرائم الإلكترونيّة ومُكافحتها والسّهر على إعداد استراتيجيات الوقاية منها، وكذا تنفيذ مخطّطات الطّوارئ من خلال تنبيه وإخطار كافة المستخدمين من مختلف التّهديدات الإلكترونيّة، والتّعاون مع نظيراتها الأجنبيّة في المجالات المتعلّقة بأمن الشّبكات والمعلومات، والإشراف على مخطّطات التّصديق والاعتماد على المراكز والوسائل والمعدّات المستخدمة في أمن أنظمة المعلومات والشّبكات الخ....[2].

---

1) **Décret n° 2009-834** du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JORF, n° 0156 du 8 juillet 2009.

Art. 01 : « Il est créé un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». Ce service est rattaché au secrétaire général de la défense et de la sécurité nationale. »

2) Voir aussi : **Anne SOUVIRA, Myriam QUÉMÉNER**, « Cyber-sécurité et entreprises : se protéger juridiquement et se former », Revue Sécurité et stratégie, 2012/4 (11), pp. 90, 91.

Olivier KEMPF, « Cyberstratégie à la française », Revue Internationale et stratégique, 2012/3 (n° 87), pp. 122-124, 125-127.

ثانيا)– التّشريعات العربيّة.

أصبحت مخاطر شبكة الإنترنت تمّس جميع الدّول التي رفعت شعار التّحول إلى مجتمع المعلومات، وبالخصوص الدّول العربيّة التي قامت بإحداث وكالات أمن وطنيّة للرّقابة والتّنبؤ من مختلف التّهديدات عبر شبكات الاتّصالات، نذكر من بينها:

1)– القانون التونسي:

قام المشّرع التّونسي بموجب الفصل الثاني(02) من القانون عدد 05– 2004 المؤرخ في 03 فيفري 2004 المتعلّق بالسّلامة المعلوماتيّة[1]، بإحداث الوكالة الوطنيّة للسّلامة المعلوماتيّة كمؤسّسة عموميّة لا تكتسي الصّبغة الإداريّة، وتتمتّع بالشّخصيّة المعنويّة والذّمة الماليّة المستقّلة وتخضع إلى التّشريع التّجاري في علاقاتها مع الغير، حيث تشرف وفقا للفصل الثالث(03) من نفس القانون، على جميع المهام المتعلّقة بمراقبة النّظم المعلوماتيّة وشبكات مختلف الهياكل العموميّة والخاصّة، مع ضمان اليقظة التّكنولوجيّة في مجال السّلامة المعلوماتيّة، والسّهر على تنفيذ التّرتيبات المتعلّقة بإجباريّة التّدقيق الدّوري للسّلامة المعلوماتيّة والشّبكات ومدى تنفيذ التّوجهات الوطنيّة، والإستراتيجيّة العامّة لسلامة النّظم المعلوماتيّة والشّبكات وكذا الخطط والبرامج المتعلّقة بالسّلامة المعلوماتيّة في القطاع العمومي باستثناء التّطبيقات الخاصّة بالدّفاع والأمن الوطنين والتّنسيق بين المتدخلين في هذا المجال، ووضع وإعداد ونشر مقاييس وأدّلة فنيّة خاصّة بالسّلامة المعلوماتيّة والعمل على تشجيع تطوير حلول وطنيّة في مجال السّلامة المعلوماتيّة.

2)– القانون الجزائري:

قام المشرع الجزائري بموجب المادة 03 من المرسوم الرئاسي رقم 20–05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، بإحداث "وكالة لأمن الأنظمة المعلوماتية"(ASSI) لدى وزير الدفاع الوطني(رئيس الجمهورية)،

---

[1] قانون عدد 05– 2004 مؤرخ في 03 فيفري 2004، يتعلق بالسلامة المعلوماتية، ر ر ج ت عدد 10، الصادر في 03 فيفري 2004.

كمؤسّسة عموميّة ذات طابع إداري تتمتّع بالشّخصيّة المعنويّة والاستقلاليّة الماليّة، مُكلّفة بموجب المادة 18 من نفس المرسوم الرئاسي[1]، بتحضير وتنسيق تنفيذ الإستراتيجيّة الوطنيّة لأمن الأنظمة المعلوماتيّة، التي يُحدّدها ويُوافق عليها "المجلس الوطني لأمن الأنظمة المعلوماتيّة" الذي يُدعى بـ "المجلس"، وضمان اليقظة التّكنولوجيّة من خلال القيام بنشاطات التّكوين والتّوعيّة وتعزيز ثقافة تأمين الأنظمة المعلوماتيّة لدى الأفراد وأعوان الهيئات والإدارات والمؤسّسات، وكذا جمع وتحليل وتقييم المعطيات المتّصلة بأمن الأنظمة المعلوماتيّة لتأمين منشئات المؤسّسات العموميّة، وتفادي مختلف التّهديدات أو الهجمات الإلكترونية، حيث يُمكن للوكالة(ASSI) في إطار مهامها، أن تَطْلُبَ من الهيئات والمؤسّسات والمتعاملين والمزوّدين(م.خ.إ)، أيّ وثيقة أو معلومة مُفيدة.

كما تقوم الوكالة(ASSI)، باقتراح مشاريع نصوص تشريعيّة أو تنظيميّة في مجال أمن الأنظمة المعلوماتيّة بعد موافقة "المجلس"، واعتماد منظومات إحداث وفحص التّوقيع الإلكتروني، ومنتجات أمن الأنظمة المعلوماتيّة والتّصديق عليها، وإعداد وتحديث المرجعيات والإجراءات وتقديم التّوصيات في مجال أمن الأنظمة المعلوماتيّة، مع اقتراح مشاريع اتفاقات التّعاون والاعتراف المتبادل مع الهيئات الأجنبيّة المثيلة لها، وإبرام مشاريع الشّراكة بعد مُوافقة "المجلس"[2].

---

[1] **مرسوم رئاسي رقم 20–05** مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04 الصادر في 26 جانفي 2020.

تنص المادة 01 منه، على ما يلي:" يهدف هذا المرسوم إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية."

وتنص المادة 03 من نفس المرسوم الرئاسي، على ما يلي:" تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، ما يأتي: – مجلس وطني لأمن الأنظمة المعلوماتية، يدعى في صلب النص "المجلس"، ويكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها،

– وكالة لأمن الأنظمة المعلوماتية تدعى في صلب النص "الوكالة"، وتكلف بتنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية. ولممارسة مهامه يتوفر المجلس، بالإضافة إلى الوكالة، على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال."

[2] راجع نصوص المواد 17 و18 و19 من المرسوم الرئاسي رقم 20–05، سالف الذكر.

بالإضافة إلى هذه الوكالة(ASSI)، أنشأ المشّرع الجزائري لدى وزير العدل، بموجب المادة 13 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها، "هيئة وطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها"، كسلطة إدارية مستقّلة تتمتّع بالشّخصيّة المعنويّة والاستقلاليّة الماليّة، مُكلّفة بمهام تنسيق عمليات الوقاية من الجرائم الإلكترونيّة ومكافحتها، كالجرائم المتعلّقة بالإرهاب أو الماسّة بأمن الدّولة، أو احتمال تواجد اعتداء على منظومة معلوماتيّة، من شأنه أن يَهَدِّدَ النّظام العام أو الدّفاع والاقتصاد الوطنيين أو مؤسّسات الدّولة، وكذا مُساعدة السّلطات القضائيّة ومصالح الشّرطة القضائيّة في التّحريات بشأن الجرائم المعلوماتيّة، بما فيها جمع المعلومات وانجاز الخبرات القضائيّة أو جمع كلّ المعطيات المُفيدة للتّعرف على المُجرمين، وتحديد مكان تَواجُدِهم من خلال تبادل المعلومات مع نظيراتها الأجنبيّة في إطار طلبات المساعدة القضائيّة الدّولية المُتبادلة، وذلك إلى جانب المهام المذكورة في المادة 04 من المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، الذي يحدّد تشكيلة وتنظيم وكيفيات سير هذه الهيئة[1].

انطلاقا من ذلك، حدّد المشّرع بموجب المادة 04 من نفس القانون الحالات التي تسمح باللّجوء إلى المراقبة الإلكترونيّة على الاتّصالات، والمتعلّقة بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التّخريب أو الجرائم الماسّة بأمن الدّولة، وكذا توافر معلومات عن احتمال اعتداء على منظومة معلوماتيّة على نحو يُهدّد النّظام العام أو الدّفاع الوطني أو مؤسّسات الدّولة أو الاقتصاد الوطني، أو يكون ذلك لمقتضيات التّحريات والتّحقيقات القضائيّة عندما يكون من الصّعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى المراقبة الإلكترونيّة، أو في إطار تنفيذ طلبات المساعدة القضائيّة الدّولية المتبادلة.

---

[1] قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، الصادر في 16 أوت 2009.

مرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 53، الصادر في 08 أكتوبر 2015.

وعليه، يُمكِن للهيئة وفقا للمادتين 19 و20 من المرسوم الرّئاسي المذكور أعلاه، أن تستعين بأيّ خبير أو شخص يُعِينُهَا في أعمالها، وأن تَطْلُبَ من أيِّ جهاز أو مؤسّسة أو مصلحة، كلّ وثيقة أو معلومة ضروريّة لانجاز المهام المسندة إليها، حيث يجب على مقدّمي الخدمات[1] الإلتزام تحت طائلة العقوبات، بتقديم المساعدة للسّلطات القضائيّة في حالة إجراء التّحريات القضائيّة حول محتوى الاتّصالات، مع وضع تحت تصّرفها في سريّة تامّة المعطيات المتعلّقة بحركة السّير، التي يتعيّن عليهم(م.خ.إ) حفظها وفقا للمادة 11 من القانون رقم 09-04، المذكور أعلاه[2].

تُمارس "الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها"، مهامها **أصلاً** تحت رقابة السّلطة القضائيّة طبقا لأحكام التّشريع السّاري المفعول، لاسيما منها قانون الإجراءات الجزائيّة والقانون رقم 09-04، المذكور أعلاه، مع مراعاة بالخصوص الأحكام القانونيّة التي تضمن "سريّة" المراسلات والاتصالات[3]، غير أنّه

---

[1] تنص **المادة 01/د-هـ** من القانون رقم 09-04، على ما يلي:" **د- مقدمو الخدمات:**

"1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات؛

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها."

هـ- المعطيات المتعلقة بحركة السير: " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المُرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة."

[2] راجع نص المادتين 10 و11 من القانون رقم 09-04، سالف الذكر.

[3] تنص **المادة 04** من المرسوم الرئاسي رقم 15-261، على ما يلي: " تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009، تحت رقابة السلطة القضائية، طبقا لأحكام التشريع الساري المفعول، لاسيما منها قانون الإجراءات الجزائية والقانون رقم 09-04 [...] المذكور أعلاه. [...]."

تنص **المادة 03** من القانون رقم 09-04، على ما يلي: "مع مراعاة الأحكام القانونية التي **تضمن سرية المراسلات والاتصالات**، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية."

بالرّجوع إلى نص المادة 11/5-7 من نفس المرسوم الرّئاسي رقم 15-261، سالف الذكر، نجد أنّ من بين مهام "مديرية المراقبة الوقائيّة واليقظة الإلكترونيّة" التّابعة للهيئة، أنّها تقوم إلى جانب المهام الأخرى المذكورة سابقا، بتنظيم أو المشاركة في عمليات التّوعية حول استعمال تكنولوجيا الإعلام والاتّصال وحول المخاطر المتّصلة بها، وكذلك تُزَوِّد السّلطات القضائيّة ومصالح الشّرطة القضائيّة "**تلقائيّا**" أو بناء على "**طلبها**"، بالمعلومات والمعطيات المتعلّقة بالجرائم الإلكترونيّة في سريّة تامّة، حيث تُشرف على جميع "الملحقات الجهويّة" التّابعة لها وعلى "مركز العمليات التّقنيّة"، الذي تُزَوِّدُهُ بمختلف المنشآت والتّجهيزات والوسائل الماديّة، والمستخدمين التّقنيين الضّروريين لتنفيذ العمليات التّقنيّة لمراقبة الاتّصالات الالكترونيّة.

وعليه، تتمتّع "الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها" بصلاحيات واسعة في مراقبة جميع الاتّصالات الإلكترونيّة، حيث يُمكِنها مباشرة مهامها الرّقابيّة حتى ولو كان ذلك خارج إطار الرّقابة القضائيّة أو القانونيّة، وذلك لغرض تحقيق هدف "إيجابي" معمول به لدى دول العالم ألا وهو التّنبؤ بمختلف التّهديدات الإلكترونيّة(الإرهاب الإلكتروني، الجرائم المنظّمة...) التي تشّكل خطرا على النّظام العام والأمن والاقتصاد الوطنيين، أو حتّى القيام بعمليات التّجسّس على الاتّصالات الدّاخلية أو الجوسسة المُضّادة(Contre espionnage) على الاتّصالات الأجنبيّة لمقتضيات الأمن والاقتصاد الوطنيين ومؤسّسات الدّولة الخ...[1]، لكن بالمقابل نجد أن مُمارسة تلك المهام

تنص **المادة 04** من القانون رقم 09-04، على ما يلي: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية: [...]؛ لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا **بإذنٍ مكتوب** من السلطة القضائية المختصة؛ [...]."

[1] تنص **المادة 06** من المرسوم الرئاسي رقم 15-261، على ما يلي: " تضم الهيئة: – لجنة مديرة؛ – مديرية عامة؛ – **مديرية للمراقبة الوقائية واليقظة الإلكترونية**؛ – مديرية للتنسيق التقني؛ – مركز للعمليات التقنية؛ – ملحقات جهوية."
وتنص **المادة 11** على ما يلي: " تُكلف **مديرية المراقبة الوقائية واليقظة الإلكترونية** على الخصوص بما يأتي:
– تنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول؛ – إرسال

على خارج الرّقابة القضائيّة أو القانونيّة يُشّكل تعدّيا أو مساسًا بسريّة المراسلات والاتّصالات والمعطيات الشّخصيّة المحميّة بموجب القوانين الخاصّة، ونحن نَعْلَمُ أنّ المادة 09 من القانون رقم 09–04 المذكور أعلاه[1]، منعت تحت "طائلة العقوبات" المنصوص عليها في التّشريع المعمول به، استعمال المعلومات المُتحصّل عليها عن طريق عمليات المراقبة على الاتّصالات الإلكترونيّة خارج الحدود الضّروريّة للتّحريات أو التّحقيقات القضائيّة.

الفرع الرابع

مراعاة التّدابير التّقنيّة لحماية المعطيات الشّخصيّة لكلّ تشريع

لا يُمكِن معالجة المعطيات الشّخصيّة إلاّ في إطار الشّفافية والأمانة واحترام كرامة المواطن وفقا لمقتضيات التّشريعات الأساسيّة(الدّساتير) والقوانين الخاصّة بحماية المعطيات الشّخصيّة[2]، حيث كرّست مختلف التّشريعات الأجنبيّة(**أولا**) والعربيّة(**ثانيا**) مستوى ملائما من السّلامة والأمان لضمان الحماية الأمنية للمعطيات الشّخصيّة من مختلف المخاطر والتّهديدات عبر شبكة الإنترنت.

المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية؛[...]؛ – جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛[...]؛ – تزويد السلطات القضائية ومصالح الشرطة القضائية، **تلقائيا** أو بناء على **طلبها**، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال؛ – وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيدة لمنشآتها وتجهيزاتها ووسائلها التقنية؛[...]. "

[1] تنص **المادة 09** من القانون رقم 09–04، على ما يلي: " تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية."

[2] **Josef DREXL**, « Le commerce électronique et la protection des consommateurs », Revue Internationale de droit économique, 2002/2 (t. XVI), pp. 436- 440.
Nicolas TILLI, « La protection des données à caractère personnel », Revue Documentaliste-sciences de l'information, 2013/3 (Vol. 50), pp. 63- 66.

أولا– التّشريعات الأجنبيّة.

فرضت مختلف التّشريعات الأجنبيّة مجموعة من التّدابير التّقنيّة لحماية المعطيات الشّخصية للأفراد، نظرا للمخاطر التي تُمثّلها المعالجة وطبيعة المعطيات الشّخصية الواجب حمايتها، والتي سنتطرّق إليها على النّحو التّالي:

1)– التّنظيم الأوروبي رقم 679/2016 المتعلّق بحماية المعطيات الشّخصيّة:

قام المشّرع الفيدرالي للإتّحاد الأوروبي بإصدار تنظيم أوروبي رقم 679/2016 مؤرخ في 27 أفريل 2016 يتعلق بحماية الأشخاص الطبيعيّة لدى معالجة معطياتهم الشّخصيّة مع حريّة تنّقلها(RGPD)، المُلغي للتّوجيه الأوروبي رقم 95–46 المؤرخ في 24 أكتوبر 1995، الذي من خلاله أعطى بموجب المادة 04(1) منه(RGPD)، مفهوماً واسعاً للمعطيات الشّخصيّة، التي تتضمّن على كلّ معلومة تتّصل بشخص طبيعي مُعرّف أو قابل للتّعرف عليه، وتُعتبر هويّة الشّخص الطّبيعي قابلة للتّعريف بصفة مُباشِرة أو غير مُباشِرة، لاسيما بالرّجوع إلى اسمه أو رقم تعريفه أو المعطيات التي تُحدّد مَوقِعه الجغرافي GPS) (Location، أو ما يسمح بتعريف هوّيته عبر الشّبكة، أو عدّة عناصر خاصّة بهوّيته البدنيّة أو الفيزيولوجيّة أو الجينيّة أو النّفسيّة أو الاقتصاديّة أو الثّقافيّة أو الاجتماعيّة، في حين تتضمّن المعالجة الآلية وفقا للفقرة(2) من نفس المادة(2/04)(RGPD)[1]، على كلّ عملية

---

1) **Règlement (UE) 2016/679** du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et **abrogeant** la directive 95/46/CE (règlement général sur la protection des données), **JOUE L 119/1 du 4/5/2016**.

1) «**Données à caractère personnel**», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2) «**Traitement**», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la

أو مجموعة من العمليات المنجزة أم لا بواسطة طرق آلية لمعالجة المعطيات الشّخصيّة، مثل الجمع أو التّسجيل أو الحفظ أو التّنظيم أو التّغيير، أو الاستغلال أو الاستعمال أو الإرسال أو التّوزيع أو النّشر، أو أيّة عملية أخرى تهدف إلى التّقريب أو التّبادل أو التّشفير أو المحو أو الإتلاف.

وعليه، فإنّ الهدف الرئيسي من إصدار هذا التّنظيم(RGPD) يتعلق بتوسيع نطاق حماية وتأمين البيانات الشّخصية لمواطني الاتحاد الأوروبي، التي تشمل على أيّ بيانات شخصيّة حسّاسة أو أخرى متعلقة بالحالة الصحيّة، أو الأصل العرقي أو التّوجُّه الجنسي أو التّعرّف على الهويّة بشكل مباشر أو غير مباشر، بالرّجوع إلى مُعرِّف شخصي كالاسم وبيانات تحديد المواقِع الجُغرافية(GPS Location)، ومُعرِّف الإنترنت(عنوان(IP) وعنوان البريد الالكتروني والأجهزة المحمولة، وغيرها...)، أو البيانات البيومترية(فصيلة الدّم، البصمات، الحمض النّووي، الخ...)، أو الفيزيولوجيّة أو النّفسيّة والعقلية أو الاقتصاديّة أو الثّقافيّة أو الاجتماعيّة، حيث أصبح للبيانات الشّخصية تعريف أوسَع بكثير بعدما أن كان في ظل

---

communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction; […] ;

7) «**Responsable du traitement**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

8) «**Sous-traitant**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement; […] ;

11) «**Consentement**» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

12) «**Violation de données à caractère personnel**», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données; […]. »

التّوجيه الأوروبي المُلغى(رقم 46/95)، يقتصر فقط على الاسم والصورة وعنوان البريد الالكتروني ورقم الهاتف ومحل الإقامة.

يجب على المسؤول القائم بمعالجة المعطيات الشّخصيّة الحصول على الموافقة الصّريحة للشّخص المعني بمعالجة معطياته، وذلك بعد إعلامه وقبوله وفقا لإرادته الذي يملك الحرّية في الرّجوع عن الموافقة في أيّ وقت، ففي حالة ما إذا كان الشّخص المعني أقل من 16 سنة فيُشترط الحصول على موافقة وليّه الشّرعي، حيث منح مشّرع الاتّحاد الأوروبي لكلّ دولة عضوة في الإتّحاد، حرّية تحديد السّن القانوني اللاّزم للحصول على موافقة الولي الشّرعي، على أن لا يكون سّن الطّفل من تَحْتِ (13) سنة [1].

كما ألزم التّنظيم الأوروبي رقم 679/2016 بموجب المادة 25 منه(RGPD) المسؤول عن المعالجة الآلية للمعطيات الشّخصيّة، بضرورة اتّخاذ التّدابير التّقنيّة والتّنظيميّة الملائمة لحماية المعطيات الشّخصيّة المُتحصَّل عليها ضّد كلّ عمل غير مشروع، فعندما تُجرى المعالجة لحساب المسؤول عن المعالجة يجب على المُعالِج من الباطن(Sous traitant) أن يحترم الإجراءات الأمنيّة المتعلّقة بأمن وسلامة وسريّة المعطيات الشّخصيّة، وأن لا يتصّرف إلاّ في حدود تعليمات المسؤول على معالجة المعطيات الشّخصيّة، إلى جانب المتطلّبات المحدّدة بموجب المادة 28 من نفس التّنظيم(RGPD) [2].

---

1) **Art.08 (Règlement (UE) 2016/679)** : « **1.** Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est **âgé de moins de 16 ans**, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-**dessous de 13 ans**.

2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

3. Le paragraphe **1** ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant. »

2) Voir l'Art.28 (Règlement (UE) 2016/679).

انطلاقا من ذلك، يجب على المسؤول عن المعالجة، أن يلتزمَ في إطار عقد المناولة بِحُسْنِ اختيار معالج من الباطن، يُقدّم الضمانات الكافية المتعلقة بإجراءات السّلامة التّقنية والتنظيميّة للمعالجات الواجب القيام بها، ويسهر على احترامها، مع التزامه بالتّصرف وفقا لتعليمات من المسؤول عن المعالجة، كما لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن(Représentant)، القيام بمعالجة المعطيات الشّخصية من دون تعليمات المسؤول عن المعالجة، باستثناء حالة تنفيذ التزام قانوني(قانون الاتحاد الأوروبي أو أي قانون وطني لدولة عضوة فيه)[1].

بالإضافة إلى ذلك، منحت المادة 37 من نفس التنظيم(RGPD)[2]، لكلٍّ من المسؤول عن المعالجة والمعالج من الباطن، إمكانية تفويض شخص من بين أعضائها أو في إطار عقد خدمة، مُكلّف بحماية المعطيات الشّخصية، الذي يجب أن تتوافر لديه (Délégué à la protection des données) مؤهلات مهنيّة، ومعارف في مجال القانون وحماية المعطيات الشّخصية، وقُدرات تُمكِّنه من مُمارسة المهام المنصوص عليها في المادة 39 من نفس التنظيم(RGPD)، حيث يجب الاستعانة بذلك الشّخص، في حالة قيام هيئة أو سلطة عمومية بمعالجة المعطيات الشّخصية باستثناء "الجهات القضائية"، أو أنّ عملية معالجة المعطيات تتطلّب من حيث طبيعتها أو خصوصياتها متابعة الأشخاص المعنيين بصفة شاملة ودائمة، أو أنّ عملية المعالجة تتطلّب متابعة مستمرة وشاملة لفئة معيّنة من المعطيات المحدّدة بموجب المادتين 09 و10 من نفس التنظيم(RGPD)، حيث يمكن لمجموعة من الشركات أو الجمعيات أو الهيئات العمومية بصفتها كمسؤول عن المعالجة أو المعالج من الباطن، تعيين شخص واحد لحماية المعطيات الشّخصية[3].

أنظر كذلك: **مروة زين العابدين صالح**، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، بين القانون الدولي الإتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، 2017، مصر، ص ص 402– 404.

1) Voir les Arts. 28 et 32 du (RGPD).

2) Art.**37** du (RGPD) : « 1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un **délégué à la protection des données** lorsque : […]. »

3) Voir les Arts. 09 et 10 et 39 du (RGPD).

2)– القانون الفرنسي:

قام الرّئيس الفرنسي(**Emmanuel MACRON**) بإصدار الأمر رقم 2018–1125 المؤرخ في 12 ديسمبر 2018، المتعلّق بتطبيق أحكام المادة 32 من القانون رقم 2018–493 المؤرخ في 20 جوان 2018، المتعلّق بحماية المعطيات الشّخصيّة، المعدّل للقانون رقم 78–17 المؤرخ في 06 جانفي 1978، المتعلّق بالإعلام والملفات والحرّيات، الذي من خلاله طبّق أحكام التّنظيم الأوروبي رقم 679/2016 المؤرخ في 27 أفريل 2016، المتعلّق بحماية الأشخاص الطبيعيّة لدى معالجة معطياتهم الشّخصيّة مع حرّية تنّقلها(RGPD) [1].

فوفقا لأحكام المواد 04 و05 و57 من الأمر المذكور أعلاه، يجب على المسئول عن المعالجة أو المعالج من الباطن، أن لا يقوم بمعالجة المعطيات الشّخصيّة إلاّ بعد الحصول على الموافقة الصّريحة للشّخص المعني (وفقا للشّروط المحدّدة بموجب المادة 11/04 والمادة 07 من التّنظيم الأوروبي رقم 679/2016(RGPD))، وأن تتّم عملية معالجتها بطريقة مشروعة ونزيهة، وفقا للغايات التي من أجلها تّم جمعها ومعالجتها وأن لا تُعالج

1) **Loi n° 2018-493** du 20 juin 2018 relative à la protection des données personnelles, J.O.R.F, n° 0141 du 21 juin 2018.
Art.32 : « **I.** - Dans les conditions prévues à l'article 38 de la Constitution et dans le respect des dispositions prévues aux titres Ier à III de la présente loi et au présent titre, le Gouvernement est autorisé à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires : 1- A la **réécriture** de l'ensemble de la **loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées des dispositions qui mettent le **droit national** en **conformité** avec le **règlement (UE) 2016/679** du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et **abrogeant** la directive 95/46/CE et **transposent** la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, telles que résultant de la présente loi ; […]
II. - Cette ordonnance est prise, après avis de la Commission nationale de l'informatique et des libertés, dans un délai de six mois à compter de la promulgation de la présente loi. »

لاحقا بطريقة تتنافى مع هذه الغايات، مع حفظها بشكل يسمح بالتّعرف على الأشخاص المعنيين خلال المدّة اللاّزمة لإنجاز الأغراض التي من أجلها تّم جمعها ومعالجتها، وذلك باستثناء حالات حفظها في الأرشيف للمصلحة العامّة أو لغايات إجراء الدّراسات العلميّة أو التاريخيّة أو عمليات الإحصاء، كما يجب وضع التّدابير التّقنيّة والتّنظيميّة اللاّزمة لضمان حماية المعطيات الشّخصيّة من الضّياع أو الإتلاف أو الولوج غير المرّخص به أو أيّ عملية معالجة غير مشروعة لهذه المعطيات[1].

---

1) **Ordonnance n° 2018-1125** du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, J.O.R.F, n°0288 du 13 décembre 2018.

Art.04 : « -Les données à caractère personnel doivent être : **1-** Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;

2- Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3- Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;

4- Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

5- Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ;

6- Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées. »

Art. 5-1 : « - Un traitement de données à caractère personnel n'est licite que si, et dans la

في حالة لجوء المسؤول عن المعالجة إلى المناولة لمعالجة المعطيات الشّخصيّة لحسابه(المسؤول عن المعالجة)، يجب على المُعالِج من الباطن(Sous traitant) أن يقدّم في إطار عقد المناولة الضّمانات الكافية المتعلّقة بإجراءات السّلامة التّقنيّة للمعالجات الواجب القيام بها مع السّهر على احترامها، مع الالتزام بعدم التّصرف إلاّ في حدود تعليمات المسؤول على معالجة المعطيات الشّخصيّة، فعندما تتعرّض هذه الأخيرة إلى انتهاكات يجب على المسؤول عن المعالجة أو ممثّله، القيام بإخطار الهيئة الوطنية للإعلام الآلي والحرّيات(CNIL)، مع تدوين كافة هذه الانتهاكات والإجراءات المتّخذة بشأنها في جرد خاص بمعالجة المعطيات الشّخصيّة وفق الشّروط المحدّدة بموجب المادة 30 من التّنظيم الأوروبي رقم 679/2016 المذكور أعلاه(RGPD) [1].

---

mesure où, il remplit au moins une des conditions suivantes : **1-** Le traitement, lorsqu'il relève du titre II, a reçu le **consentement** de la personne concernée, dans les conditions mentionnées au 11 de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du 27 avril 2016 précédemment mentionné ; […].

1) **Art.57 (Ordonnance n° 2018-1125** du 12 décembre 2018…**)** : « - En application de l'article 24 du règlement (UE) 2016/679 du 27 avril 2016, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à ce même règlement et à la présente loi. Le responsable du traitement et, le cas échéant, son représentant tiennent le registre des activités de traitement dans les conditions prévues à l'article 30 de ce règlement. Ils désignent un délégué à la protection des données dans les conditions prévues par la section 4 du chapitre IV du même règlement. »

Art. 58-.I(Même Ordonnance) : «- Le responsable de traitement notifie à la Commission nationale de l'informatique et des libertés et communique à la personne concernée toute **violation** de données à caractère personnel en application des articles 33 et 34 du règlement (UE) 2016/679 du 27 avril 2016. […]. »

Art. 60(Même Ordonnance): «- La qualité de sous-traitant n'exonère en rien du respect des dispositions applicables du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi.

Le traitement réalisé par un sous-traitant est régi par un contrat ou tout acte juridique qui lie le sous-traitant à l'égard du responsable du traitement, sous une forme écrite, y compris en format électronique, respectant les conditions prévues à l'article 28 du règlement.

Le sous-traitant et, le cas échéant, son représentant doivent tenir le registre mentionné à l'article 30 de ce même règlement. Lorsqu'un sous-traitant a recours à un autre sous-traitant pour mener les activités de traitement spécifiques pour le compte du responsable du traitement, il conclut avec ce sous-traitant le contrat mentionné au deuxième alinéa. Le troisième alinéa s'applique également. »

3)– القانون الفيدرالي السّويسري:

قام المشرّع الفيدرالي السّويسري بإصدار قانون فيدرالي حول حماية المعطيات(LPD) في 19 جوان 1992، دخل حيّز التّنفيذ ابتداء من أوّل(01) جويلية 1993، الذي يهدف إلى حماية الحقوق الأسّاسية للأشخاص(الطّبيعيّة والمعنويّة) لدى مباشرة الهيئات الفيدرالية أو الأشخاص الخاصّة للمعالجة الآلية لمعطياتهم الشّخصية، فالمعطيات الشّخصيّة وفقا للمادة (a)/03)) من نفس القانون(LPD)، تتضمّن على كافة المعلومات المتّصلة بالشّخص الذي تم التّعريف بهويته أو قابلة للتّعريف(الهويّة).

ويُقْصَدُ بالمعالجة الآلية للمعطيات، وفقا للفقرة(e) من نفس المادة(e)/03))، أيّة عملية تُستخدم فيها الوسائل والمنظومات لغرض جمع أو حفظ أو استغلال أو تعديل أو إيصال أو تخزين أو إتلاف المعطيات، حيث يجب على المسؤول عن المعالجة مراعاة أحكام المواد 04 و1/05 و1/07 من نفس القانون(LPD)[1]، التي من خلالها يجب عليه الحصول على

---

1) **Loi fédérale sur la protection des données** (**LPD**) du 19 juin 1992, RS 235.1 (État le 1er mars 2019).

Art.39 : Référendum et entrée en vigueur **1-** La présente loi est sujette au référendum facultatif. **2-** Le Conseil fédéral fixe la date de l'entrée en vigueur. (Date de l'entrée en vigueur: 1er juillet 1993).

Art.01 : « But La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données. »

Art.03 : « On entend par: **a)- Données personnelles (données)**, toutes les informations qui se rapportent à une personne identifiée ou identifiable; **b)- Personne concernée**, la personne **physique** ou **morale** au sujet de laquelle des données sont traitées; **e)- Traitement**, toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données; […]. »

Art.04 : « Principes **1-** Tout traitement de données doit être **licite**.

2- Leur traitement doit être effectué conformément aux principes de la **bonne foi** et de la **proportionnalité**.

3- Les données personnelles ne doivent être traitées que dans le **but** qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.

4- La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée.

5- Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa **volonté**

الموافقة الصّريحة للمعني وفقا لإرادته الحرّة، وذلك قبل مباشرة عملية المعالجة الآلية لمعطياته الشّخصية، التي يجب أن تتّم في إطار مشروع مع احترام الغرض الذي جُمعت من أجله تلك المعطيات، كما ينبغي على ذلك المسؤول أن يتأكّدَ من سلامة وصحة المعطيات الشّخصيّة التي تَحَصَّلَ عليها مع اتخاذ التّدابير اللاّزمة لحذف أو تصحيح المعطيات الخاطئة أو النّاقصة وفقا للغاية التي جُمعت من أجلها، مع اتّخاذه جميع إجراءات الحماية الأمنيّة من النّاحية التّقنيّة والتّنظيميّة للمعطيات الشّخصيّة المُحصّلة ومنع أيّ نفاذٍ إليها من دون الحصول على ترخيص، في حين يتولّى المجلس الفيدرالي كسلطة تنفيذيّة في الكُنْفِيدِرَالِيَّة السّويسريّة مهمّة إعداد الأحكام الخاصّة بأمن المعطيات الشّخصيّة[1].

ثانيا– التّشريعات العربيّة.

تُحظى المعطيات الشّخصيّة بأهمّية لدى تشريعات الدّول العربيّة على غرار كل من تونس(**1**) والجزائر(**2**)، التي نصّت من خلالها على مجموعة من التّدابير التّقنيّة لحمايتها من مخاطر المعالجة.

1)– القانون التّونسي:

قام المشّرع التّونسي بإصدار القانون الأساسي عدد 63–2004 المؤرخ في 27 جويلية 2004 المتعلّق بحماية المعطيات الشّخصيّة، الذي اعتبر المعطيات الشّخصيّة بموجب

---

librement et après avoir été **dûment informée**. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite. »

[1] **Art.05(LPD)**: « **1-** Celui qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

2- Toute personne concernée peut requérir la rectification des données inexactes. »

Art.6(LPD): « **1-** Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat; […]. »

Art.07(LPD): « **1-** Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

2- Le Conseil fédéral édicte des dispositions plus détaillées sur les exigences minimales en matière de sécurité des données. »

الفصل الأوّل منه ضمن الحقوق الأساسيّة المتعلّقة بالحياة الخاصّة للأشخاص والمضمونة بموجب الدّستور، حيث لا يجوز معالجتها إلاّ في إطار الشّفافية والأمانة واحترام كرامتهم وفقا لمُقتضيات هذا القانون[1]، في حين نص الفصل 27 من نفس القانون، على عدم إمكانية معالجة المعطيات الشّخصيّة، إلاّ بعد الحصول على الموافقة الصّريحة والكتابيّة للمعني بالأمر أو وليّه في حالة ما إذا كان قاصرا أو محجورا عليه أو غير قادر على الإمضاء، إذ يمكن للمعني بالأمر أو وليّه الرّجوع عن الموافقة في أيّ وقت، وعليه يجب أن تتّم عملية جمع المعطيات لغرض تحقيق الغاية التي جُمعت من أجلها، وذلك باستثناء الحالات المذكورة في المادة 12 من نفس القانون، والمتمثّلة في مُوافقة المعني بالمعالجة الآلية لمعطياته الشّخصيّة، وما إذا كان في ذلك تحقيق مصلحة حيويّة له (المعني بالأمر) أو إذا كانت لتحقيق أغراض عِلميّة ثابتة.

2)– القانون الجزائري:

نص المشّرع الجزائري بموجب المادة 02 من القانون رقم 18–07 المؤرخ في 10 جويلية 2018 المتعلّق بحماية الأشخاص الطّبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي، على أن تتّم عملية المعالجة الآلية للمعطيات الشّخصيّة مهما كان

---

[1] القانون الأساسي عدد 63–2004 المؤرخ في 27 جويلية 2004، الذي يتعلق بحماية المعطيات الشخصية، ر.ر.ج.ت عدد 61 الصادر في 30 جويلية 2004.

ينص **الفصل 10** من القانون الأساسي، على ما يلي:" لا يجوز جمع المعطيات الشخصية إلاّ لأغراض مشروعة ومحددة وواضحة."

وينص **الفصل 11** على ما يلي:" يجب أن تتم معالجة المعطيات الشخصية بكامل الأمانة وفي حدود ما كان منها ضروريا للغرض الذي جُمعت من أجله. كما يجب على المسؤول عن المعالجة الحرص على أن تكون المعطيات صحيحة ودقيقة ومحينة."

وينص **الفصل 12** على ما يلي:" لا تجوز معالجة المعطيات الشخصية في غير الأغراض التي جُمعت من أجلها إلا في الحالات التالية: – إذا وافق المعني بالأمر على ذلك؛ – إذا كان في ذلك تحقيق لمصلحة حيوية للمعني بالأمر؛ – إذا كانت لأغراض علمية ثابتة."

مصدرها أو شكلها في إطار احترام الكرامة الإنسانيّة والحياة الخاصّة والحرّيات العامّة وألاّ تمسّ بحقوق الأشخاص وشرفهم وسمعتهم.

فالمعطيات الشّخصيّة، وفقا للمادة 03 من نفس القانون(رقم 18-07)[1]، تشتمل على كلِّ معلومة مهما كانت دعامتها، تتعلّق بشخص معرّف الهويّة أو قابل للتّعرف عليها بصفة مباشرة أو غير مباشرة، عن طريق الرّجوع إلى رقم التّعريف أو عنصر أو عدة عناصر خاصة بهوّيته البدنيّة أو الفيزيولوجيّة أو الجينيّة أو البيوميتريّة أو النّفسيّة أو الاقتصاديّة أو الثّقافيّة أو الاجتماعيّة، حيث لا يمكن القيام بعملية المعالجة الآلية لهذه المعطيات إلا بعد الحصول على الموافقة الصّريحة للشّخص المعني، الذي يملك الحرّية الكاملة في التّراجع عن موافقته في أيّة لحظة، فإذا كان ذلك الشّخص عديم أو ناقص الأهليّة فإنّ الموافقة تخضع للإجراءات المنصوص عليها في التّقنين المدني، وفي جميع الظّروف ينبغي أن تتّم عملية جمع المعطيات الشّخصيّة لغرض تحقيق الغاية التي جُمعت من أجلها وبعد الحصول على الموافقة المُسبقة للشّخص المعني، وذلك باستثناء الحالات الواردة على الموافقة المسبقة بموجب أحكام نص الفقرة الأخيرة من المادة 07 من القانون رقم 18-07[2].

---

[1] تنص المادة 03 من القانون رقم 18-07، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، على ما يلي:"[...]. "**الشخص المعني**": كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة؛

"**معالجة المعطيات ذات الطابع الشخصي**" المشار إليها أدناه "معالجة": كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل أخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف؛

"موافقة الشخص المعني": كل تعبير عن الإرادة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية؛

"المعالجة الآلية": العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها؛ [...]."

[2] راجع أحكام المواد 07 و08 و09 من القانون رقم 18-07، سالف الذكر.

انطلاقا من ذلك، ألزم المشّرع الجزائري المسؤول عن المعالجة إرساء واحترام إجراءات السّلامة التّقنيّة والتّنظيميّة لحماية المعطيات الشّخصيّة بما يتلاءم مع المخاطر المحيطة بها، فعندما تُجرى المعالجة لحساب المسؤول عن المعالجة، يجب عليه اختيار "مُعالِج من الباطن" يُقدّم الضّمانات الكافية بإجراءات السّلامة التّقنيّة والتّنظيميّة للمعالجات الواجب القيام بها مع السّهر على احترامها، حيث ينبغي على المعالج من الباطن أن لا يتصّرف إلاّ بناء على تعليمات من المسؤول على المعالجة والتّقيّد بالتزاماته العقديّة والقانونيّة، كما يجب على كل شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن، ويقوم بمعالجة المعطيات الشّخصيّة أن يَحْتَرِمَ تعليمات المسؤول عن المعالجة، وذلك باستثناء حالة تنفيذ التزام قانوني، وفي جميع الظّروف يجب على المسؤول عن المعالجة والأشخاص الذين اِطَّلَعُوا أثناء ممارسة مهامهم على المعطيات الشّخصيّة، الالتزام بالسّر المِهني حتى بعد انتهاء مهامهم وذلك تحت طائلة العقوبات المنصوص عليها في التّشريع السّاري المفعول[1].

فإذا تعرّضت المعطيات الشّخصيّة عبر شبكات الاتّصالات المفتوحة للجمهور إلى الإتلاف أو الضّياع أو إفشائها أو الولوج غير المرخّص إليها، يجب على مقدّم الخدمات(Fournisseur)، أن يقوم وفقا للمادة 43 من القانون رقم 18-07 المتعلّق بحماية المعطيات الشّخصيّة، بإخطار السّلطة الوطنيّة والشّخص المعني في حالة المساس بحياته الخاصّة، وذلك ما لم تُقرّر السّلطة الوطنيّة أنّ الضّمانات الضّروريّة لحماية المعطيات الشّخصيّة لصاحبها قد تّم اتّخاذها من قِبَلِ مُقدّم الخدمات، حيث يجب على هذا الأخير(Fournisseur) أن يكون لديه جردا محيّنا(Un inventaire à jour) حول الانتهاكات المتعلّقة بالمعطيات الشّخصيّة والإجراءات التي اتّخذها بشأنها.

تخضع عملية معالجة المعطيات الشّخصيّة لتصريح مُسبق لدى السّلطة الوطنيّة أو لترخيص منها، وذلك ما لم يوجد نص قانوني يقضي بخلاف ذلك، حيث يمكن للمسئول عن

[1] راجع أحكام المواد من 38 إلى 41 من القانون رقم 18-07 المؤرخ في 10 جويلية 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

المعالجة أن يباشر تحت مسؤوليته عملية معالجة المعطيات الشّخصيّة بمجرّد استلامه وصل الإيداع(يُسلم أو يُرسل إليه إلكترونيا في أجل أقصاه 48 ساعة)، فعندما يتبيّن للسّلطة الوطنيّة أثناء دراسة التّصريح أنّ المعالجة المعتزم القيام بها تتضمّن أخطارا ظاهرة على احترام وحماية الحياة الخاصّة والحرّيات والحقوق الأساسيّة للأشخاص، فإنها تُقرّر إخضاع المعالجة المعنيّة لنظام الترخيص المُسبق حيث يجب أن يكون القرار مُسببا مع تبليغه للمسئول عن المعالجة في أجل العشرة(10) أيام التي تلي تاريخ إيداع التّصريح[1].

المطلب الثاني
الحماية الوقائيّة للمستهلك الإلكتروني

تُتِيحُ مواقع التّجارة الإلكترونيّة للمستهلك الإلكتروني تسهيلات مُتعدّدة عبر شبكة الإنترنت، كعرض مختلف السّلع والخدمات، والقيام بعمليات البيع والشّراء مع دفع ثمن المستحقّات بطرق إلكترونيّة حديثة، وخدمات ما بعد البيع الخ...**(الفرع الأول)**، حيث تتّم هذه العمليات في بيئة إلكترونيّة افتراضيّة مملوءة بالمخاطر المتعلّقة بعمليات الاحتيال وانتشار المواقِع الإلكترونيّة الوهميّة وسرقة البيانات الإلكترونيّة وانتحال الهوّيات، التي تستوجب على المُتسوّقين اتخاذ الاحتياطات أو التّدابير الأمنيّة اللاّزمة أثناء مباشرتهم لعمليات التّسويق عبر المتاجر الافتراضيّة**(الفرع الثاني)**، والتّوعية بكلّ التّهديدات الإلكترونيّة المحتملة حيث يتعيّن عليهم الاستعانة بمعايير الحماية الأمنيّة الحديثة المستخدمة في تشفير معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة التي تتّم عبر شبكة الإنترنت**(الفرع الثالث)**، واستخدام تقنيّة التّوقيع الإلكتروني المحمي كوسيلة أمان حديثة تحقّق وظائف التّوقيع التّقليدي**(الفرع الرابع)**.

[1] راجع أحكام المواد من 12 إلى 21 من القانون رقم 18-07 المؤرخ في 10 جويلية 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

الفرع الأول
التّنوير المعلوماتي للمستهلك الالكتروني

يعتبر المستهلك الطرف الأقّل خِبرة ودِراية في مُعاملات التّجارة الإلكترونيّة والأقّل قوّة في المعادلة الاقتصاديّة، حيث أتاحت الثّورة الرّقميّة العديد من التّقنيات التّكنولوجيّة لتعريف المستهلك بمختلف السّلع والخدمات المُتاحة عبر المتاجر الافتراضيّة(**أولا**)، في حين تزايدت المخاطر التي تُهدّد المُستهلكين خاصّة بعد تطوّر أساليب الدّعاية والإعلان التّضليلي(**ثانيا**)، وكثرة عمليات الاحتيال والتّدليس حول وسائل الدّفع عبر الإنترنت(**ثالثا**).

أولا– إعلام المستهلك بالشّروط والمعلومات الضّروريّة لإبرام العقد الإلكتروني.

الالتزام بالإعلام الإلكتروني قبل التّعاقد هو التزام عام ينشأ في المرحلة السّابقة على إبرام العقد، ويهدف إلى تنوير رضاء المتعاقد الذي قُدِّمَتْ إليه تلك المعلومات، وبالتّالي فالالتزام بالإعلام لا يحتاج إلى عقد يُقرّره بل يلتزم به المُورّد الإلكتروني قبل إبرام العقد من النّاحية الشّكلية، إذ يهدف إلى تنوير وتبصير المستهلك بالمعلومات والشّروط الجوهريّة الضّروريّة التي على أساسها يتّم إبرام العقد الإلكتروني، فأيّ إخلال من جانب المُورّد الإلكتروني لهذا الواجب(الإعلام الإلكتروني) قبل إبرام العقد، يعتبر من قَبِيلِ وسائل التّدليس والاحتيال على المستهلك التي تؤدّي إلى قابلية العقد للبطلان، بينما الالتزام بالإعلام اللاّحق على التّعاقد أو التّعاقدي يترتّب عنه التزاما من العقد أو هو أثر من آثار العقد، فأيّ إخلال بهذا الالتزام لا يؤدّي إلى بطلان العقد من النّاحية الشّكليّة، ولكن يؤدّي إلى انعقاد المسؤوليّة العقديّة للمُورّد الإلكتروني[1].

---

[1] **عبد الله ذيب عبد الله محمود**، "حماية المستهلك في التعاقد الالكتروني(دراسة مقارنة)"، رسالة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009، ص ص 48، 49.

نزيه محمد الصادق المهدي، الالتزام قبل التعاقدي بالإدلاء بالبيانات المتعلقة بالعقد وتطبيقاته على بعض أنواع العقود(دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 1999، ص 15.

خالد جمال أحمد، الالتزام بالإعلام قبل التعاقد، دار النهضة العربية، القاهرة، مصر، 1996، ص 82.

وعليه، يُعتبر العرض الإلكتروني أحد التّقنيات الحديثة التي يُعوّل عليها المُورّد الإلكتروني لتنوير وتبصير المُستهلك بالمعلومات الضّروريّة المتعلّقة بإبرام العقد الإلكتروني، حيث يجب أن يُقدّم العرض الإلكتروني بطريقة مرئيّة ومقروءة ومفهومة، وأن يتضمّن على المعلومات المتعلّقة بالتّعريف بهوّية ونشاط المُورّد الإلكتروني(الأرقام المتعلّقة بالهاتف، التّعريف الجبائي، السّجل التّجاري، البطاقة المهنيّة...)، وتحديد الوصف الكامل لجميع مراحل تنفيذ المعاملة التّجارية والشّروط العامّة للبيع وما بعد البيع، وتحديد طبيعة وخصائص السّلع أو الخدمات المقترحة(باحتساب الرّسوم) وآجال العدول وطريقة إرجاع المنتوج أو استبداله أو تعويضه، وشروط البيع بالتّجريب وكيفية تأكيد الطلبيّة وإلغاءها ومصاريف وإجراءات الدّفع وشروط التّسليم والضّمان التّجاري، مع تحديد سعر المنتوج أو طريقة حساب السّعر في حالة عدم تَحْدِيدِهِ مُسبقًا في العرض الإلكتروني، وكذا تكلفة استخدام وسائل الاتّصالات الالكترونية في حالة احتسابها على أساس آخر غير التّعريفات المعمول بها، وكيفيات معالجة الشّكاوى وشروط فسخ العقد الإلكتروني[1].

ثانيا– حماية المستهلك من الإشهار الإلكتروني المُضّلل.

يتمثّل الإشهار الإلكتروني، وفقا للمادة 06/06 من القانون رقم 05/18 المؤرخ في 10 ماي 2018 المتعلّق بالتّجارة الإلكترونيّة، في كل "إعلان" يهدف بصفة مُباشِرة أو غير مُباشِرة إلى ترويج بيع السّلع أو الخدمات عن طريق الاتّصالات الالكترونيّة، حيث يجب أن يُلبّي المُقتضيات الواردة بموجب أحكام نص المادة 30 من نفس القانون، كوضوح الرّسالة الإعلانيّة التّجاريّة التي يجب أن تُحَدِّدَ الشّخص الذي تّم تصميمها (الرّسالة الإعلانيّة) لحسابه(الشّخص)، وأن لا تمّس تلك الرّسالة بالنّظام العام والآداب العامّة، وأن تُحدّدَ بوضوح ما إذا كان العرض التّجاري(تنافسيا أو ترويجيا) يشمل على تخفيضات، أو مكافآت أو هدايا

[1] للمزيد من المعلومات حول الموضوع، راجع أحكام نصوص المواد من 10 إلى 15، من القانون رقم 18–05 المؤرخ في 10 ماي 2018، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

مع التّأكد من أن جميع الشّروط الواجب استيفاؤها للاستفادة من العرض التّجاري، "غير مُضلّلة وليست غامضة"[1].

وعليه، لم يتطرّق المشّرع الجزائري من خلال أحكام القانون رقم 18-05 المتعلّق بالتّجارة الإلكترونيّة، إلى تعريف الإشهار التّضليلي، بل نص عليه صراحة بموجب أحكام نص المادة 28 من القانون رقم 04-02 المؤرخ في 23 جويلية 2004 المُحدّد للقواعد المطبّقة على الممارسات التّجاريّة، التي من خلالها اعتبر كل إشهار تضليلي إشهارا ممنوعا وغير شرعي، في حالة ما إذا تضمّن على تصريحات أو بيانات أو تشكيلات يمكن أن تؤدّي إلى التّضليل بتعريف منتوج أو خدمة أو بكمّيته أو وفرته أو مميّزاته، أو يتضّمن الإشهار التّضليلي على عناصر من شأنها أن تؤدّي إلى الالتباس مع بائع آخر أو مع منتوجاته أو خدماته أو نشاطه، أو يتعلّق ذلك الإشهار بعرض معيّن لسلع أو خدمات في حين أنّ العون الاقتصادي لا يتوّفر على مخزون كاف من تلك السّلع، أو لا يمكنه ضمان الخدمات التي يجب تقديمها عادة بالمقارنة مع "ضخامة الإشهار"[2].

---

[1] تنص **المادة 06/06** من القانون رقم 18-05، الذي يتعلق بالتجارة الإلكترونية، على ما يلي:" الإشهار الإلكتروني: كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتصالات الالكترونية."
راجع كذلك أحكام نصوص المواد من 30 إلى 34 من القانون رقم 18-05، سالف الذكر.

[2] قانون رقم 04 -02 مؤرخ في 23 جويلية 2004، يحدد القواعد المطبقة على الممارسات التجارية، ج ر عدد 41، الصادر في 27 جويلية 2004، معدل ومتمم.
تنص المادة 03 على ما يلي:" يقصد في مفهوم هذا القانون بما يأتي:"[...]؛
3- إشهار: كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع السلع أو الخدمات مهما كان المكان أو وسائل الاتصال المستعملة؛ [...]."
تنص المادة 28 على ما يلي:" دون الإخلال بالأحكام التشريعية والتنظيمية الأخرى المطبقة في هذا الميدان، يعتبر إشعار غير شرعي وممنوعا، كل إشهار تضليلي، لاسيما إذا كان:
- يتضمّن تصريحات أو بيانات أو تشكيلات يمكن أن تؤدي إلى التضليل بتعريف منتوج أو خدمة أو بكميته أو وفرته أو مميزاته،
- يتضمن الإشهار التضليلي على عناصر يمكن أن تؤدي إلى الالتباس مع بائع آخر أو مع منتوجاته أو خدماته أو نشاطه،

كما تطرّق المشّرع الفيدرالي للاتّحاد الأوروبي، بموجب المادة 02/(b) من التّوجيه الأوروبي رقم 114/2006 المؤرخ في 12 ديسمبر 2006 المتعلّق بالإشهار المُضّلل والإشهار المُقارن، إلى تعريف الإشهار المُضّلل على أنّه أي إعلان خادع يكون القصد من وراءه تضليل الأشخاص الذين تّم تصميم الرّسالة الإشهاريّة لحسابهم، حيث يُؤثّر على سلوكهم الاقتصادي ويُلحق الضّرر بالشّخص المُنافس[1]، في حين يُؤخذ بعين الاعتبار في عملية تحديد الإشهار المُضّلل، المواصفات المتعلّقة بطبيعة السّلع والخدمات المُروّج لها ومكوّناتها وتاريخ الصُّنع أو تنفيذ الخدمة، مع تحديد طريقة الاستعمال والكمّية والمصدر الجغرافي أو التّجاري لها، والنتائج المَنْتَظَرَة أو المَرْجُوَّةِ من الاستعمال أو النتائج والخصائص الضّروريّة لعمليات التّجريب(Tests) أو الرّقابة التي تمّت على السّلعة أو الخدمة، وكذلك السّعر أو طريقة تحديده(السّعر) وشروط تقديم السّلع أو الخدمات، مع تحديد طبيعة وصِفَاتِ

– يتعلق بعرض معين لسلع أو خدمات في حين أنّ العون الاقتصادي لا يتوفر على مخزون كاف من تلك السلع أو لا يمكنه ضمان الخدمات التي يجب تقديمها عادة بالمقارنة مع ضخامة الإشهار."

1) Directive 2006/114/CE du parlement européen et du conseil du 12 décembre 2006 en matière de publicité trompeuse et de publicité comparative (version codifiée), J.O.U.E, L 376/21 du 27/12/2006.

Art. 02 : « Aux fins de la présente directive, on entend par:

a)- «**Publicité**», toute forme de communication faite dans le cadre d'une activité commerciale, industrielle, artisanale ou libérale dans le but de promouvoir la fourniture de biens ou de services, y compris les biens immeubles, les droits et les obligations;

b)- «**Publicité trompeuse**», toute publicité qui, d'une manière quelconque, y compris sa présentation, induit en erreur ou est susceptible d'induire en erreur les personnes auxquelles elle s'adresse ou qu'elle touche et qui, en raison de son caractère trompeur, est susceptible d'affecter leur comportement économique ou qui, pour ces raisons, porte préjudice ou est susceptible de porter préjudice à un concurrent;

c)- «**publicité comparative**», toute publicité qui, explicitement ou implicitement, identifie un concurrent ou des biens ou services offerts par un concurrent;[…]. »

Art.10 : « La **directive 84/450/CEE est abrogée**, sans préjudice des obligations des États membres en ce qui concerne les délais de transposition en droit interne et d'application des directives indiqués à l'annexe I, partie B. Les références faites à la directive abrogée s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à **l'annexe II**. »

Art.11 : « La présente directive entre en vigueur le 12 décembre 2007. »

وحُقوق الشّخص المَعْلِنُ على غرار هوّيته، مؤهّلاته وممتلكاته وحقوق ملكيته الأدبيّة والصّناعيّة والتّجاريّة والجوائز (Prix) التي تحصّل عليها أو مُميّزاتها[1].

وعليه، تعتبر إعلانات روابط الإحالة الخادعة (Email de Malware, Phishing, Arnaques de brouteurs, etc.) ، من بين التّقنيات الحديثة التي يُعَوَّلُ عليها لنشر الإعلانات المُضّللة عبر مواقِع التّجارة الإلكترونيّة، في حين تُمثّل إعلانات الرّوابط عبر منصّة التّواصل الاجتماعي (Facebook) أحد الأساليب التي يعتمد عليها كثيرا المُحتالين لممارسة الأنشطة التّجاريّة غير المشروعة[2]، التي من خلالها يتّم تزويد المستهلكين

---

1) **Art. 03(Directive 2006/114/CE** du parlement européen et du conseil du 12 décembre 2006 en matière de publicité trompeuse et de publicité comparative**)** : « Pour **déterminer si une publicité est trompeuse**, il est tenu compte de tous ses éléments et notamment de ses indications concernant: **a)**- les caractéristiques des biens ou services, telles que leur disponibilité, leur nature, leur exécution, leur composition, le mode et la date de fabrication ou de prestation, leur caractère approprié, leurs utilisations, leur quantité, leurs spécifications, leur origine géographique ou commerciale ou les résultats qui peuvent être attendus de leur utilisation, ou les résultats et les caractéristiques essentiels des tests ou contrôles effectués sur les biens ou les services; **b)**- le prix ou son mode d'établissement et les conditions de fourniture des biens ou de prestation des services; **c)**- la nature, les qualités et les droits de l'annonceur, tels que son identité et son patrimoine, ses qualifications et ses droits de propriété industrielle, commerciale ou intellectuelle ou les prix qu'il a reçus ou ses distinctions. »

2) **Directive 2005/29/CE** du parlement européen et du conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («**Directive sur les pratiques commerciales déloyales**»), J.O.U.E, L 149/22 du 11/6/2005.

Art. 02 : « Aux fins de la présente directive, on entend par: […] ; **d)** «Pratiques commerciales des entreprises vis-à-vis des consommateurs» (ci-après également dénommées «pratiques commerciales»): toute action, omission, conduite, démarche ou communication commerciale, y compris **la publicité** et le marketing, de la part d'un professionnel, en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs; […] ;

h) «**Diligence professionnelle**»: le niveau de compétence spécialisée et de soins dont le professionnel est raisonnablement censé faire preuve vis-à-vis du consommateur, conformément aux pratiques de marché honnêtes et/ou au principe général de bonne foi dans son domaine d'activité; […]. »

Art.5 : « (**Interdiction des pratiques commerciales déloyales) 1-** Les pratiques commerciales déloyales sont interdites.

بالمعلومات الكاذبة عن مختلف العروض التّجاريّة الإلكترونيّة وتوجيههم إلى صفحة الويب المُزيّفة، بِمُجَرَّدِ النّقر على الصّورة أو الضّغط على أحد أزرار الدّعوة المُحدّدة مُسبقا، مثل "تسوّق الآن" و"تَعرَّف المزيد" و"تسجيل" و"حجز الآن" و"تنزيل"، الخ...، لتشجيع المستهلكين على اتخاذ الإجراء الذي يَتَنَاسَبُ مع هدف التّسوق، وبالتّالي فإنّ فئة كبيرة من المُعلِنين يُفضّلون إعلانات شبكة فيس بوك، لأنّه من السّهل إنشاء أيّ إعلان كاذب أو مُزيّف ويتّم الموافقة عليه بسُرعة من طرف شركة فيس بوك، حيث أنّ هذه الأخيرة(Facebook) لا تُراجِعُ الإعلانات الجديدة بشكل عميق، بل تكتفي بالموافقة عليها ولا يَهُمُّهَا مُحتويات تلك الرّوابط ومِصداقيّتها، فمن السّهل إذًا على المُحتالِين إنشاء إعلانات تجاريّة مُضلّلة والتّلاعب بالعروض التّجاريّة والتّحايل على أسماء النّطاقات، فبِمجرّد النّقر على أحد هذه الإعلانات يجد المُستهلك نَفْسَهُ في صفحة ويب مَلغُومة وغير صحيحة وعلى اسم نطاق مُختلف[1].

2- Une pratique commerciale est déloyale si: **a)** elle est contraire aux exigences de la diligence professionnelle, et **b)** elle altère ou est susceptible d'altérer de manière substantielle le comportement économique, par rapport au produit, du consommateur moyen qu'elle touche ou auquel elle s'adresse, ou du membre moyen du groupe lorsqu'une pratique commerciale est ciblée vers un groupe particulier de consommateurs. **3-** Les pratiques commerciales qui sont susceptibles d'**altérer** de manière substantielle le comportement économique d'un groupe clairement identifiable de consommateurs parce que ceux-ci sont particulièrement vulnérables à la pratique utilisée ou au produit qu'elle concerne en raison d'une infirmité mentale ou physique, de leur âge ou de leur crédulité, alors que l'on pourrait raisonnablement attendre du professionnel qu'il prévoie cette conséquence, sont évaluées du point de vue du membre moyen de ce groupe. Cette disposition est sans préjudice de la **pratique publicitaire** courante et légitime consistant à formuler des déclarations exagérées ou des déclarations qui ne sont pas destinées à être comprises au sens littéral. **4-** En particulier, sont déloyales les pratiques commerciales qui sont: **a)** trompeuses au sens des articles 6 et 7, ou **b)** agressives au sens des articles 8 et 9. **5- L'annexe I** contient la liste des pratiques commerciales réputées déloyales en toutes circonstances. Cette liste unique s'applique dans tous les États membres et ne peut être modifiée qu'au travers d'une révision de la présente directive. »

Voir aussi : l'Art. **L121-1** du **Code de la consommation**(**France**) - Dernière modification le 10 novembre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www/legifrance.gouve.fr

[1] للمزيد من المعلومات حول الموضوع، أنظر: **أمناي أفشكو**، "إعلانات فيس بوك: أفضل وسيلة لنشر الأخبار المزيفة والفيروسات"، مقال منشور بتاريخ 06 مارس 2017، عبر الموقع الإلكتروني التالي: https://www.google.com/amp/s/www.amnaymag.com/ (تم الاطّلاع عليه في 10 سبتمبر 2018.)

ثالثا– الإخطار عن النّشاطات المشبوهة حول استعمال بطاقة الائتمان الذّكيّة.

تعتبر سرقة أرقام البطاقات المصرفية الذّكيّة وبياناتها من أهم المخاطر التي تَشغل بال المستهلكين، حيث يتفنّن أصحاب الاختصاص في عمليات الاحتيال والنّصب على أصحاب بطاقات الائتمان المصرفيّة، أو في عمليات اختراق قواعد بيانات المتاجر الافتراضيّة التي تّم فيها حفظ جميع البيانات السّريّة لبطاقات الائتمان الذّكيّة، وبالتّالي يجب على المستهلك باعتباره مسئول عن استخدام بطاقته الإلكترونيّة المصرفيّة، أن يقوم في حالة ما إذا شّكك أو معاينة أيّ نشاط مشبوه يتعلّق باستعمال بطاقته المصرفيّة من طرف الغير، بإخطار الجهة المصرفيّة المُصدِرة لهذه البطاقة، من أجل اتّخاذ التّدابير اللاّزمة لإيقاف البطاقة المصرفيّة في أقرب وقت مُمكِن، حيث يجب على المُورّد الإلكتروني أن يقوم بنفس الإخطار في حالة اكتشافه لأيّة عملية اختراق لقواعد بيانات متجره الافتراضي، التي تّم فيها حفظ بيانات البطاقات المصرفيّة الإلكترونيّة.

الفرع الثاني
التّسوق الآمن عبر شبكة الإنترنت

لقد أصبح المستهلك في ظل بيئة الإنترنت وتحكّم تقنيات الثورة الرقمية على إستراتيجيات التسويق وتطبيقات التّجارة الإلكترونيّة، عُرضةً لمختلف المخاطر أو الهجمات الإلكترونيّة المنّفذة من طرف أشخاص مجهولة عبر بيئة الكترونيّة افتراضيّة معقّدة، حيث يجب على المستهلك قبل مباشرة إجراءات الشّراء عبر مواقع التّجارة الإلكترونيّة أن يحترم إجراءات التّسويق الآمنة التي نتطرّق إليها على النّحو التّالي:

أولا– التّعامل مع المتاجر الافتراضية الموثوقة والتّأكد من مصدرها:

يعتمد القراصنة كثيرا على أساليب الهندسة الاجتماعيّة للتّحايل أو انتحال الهوّيات الحقيقيّة لعناوين أسماء مواقع التّجارة الإلكترونيّة (IP spoofing, DNS spoofing, Cross-Site Scripting(XSS), etc.)، من خلال إحداث روابط لمواقع تجاريّة إلكترونيّة وهميّة متشابهة مع المواقع الأصليّة من حيث معايير الإعداد والتّصميم التي عادة لا تثير الشّكوك أو الانتباه فيها، حيث تُستخدم من أجل إغراء أو إيهام المُتسّوقين أو العملاء المستهدفين

بحقيقة الأمر لغرض الحصول على معلوماتهم السّريّة، التي تفسح المجال فيما بعد لأصحاب الاختصاص(Hacker) للقيام بعمليات تجاريّة غير مشروعة[1].

فبمجرّد أن يقوم العميل أو صاحب البطاقة المصرفيّة بالضّغط على رابط الموقع الإلكتروني المقلّد أو المُزوّر، تظهر له على الواجهة الأماميّة لصفحة ويب المصرف على أنّها فعلاً تلك التي كانت تظهر له عادة عند أو أثناء تصفّحه للموقع الحقيقي المؤمّن للمصرف، أي أنّ صفحة ويب الموْقِع المُزوَّر تحتوي فِعْلاً على بروتوكول الاتّصال المؤمّن(https://)، وذلك لغرض فقط إيهام أو جذب الشّخص المستهدف والحصول على معلوماته أو بياناته السّريّة المتعلّقة ببطاقة الائتمان أو بطاقة الضّمان الاجتماعي الخ...، حيث يُحال(العميل أو المستهلك) بعدها مباشرة إلى الموقِع الحقيقي المؤمّن للمصرف الأصلي من دون علم الضّحية بذلك[2]، فمن الصّعب إذًا على أيّ شخصٍ مهما كَانَ، أن يُدرِكَ ذلك ما لم يَقُمْ بالتّأكد من مدى موثوقيّة الموقع الإلكتروني المؤمّن.

لذا يجب على المستهلك أن يتأكّد مُسبقا من سلامة وصّحة أسماء المواقع التّجاريّة الإلكترونيّة ومن موثوقيتها، حيث أنّ بروتوكولات عناوين المواقع الإلكترونيّة المؤمّنة تكون على نحو(https://) بدلاً من صيغة(http://)، أي أنّها تتضمّن دائما على حرف أمن((Secure(S))، فبالرّغم من تأمين المواقع الإلكترونيّة بهذه الصّيغة إلاّ أنّ المستهلك يجب أن يأخذ الحيطة والحذر قبل تصفّح الموقع الإلكتروني المؤمّن، من خلال التّأكد من مصدره وموثوقيّته ومدى احتواءه على قفل(Cadenas)، يحتوي على شهادة تصديق إلكترونيّة سارية

---

[1] **بشار محمود دودين، محمد يحيى المحاسنة**، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص ص 257– 260.

رضا متولي وهدان، النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية(دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي)، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2008، ص ص 16، 17.

[2] **Pierre-HUGUES VALLÉE et Ejan MACKAAY**, « La confiance, sa nature et son rôle dans le commerce électronique », Revue Lex Electronica, vol. 11 n° 2 (Automne / Fall 2006), p. 29.

المفعول تضمن بموجب بياناتها مصداقيّة محتوى الموقِع الالكتروني وأنّه فعلاً مؤمّن، حيث تعتبر هذه الخُطوة من بين الخطوات الأولى الرّئيسيّة التي يجب على المستهلك مباشرتها قبل تصفّح صفحات الموقع التّجاري واتّخاذ قرار الشّراء مع دفع قيمة المنتجات عبر الإنترنت[1].

ثانيا– تفادي الرّوابط المُزيّفة لرسائل البريد الإلكتروني:

يجب على المستهلك أن يتوّخى الحذر عند القيام بفتح روابط انطلاقا من البريد الإلكتروني لضمان عدم استدراجه إلى مَوقِع إلكتروني مقلّد أو مزوّر، وأن يَجْتَنِبَ عمليات فتح مُلحقات الرّسائل الإلكترونيّة لتفادي الإصابة بمختلف الفيروسات والبرامج المعلوماتيّة الخبيثة أو الضّارة، والقيام بتعطيل ميزتي التّشغيل(Autorun) والقراءة(Auto play) التّلقائيتين في جميع الأجهزة[2] ضمن نظام التّشغيل(Windows)، كما يجب عليه أن يتفادي قراءة محتوى رسائل الاصطياد الخادعة أو الضّغط على الرّوابط المُلحقَة بها لأنّ الشّركات المصرفيّة لا تقوم أبدًا بإرسال هذا النّوع من الرّسائل إلى عملائها[3].

ثالثا– تَجنُّب حَفظ البيانات الإلكترونيّة في المواقع الإلكترونيّة:

غالبا ما تشترط مواقع التّجارة الإلكترونيّة على المستهلك القيام بإجراءات التّسجيل سواء عند الدّخول إلى الموقع أو أثناء مباشرة المستهلك لإجراءات الشّراء، حيث يجب على المستهلك في كلتا الحالتين أن يتجنّب عملية تسجيل أو حفظ بياناته الإلكترونيّة عبر مُتصفّح الويب الذي عادة ما يطلب فِعْلَ ذَلِكَ من المُسْتَهْلِكِ(Navigateur Web)، أو عبر قاعدة بيانات الموقِع التّجاري الإلكتروني، وذلك لتفادي اللّجوء في كل مرّة إلى إعادة كتابة نفس البيانات الإلكترونيّة(كلمة السّر، بيانات البطاقة المصرفيّة، المعطيات الشّخصيّة...).

---

[1] **ناصر خليل**، مرجع سابق، ص ص 273– 278.

[2] **Jérôme DENIS**, « L'informatique et sa sécurité. Le souci de la fragilité technique », Revue Réseaux, 2012/1, n° 171, p. 170.

[3] Voir le lien « Avertissement de courriel frauduleux » sur CIBC: https://www.cibconline.cibc.com/bvtrx01/script-root-tran/authentication/PreSignOn.cibc?locale=fr_CA, consulté le 05/02/2019.

والجدير بالذكر، أنّ الكثير من مُتصّفحي مَواقِع التّجارة الإلكترونيّة يقومون بتسجيل وحفظ كلمات المرور بصفة تِلقائيّة في ملفات الكوكيز أو سجّلات المتصّفح(Cookies)[1] ممّا يُسهّل مُهمّة العثور عليها من قِبَلِ القراصنة، الذين يتفنّنون في تقنيات التّلاعب مع أرقام البطاقات المصرفيّة الذّكيّة والقيام بعمليات تحويل الأموال بطرق غير مشروعة وفي سريّة تامّة من دون علم أصحابها، حيث يجب على المستهلك أن يتفادى كلّ ذلك والسّعي إن قام بذلك(تسجيل بياناته الإلكترونيّة) على إلغاء ملفات الكوكيز (Cookies) للمتصّفح بانتظام، مع التّأكد من عدم حفظ المتصّفح بسجّل الدّخول حيث تُشّكل ملفات الكُوكيز المصدر الحقيقي لتنفيذ الهجمات الإلكترونيّة عبر شبكة الإنترنت.

رابعا– استخدام كلمات مرور قويّة:

يجب على المستهلك أن يقوم بتشفير جميع مراسلات بريده الإلكتروني عبر شبكة الإنترنت، مع حماية كلّ البيانات الحسّاسة له التي يحتويها جهاز الحاسوب(القرص الصّلب) أو التي تم تخزينها في أجهزة التّخزين المحمولة[2]، من خلال إتّباع إستراتيجيّة كلمات مرور مُحكمة معقّدة وطويلة التي تُسْتَخْدَمُ فيها سِلْسِلَة من مختلف الأرقام والرّموز، والصِّيغ الخاصّة والألفاظ أو المصطلحات غير المعروفة أو ليس لها وجود عبر معاجم اللّغات المقروءة أو المكتوبة، وذلك للتّصدي لمختلف هجمات مُصّدع كلمات المرور (Prévention des attaques par BruteForce Hybride)، فأغلبية مواقع الإنترنت تَشترِط على المستخدمين استعمال كلمات مرور مؤمّنة لا يقّل عَدَد مُكَوِّنَاتِهَا عن ثمانية(08) على الأقل، تتضمّن على خليط من الحروف والأرقام والرّموز الخاصّة، وفي حالة استخدام الكلمات يجب ألا تكون من

---

1) Les cookies sont des petits fichiers stockés dans la mémoire des ordinateurs gérés par des responsables d'application et permettant de conserver une trace des actions de l'utilisateur du terminal sur cette application. ce sont les cookies qui servent notamment lors d'une navigation sur internet pour analyser les préférences d'un utilisateur, […]. ⇒ **Fabrice MATTATIA**, op.cit., pp. 24, 25, 44, 45.

2) **سوسن زهير المهتدى**، مرجع سابق، ص ص 391، 392.

الكلمات التي يُمكن إيجادها باستخدام القواميس، وألاّ يكون جزء من الكلمات المُستخدمة اختصارًا أو اسمًا لشيء معروف كاسم العائلة أو يُشْبِهُ اسم المستخدم ذاتّه.

وعليه، فإنّ مواقع التّجارة الإلكترونيّة عَادَةً ما تَطْلُبُ من المُستهلِكين إتّباع إجراءات التّسجيل سواء قبل الدّخول إلى الموقع الإلكتروني، أو التّسجيل باعتباره كجزء من عملية الشّراء، الأمر الذي يَدْفَعُ بالمُستهلكِ إلى إدخال عنوان بريده الإلكتروني أو اسم المستخدم الخاص به مع كلمة السّر أو المرور، حيث يجب أن تستجب هذه الأخيرة للمُمَيِّزَاتِ التّالية[1]:

أ– وضع كلمة مرور صعبة التّخمين: يجب على المستهلك عند إحداث كلمة السّر الخاصّة به أن يتجنّب استخدام اسم العائلة وتاريخ ميلاده أو التّواريخ المهمّة لديه، الخ...، حيث يتعيّن عليه دمج الأحرف والأرقام التي يختارها عشوائيا مع إضافتها بعض الرّموز والإشارات الخ...، وذلك لجعل كلمة المرور قويّة وصعبة الاختراق.

ب– تغيير كلمة المرور بانتظام: لتأمين عمليات الشّراء التي يقوم بها المستهلك عبر مواقع التّجارة الإلكترونيّة، يجب عليه أن يقوم في كل مرّة بتغيير كلمة المرور الخاصّة به التي يستعملها سواء عند الدّخول إلى الموقع الإلكتروني أو أثناء تنفيذه لإجراءات الشّراء عبر المتجر الافتراضي.

ج– وضع كلمة مرور مختلفة لكلّ مَوقِع إلكتروني: يجب على المستهلك أثناء قيامه بزيارة أو تصّفح عدّة مواقع إلكترونيّة أن يتجنّب استخدام كلمة المرور نَفْسَهَا على نحو مُتكرِّر، وذلك لمنع القراصنة من الحصول عليها واختراق جميع حساباته الالكترونيّة وبالتّالي القيام بالعمليات غير المشروعة من دون علمه بذلك.

---

[1] للمزيد من المعلومات حول الموضوع، أنظر:

علي وديع حسن، "كيف تختار كلمة مرور قوية قدر الإمكان لتحمي نفسك من الاختراق ؟"، مقال منشور في 24 أغسطس 2018، عبر الموقع الإلكتروني التالي: https://www.tech247.me/how-to-choose-a-password/ (تم الاطّلاع عليه في 2019/02/20.)

خامسا– حماية أجهزة التَّسَوُقِ الشّخصي للمُستهلك:

يمكن للمستهلك أن يقوم بعملية التّسوق عبر مواقع التّجارة الإلكترونيّة باستخدام جهاز حاسوب منزلي أو محمول(Ordinateur portable)، أو هاتف ذكي(Smartphone)، أو لوحة إلكترونية(Tablette) أو حتّى ساعة ذكيّة(Montre intelligente(Smart Watch)) وما غير ذلك، في حين تتّم عمليات التّجارة الإلكترونيّة في بيئة افتراضيّة مملوءة بالمخاطر والتّهديدات الإلكترونيّة على غِرار البرمجيات الخبيثة الضّارة، الفيروسات، الرّسائل الخادعة، الخ...، حيث لا يستطيع أيّ جهاز أو برنامج معلوماتي أن يَضْمَنَ درجة ثقة أو أمان عالية تَصِلُ إلى نِسبة مَائَة بِالمائَة(100%)، والتي من المُستحيل تحقيقها من النّاحية العمليّة أو التّقنيّة، وللتّقليل من هذه المخاطر يتعيّن على المستهلك اتخاذ تدابير الحماية الأمنيّة اللاّزمة في جهاز تسوّقِه، قبل مباشرته لنشاطات التّسوق عبر مواقع التّجارة الإلكترونيّة، حيث أنّ أغلبية المستهلكين يتجاهلون أو لا يهتّمون عادة بحيثيات الحماية الأمنيّة، ممّا يؤدّي بهم إلى تحمّل نتائج غير مرغوبة فيما بعد[1].

وعليه، يجب على المستهلك تحصين نظام التّشغيل ببرنامج جدار الحماية(Firewall) الخاص بجهاز تسوّقه الشّخصي، مع تدعيمه بأحدث البرامج المضّادة للفيروسات والبرمجيات الضّارة، التي تُزِيد الحماية في مُواجهة انتشارها وكَشفها والعمل على انتزاعها أو إلغاءها إن أَمْكَنَ بصفة نهائيّة في جهاز الحاسوب وأجهزة التّخزين المتّصلة به، ولضمان الحماية التّامة لأجهزة التّسوّق الإلكتروني الشّخصي، يجب على مُستخدمِيها الاستعانة بخدمات برامج الحماية الأمنيّة غير المجانيّة، وذلك لغرض استيفاء جميع مستويات الأمان المتطلّبة في معاملات التّجارة الإلكترونيّة والمحافظة على تنزيل تحديثاتها بصيغتها الأصليّة

---

1) Afin de se tenir à jour des « **dernières vulnérabilités** » logicielles existantes, il est important de consulter chaque jour quelques flux d'informations relatifs à la sécurité informatique tels que ceux cités ci-dessous :
http://www.cert-ist.com/fra/rss/advisories.xml et http://www.cert-ist.com/fra/rss/vigilance.xml et http://www.exploit-db.com/rss.php et http://www.secuobs.com/rss/btxml10.xml et http://www.secuobs.com/rss/vwxml10.xml et http://securityvulns.com/exploits/rss.asp et http://www.securityfocus.com/vulnerabilities et http://www.securityfocus.com/archive/1

وتثبيتها باستمرار، مما يُساعد ذلك أكثر في القضاء على الثّغرات الأمنيّة المُتواجِدة عبر نُظم التّشغيل، وتفادي الإصابة بمختلف الفيروسات والبرامج المعلوماتيّة الضّارة، وعليه تُعتبر أنظمة تشغيل(Linux, OS X, Open Office, etc.) حسب خبراء أمن تكنولوجيا المعلومات والاتصال، الأقل عُرضة لمخاطر وتهديدات الإصابة بمختلف البرمجيات الضّارة[1].

سادسا– تحديث البرمجيات الخاصّة بجهاز التّسوق الشّخصي:

إنّ أكبر مخاطر الشّبكة الافتراضيّة تمسّ بكِثرة نُظُمِ تشغيل أجهزة حاسوب العملاء أو المستهلكين كمُستهدفين حقيقيين لعمليات التّجسّس والاختراق، أو التّسلّل إلى قواعد بياناتهم من خلال نشر أو زرع مختلف البرمجيات المعلوماتية الخبيثة مُستغلين في ذلك الثّغرات الأمنية المتواجدة في نُظم الحِماية، التي تُتيح أو تُسهّل للقراصنة إمكانية التّحكّم والسّيطرة على أجهزة الحاسوب عن بُعد، من أجل القيّام بما يجب فِعْلُهُ من أعمال إجراميّة من دون علم أصحابها بما يَجْرِي، فإذا عَلِمُوا في الحالة العكسيّة فإنّما يُكتشف ذلك على مُجرّد الصُدْفَة، ولتفادي كل ذلك، يجب على المستهلك أن يقوم بتحديث برامج جهاز تسوّقه الشّخصي بانتظام (Système d'exploitation, Anti virus-Malwares, Navigateurs, etc.)، وذلك وفقا لنسخته الأصليّة الصادرة من الشّركة المُورّدة لَهُ.

سابعا– الاستعانة بمراكز الاسترشاد الوطنيّة لأمن المعلومات:

استحدثت غالبية الدّول لدى الوكالات الوطنيّة للأمن والسّلامة المعلوماتية وكذا الإدارات العموميّة والشّركات والمؤسّسات الصّناعيّة الخ...، مراكز استرشاد لأمن المعلومات (Computer Emergency Response Teams(**CERT**)) للتّنبؤ أو الإنذار والدّفاع ضدّ

---

[1] **Marc ZAFFANI**, « OS X, IOS, Windows: quels sont les systèmes les plus vulnérables ? », article publié sur futura-sciences.com, le 26/02/2015. https://www.futura-sciences.com/tech/actualites/technologie-osx-io/, consulté le 23/01/2016.
Dave TAYLOR, « Pour quoi Linux est meilleur que Windows ou macOS pour la sécurité », article publié le 19/02/2018 sur le site: https://www.global-informatique-securite.com/2018/02/19/, consulté le 02/03/2018.

التّهديدات والهجمات الإلكترونيّة التي تُشكّل خطرا على الأمن والاقتصاد الوطنيين[1]، حيث تشرف هذه المراكز(CERT) على المهام المتّعلقة بإعداد وتنظيم مخطّطات التّوعية لمستخدمي الشّبكات والأنظمة المعلوماتيّة(الشّركات، المُستهلك، الخ...)، من خلال نشر تقارير متاحة للجمهور تتضمّن على جميع المعلومات الضّروريّة التي من شأنها أن تُقلِّصَ من احتمالات الإصابة بمختلف الهجمات الإلكترونيّة أو تضع حدّ لها، وكذا القيام بجمع المعلومات المتّعلقة بمختلف التّهديدات أو الهجمات الإلكترونيّة لمعالجتها وبحث كيفيات التّصدي لها، والمُساهمة في تنسيق التّعاون مع المراكز الأجنبيّة(CERTs) المثيلة لها، من خلال تبادل المعلومات وإعداد الخُطط والدّراسات التّقنيّة الخاصّة بأمن أنظمة المعلومات والشّبكات، وإعداد وصيانة قاعدة بيانات خاصّة بمختلف الثّغرات والتّهديدات الإلكترونيّة التي تُشكّل خطرا على الأنظمة والشّبكات، وتنسيق الجهود مع مقدمي خدمات الإنترنت والمراكز الأخرى المتخصّصة في أمن الشّبكات الخ... [2].

ثامنا– عدم التسوّق عبر شبكات الاتصال اللاسلكية غير المؤمنة(Wifi):

تتوّفر خدمة الويفي(Wi-Fi) حاليا بصفة مجّانية كميزة إضافية تُتيحها الشّركات لجذب العملاء على استخدام خدماتها، حيث تتواجد هذه الخدمة عبر العديد من الأماكن مثل

---

1) **Solange GHERNAOUTI, Christian AGHROUM**« Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité », Revue Sécurité et stratégie 2012/4 (n°11), pp. 76, 77.

2) Les **Centres d'alerte** et de **réaction** aux attaques informatiques(**CERTs**), sont destinés aux entreprises ou aux administrations, dont les informations sont généralement accessibles à tous. Il existe plusieurs CSIRT : **En France** : - le CERT-FR est un organisme français qui participe à la mission d'autorité nationale de défense des systèmes d'information de l'ANSSI;
- Le CSIRT-BNP Paribas est le CSIRT dédié au groupe BNP Paribas ;
- Le CERT Crédit Agricole est le CSIRT dédié au groupe Crédit Agricole ;
- Le CERT CYBERPROTECT est le CSIRT privé de la société Cyberprotect ouvert à l'ensemble des entreprises et des institutions ; etc.
En Belgique : Le CERT.be est le CERT fédéral géré par le Centre de la Cybersécurité Belgique, celui-ci est chargé de détecter, observer et analyser les problèmes de sécurité en ligne ainsi que d'informer en permanence les utilisateurs à ce sujet, etc.
En Suisse : Le Switch-CERT est employé par Switch, fondation responsable du réseau informatique universitaire, etc.

المطارات والفنادق والمقاهي ومراكز التّسوق والمطاعم والمباني الحكوميّة، الخ...، التي لا تمتلك لإجراءات الحماية الكافية لشبكة الويفي التي تكون عُرضة للمُتسلّلين والمُحتالين الذي يقومون بعمليات الاختراق والتّنصت للوصول إلى المعلومات المُستهدفة، لذا يُوصي خبراء أمن المعلومات[1]، المستهلكين عند القيام بعملية التّسوق عبر شبكة الويفي بالاستعانة بالشّبكات الإفتراضيّة(VPN) التي من خلالها يتّم تشفير جميع معاملاته الإلكترونيّة(الرّسائل، المعاملات المصرفيّة) عبر قنوات اتصال مؤمّنة من دون أن يتجسّس عليها أحد.

تاسعا– الاحتفاظ بأمر الشّراء الإلكتروني:

عند إتمام المستهلك لعملية الشّراء من المتجر الافتراضي، يقوم المورّد الإلكتروني بإرسال بريد إلكتروني للمستهلك يحتوي على أمر شراء يؤكّد من خلاله عملية الشّراء، حيث يجب على المُستهلِك أن يقوم بطباعة أو حتى تصوير أمر الشّراء مع الاحتفاظ به في وسيلة إلكترونيّة آمنة، لكي يستعين به(أمر الشّراء) المُستهلِك كدليل إثبات عند تَفَقُّدِهِ للبِضاعة حين استلامها، والتّأكد من مدى مُطابقتها تَمَامًا للبضاعة المَطْلُوبَةِ[2].

عاشرا– تفادي التَّسوُق عبر سلاسل البيع الهرمي:

يجب على المستهلك أو المشتري أن يتفادى سلاسل التّسويق غير القانونيّة التي تعتمد عليها الشّركات أو الأشخاص، كأسلوب بيع هرمي للاحتيال على الأفراد والحصول على حسابهم لأرباح وثروات خياليّة تُقدّر بالبلايين(01Billion= mille milliards)، أو التريليونات((01Trillion= milliard des milliards)، حيث لا يستفيد منها سوى الشّركة أو الشّخص الذي هو على رأس شبكة البيع الهرمي، الذي يعتمد على المنتوج كغطاء أو وسيلة فقط للالتحاق بشبكة البيع وتبرير أعمال الغّش والتّدليس والتّلبِيس على الأفراد، حيث يطلب

---

[1] للمزيد من المعلومات أنظر الموقع الإلكتروني التالي: https://www.kaspersky.com/resource-center/preemtive-safety/public-wifi/(consulté le 13/12/2018.)

[2] للمزيد من المعلومات حول الموضوع، أنظر: **عبد الحق حميش**، "حماية المستهلك الالكتروني"، بحث مُقدّم إلى مؤتمر "الأعمال المصرفية بين الشريعة والقانون"، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و12 ماي 2003، المجلد الثالث، ص ص 1293، 1295.

المُروّجين أو المُسوّقين من المستهلكين أن يَستدِينُوا المال، مُقابل إغرائِهم بالحصول في فترة زمنية قصيرة على ثروات أو عمولات قد تتحقّق أو لا تتحقّق[1].

وفي جميع الظّروف، فإنّ الشّخص المُشترِك في برنامج البيع الهرمي لا يُدْرِكُ أو يَعْلَمُ تماماً حين انضمامه للهرم، هل سيكون في الطّبقات العُليا مِنْهُ(Pyramide) لكي يربح المال، أوفي الطّبقات الدُّنيا من الهرم التي تُقلّص حظوظ أو احتمالات تحقيق أو عدم الحصول على الأرباح، فحتّى لو تحصّل الشّخص المشترك(المُتأخّر) المُتواجِد في الشّبكة الهرميّة على أرباح فإنّ قيمة هذه الأخيرة(الأرباح)، تبقى ضئيلة جِدًّا بالمقارنة مع نسبة أو قيمة الأرباح التي يتحصّل عليها الشّخص المُشترك الأوّل أو السّابق له في الانضمام إلى شبكة البيع الهرميّة، وهكذا تزداد نِسب الأرباح كلّما تصاعدت طبقات المشتركين إلى غاية الوصول إلى صاحب المرتبة أو الطّبقة العُليا المجهول الهويّة الذي يكون أكثر غناء وثراء[2].

علاوة على ذلك، فإنّ معاملات البيع الهرمي(Vente pyramidale) تُشجّع التّعاملات الماليّة المجهولة عبر الإنترنت، التي تعتمد على العملات الافتراضيّة المُشّفرة-Crypto)

---

1) **Loi fédérale** contre la concurrence déloyale (**LCD**) du 19 décembre 1986, RS 241 (État le 1er juillet 2016).

Art.02: « Principe Est déloyal et illicite tout comportement ou pratique commerciale qui est trompeur ou qui contrevient de toute autre manière aux règles de la bonne foi et qui influe sur les rapports entre concurrents ou entre fournisseurs et clients. »

Art.03: « Méthodes déloyales de publicité et de vente et autres comportements illicites

1- Agit de façon déloyale celui qui, notamment: **a.** dénigre autrui, ses marchandises, ses œuvres, ses prestations, ses prix ou ses affaires par des allégations inexactes, fallacieuses ou inutilement blessantes; […];

r. subordonne la livraison de marchandises, la distribution de primes ou l'octroi d'autres prestations à des conditions dont l'avantage pour l'acquéreur dépend principalement du **recrutement** d'autres personnes **plutôt que** de la vente ou de l'utilisation de marchandises ou de prestations (système de la **boule de neige**, de l'**avalanche** ou de la **pyramide**); […]. »

Art.28: « Abrogation du droit fédéral La loi fédérale du 30 septembre 1943 sur la concurrence déloyale est abrogée. »

2) **Cyril FIÉVET, «** Bitcoin peut-il devenir la banque des pauvres ? », article publié à partir de l'adresse suivante: https://www.bitcoin.fr/bitcoin-peut-il-devenir-la-banque-des-pauvres.html, consultée le 03/09/2018.

(monnaies كسلعة تبادل أو كأسلوب حديث لدفع قيمة المستحقات لمختلف السّلع والخدمات، من دون اشتراط إثبات هويّة أطراف التّعامل الإلكتروني(عناوينهم الإلكترونيّة فقط) أو الاعتماد على وسيط لتحويل الأموال فيما بين الأرصدة، أو حتّى الحصول على ترخيص لمزاولة النّشاطات الماليّة في حالة بيع وشراء العملات الافتراضيّة مقابل العملات التّقليديّة للدّول أو العكس(Achat/vente de bitcoins c/ des devises(Euro, dollar, etc.)).

وعليه، فإنّ الوسطاء الذين يقترحون تبادل العملات الافتراضيّة مقابل العملات الرّسميّة للدّول يستوجب عليهم الحصول على اعتماد أو ترخيص من قِبَلِ الجهات الرّسميّة وفقا للأحكام المُنظّمة للمعاملات المصرفيّة والماليّة لَدَيْهَا[1]، حيث تضاربت الآراء حول استخدام العملات الافتراضيّة المشّفرة بين مؤيّدين يُناشدُون السّلطات الرّسميّة بضرورة تنظيم تعاملات هذه العملات بدلا من مَنْعِهَا، ومن مُحذّرين(المصارف المركزيّة) لاستعمال العملات الافتراضيّة المشّفرة في المعاملات غير المشروعة.

---

1) **Position** du 29 Janvier 2014 de l'Autorité de contrôle prudentiel et de régulation (**ACPR**), relative aux opérations sur Bitcoins en France, p. 01. Disponible sur le site : https://www.sacpr.banque-france.fr/fileadminuser_uploadacppublicationsregistre-officiel201401-Position-2014-P-01-de-l-ACPR.pdf, consulté 12/02/2016.

- « […]. En tant qu'autorité(**ACPR**) chargée de délivrer les agréments aux prestataires de services de paiement en France, l'ACPR a adopté la **position** suivante : Dans le cadre d'une opération d'**achat/vente de Bitcoins** contre une **monnaie ayant cours légal**, l'activité d'**intermédiation** consistant à recevoir des fonds de l'acheteur de Bitcoins pour les transférer au vendeur de Bitcoins relève de la fourniture de services de paiement. Exercer cette activité à titre habituel en France implique de disposer d'un **agrément de prestataire de services de paiement** (établissement de crédit, établissement de monnaie électronique ou établissement de paiement) délivré par l'ACPR. […].»

Voir aussi : La **Fiche d'information**(**Suisse**) de l'autorité fédérale de surveillance des marchés financiers (**FINMA**) sur : « le Bitcoins », du 25 juin 2014, pp. 01, 02, publiée sur le site: https://www.finma.chfrdocumentationpublications-finmafiches-d-information/, consulté le 16/03/2016.

Fiche d'information(**Suisse**) de l'autorité fédérale de surveillance des marchés financiers (**FINMA**) sur : « Lutte contre le blanchiment d'argent : les intermédiaires financiers doivent respecter les obligations de diligence », du 01 juillet 2016, pp. 01, 02, publiée sur le site : https://www.finma.chfrdocumentationpublications-finmafiches-d-information/, consulté le 16/08/2016.

نتيجة لذلك، يجب على المستهلك أن تكون لديه ثقافة قانونيّة، مع اتّخاذ الحيطة والحذر عند التّعامل بالعملات الافتراضيّة المشّفرة وإدراك المخاطر المُحدِقة المحيطة بها والوعي بالعَواقِب المُنْبَثِقَة من استعمال هذه العملات[1]، ما دام أنّ التّعامل أو المُخاطرة بها كوسيلة دفع حديثة عبر الإنترنت في المجال المشروع قانونا جائز، ولا يوجد أيّ نص قانوني يمنع التّعامل بها كوسيلة دفع حديثة عبر الإنترنت في مجالات التّجارة الإلكترونيّة[2]، حيث أنّ بعض الدّول على غِرار كلّ من ألمانيا، سويسرا، الولايات المتّحدة الأمريكيّة، كندا، أستراليا، فرنسا، الخ...، بصدد التّفكير في مشاريع قانونية لتنظيم التعامل بالعملات الافتراضيّة، لتفادي استخدامها في الأنشطة غير المشروعة(التّهرّب الضّريبي، تجارة المخدّرات، الغّش التّجاري، تمويل الإرهاب، الخ...) [3].

تجدر الإشارة، إلى أنّ أعوان المكتب الفيدرالي الأمريكي للتّحقيقات الدّاخليّة (Federal Bureau of Investigations (**FBI**))، قاموا في أكتوبر 2013 بغلق المَوقِع الإلكتروني التّجاري(Silk Road) الذي أحدثه السّيد(Ross Ulbrich)، بناء على حكم صادر من قاضية

---

1) « **Focus** » n° 10 du 05/12/2013 de la banque de France sur : « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », pp. 03-06, disponible sur le site: http://www.sibfi.banque-france.fruploadstx_bdfgrandesdatesFocus-10-stabilite-financiere.pdf, consulté le 10/04/2016.

Voir aussi : Le **Rapport** de groupe de travail(**Tracfin**)- Juin 2014 sur l'encadrement des monnaies virtuelles (Recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment), pp. 04- 07. Disponible sur le site: http://www.economie.gouv.fr/filesrapport_monnaiesvirtuelles_web.pdf, consulté le 20/03/2016.

2) Arrêt de la C.J.U.E (5ème ch.), 22 octobre 2015, Skatteverket c/ David Hedqvist, (affaire C-264/14). https://www.curia.europa.eu/document/(consulté le 14/02/2017.)

«[…]. La devise virtuelle «bitcoin» fait partie des devises virtuelles dites «à flux bidirectionnel», que les utilisateurs peuvent acheter et vendre sur la base de taux de change. De telles devises virtuelles sont analogues aux autres devises échangeables s'agissant de leur usage dans lemonde réel. Elles permettent d'acheter des biens et des services aussi bien réels que virtuels. […]. Il convient de constater, en premier lieu, que la devise virtuelle à flux bidirectionnel «bitcoin», qui sera échangée contre des devises traditionnelles dans le cadre d'opérations de change, ne peut être qualifiée de «bien corporel» au sens de l'article 14 de la directive TVA étant donné que, ainsi que l'a relevé Mme l'avocat général au point 17 de ses conclusions, cette devise virtuelle n'a pas d'autres finalités que celle de moyen de paiement. […]. l'article 135, paragraphe 1, sous d) et f), de la directive TVA doit être interprété en ce sens que de telles prestations de services ne relèvent pas du champ d'application de ces dispositions. […].»

3) **Y. POULLET et H. JACQUEMIN**, op.cit., pp. 814-815.

(La juge **Katherine Forrest** de la Southern District المحكمة الفيدراليّة لولاية نيويورك Court de New-York (Juridiction fédérale))، الذي بموجبه تّم إدانته على أساس جريمة تبيض الأموال من خلال استخدام عملة البِتْكُويْنْ(Bitcoin)، كوسيلة دفع في الأنشطة المحظورة(المخدّرات، بيع الأسلحة،...) مع تحويلها مقابل العملة الماديّة أو الرّسميّة، حيث يعتبر هذا الحُكم الصادر في هذه القضيّة كسابقة أولى في مجال التّعامل بالعملات الافتراضيّة، أين وضّح معالم وحدود استخدام العُملات الافتراضيّة[1]، التي تستوجب الحذر واليقظة من جانب المستهلك أو المشتري تُجَاهَ هذه العملات(Crypto- monnaies).

الفرع الثالث

استخدام بروتوكولات الطّبقات الأمنيّة

ينبغي على أطراف التّعامل الإلكتروني اعتماد بروتوكولات تشفير البيانات الإلكترونيّة المتداولة عبر شبكة الإنترنت، حيث تسّمى ببروتوكولات الطّبقات الأمنيّة، لكون برامجها تعمل كطبقات وسيطة تربط بين بروتوكول التّحكّم بالنّقل وبروتوكول الاتّصال بشبكة الإنترنت(http://)، إذْ يتّم التّواصل المُشّفر على الإنترنت باستخدام بروتوكولات مؤمّنة-TLS) SSL, SET, C-SET, 3D-Secure, etc.) لتشفير البيانات المتداولة بين أطراف التّعامل الإلكتروني، أو بروتوكولات أمن طبقات نقل الملفات أو رسائل البريد الإلكتروني ,S/MIME) PGP, etc.) حيث يتّم استخدام هذه البروتوكولات خاصّة في عقود التّجارة الإلكترونيّة والعمليات المصرفيّة، لغرض الحفاظ على خصوصيّة وسلامة المعلومات التي تم تحويلها

---

[1] **Arthur MILLERAND**, « Le Bitcoin peut servir à réaliser du blanchiment selon la justice américaine », article publié sur droitdupartage.com, le 20 Août 2014 à 20 H 07 Min. https://droitdupartage.com/2014/08/20/le-bitcoin-peut-servir-a-realiser-du-blanchiment/, consulté le 06/08/2016.
United States of America v. Ross William ULBRICHT, United States District Court Southern District of the New York. Jul 09, 2014. Disponible à partir de l'adresse : https://fr.scribd.com/document/233234104/Forrest-Denial-of-Defense-Motion-in-Silk-Road-Case(consultée le 06/08/2016.)

عبر شبكة الإنترنت فيما بين أصحاب البطاقات المصرفيّة الذّكيّة، والتّجار أصحاب المَواقِع الإلكترونيّة وضمان صحّة المعلومات المتبادلة مع عدم إنكارها[1].

لضمان فعالية بروتوكولات الحماية الأمنيّة في معاملات التّجارة الإلكترونيّة، يجب على المستهلك(Acheteur-Client)، أن يقوم بعملية الشراء لدى صاحب الموقِع التّجاري (Marchand) الذي يربطه عقد مع المصرف(Banque) حول قبول الدّفع الإلكتروني باستخدام البطاقات المصرفيّة الذّكيّة عبر موقِعه الالكتروني، وطرف ثالث موثوق به ومحايد(Tiers de confiance) يشرف على خدمات إصدار شهادات الكترونية موثوقة والتّحقّق في هوّيات المستفيدين من خلال إجراءات التّسجيل، ولضمان سريان عمليات الدّفع يجب أن يتوافر جسر الدّفع الإلكتروني(Passerelle de paiement) كوسيط بين المصرف وأطراف المبادلة التّجارية(المشتري والبائع)، لضمان عمليات الدّفع عبر الشّبكة الدّاخليّة المصرفية الخاصّة، حيث يقوم أطراف المبادلة التّجارية(المشتري والبائع)، بتبادل الرّسائل الإلكترونيّة عبر شبكة الإنترنت التي يتّم تشفيرها وتوقيعها بآليات إلكترونيّة مؤمّنة، لتأكيد سريّة وسلامة محتوى التّبادل الإلكتروني وضمان عدم إنكاره من جانب الأطراف، التي من خلالها يلتزم المصرف بقبول الدّفع عن طريق البطاقة المصرفيّة الذّكيّة من دون الاطّلاع على بياناتها السّريّة[2].

---

1) **Yves RANDOUX**, « La sécurisation du paiement sur les réseaux ouverts », Revue d'économie financière, n°53, 1999, pp. 41- 49.
Olivier GOFFARD, « Risques et responsabilités en cas de transfert électronique de fonds sur Internet », Revue de Droit commercial Belge(R.D.C)- Larcier, n°1, Janvier 2005, pp. 15, 16, 17.

2) **David BOUNIE, Marc BOURREAU**, « Sécurité des paiements et développement du commerce électronique », Revue Économique, 2004/4 (Vol. 55), pp. 692- 695.
Yves RANDOUX, op.cit., p.48-50. ET **Olivier GOFFARD**, op.cit., pp. 15, 16, 17.

فمن أجل عصرنة النّظام المصرفي الجزائري، وتشجيع استعمال طرق الدّفع الإلكتروني المصرفيّة على المستوى المحلّي[1]، قام المصرف المركزي الجزائري بصفته مصرف المصارف في منتصف التّسعينيات(1995) بمبادرةٍ من المصارف العموميّة، بإنشاء شركة تألية العمليات المصرفيّة فيما بين البنوك (Société d'Automatisation des Transactions Interbancaires et de Monétique(SATIM)) كشركة مساهمة تضم ثمانية(08) مصارف عمومية(BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, ALBARAKA)، التي تحوّلت إلى تكتّل مصرفي(Consortium) يضّم مصارف وطنيّة وأجنبيّة (BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, ALBARAKA, Algérie – Poste, Société Générale Algérie , BNP Paribas El Djazair, Housing bank, AGB, Natixis, Fransa-Banque, HSBC, ABC, ARAB Bank et AL SALAM Banque.)[2]، حيث قامت في 1997 بإحداث شبكة مصرفيّة مُشتركة فيما بين المصارف، مع إطلاق خدمة السّحب بالبطاقة المصرفيّة الإلكترونيّة(Carte Interbancaire(CIB))، على مستوى جميع الموزّعات الآلية للنّقود(Distributeur Automatique de Billets(D.A.B))، وأجهزة الشّباك الآلي للمصارف(Guichet Automatique de Banque(G.A.B))، وأجهزة الصّراف الآلي(Teller Machine Automatic(A.T.M)) ونهائيات الدّفع الإلكتروني (Terminal de Paiement Électronique (TPE))[3].

---

[1] نظمت سلطة ضبط البريد والاتصالات الإلكترونية(ARPCE) مؤتمرين دوليين حول التصديق الإلكتروني بالجزائر بالشراكة مع الإتحاد الدولي للإتصالات السلكية واللاسلكية، فالأول تم تنظيمه يومي 08 و09 ديسمبر 2009 بفندق الهيلتون، الجزائر العاصمة، أما الثاني يُعد كتكملةً للمؤتمر الأول والذي تم تنظيمه في أيام 28، 29 و30، جوان 2011، بالنادي الوطني للجيش، الجزائر العاصمة. https://www.arpce.dz

[2] **Nejla BELOUIZDAD**, « La certification électronique appliquée au réseau monétique interbancaire (RMI) », pp. 04-06. (SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, Alger au Cercle National de l'Armée. https://www.arpce.dz

أنظر كذلك الموقع الالكتروني التالي: (consulté le 26/12/2018.) http://www.satim.dz.com

[3] **Nejla BELOUIZDAD**, (SICE' 2011 ARPCE), op.cit., pp. 04-07.

فمن بين مهام شركة(SATIM)، نجد أنّها تضمن المبادلات التّجاريّة والعمليات المصرفيّة عبر الشّبكة المصرفيّة المُشتركة فيما بين المصارف (Réseau Monétique Interbancaire(RMI)) ، وتساهم في إعداد القواعد المتعلّقة بتحديث المعدّات المصرفيّة فيما بين المصارف، وفقا للمعايير المعمول بها بموجب القانون، ومُساعدة المصارف على تطوير خدماتها المتاحة وتشجيعها على عصرنة ورقمنة عملياتها المصرفيّة، مع حسن التّعامل مع التّقنيات التّكنولوجيّة الحديثة التي تستوجب الخبرة والتّدريب واليقظة من مخاطر الجريمة الإلكترونيّة بشتى أنواعها، فمن أجل تأمين جميع العمليات المصرفيّة التي تتّم عبر الشّبكة المصرفيّة المشتركة فيما بين المصارف، تقوم الشّركة(SATIM) باعتبارها كطرف ثالث موثوق به بإصدار شهادة تصديق إلكتروني، تربط من خلالها الشّبكة المصرفيّة بمفتاح عمومي يضمن قبول جميع البطاقات المصرفيّة المشتركة على مستوى جميع أجهزة الموزّع الآلي للنّقود(D.A.B)، ونهائيات الدّفع الإلكتروني(TPE) للتّجار المنخرطين في الشّبكة مع تأمين عمليات المقاصة فيما بين المصارف[1].

تجدر الإشارة في هذا السّياق، أنّ التّعديل الجزئي الأخير الذي مسّ الحكومة الجزائريّة تم فيه استحداث وزارة منتدبة للاقتصاد الرّقمي، يُشرف عليها وزير منتدب لدى وزير الماليّة مُكلّف بالاقتصاد الرّقمي وعصرنة الأنظمة الماليّة، حيث تشرف هذه الوزارة على المسائل المتعلّقة بعصرنة الإدارة الماليّة والمصارف بما فيها الإدارة الجبائيّة(الضّرائب) والإعلام الآلي وتقنيات المعلومات، وتشجيع مبادلات التّجارة الإلكترونيّة مع استخدام تقنيات الدّفع الإلكتروني الجديدة بغية تحريك أو دفع عجلة التّنمية في الاقتصاد الوطني في ظل الأزمة

---

1) **Nejla BELOUIZDAD**, (SICE' 2011 ARPCE), op.cit., pp. 07-14, et suiv.

تجدر الإشارة في هذا السياق، أنّ **المادة(77)** من القانون رقم 15–04 المؤرخ في 01 فيفري 2015، الذي يحدّد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر، اعتبرت جميع شهادات التصديق الإلكتروني المُصدرة من طرف الهيئات المُستعمِلة للتوقيع والتصديق الإلكترونيين قَبْلَ إصدار هذا القانون، صالحة إلى غاية تاريخ انتهاء مدة صلاحيتها في حدود الآجال القصوى التي تُحدِّدُهَا السلطة الوطنية للتصديق الإلكتروني**(ANCE)**، باعتبارها سلطة تصديق رئيسية في الجزائر، التي سنتطرق إليها لاحقا.

الماليّة التي تعيشها البلاد، حيث شهدت الجزائر تأخّرا كبير في عصرنة النّظام المصرفي بالمقارنة مع الجارتان تونس والمغرب والدول الغربيّة السّباقة إلى ذلك[1].

وفي غياب الإطار القانوني المُنظِّم لخدمة الدّفع عبر الإنترنت، تّم "مُسْبَقًا" الإطلاق الرّسمي لخدمة الدّفع الإلكتروني عبر شبكة الإنترنت، التي دخلت حيّز التّنفيذ في 04 أكتوبر2016(أي قَبْلَ صدور القانون رقم 18–05 المؤرخ في 10 ماي 2018 المتعلّق بالتّجارة الإلكترونيّة)، حيث مسّت هذه الخدمة تسعة(09) مصارف عموميّة، إلى جانب القطاعات الخدماتيّة والتّجاريّة الأخرى، على غرار شركة الخطوط الجوّية الجزائريّة (Aire Algérie)، وشركة الطّاسيلي للطّيران(Tassili Airways) واتّصالات الجزائر (Algérie télécom)، وشركة توزيع الكهرباء والغاز(SONELGAZ) والمؤسّسة الوطنيّة لتوزيع الميّاه(SEAAL) بالإضافة إلى مُتعاملي الهاتف النقّال الثّلاثة (Ooredoo, Mobilis, Djezzy)، والشّركة الوطنيّة للنّقل بالسّكك الحديديّة والصندوق الوطني للضّمان الاجتماعي وكذا شركة بريد الجزائر التي أطلقت مؤخرًا خدمة الدفع الالكتروني عبر الإنترنت عن طريق البطاقة الذّهبية، وغيرها من القطاعات الأخرى التي ستستفيد من خدمة الدّفع عبر الإنترنت لاحقا، حيث لا يَستبعِد خبراء المعلوماتيّة أن يتّم تعميمُها مستقبلا على اقتناء المشتريات من المتاجر الافتراضيّة، وتسديد تكلفة وجبة الغذاء في المطاعم أو حتى شراء ملابس وأحذيّة أو الحجز في الفنادق عبر شبكة الإنترنت الخ...

فبصدور القانون رقم 18–05 المؤرخ في 10 ماي 2018 المتعلّق بالتّجارة الإلكترونيّة[2]، أصبح بإمكان كلّ شخص يَمْلِك حسابا مصرفيا مع بطاقة دفع (Carte Interbancaire(CIB)) وجهاز حاسوب أو هاتف ذكي أو لوحة إلكترونيّة الخ...، من الانتفاع بخدمة الدّفع الالكتروني عبر المواقع الإلكترونيّة المؤمّنة للشّركات أو المؤسّسات

---

[1] **عبلة عيساتي**، "وزارة الاقتصاد الرقمي ماذا ستضيف للجزائر؟"، مقال منشور في جريدة أخبار اليوم، في 26 جويلية 2016، عبر الموقع الإلكتروني التالي: http://www.akhbarelyoum.dz (تم الاطّلاع عليه في 2016/07/28.)

[2] قانون رقم 18–05 مؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، سالف الذكر.

المُشرفة على قطاعات الخدماتيّة أو التّجاريّة، التي قبِلت مُسبقا التّعامل بهذه البطاقات في إطار الاتّفاقيات التي تربطها بالمصارف العموميّة، حيث يستطيع المستهلك أن يُباشر إجراءات الدّفع الالكتروني عبر أيّ مَوقِع إلكتروني مُؤمّن لغرض دفع فواتير مستحقات الميّاه والكهرباء والغاز، ودفع الضّرائب أو شراء تذكرة على متن شركة الخطوط الجوّية الجزائريّة أو خطوط الطّاسيلي للطّيران.

لذا يُمكِن للمستهلك مع دخول تطبيقات وتقنيات مُخطّط التّصديق الإلكتروني الهرمي في الجزائر حيّز التّنفيذ، الاعتماد على بطاقات الائتمان المحليّة والأجنبيّة (Master Card, VISA, American Express, Diner Club International, etc.)، للقيام بعمليات الشّراء والدّفع لقيمة المُستحقات بطريقة إلكترونيّة مؤمّنة وموثوقا بها، في أيّ منطقة من العالم من دون أيّ مجهود أو تكلفة مع كسب الوقت في آنٍ واحد، فإذا أراد مثلا أيّ شخص في السّفر إلى بلدٍ معيّن يُمكنه القيام مُسبقًا في نفس المكان والزّمان بشراء تذكرة للسّفر على متن أيّة شركة طيران، ويقوم بعملية الحجز في إحدى الفنادق الأجنبيّة مع كراء سيارة في بلد الوصول، وإبرام أيّة صفقة تجارية بطريقة إلكترونيّة، بشرط توافر الرّصيد الكافي كضمان للوفاء بمُستحقّاته.

فلتأمين عمليات إبرام الصّفقات التّجاريّة وضمان تقنيات الدّفع الإلكتروني عبر شبكة الإنترنت ينبغي على المصرف المركزي الجزائري باعتباره مصرف المصارف، أن يُبَادِرَ بإحداث خادم أو مُشّغل دفع إلكتروني أمن(Serveur de Paiement Sécurisé(SPS))، تشرف عليه شركة تألية العمليات المصرفيّة فيما بين المصارف(SATIM)، يَقْبَلُ(SPS) التّشغيل على أيّ برنامج معلوماتي مهما كان الجهاز المُستعمل، بإحدى برتوكولات الطّبقات الآمنة(TLS-SSL, SET, C-SET, 3D-Secure, etc.) التي تستجيب لمعايير الثّقة والأمان التي تتطلّبها معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة والمعترف بها دوليا، حيث يعتمد بدوره(SPS) على بطاقات الائتمان المصرفيّة الذّكيّة المحليّة والأجنبيّة أثناء عمليات الدّفع الإلكتروني عبر شبكة الإنترنت (Carte CIB, Master Card, VISA, American Express, etc.)، الذي من خلالها يقوم بإتاحة تراخيص (Offrir des autorisations sur les

(cartes bancaires تحت رقابة الشّركة المصرفيّة(SATIM)، يستعملها أطراف التّعامل الإلكتروني في وسط أمن وسليم، مع تمكين مواقع التّجارة الإلكترونيّة من قبول عملية الدّفع الفّوري وتوفير أقصى مُستويات الثّقة والأمان لدى أطراف التّبادل التّجاري.

فعن طريق ذلك الموزّع أو المشّغل تتّم عملية تشفير الصّفقات التّجاريّة المبرمة عبر الموقِع الإلكتروني للتّاجر، مع مُعالجة البيانات المصرفيّة المتبادلة بينه وبين المستهلك بطريقة إلكترونيّة آمنة، حيث يتلقى مُشغّل الدّفع الإلكتروني لدى التّاجر تأكيده بالدّفع مع تسليمه للسّلعة(Un acquittement pour livrer la marchandise)، ويتلقى المستهلك بدوره وصل(Fournir au consommateur un reçu) بدفع تلك السّلعة كضمان له، مما يُزيدهما ثِقَةً وأماناً على إتمام المراحل النّهائيّة للعمليّة.

الفرع الرابع
استخدام تكنولوجيا التّوقيع الرّقمي الموثوق به

إنّ استخدام تقنيات التّشفير أصلا مُقيّدة من طرف تشريعات الدّول لكونها تتعلّق باعتبارات السّياسة العامّة المُنطويّة حول الدّفاع الوطني، والحفاظ على سريّة المعلومات المتبادلة التي لا يتمكّن من قراءتها سوى المُرسِل(منشئ الرّسالة) والمُرسَل إليه(مستقبل الرّسالة)[1]، وبالتالي فإنّ استخدام تقنيات التّشفير لأغراض توثيق التّوقيعات الإلكترونيّة لا تنطوي بالضّرورة على الاستخدام الأعم للتّرميز(Cryptographie) للحفاظ على سريّة أيّة معلومات أثناء عملية الاتّصال، وذلك لكون أنّ إحداث التّوقيع الرّقمي باستخدام تقنيات التّشفير لا يضّر بالضّرورة الأمن أو الدّفاع الوطنيين لأيّة دولة، كما أنّ تقنيات التّوقيع

---

[1] **عيسى غسان ربضي**، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص ص 72– 78.

سلطان عبد الله محمود الجواري، عقود التجارة الإلكترونية والقانون الواجب التطبيق(دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص ص 201، 202.

الرّقمي تتعلّق بضمان مبادلات التّجارة الإلكترونيّة، ولا تُستخدم سِوى لتوثيق رسالة إلكترونيّة تحتوي على بيانات مقدّمة في صيغة رقميّة[1].

وعليه، يعتبر التّوقيع الإلكتروني المحمي كوسيلة أمان حديثة لتوثيق المعاملات الإلكترونيّة وبخصوص معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة، حيث يسمح بالتّعرف على هوّية المُوقّع المحدّدة وضمان الارتباط الوثيق بين صاحب التّوقيع والمستند الإلكتروني المُوقّع من طرفه وبالتّالي عدم إنكاره، حيث يظهر التّوقيع الإلكتروني بمظاهر أو تقنيات مختلفة تُستخدم فيها تقنيات نظم التّشفير اللاّتماثلي، التي يُشار إليها عادة بنظم التّرميز بالمفتاح العمومي، الذي يستند كثيرا إلى استخدام دوال خوارزمية ذات الاتّجاه الوَاحِدْ(Hach fonction) لإنتاج مفتاحين مختلفين ومترابطين رياضيّا، إذْ يتّم الحصول عليهما باستخدام سلسلة من الصّيغ الرّياضيّة المُطبّقة على الأعداد أو المنحنيات التي تُتيح درجة عالية من الثّقة والأمان[2].

حيث يُستخدم المفتاح الخاص من طرف صاحبه لإحداث التّوقيع الرّقمي أو تحويل بيانات الرّسالة الإلكترونيّة إلى صيغة غير مفهومة في ظاهرها، حتّى وإن كانت الحروف أو الرّموز أو الأشكال المستعملة في تحقيق ذلك قابلة للقراءة، بينما ينبغي على المُوقِّع أن يُحافظ على سريّة مفتاحه الخاص باستخدام بطاقة ذكيّة أو رقم سرّي أو أيّة أداة بيومتريّة لتحديد الهويّة، تمنع الوصول إليه(Clé privée) باستخدام الوسائل التّكنولوجيّة المتاحة، وأمّا المفتاح العام يُستخدم للتّحقق من صّحة التّوقيع الرّقمي أو لإعادة رسالة البيانات المُوقّعة إلى

---

[1] **عمر خالد زريقات**، عقود التجارة الإلكترونية، عقد البيع عبر الإنترنت(دراسة تحليلية)، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007، ص ص 269، 278.

محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية: أركانها، إثباتها، حمايتها(التشفير)، التوقيع الإلكتروني، القانون الواجب التطبيق(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 158.

[2] **Aude PLATEAUX,** op.cit., pp. 28- 35.

William STEINMETZ, Brian WARD, op.cit., 47, 48.

صيغتها الأصليّة، حيث تربط بين المفتاح الخاص والعام معادلة رياضيّة معقّدة يستحيل حسابيّا اشتقاق المفتاح الخاص السّري من المفتاح العمومي[1].

انطلاقا من ذلك، فإنّ استخدام تكنولوجيا التّوقيعات الرّقميّة تتجاوز نطاق "التّوقيع" لتُستخدم في مجالات أوسع بكثير من ذلك، كتوثيق الخوادم أو المواقع الإلكترونيّة الشّبكيّة باستخدام شهادات التّصديق الإلكتروني الموقّعة رقميّا من طرف الجهات الرّسميّة المُصدرة لها، وذلك لضمان الثّقة لدى مُستعملي الخوادم أو المواقع الإلكترونيّة والتّأكد من مَصدَرِها الحقيقي، كما تُستخدم تكنولوجيا التّوقيع الرّقمي لتوثيق برمجيات الحاسوب بشتى أنواعها خاصّة تلك المُنّزلة من المواقع الإلكترونيّة عبر شبكة الإنترنت، أو لتوثيق أيّ بيانات أخرى مُستخدمة أو مُخزّنة رقميًّا.

لضمان الثقة والأمان بين المُوقِّع ومُتلقي الرّسالة الإلكترونيّة وتسهيل عملية التّحقّق من صّحة التّوقيع الرّقمي المُرفَق بها، يجب أن تُتاح للقائم بعملية الفّحص سُبُلْ الوصول إلى المفتاح الخاص بالمُوقِّع وأن يكون لديه(المُحقّق) ما يضمن تَناظُره(Clé privée) مع المفتاح العام(Clé publique)، غير أنّه لا يوجد ما يُثبت أيّ ارتباط جوهري أو رسمي لزوج مفاتيح التّشفير بأيّ شخص معيّن، وعليه لا بُدّ من توافر آلية إضافيّة يُشرف عليها طرف ثالث موثوق به ومحايد، للرّبط بين صاحب التّوقيع الإلكتروني وزوج مفاتيح التّشفير(الخاص والعام)، وبالتّالي يجب أن تكون لدى أطراف المبادلة التّجاريّة الثّقة والأمان فيما يصدر من مفاتيح عموميّة وخاصّة[2].

---

[1] **لورنس محمد عبيدات**، إثبات المحرر الالكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص ص 134-142.

[2] المرجع نفسه، ص 132.

سلطان عبد الله محمود الجواري، مرجع سابق، ص ص 205، 206.

Michelle Jean- BAPTISTE, Créer et exploiter un commerce électronique, Litec, France, 1998, pp. 149, 150, 151.

Olivier GOFFARD, op.cit., pp. 12, 13, 14, 15.

المبحث الثاني
دور التّصديق الالكتروني في ضمان أمن مواقع التّجارة الالكترونيّة

إذا كانت مسألة تحقيق الثّقة والأمان تَنْعَدِمُ بَتَاتًا في الفضاء الكوني الشّاسع-Univers) (Cosmos، الذي تتواجد فيه المجموعة الشّمسية لكوكب الأرض إلى جانب العديد من المجموعات الشّمسية(Systèmes solaires)، نظرا للمخاطر المفاجئة المُنبثِقة من الجاذبيّة(Gravitation)، والتّصادم أو التّلاحم فيما بين المجرّات(Galaxies- Voies lactées) والإنفجارات التِلْقَائِيَّة للنُّجُومِ(Étoiles-Astres)، وما ينجرّ عنها من مخاطر إشعاعيّة نوويّة ومِغناطيسيّة ضارّة، تُؤدّي في بعض الأحيان إلى حدوث ظواهِر فيزيائيّة غَرِيبَة، على غرار الثّقوب السّوداء واتّساع الكون، الخ...(Trous Noirs, extension de l'univers, etc.)، التي لا يُمكِن للإنسان أو أيّة آلة أخرى تفادِيها أو التّصدي لها، فإنّ فرضيّة تحقيق هاذين العُنصرين(الثّقة والأمان) مُمكِنة في الفضاء الإلكتروني الافتراضي ولو كان ذلك بصفة "نِسْبِيَّة"، ما دَامَ يُسَيْطِرُ فيه "الإنسان" على جميع الأجهزة الآلية والبرمجيات المعلوماتيّة الخ...، كما أنّه(الإنسان) يُعْتَبَرُ المَصْدَرُ الوحيد لمختلف المخاطر والعقل المُدبِّر في تنفيذ الهجمات الإلكترونيّة المتعلّقة بالمعاملات الإلكترونيّة، وبالخصوص معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة، التي تستوجب إرساء تدابير الحماية الأمنيّة والاستعانة بالتّقنيات التّكنولوجيّة الحديثة التي يُشرف عليها طرف ثالث موثوق، ومُحايد عن أطراف التّعامل الإلكتروني يُتيح من خلالها خدمات التّصديق الإلكتروني بما فيها تأمين مواقِع التّجارة الإلكترونيّة **(المطلب الأول)**.

انطلاقا من ذلك، فإنّ الطرف الثالث يُشار إليه عادة عبر مختلف التّشريعات بمقدّم خدمات التّصديق أو سلطة التّوثيق أو مُورّد خدمات التّصديق، حيث تُنظّم خدماته في إطار كيان أو نموذج تنظيمي يسمّى بمرفق المفاتيح العموميّة، الذي من خلاله يتّم إحداث سلطات تصديق في بنيات متنوّعة تتوافق مع السّياسة العامّة لكلّ دولة، إذ يمكن أن تكون بعض سلطات التّصديق تابعة لسلطات تصديق أخرى في شكل هرمي أو تعمل في بنى أخرى على قِدَمِ المُساواة بعضها البعض كما هو الحال للبنية المُتشابكة، فمهما كانت بينية مرفق

المفاتيح العموميّة فإنّ جدارة الثّقة والأمان في مقدّم خدمات التّصديق الإلكتروني تتوقّف على مدى امتثاله لمُقتضيات السّياسة العامّة المتّبعة في خدمات التّصديق ومُراعاته للتّأكيدات المقدّمة فِيهِ (**المطلب الثاني**).

المطلب الأول
التّصديق على معاملات التّجارة الإلكترونيّة

تعتبر مواقِع التّجارة الإلكترونيّة أسلوبا تقنيا حديثا، تُستخدم فيها مختلف التّكنولوجيات لتغيير وتسريع نمط أداء النّشاطات التّجاريّة، والوصول إلى أسواق جديدة وفتح منافذ توزيع، لا تعترف بحدود زمانيّة أو مكانيّة معيّنة تعمل على مدار السّاعة في جميع أنحاء العالم، وبالتالي فإنّ المحيط الذي تُمارس فيه مبادلات التّجارة الإلكترونيّة غير أمن نظرا لتزايد وانتشار مخاطر الفيروسات والبرمجيات الخبيثة، التي كثرت في الآونة الأخيرة بشكل سريع وكثيف مُستهدفة أنظمة الحماية الأمنيّة للشّبكات ونظم تشغيل المعلومات، ولعلّ أنّ أحدث التّقنيات التي وصل إليها الفكر البّشري لضمان الثّقة والأمان فيما بين أطراف التّصرف الإلكتروني، تتعلّق بإيجاد آلية إضافيّة(Un mécanisme supplémentaire) حديثة تضمن الارتباط الجوهري لزوج مفاتيح التّشفير غير المتناظرة بصاحب التّوقيع الإلكتروني، حيث يشرف عليها(م.خ.ت.إ) محايد ومعتمد من طرف الجهات الرّسميّة، وللتّعرف أكثر على خدمات التّصديق الإلكتروني، يستوجب الأمر التَّطرُق إلى الجوانب الأمنيّة لعملية التّصديق الإلكتروني(**الفرع الأول**)، ومجالات تطبيق خدمات التّصديق الإلكتروني(**الفرع الثاني**)، وكذا التّعرف على السّلطة المكلّفة بتوثيق عقود التّجارة الإلكترونيّة(**الفرع الثالث**).

الفرع الأول
الجوانب الأمنيّة للتّصديق الإلكتروني

يلعب التّصديق الإلكتروني دورا رئيسيا في منظومة أمن معاملات التّجارة الإلكترونيّة(**أوّلا**)، حيث تقوم سلطات التّصديق الإلكتروني الموثوقة بإصدار شهادات إلكترونيّة موصوفة وفقا للأغراض التي صُدرت من أجلها(**ثانيا**)، التي من خلالها يجب على هذه السّلطات مراعاة مجموعة من المتطلّبات التّقنيّة المتعلّقة بالتّوقيعات الإلكترونيّة الموصوفة(**ثالثا**).

أولا– أهداف التّصديق الإلكتروني.

تضمن عملية التّصديق الإلكتروني ثلاثة أهداف أمنيّة رئيسيّة في معاملات التّجارة الإلكترونيّة والمتمثّلة فيما يلي:

1)– تحديد هويّة أطراف التّصرف الإلكتروني(Identification+Authentification):

تتّم معاملات التّجارة الإلكترونيّة في بيئة إلكترونية افتراضية مملوءة بالمخاطر أو التّهديدات الإلكترونيّة، المتعلّقة بالخصوص في انتحال هوية أطراف التّعامل الإلكتروني واختراق بياناتهم الإلكترونيّة المتداولة، الشّيء الذي يدفعهم إلى الاستعانة بخدمات جهة توثيق إلكتروني معتمدة تقوم بتزويد توقيعاتهم الإلكترونيّة بشهادات تصديق إلكتروني موصوفة[1]، تؤكّد ارتباط بيانات فحص التّوقيع الإلكتروني للمُوقِّع، وذلك بعد التّحقق من هويّتهم وصفاتهم القانونيّة بجميع الوسائل التّكنولوجية والقانونيّة المتاحة لها بموجب القوانين والتّنظيمات المتعلّقة بنشاطات التّصديق الإلكتروني.

---

1) **Louise MARTEL, René ST-GERMAIN**, « Les sceaux de certification des sites web : un outil de confiance, outil de confusion », pp. 03- 08. Article disponible à partir de l'adresse: https://halshs.archives-ouvertes.fr/halshs-00584496, consultée le 20/02/2019.
Jeffrey F. RAYPORT, Bernard J. JAWORSKI, op.cit., pp. 58- 62.

لذا تعتبر شهادة التّصديق الإلكتروني الموصوفة بمثابة وثيقة إثبات هويّة صاحبها(بطاقة التّعريف الوطنية أو جواز السّفر) التي ينبغي أن تستجيب للمواصفات أو المعايير المعترف بها دوليا والمعمول بها بموجب قوانين الدول، كتحديد هويّة كلّ من(م.خ.ت.إ) والمُوقّع الذي كان يتحكّم في بيانات إحداث توقيعه الإلكتروني في وقت إصدار الشّهادة، كما ينبغي لهذه البيانات أن تكون مطابقة لبيانات فحصه في وقت أو قبل إصدار الشّهادة مع عدم تعرّضها لما يثير الشّبهة فيها، وعند الضّرورة ينبغي تحديد القيود المفروضة على القيمة التي تستخدم من أجلها الشّهادة، أو على نطاق المسؤوليّة التي اشترطها مقدّم خدمة التّصديق تجاه أي شخص بالإضافة إلى ذلك يجب ذكر التّوقيع الإلكتروني الجّذري لجهة التّوثيق الإلكتروني(AC) المُصدِرة لشهادة التّصديق الإلكتروني، وفي هذا السّياق تجدر الإشارة إلى أنّ تقنيات إصدار شهادات التّصديق الإلكتروني لا تتعلّق فقط بتوثيق هويّة الأفراد بل تُمكّن كذلك من إثبات أو توثيق هويّة مكوّنات الشّبكات ومواردها، بما فيها من الخوادم أو المواقع الإلكترونيّة الشّبكيّة وبرامج الحواسيب أو أيّة بيانات رقميّة أخرى.

2)– ضمان سريّة وسلامة محتوى البيانات المتداولة(Intégrité-Confidentialité):

تُستخدم تقنيات التّشفير غير المتناظرة من أجل كفالة صّحة الرّسائل الإلكترونيّة وضمان سريّة وسلامة محتويات هذه الرّسائل، حيث تعتمد عملية إحداث التّوقيعات الإلكترونيّة الموصوفة على أدوات أو معدّات مؤمّنة وموثوق بها، تضمن في سريّة تامّة أُحادية اتجاه بيانات إنشاء التّوقيع الإلكتروني لمرّة واحدة فقط، على نحو تُمكِّن من كشف أيّ تغيير أو تعديل يمّس بمُحتوى البيانات الإلكترونيّة بعد التّوقيع عليها[1]، حيث تُستخدَم من خلالها دوال خوارزميّة لإنتاج زوج مفاتيح مترابطة فيما بينها بعملية رياضيّة مُعقّدة، فالمفتاح الخاص يُستخدم لإحداث التّوقيع الإلكتروني، ويرتبط هذا المفتاح بالمفتاح العام إذْ ينبغي على المُوقّع الاحتفاظ به(المفتاح الخاص) بطريقة مؤمّنة، وأمّا المفتاح العام يُستخدم للتّحقّق من صّحة التّوقيع الإلكتروني حيث يكون مُتاحا للجمهور.

[1] **محمد سعيد أحمد إسماعيل**، مرجع سابق، ص ص 259– 265.

فقبل التّوقِيع على المُسْتَنَدِ أو أيّ معلومات أخرى يتعيّن على المُوَقِّعِ أن يُبيّن حُدود ما يُريد التّوقِيع عَلَيْهِ، قصد السّماح لدالة البَعْثَرَةِ المُؤمّنة-Hachage à sens unique) (Unidirectionnelle المعيّنة في حاسوبه باستخلاص قيمة الهاش الأصليّة للرّسالة، في صورة رقميّة معيّنة(bits) أو بصمة بطول مقياسي يكون عادة أصغر من الرّسالة ومحصورا بها حيث تنفرد بها المعلومات التي يُراد التّوقيع عليها، وعندئذ يقوم البرنامج الحاسوبي لدى الموقّع بتشفيرها بإحدى خوارزميات المفتاح العام وتحويلها إلى توقيع إلكتروني بإستعمال المفتاح الخاص للمُوَقِّعْ، فكلّ تغيير في الرّسالة الأصليّة ينتج عنه قيمة هاش مُختلفة عند استخدام وظيفة الهاش نفسها أثناء التّدقيق في صّحة التّوقيع الإلكتروني[1].

فعن طريق شهادة التّصديق التي يتحصّل عليها الطّرف المعوّل(متلقي الرّسالة الإلكترونيّة) من(م.خ.ت.إ) الموثوق به، يقوم برنامج تحقّق حاسوب مُتَلَقِّي الرّسالة الإلكترونيّة الأصليّة لعملية تدقيق مدى مطابقة بيانات فحص التّوقيع الإلكتروني لبيانات إحداثه، عن طريق إعادة احتساب قيمة هاش جديدة(خلاصة الرّسالة) باستخدام نفس خوارزميّة دالة البَعثرة المؤمّنة المُستعملَة في التّوقِيع، وذلك لغرض المقارنة والتّأكد من مدى مُطابقتها لخُلاصة الهاش الأصليّة التي تمّ تحويلها إلى توقيع إلكتروني موصوف، فإذا توصّل الحاسوب إلى تحصيل نفس قيمة الهاش، فيعني عدم تعرّض البيانات الإلكترونيّة الموقّعة لما يثير الشّبهة فيها، وبالتّالي فإنّ برمجيات التّحقّق من صّحة التّوقيع الإلكتروني تؤكّد:

– ما إذا كان المفتاح الخاص المُستخدم لتوقيع الرّسالة الإلكترونيّة يناظر بالفّعل المفتاح العام المُشار إليه في شهادة التّصديق الإلكتروني، لأنّ المفتاح العام للمُوقِّع لا يُثبِت إلاّ صّحة توقيع إلكتروني تّم إنشاءه بواسطة المفتاح الخاص للمُوقِّع؛

---

[1] **عيسى غسان ربضي**، مرجع سابق، ص ص 81– 84.

علاء حسين الحمامي، سعد عبد العزيز العاني، مرجع سابق، ص ص 232– 240.

Jaime ANGELES, « Commerce électronique : de la perspective américaine à un cadre international », Collection Droit du cyberespace, Édition UNESCO/ ECONOMICA, 2005, pp. 98- 101.

– أنّ الرّسالة الإلكترونيّة الموقّعة لم يطرأ عليها أيّ تغيير وهو ما يتحقّق في حالة ما إذا كانت نتيجة البَعثرة التي حَسَبَهَا القائِم بعملية الفحص، مُطابقة لنتيجة البَعثرة المُستخرَجة من التّوقيع الإلكتروني أثناء عملية التّدقيق من صّحته.

3)– ضمان عدم إنكار رسالة البيانات المتداولة(Non-Répudiation):

من المُعتاد على برمجيات إحداث التّوقيع الإلكتروني الموصوف أن تُلْحِقَ هذا الأخير(نتيجة بعثرة للرّسالة مُوَقَّع عليها رقميًّا) بالرّسالة الإلكترونيّة ويُخَزَّن ويُرسَل مع تلك الرّسالة، ومن المُمْكِنِ كذلك إرسال أو تخزين التّوقيع الإلكتروني على أنّه عنصر بيانات إلكترونيّة منفصل عن الرّسالة وذلك ما دام أنّه(التّوقيع) مُرتبطا بالرّسالة المُناظرة ارتباطا يمكن التّعويل عليه ويخص الرّسالة التي تحتضنه دون سواها، غير أنّه يكون عديم الجدوى أو لا يصلح للاستعمال بتاتا في حالة ما إذا تّم فصله(التّوقيع) عن الرّسالة الإلكترونيّة بصفة دائمة ونهائيّة[1]، وبالتّالي فدوال البعثرة الأُحَادِيَّة الاتجاه تُمكّن برمجيات إحداث التّوقيعات الإلكترونيّة الموصوفة بالعمل بمقادير أصغر من البيانات، على نحو يُتيح إمكانية التّنبؤ بها كما تكرّس في الوقت نفسه ارتباطا استدلاليّا قويًا بمحتوى الرّسالة الإلكترونيّة الأصليّة وتُوّفر تأكيدا كافيًا على أنّه لم يطرأ على تلك الرّسالة، أي تعديل أو تغيير أو تزوير أثناء وقبل إصدار شهادة التّصديق، وبالتّالي عدم إنكارها من جانب أطراف التّعامل الإلكتروني.

ثانيا– أنواع شهادات التّصديق الإلكتروني.

تُستخدم تقنيات التّوثيق الإلكتروني تبعا للسّياق الذي تُستخدم فيه، كالتّركيز على تحديد الهويّة أو تأكيد امتيازات الصّلاحيات الممنوحة لسلطة شخص معيّن، أو ضمان سلامة المعلومات، أو إقرار مستوى معيّن من الثّقة في المعاملات الإلكترونيّة، وعليه فإنّ استخدام تكنولوجيات التّوقيعات الإلكترونيّة الموصوفة كوسيلة توثيق معتمدة، لا تقتصر فقط على توثيق هوّية الأفراد بل تستطيع أن تُوثّق مُكوّنات شبكات المعلومات ومواردها الحسّاسة، بما

1) **Hélie- Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 128, 129, 130.

فيها الخَوادم والمواقع الإلكترونيّة ومختلف برمجيات الحاسوب أو أي معدّات أو بيانات أخرى تستدعي الحماية الأمنيّة لها، وعلى العموم تقوم جهات التّصديق الإلكتروني الموثوق بها بإصدار شهادات التصديق الإلكتروني وفقا لمستويات الثّقة الآمان المتطلّبة وبِحَسَبِ الأغراض التي تُستعمل من أجلها في إطار المعاملات الإلكترونيّة[1]، حيث يمكن تصنيفها على النّحو التّالي:

1)– شهادة الإمضاء الإلكتروني(Certificat de signature):

يُطلق عليها في بعض التّشريعات الوطنيّة مصطلح "الشّهادة الشّخصيّة" المُستخدمة لتوثيق التّوقيع الإلكتروني المرتبط بالرّسالة الإلكترونية[2]، حيث تربط هوّية صاحبها بمفتاح عام إذْ تُمكّن المُوقِّع من إثبات هويّته وتأكيد صّحة وسلامة البيانات الإلكترونيّة المرتبطة بتوقيعه الإلكتروني الموصوف[3]، كما تُتيح للطرف المُعوِّل(مُستقبل الرّسالة الإلكترونيّة) على شهادة التّصديق إمكانية التّحقق من مصداقيّة البيانات الإلكترونيّة الواردة فيها، كالتّعرف على هوّية كلٍّ من المُوَقِّعْ والجهة المُصدرة لها، والتّأكد من ارتباط بيانات إنشاء التّوقيع الإلكتروني بصاحبه، فعن طريق هذه الشّهادة يقوم برنامج حاسوب المُتلّقي إعادة احتساب قيمة بعثرة(هاش) جديدة بنفس الخوارزميات المستعملة في دالة البَعثرة الأصليّة، لغرض التّأكد من مدى مطابقتها لقيمة البَعثرة(الأصليّة) المستخدمة في إحداث التّوقيع الإلكتروني للمُرسِل، فإذا تَوصَّل إلى تحصيل قيمة هاش مُطابقة لقيمة الهاش الأصليّة فيعني عدم تعرّض البيانات الإلكترونيّة لما يُثير الشّبهة فيها والعكس صحيح.

---

[1] أنظر **الملحق رقم (28)**، ص 502.

[2] أنظر الفصل(07) في الباب الثالث من الأمر عدد 1667– 2001 المؤرخ في 17 جويلية 2001، الذي يتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية، ر.ر.ج.ت عدد 60، الصادر في 27 جويلية 2001.

[3] **Hélie - Solange GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 130, 140.

2)– شهادة مُوزّع ويب(Certificat serveur (Web)):

تعتبر الخوادم(Servers) من بين المُكوّنات الرّئيسيّة الفاعلة(Composants actifs) لشبكات الحاسوب(الدّاخليّة والخارجيّة)، التي تؤدّي العديد من الخدمات بحسب الدّور الذي تلعبه في داخل الشّبكة، حيث تسمح باحتضان المواقع الإلكترونيّة والاحتفاظ بقواعد البيانات وترجمة العناوين(DNS) الإلكترونيّة وتوزيعها وخدمات تصّفح المحتوى الخ...، كما أنّها تُشّكل الواجهة الأماميّة التي تستقبل مختلف الاتّصالات التي تمرّ عبرها البيانات الإلكترونيّة حيث تكون عُرضة لمختلف المخاطر والتّهديدات الإلكترونيّة، وعليه تُستخدم شهادة موزّع الويب لتوثيق خوادم شبكات الحاسوب(الدّاخليّة والخارجيّة)، بهدف تمكين مستخدميها من التّأكد من مصدرها الحقيقي، حيث تُؤدّي وظائف الحماية الأمنيّة الحسّاسة لمكوّنات هذه الشّبكات التي تمرّ عبرها مختلف الاتّصالات الخارجيّة[1].

فعن طريق هذه الشّهادة تتّم عملية تحديد هوّية مُوزّع الويب والتّصديق على مُحتواه، عن طريق اتّفاق سلطة التّصديق مع الخادم(Serveur (Web)) حول قبول والاعتراف بشهادة التّصديق الرّئيسيّة لها، عن طريق ربط هوّية ذلك الموزّع بمفتاح عمومي يسمح بتبادل البيانات الإلكترونيّة بين الموزّع وعملائه في إطار مناخ ثقة أمن، إذ يقوم المتعامل الإلكتروني بتثبيت(Installer) الشّهادة على برنامج حاسوبه من أجل تأمين عمليات البيع والشّراء، أو التّبادل أو الدّفع الإلكتروني عبر موقع تجاري من دون إطلاق الموزّع أو الخادم(Serveur) لرسائل تحذير على جهاز الحاسوب[2].

---

1) **Hélie - SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 140, 141, 142.

2) **Marc LACOURSIÈRE et Édith VÉZINA**, « La sécurité des opérations bancaires par Internet », Revue juridique Thémis, R.J.T, vol 41, n°1/2007, pp. 126, 127.
Louise MARTEL et René ST-GERMAIN, « la Certification de Conformité des Sites Web », Revue gestion, 2002/5 Vol. 27, pp. 91, 92.

3)– شهادة توثيق مواقع الإنترنت(Certificat d'authentification de site Interne):

تسمح هذه الشّهادة بالتّعريف عن الهويّة الأصليّة لمواقع الإنترنت حيث تُمَكِّنُ المُستخدِم أو المستهلك من مَعْرِفَةِ ما إذا كان المَوقِع الإلكتروني الذي يَزُورُهُ، هو حَقًّا ذلك المُستهدَف من تلك الزّيارة ولم يتعرّض إلى عملية التّزوير أو انتحال اسم الموقع الإلكتروني، وبالتّالي تفادي الوقوع في فخ القراصنة الذين يقومون بعمليات الاختراق والنّهب، والاستيلاء على الأموال بعد الاستحواذ على البيانات الإلكترونيّة الخاصّة بأصحاب البطاقات المصرفيّة الذّكيّة، أو حتّى السّطو الإلكتروني على اسم النّطاق الذي يحتوي على أحد عناصر الملكيّة الفكريّة، ومطالبة أصحابها بدفع الأموال مُقابل التّنازل عن اسم الموقِع المُسَجّل، الخ...

ولضمان مصداقيّة تلك الشّهادات، ألزم المشّرع الفيدرالي للإتّحاد الأوروبي بموجب المادة 45 من التّنظيم رقم 910/2014 المؤرخ في 23 جويلية 2014 المتعلق بالهويّة الإلكترونيّة وخدمات الثّقة المتّصلة بالمعاملات الإلكترونيّة في إطار السّوق الدّاخلي، المُلغي للتّوجيه الأوروبي رقم 93/1999 المتعلّق بالتّوقيعات الإلكترونيّة(eIDAS)[1]، أن تستجيب الشّهادات الإلكترونيّة الموصوفة لتوثيق مواقع الإنترنت، للمواصفات أو المعايير التّقنيّة المحدّدة في الملحق الرّابع(Annexe IV) من نفس التّنظيم(eIDAS)، كتحديد بيان يؤكّد أنّ الشّهادة الموصوفة تتعلّق بتوثيق موقع الإنترنت وذكر اسم أو الاسم المُستعار(الشّخص الطّبيعي) واسم أو عند الاقتضاء رقم تسجيل مؤدّي خدمات الثّقة المؤهّل المُصدر للشّهادة

---

1) **Art. 52(Règlement (eIDAS))** : « (**Entrée en vigueur**) **1.** Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. **2.** Le présent règlement est applicable à partir du 1er juillet 2016, à l'exception des dispositions suivantes:[…]. »

Art. 45(Règlement (eIDAS)): « **1-** Les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à **l'annexe IV**.

2- La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site internet. Un certificat qualifié d'authentification de site internet est présumé satisfaire aux exigences fixées à l'annexe IV lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2. »

Voir aussi : - **Didier GOBERT**, Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie, p. 45, Article publié en février 2015, sur le site : https:// www.droit-technologie.org, consulté le 09/09/2016.

في حالة ما إذا كان شخص معنوي، وكذا عنوان إقامته مع إبراز اسم النّطاق المُستغَّل من طرف الشّخص المعنوي أو الطبيعي الذي أُصدرت من أجله شهادة التّصديق الموصوفة، ومُدّة بداية ونهاية صلاحية تلك الشّهادة ورقم تعريفها والتّوقيع الإلكتروني المُتقدّم أو الختم الإلكتروني المُتقدّم لجهة التّصديق المؤهّلة المُصدرة للشّهادة [1].

4)– شهادة الشّبكات الافتراضيّة الخاصّة(Certificats VPN):

تُمكّن هذه الشّهادة من تحديد هوّية الشّبكات الافتراضيّة الخاصّة وتضمن سلامة جميع المبادلات التي تتّم عبر أنفاق خاصّة محميّة، حيث تربط المعلومات أو البيانات المتعلّقة ببعض المواقع على شبكة معيّنة(مُحوّلات routeurs، جدران ناريّة firewalls، مركزات

---

1) **ANNEXE IV(Règlement (eIDAS))** : « Les certificats qualifiés d'authentification de site internet contiennent: **a)** une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de site internet;
b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et: - pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels, - pour une personne physique: le nom de la personne;
c) pour les personnes physiques: au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme. Si un pseudonyme est utilisé, cela est clairement indiqué; pour les personnes morales: au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels;
d) des éléments de l'adresse, dont au moins la ville et l'État, de la personne physique ou morale à laquelle le certificat est délivré et, le cas échéant, ces éléments tels qu'ils figurent dans les registres officiels;
e) le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré;
f) des précisions sur le début et la fin de la période de validité du certificat;
g) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;
h) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;
i) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé visés au point h);
j) l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.»

concentrateurs...) بالمفتاح العام لسلطة التّصديق الإلكتروني الموثوق بها، ويتم استخدام هذه الشّهادة لضمان سلامة المبادلات بين منظّمة وفروعها المُوزّعة جُغرافيا عبر مسالك أو أنفاق مؤمّنة في شبكة الاتّصالات، كما تسمح(الشّهادة) بإقامة علاقة ثقة بين المحترف والمُستهلك في إطار مناخ أمن عبر شبكة الإنترنت[1].

5)– شهادة إمضاء الرّمز(Certificat de signature de code):

تسمح بالإمضاء على أيّ برنامج أو نص أو برمجيّة لضمان تعريفه بتوقيع صاحبه، كما تمكّن من حمايته ضّد مخاطر القرصنة[2].

6)– الشّهادة المُتقاطعة(Certificat croisé-réciproque):

تُصدر هذه الشّهادات من طرف سلطات التّصديق الرّئيسيّة في مرافق المفاتيح العموميّة لغرض الاعتراف بشهادات التّصديق التي يُصدرها(م.خ.ت.إ) التّابعين لكلّ مرفق، حيث تقوم كلّ جهة تصديق على حِدَا بإصدار شهادة تصديق متقاطعة(Certificat Croisé)، التي تسمح لها بالتّوقيع على المفتاح العام التّابع لجهة التّصديق الإلكتروني المثيلة لها في مرفق المفاتيح العموميّة الأخر، التي تقوم بدورها بإصدار شهادة تصديق متقاطعة تُوقّع من خلالها على المفتاح العام التّابع للجهة الأولى، وتتم نفس العملية بالنسبة لجهات التّصديق الأخرى في إطار التّصديق المتبادل فيما بين مرافق المفاتيح العموميّة، بينما يُبيّن زوج الشّهادات المُصدرة من طرفهم(Cross-Certificat) علاقة الثّقة المتبادلة فيما بين سلطات التّصديق الرّئيسيّة، بالشّكل الذي يُؤدّي إلى الاندماج الكلّي أو الجزئي لنطاقات مرافق المفاتيح العموميّة ضمن نطاق أكبر حجماً، وخلق التّكافؤ والتّناسق في السّياسات العامّة المتّبعة في خدمات التّصديق الإلكتروني[3].

---

[1] أنظر الموقع الالكتروني لسلطة ضبط البريد والمواصلات الإلكترونية: http://www.arpce.dz (consulté le 26/02/2019.)

[2] المرجع نفسه.

[3] **Arnaud- F.FAUSSE**, op.cit., pp. 127-130.

ثالثا– الشّروط التّقنية المتطلّبة في التّوقيع الإلكتروني الموصوف.

يُعتبر التّوقيع الإلكتروني الموصوف وسيلة أمان حديثة تُحقّق وظائف عدّة تتجاوز في نطاقها الوظائف النّمطية الخاصّة بالتّوقيع المكتوب بخط اليد، ومن أجل إضفاء الحجّية القانونيّة في الإثبات على هذا النّوع من التّوقيعات الإلكترونيّة اشترطت أغلبيّة التّشريعات الدوليّة والوطنيّة توافر شروط تقنيّة معيّنة[1]، باعتبارها(الشّروط) أحد دعائم الاعتراف بالتّوقيعات الإلكترونيّة الموصوفة التي من شأنها أن تُعزّز الثّقة والأمان في المعاملات الإلكترونيّة وبالخصوص معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة، ولتوضيح هذه الشّروط سنُركّز على ما وُرِدَ في أحكام المادة 07 من القانون رقم 04/15 المحدّد للقواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، التي تنّص:" **التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفّر فيه المُتطلبات الآتية:**

1)– أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة؛

2)– أن يرتبط بالموقع دون سواه؛

3)– أن يمكن من تحديد هوية المُوقّع؛

4)– أن يكون مُصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني؛

5)– أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقّع؛

---

1) **Décret(France) n° 2017-1416** du 28 septembre 2017 relatif à la signature électronique, JORF n° 0229 du 30 septembre 2017.

Art. 1er. « – La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement. »

Art. 2. – I. « – Le **décret n° 2001-272** du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique **est abrogé**. II. – Les références au décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique abrogé par le I, contenues dans des dispositions de nature réglementaire, sont remplacées par les références au présent décret. »

6)- أن يكون مُرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات."

فمن خلال ما وُرِدَ في أحكام هذه المادة(07) يمكن استخلاص المتطلّبات التّقنيّة التي يجب توافرها في التّوقيعات الإلكترونيّة الموصوفة والمتمثّلة فيما يلي:

أ)- ارتباط التّوقيع الإلكتروني بشهادة تصديق إلكتروني موصوفة:

لضمان تحديد هوّية المُوقّع وتأكيد ارتباطه الوثيق بالتّوقيع الإلكتروني لوحده دون غيره يجب أن يتّم إحداث توقيعه الإلكتروني على أساس شهادة تصديق إلكتروني موصوفة، تُمنح له(المُوقِّع) من طرف ثالث موثوق أو من(م.خ.ت.إ)، حيث تتضمّن على البيانات الإلزاميّة التي نصّت عليها المادة 3/15 من نفس القانون[1]، كالإشارة بأنها شهادة تصديق موصوفة مع تحديد هوّية المُوقِّع وصِفته عند الاقتضاء وهوّية الجهة المُصدرة للشّهادة الإلكترونيّة وبلد إقامتها، وذكر بيانات إحداث التّوقيع الإلكتروني المطابقة مع بيانات فحصه والتّوقيع الإلكتروني الموصوف للجهة المصدرة للشّهادة، مع الإشارة في مَتْنْ هذه الأخيرة إلى كلّ من تاريخ بداية ونهاية صلاحيته(الشّهادة) ورمز تعريفها، مع توضيح ما إذا كانت هناك أيّة قيود على نطاق استعمال الشّهادة أو على القيمة التي تُستخدم من أجلها تلك الشّهادة، وعليه فمهما كانت هوّية مُنشئ التّوقيع الإلكتروني الموصوف المناظر لرسالة معيّنة، سواء أحدثه(التّوقيع) المُوقّع لتوثيق رسالته، أو أنشئه(م.خ.ت.إ) لتوثيق شهادته الإلكترونيّة(يمكن لشهادة أن تُوثق باستخدام مفتاح عمومي مبيّن في شهادة أخرى غير تلك الشّهادة)، فينبغي عموما أن يُختم زمنيا في وقت إصدار الشّهادة على نحوٍ يُعوّل عليها.

انطلاقا من ذلك، فإنّ الوظيفة الرّئيسية لشهادة التّصديق الموصوفة تكمن في ربط مفتاح عام بصاحب الشّهادة(المُوقّع أو جهة التّوثيق)، حيث تسمح(الشّهادة) للطرف المعوّل عليها(متلقي الرّسالة الإلكترونيّة) استعمال المفتاح العام المذكور فيها، للتّحقّق من أنّ التّوقيع

[1] راجع أحكام المادتين 07 و15 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر.

الرّقمي أنشئ باستخدام المفتاح الخاص المناظر له(المفتاح العام)، كما يمكن كذلك التّحقق من صّحة التّوقيع الرّقمي على الشّهادة من جانب(م.خ.ت.إ) مُصدر الشّهادة، باستخدام المفتاح العام الخاص بـ(م.خ.ت.إ) المبيّن في شهادة أخرى صادرة عن(م.خ.ت.إ) آخر[1].

ب)– سيطرة الموقّع لوحده دون غيره على الوسيط الإلكتروني:

يُقصد بالوسيط الإلكتروني أيّ جهاز أو برنامج معلوماتي مُعدّ لتطبيق بيانات إحداث التّوقيع الإلكتروني الفريدة بالموقّع، حيث تشتمل هذه الأخيرة(البيانات) على كلّ من زوج مفاتيح التّشفير(الخاص والعام) أو الرّموز أو العناصر الأخرى المُستخدمة في عملية إحداث التّوقيعات الإلكترونيّة الموصوفة[2]، بينما ينبغي أن ترتبط هذه البيانات ارتباطا وثيقا بصاحب التّوقيع الإلكتروني لوحده فقط، وبالتّالي يجب على الرّاغب في إحداث توقيع إلكتروني موصوف الاستعانة بالآلية المؤمّنة لإحداثه تتوّفر فيها المتطلّبات المحدّدة بموجب المادة(11) من نفس القانون، كضمان سريّة وأحادية البيانات المستخدمة في إحداث التّوقيع الإلكتروني أي(عدم مُصادفتها لأكثر من مرّة واحدة) مع عدم اكتشافها عن طريق عملية الاستنتاج، وأن لا تُغيّر(الآلية المؤمّنة) من البيانات التي ستُوقّع أو تَمْنَع من عرضها للمُوقِّع قبل عملية التّوقيع عليها، كما ينبغي أن تكون بيانات إحداث التّوقيع الإلكتروني محميّة بطريقة مؤمّنة من قِبَلِ المُوقّع الشّرعي لها ضّد أيّ استعمال تعسّفي من قِبَلِ الغَيْرِ.

لذا ينبغي على الرّاغب في إحداث توقيع إلكتروني موصوف أن يمارس العناية اللاّزمة لضمان دّقة واكتمال كلّ ما يُقدّمه من تأكيدات جوهريّة، ذات صلة بالشّهادة طيلة مُدَّة سريانها وأن يَجْتَنِبَ أو يتفادى الاستخدام غير المأذون به، لبيانات إحداث توقيعه الإلكتروني

---

[1] **عبد الله أحمد غرايبة**، حجية التوقيع الإلكتروني في التشريع المعاصر، دار الراية للنشر والتوزيع، عمان، الأردن، 2008، ص ص 150– 153.

[2] **Art. 03-23 (Règlement (eIDAS))**: « Dispositif de création de signature électronique qualifié», un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'**annexe II**.»

محمد محمد سادات، حجية المحرّرات الموقعة إلكترونيًّا في الإثبات (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2011، ص ص 131– 133.

مع استعمال جميع الوسائل المُسّخرة من طرف(م.خ.ت.إ) الموثوق به، في حين يجب على صاحب شهادة التّصديق أن يطلب إلغاءها لدى الجهة المُصدِرة لها في حالة الشّك من تعرّض بياناتها لما يثير الشّبهة فيها، ففي حالة انتهاء مدة صلاحية الشّهادة أو تّم إلغاءها فلا يجوز استعمال بيانات إنشاء التّوقيع المُوافِقة لها لدى(م.خ.ت.إ) آخر من أجل توقيع أو تصديق تلك البيانات(نفسها).

ج)– إمكانية كشف أي تعديل أو تبديل في البيانات الإلكترونيّة المُوقّعة:

توجد إلى جانب عملية إحداث أزواج مفاتيح التّشفير غير المتناظرة(المفتاح الخاص والعام) تقنيّة أساسيّة أخرى معروفة، بدالة البَعثرة ذات الاتّجاه الواحد (Hachage à sens unique)، حيث تُستخدم في إنشاء التّوقيعات الرّقميّة وفي التّحقق من صّحتها، فمن خلالها يتّم ربط التّوقيع الإلكتروني الموصوف بطريقة آلية بالمحرّر الإلكتروني ارتباطا وثيقا يسمح بكشف أيّ تعديل أو تغيير أو تزوير في بيانات المحرّر الإلكتروني عند مباشرة إجراءات التّحقق من صّحته.

وعليه، تعتمد دالة البَعثرة على خوارزميات رياضيّة خاصّة بها (Algorithmes de compression à sens unique -ou- Cryptographie à clé privée)، حيث تقوم برمجيات إعداد التّوقيع الإلكتروني بإنشاء خلاصة للمحرّر الإلكتروني في شكل مضغوط(Comprimé-Abrégé)، أو بصمة رقميّة(Empreinte digitale du message) لتشفيرها بإحدى خوارزميات وظيفة الهاش الأحادية الاتّجاه (MD5, SHA-1, RIPE-MD 160, MAC DES, etc.)، لغرض الحصول على قيمة أو نتيجة هاش (Résultat-Valeur de hachage) ذات طول مُوحّد يكون عادة أصغر بكثير من المحرّر الإلكتروني، حيث ينفرد بها(القيمة أو النتيجة) هذا المحرّر إلى حدّ كبير[1]، وبعدها يقوم برنامج الحاسوب بتشفير قيمة الهاش المُستخلصة عن طريق إحدى خوارزميات المفتاح العام (DSA, ECC,RSA, etc.) باستعمال المفتاح الخاص بالمُوقِّع لأجل إحداث التّوقيع الإلكتروني الموصوف، فأيّ

1) **Arnaud-F. FAUSSE**, op.cit., pp. 316, 317, 321, 322,

تغيير يطرأ على المحرّر الإلكتروني بعد توقيعه تترتّب عنه حتمًا نتيجة بعثرة(هاش) مختلفة عندما يتم إعادة احتساب دالة البعثرة نفسها.

انطلاقا من ذلك، فإنّ دوال البعثرة المؤمّنة(Fonction de hachage sécurisée) التي يُطْلَقُ عليها عادة مُصطلح دالة البعثرة الأُحادية الاتِّجاه (Fonction de hachage unidirectionnelle) تضمن الارتباط القّوي والوثيق للتّوقيع الإلكتروني بمحتوى المحرّر الإلكتروني الأصلي، وتؤكّد مدى تعرّض محتوى بياناته لأيّ تغيير أو تعديل في وقت أو قبل صدور شهادة التّصديق الإلكتروني الموصوفة، كما يجب على القائم بعملية الفحص(الطرف المعوّل على الشّهادة) التّأكد من موثوقيّة وصلاحية شهادة التّصديق الإلكتروني المطلوبة عند التّحقق من التّوقيع الإلكتروني، وعليه ألزم المشّرع الجزائري بموجب المادة(12) من القانون رقم 04/15 المتعلّق بالتّوقيع والتّصديق الإلكترونيين، أن تكون آلية فحص التّوقيع الإلكتروني الموصوف موثوقة تتوّفر فيها المتطلّبات المحدّدة في المادة(13) من نفس القانون، كضمان تحديد هوّية المُوقِّع وعرض نتيجة مطابقة بيانات إحداث توقيعه الإلكتروني لبيانات فحصه بوضوح، مع كشف أيّ تغيير أو تعديل في محتوى البيانات الإلكترونية بطريقة مؤمّنة[1].

[1] تنص المادة 12 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، على ما يلي:" يجب أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة."
تنص المادة 13 من نفس القانون، على ما يلي:" الآلية الموثوقة للتحقق من التوقيع الإلكتروني هي آلية تحقق من التوقيع الإلكتروني تتوفر فيها المتطلبات الآتية: 1- أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الالكتروني؛
2- أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة وأن تكون نتيجة هذا التحقق معروضة عرضا صحيحا؛
3- أن يكون مضمون البيانات الموقعة، إذا اقتضى الأمر، محددا بصفة مؤكدة عند التحقق من التوقيع الالكتروني؛
4- أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الالكتروني المطلوبة عند التحقق من التوقيع الالكتروني؛
5- أن يتم عرض نتيجة التحقق وهوية الموقّع بطريقة واضحة وصحيحة."

الفرع الثاني
تطبيقات التّصديق الإلكتروني في مجال التّجارة الإلكترونيّة

إنّ تطبيقات التّصديق الإلكتروني في مجال التّجارة الإلكترونيّة متعدّدة ومتنوّعة بحسب الخدمات التّجارية والمصرفيّة المتاحة عبر شبكة الإنترنت، والمتمثّلة فيما يلي:

أولا– توثيق مواقع التّجارة الإلكترونيّة:

تقوم سلطات التّصديق الإلكتروني باصدار الشّهادات الالكترونيّة وفقا لمستويات الأمان المطلوبة وكذا الأغراض التي أصدرت من أجلها كل شهادة، وبالتّالي فشهادات التّصديق الإلكتروني تُستخدم في أغراض متعدّدة فقد تُستعمل لتوثيق الخوادم أو المواقع الإلكترونيّة عبر شبكة الإنترنت، من أجل جذب والحصول على ثقة مستخدمي خادم الويب أو أي موقِع إلكتروني مع ضمان أنّ ذلك الخادم أو الموقِع الإلكتروني هو ذاته المَقصُودْ أو التّابع للشّركة الأصليّة الذي تُديره، وبالتّالي لم يتعرّض كل مِنْهُمَا إلى عملية الاختراق أو إنتحال اسم النّطاق الخ...، وكذلك يُمْكِنُ استخدام شهادات التّصديق الإلكتروني لغرض توثيق برمجيات الحاسوب، من أجل ضمان صحّة برنامج معلوماتي في مواقِع الإنترنت أو لضمان استعمال خادم تطبيقات برمجية معيّن معتَرف به على نطاق واسع على أنّه يُوفّر مُستوى مُعيّنًا من الثّقة والأمان في الاتّصال الشّبكي، كما يمكن أن يكون الغرض من إصدار شهادة التّصديق الإلكتروني لغرض توثيق أي بيانات أخرى مُوزَّعة أو مُخزَّنة بطريقة إلكترونيّة[1].

ثانيا– تأمين تقنيات الدّفع الإلكتروني عبر الإنترنت :

تتّم معاملات التّجارة الإلكترونيّة في بيئة افتراضيّة مملوءة بالمخاطر المتعلّقة بانتحال الهويّة، واختراق البيانات الإلكترونيّة المتداولة وإنكار عملية البيع أو الدّفع فيما بين أطراف التّصرف الإلكتروني، ولضمان تبادل البيانات عبر الإنترنت يتّم الإستعانة بتقنيات

1) **Louise MARTEL, René ST-GERMAIN**, « Les sceaux de certification des sites web : un outil de confiance, outil de confusion », op.cit., pp. 10- 13.

التّصديق الإلكتروني الموثوق بها، التي تضمن تحديد هوّية أطراف العقد الإلكتروني، وتؤكّد سلامة وسريّة البيانات المتداولة فيما بينهم مع عدم إنكارها في وقت إصدار شهادة التّصديق الموصوفة، فعن طريق هذه الأخيرة يمكن للمصارف والمؤسّسات الماليّة والمتاجر الافتراضيّة أن تضمن العمليات الماليّة التي تتّم عبر منصّاتها الإلكترونيّة، التي من خلالها يقوم المُستهلك بمُباشرة إجراءات الدّفع الإلكتروني المؤمّنة لمُستحقات فواتير الغاز والكهرباء والميّاه، والشّيكات الإلكترونيّة والاعتماد المستندي الإلكتروني والأوامر التّجارية أو أيّ وثائق تجارية أخرى بشكل عام[1].

ثالثا– توثيق الصّفقات التّجارية الإلكترونيّة:

تتّم معاملات التّجارة الإلكترونيّة في بيئة إلكترونيّة افتراضيّة مملوءة بالمخاطر المتعلّقة بانتحال الهويّة واختراق البيانات الالكترونيّة وإنكار عملية التّبادل والدّفع الإلكترونيين، الأمر الذي يستوجب توفير الضّمانات الكفيلة بتحديد هوّية أطراف العقد الالكتروني ومضمونه، والتّيقن من إرادة كل من المتعاقدين وصّحتها ونسبتها إلى من صدرت منه[2]، ولتحقيق كل ذلك يستلزم على أطراف العقد الإلكتروني الاستعانة بخدمات طرف ثالث محايد وموثوق به، يقوم بدور الوسيط بين المتعاقدين لغرض توثيق تعاملاتهم الإلكترونيّة بالتّعويل على تقنيات تصديق إلكترونيّة مؤمّنة وموثوقة وفقا للمعايير المُعترف بها دوليا.

عليه، فإنّ الطرف الثالث قد يكون في هيئة فرد أو شركة أو جهة مستقّلة محايدة تقوم بإصدار شهادات تصديق إلكتروني موصوفة لأطراف العقد الالكتروني، لغرض الاعتراف

---

1) **Tarik CHALLALI**, « Solutions d'accès sécurisées pour opérer une Market Place Saas multitenante », pp. 05-15. **(**SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, au Cercle National de l'Armée, à Alger. https://www.arpce.dz

للمزيد من المعلومات حول الموضوع، راجع أحكام نصوص المواد 414، 3/467، 502، ومن 472 إلى 543، من الأمر رقم 75–59 المؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، المعدل والمتمم بموجب القانون رقم 05–02 المؤرخ في 06 فيفري 2005، ج ر عدد 11، الصادر في 09 فيفري 2005.

2) **صالح بن علي بن حمد الحراصي**، الإثبات في عقود التجارة الالكترونية في القانون العماني والقانون المقارن، مكتبة الضامري للنشر والتوزيع، السيب، سلطنة عمان، 2009، ص ص 126، 127.

بوجود صلة بين بيانات إحداث التّوقيع الالكتروني الموصوف والمُوقّع أو بيان وجود تلك الصّلة أو تأكيد وجودها، وتُنشأ تلك الصّلة عند إحداث بيانات التّوقيع الإلكتروني الموصوف، فالوظيفة الرّئيسيّة لشهادة التّصديق تتمثّل في ربط المفتاح العام بالمفتاح الخاص بالمُوقِّع، حيث يُستعمل المفتاح العام المذكور فيها(شهادة التّصديق) للتّحقّق من أنّ بيانات إحداث التّوقيع الإلكتروني مُطابقة تماما لبيانات فحصه في وقت إصدار الشّهادة أو قبل ذلك، فإذا توصّل القائم على عملية الفّحص من صّحة عملية المُطابقة فيعني أنّ بيانات إحداث التّوقيع الإلكتروني صحيحة ولم تتعرّض لما يُثير الشُّبهة ولم يتّم التّلاعب فيها بأيّ شكل سواء بالحذف أو التّعديل أو بالإضافة، وبالتّالي تصبح بيانات العقد الإلكتروني موثّقة ولا يُمكن إنكارها[1].

رابعا– ضمان خدمات المؤسّسات الصّغيرة والمتوسّطة:

تضمن تقنيات التّصديق الإلكتروني الموثوق بها للمؤسّسات الصّغيرة والمتوسّطة[2]، مُعالجة العديد من التّصرفات الإلكترونيّة عبر شبكة الإنترنت بكلّ سريّة وأمان، فعن طريق

---

[1] **صالح بن علي بن حمد الحراصي**، مرجع سابق، ص ص 141، 142.

[2] قانون رقم 17–02 مؤرخ في 10 جانفي 2017، يتضمن القانون التوجيهي لتطوير المؤسسات الصغيرة والمتوسطة، ج ر عدد 02، الصادر في 11 جانفي 2017.

تنص **المادة 05** على ما يلي:" تعرّف المؤسسة الصغيرة والمتوسطة، مهما كانت طبيعتها القانونية، بأنّها مؤسسة إنتاج السلع و/أو الخدمات: – تُشغّل من واحد(1) إلى مائتين وخمسين(250) شخصا، – لا يتجاوز رقم أعمالها السنوي أربعة(4) ملايير دينار جزائري أو لا يتجاوز مجموع حصيلتها السنوية مليار(1) دينار جزائري، – تستوفي معيار الاستقلالية كما هو محدد في النقطة 3 أدناه.

يقصد في مفهوم هذا القانون، بما يأتي: [...]. **3– المؤسسة المستقلة:** كل مؤسسة لا يُمتلك رأس مالها بمقدار 25% فما أكثر من قِبَلِ مؤسسة أو مجموعة مؤسسات أخرى، لا ينطبق عليها تعريف المؤسسات الصغيرة والمتوسطة. [...]."

وتنص **المادة 08** على ما يلي:" تعرّف المؤسسة المتوسطة بأنّها مؤسسة تشغل ما بين خمسين(50) إلى مائتين وخمسين(250) شخصا، ورقم أعمالها السنوي ما بين أربعمائة(400) مليون دينار إلى أربعة(4) ملايير دينار جزائري، أو مجموع حصيلتها السنوية ما بين مائتي(200) مليون دينار إلى مليار(1) دينار جزائري."

وتنص **المادة 09** على ما يلي:" تعرّف المؤسسة الصغيرة بأنّها مؤسسة تُشغّل ما بين عشرة(10) إلى تسعة وأربعين(49) شخصا، ورقم أعمالها السنوي لا يتجاوز أربعمائة(400) مليون دينار جزائري، أو مجموع حصيلتها السنوية لا يتجاوز مائتي(200) مليون دينار جزائري."

شهادة التّصديق الإلكتروني الموصوفة يتم تخفيض ميزانية مُراسلات البريد الورقي وتجريدها من طابعها المادّي إلى الإلكتروني، وكذا إبرام العقود الإلكترونيّة وإمضاء أوامر الشّراء، والإشعارات المتنوّعة والرّسائل الأخرى[1]، كما تضمن شهادة التّصديق المُشاركة في المناقصات عبر الإنترنت، أين يتّم تحميل مِلّف المشاركة وتنظيم وتوقيع الوثائق والإيداع المُباشر لسّجل المناقصة عبر الإنترنت، الخ...[2].

خامسا– ضمان أمن الحِساب الضّريبي عبر الإنترنت:

تضمن شهادة التّصديق الإلكتروني للمورّد الإلكتروني أو المستهلك الاطّلاع على بياناتهم الالكترونيّة بكل سريّة وأمان عبر الموقِع الإلكتروني لإدارة الضّرائب، الذي من خلاله يتم التّصريح عن جميع المداخيل الخاضعة لضريبة القيمة المُضافة(TVA) ومُتابعة المدفوعات الضّريبيّة وإجراء الطّعون، والدّفع الإلكتروني للضّريبَة المستّحقة عن طريق البطاقة المصرفيّة الذّهبيّة(CIB) الخ...[3].

وتنص **المادة 10** على ما يلي:" تعرّف المؤسسة الصغيرة جدّا بأنّها مؤسسة تُشغل من شخص(1) إلى تسعة(9) أشخاص، ورقم أعمالها السنوي أقل من أربعين مليون(40) مليون دينار جزائري، أو مجموع حصيلتها السنوية لا يتجاوز عشرين(20) مليون دينار جزائري."

وتنص **المادة 11** على ما يلي:" إذا صنفت مؤسسة في فئة معينة وفق عدد عمالها، وفي فئة أخرى طبقا لرقم أعمالها أو مجموع حصيلتها، تعطى الأولوية لمعيار رقم الأعمال أو مجموع الحصيلة لتصنيفها."

وتنص **المادة 12** على ما يلي:" عندما تسجل مؤسسة، عند تاريخ إقفال حصيلتها المحاسبية فارقا أو فوارق بالنسبة للحد أو الحدود المذكورة أعلاه، فإنّ هذا لا يكسبها أو يفقدها صفة المؤسسة الصغيرة والمتوسطة، طبقا للمواد 8 و9 و10 أعلاه، إلاّ إذا استمرت هذه الوضعية لمدة سنتين(2) ماليتين متتاليتين."

[1] للمزيد من المعلومات أنظر الموقع الإلكتروني التالي: https://www.arpt.gouve.dz

[2] أنظر الموقع الإلكتروني التالي: https://www.arpt.gouve.dz

[3] للمزيد من المعلومات أنظر المواقع الإلكترونية التالية: https://www.mf.gouve.dz et http //www.dgi.gouve.dz

الفرع الثالث
جِهة توثيق العقد الإلكتروني

يعتبر عنصر الثّقة والأمان من بين الضّمانات الرّئيسيّة التي يجب توافرها في معاملات التّجارة الإلكترونيّة، حيث ارتأت مختلف التّشريعات الدّوليّة والوطنيّة إلى ضرورة إيجاد طرف ثالث محايد يُشرف على مهام خدمات التّصديق الإلكتروني**(أوّلا)**، الذي يستوجب عليه مراعاة مجموعة من الشّروط المفروضة عليه من قِبَلِ التّشريعات التي تُمّكنُهُ من مُباشرة خدمات التّصديق الإلكتروني الموثوق بها**(ثانيا)**.

أولا– المقصود بجهة توثيق العقد الالكتروني.

يُشَارُ عُمُوماً إلى الطرف الثالث المُحايِد عن أطراف العقد الإلكتروني بعبارة "سلطة التّصديق"، أو "مقدّم خدمات التّصديق"، أو "مورّد خدمات التّصديق"، أو "مؤدّي خدمات التّوثيق"، أو "الطرف الثالث الموثوق"، الخ...، فخدمات التّصديق الالكتروني تشمل على العديد من المجالات حيث يُمكِن أن تتّم في إطار القطاع العام لحساب المؤسّسات العموميّة والجهات الحكوميّة، أو في القطاع الخاص على غرار التّجارة الإلكترونيّة والعمليات المصرفيّة الإلكترونيّة الخ...، فقد تطرّق المشّرع الجزائري بموجب المادة 12/02 من القانون رقم 04/15 المؤرخ في 01 فيفري 2015، الذي يُحدّد القواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين[1]، إلى تعريف مؤدّي خدمات التّصديق على أنّه:" شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات تصديق أخرى في مجال التصديق الإلكتروني."، بينما عرّف الطرف الثالث الموثوق بموجب الفقرة 11 من نفس المادة(11/02) على أنّه:" شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في القطاع الحكومي."

[1] راجع أحكام المادة 11/02–12–13 من القانون رقم 15–04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر.

وعليه، يُقْصَدُ بِالْمُتَدَخِّلِينَ في الفرع الحكومي وفقا للفقرة 13 من نفس المادة(13/02) على أنّهم:" المؤسسات والإدارات العمومية والهيئات العمومية المحددة في التشريع المعمول به، والمؤسسات المستقلة وسلطات الضبط، والمتدخلين في المبادلات ما بين البنوك، وكذا كل شخص أو كيان ينتمي إلى الفرع الحكومي بحكم طبيعته أو مهامه."

أمّا بالنّسبة للمشّرع التّونسي، فقد تطرّق بموجب الفصل 4/02 من القانون عدد 83/2000 المؤرخ في 09 أوت 2000 المتعلّق بالمبادلات والتّجارة الإلكترونيّة[1]، إلى تعريف مُزوّد خدمات المصادقة الإلكترونيّة على أنّه:" كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني."

كما أنّ القانون النّموذجي بشأن التّوقيعات الإلكترونيّة مع دليل الإشتراع لسنة 2001، الذي وضعته لجنة الأمم المتّحدة للقانون التّجاري الدّولي(الأونسيترال)[2]، تطرّق بموجب المادة 02/(هـ) منه إلى تعريف مقدّم خدمات التّصديق على أنّه:" يعني شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية."

بالإضافة إلى ذلك، تطرّق المشّرع الفيدرالي للاتّحاد الأوروبي بموجب المادة 19/03 من التّنظيم رقم 910/2014 المؤرخ في 23 جويلية 2014، المتعلّق بالهويّة الإلكترونيّة وخدمات الثّقة المتّصلة بالمعاملات الإلكترونيّة في إطار السّوق الدّاخلي، المُلغي للتّوجيه الأوروبي رقم 93/1999 المتعلّق بالتّوقيعات الإلكترونيّة(eIDAS)[3]، إلى تقديم مفهوم عام

---

[1] راجع الفصل 4/02 من القانون عدد 2000/83 المؤرخ في 09 أوت 2000، الذي يتعلق بالمبادلات والتجارة الإلكترونية(تونس)، سالف الذكر.

[2] القانون النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع لسنة 2001، الذي اعتمدته لجنة الأمم المتحدة للقانون التّجاري الدولي(الأونسيترال). http://www.uncitral.org

[3] **Art.03-19 et 20 (Règlement (eIDAS)):** « (**Prestataire de services de confiance**), une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié;

لمقدّم خدمات الثّقة على أنّه:" شخص طبيعي أو معنوي يتيح خدمة أو العديد من خدمات الثقة، بصفته كمقدم خدمات الثقة المؤهل أو الغير المؤهل."، حيث يُقْصَدُ بمقدّم خدمات الثّقة المؤهّل وفقا للفقرة 20 من نفس المادة(20/03)(eIDAS) على أنّه:" مقدم خدمات الثقة الذي يُتيح خدمة أو العديد من خدمات الثقة المؤهلة، حيث تَحَصَّلَ على تأهيل من طرف هيئة الرقابة."

فخدمات الثّقة، وفقا للفقرة 16 من نفس المادة(16/03)(eIDAS)، تشمل خدمات إحداث وفحص صّحة التّوقيعات والأختام والتّواريخ الإلكترونيّة، وخدمات الإرسال الإلكتروني المُوصَى عليهِ(Envoi recommandé électronique)، والشّهادات المتعلّقة بهذه الخدمات، أو تتضمّن على خدمات إحداث وفحص صّحة شهادات التّعريف بمواقع الإنترنت، وكذا حفظ التّوقيعات والأختام الإلكترونيّة أو الشّهادات المتعلّقة بهذه الخدمات[1].

فإلى جانب ذلك، تطرّق المشّرع الفيدرالي للكُنْفِدِيرَالِيَّة السَّوِيسْرِيّة بموجب المادة 02/(k) من القانون الفيدرالي المُتعلّق بخدمات التّصديق في مجال التّوقيع الالكتروني والخدمات الأخرى المتعلّقة بالشّهادات الرّقمية، المؤرخ في 18 مارس 2016 (Loi sur la signature électronique, SCSE du 18 mars 2016)، و**المُلغي** للقانون الفيدرالي المؤرخ في 19

« **Prestataire de services de confiance qualifié**», un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié ; […].»

1) **Art.03-16 et 17 (Règlement (eIDAS))**: «(**service de confiance**), un service électronique normalement fourni contre rémunération qui consiste: **a)** en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou **b)** en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou **c)** en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;

- «**service de confiance qualifié**», un service de confiance qui satisfait aux exigences du présent règlement;[…]»

ديسمبر 2003 المتعلق بالتوقيعات الإلكترونية[1]، إلى تعريف مزوّد خدمات التّصديق على أنّه:" هيئة تقوم بتوثيق البيانات في بيئة إلكترونية وتقوم بإصدار الشهادات الرقمية."

ثانيا– شروط مزاولة خدمات التصديق الإلكتروني.

نظّم المشّرع الفيدرالي للاتّحاد الأوروبي في إطار أحكام المادتين 21 و22 من التنظيم رقم 910/2014 المؤرخ في 23 جويلية 2014، المتعلّق بالهويّة الإلكترونية وخدمات الثّقة المتّصلة بالمعاملات الإلكترونيّة في إطار السّوق الدّاخلي(eIDAS)، شروط مزاولة خدمات الثّقة المؤهّلة(Service de confiance qualifié) التي من خلالها يجب على المزوّد(PSC) الرّاغب في مُباشرة هذه الخدمات[2]، أن يُقدّم إلى هيئة الرّقابة طلب مَصحوب بتقرير تقييم

---

1) **Art.02** (**LFSCSE du 18 mars 2016**): « Définitions Au sens de la présente loi, on entend par : […] ; **c. Signature électronique réglementée**: une signature électronique avancée créée au moyen d'un dispositif sécurisé de création de signature au sens de l'art. 6 et fondée sur un certificat réglementé se rapportant à une personne physique et valable au moment de sa création;[…] ;
e. Signature électronique qualifiée: une signature électronique réglementée fondée sur un certificat qualifié;[…] ;
g. Certificat réglementé: un certificat numérique qui remplit les conditions fixées à l'art. 7 et est délivré par un fournisseur de services de certification reconnu en vertu de la présente loi;
h. Certificat qualifié: un certificat réglementé qui remplit les conditions fixées à l'art.8; […] ;
l. organisme de reconnaissance: un organisme qui est habilité à reconnaître et à surveiller les fournisseurs en vertu des règles d'accréditation de la législation sur les entraves techniques au commerce. »
Art. 22(**LFSCSE du 18 mars 2016**): « Abrogation et modification d'autres actes L'abrogation et la modification d'autres actes sont réglées en annexe. **Annexe (art. 22)** Abrogation et modification d'autres actes. **I-** La **loi du 19 décembre 2003** sur la signature électronique est **abrogée**. […]. »
Art. 23(**LFSCSE du 18 mars 2016**) : « Référendum et entrée en vigueur **1**- La présente loi est sujette au référendum.
2- Le Conseil fédéral fixe la date de l'entrée en vigueur.
- Expiration du délai référendaire et entrée en vigueur
1- Le délai référendaire s'appliquant à la présente loi a expiré le 7 juillet 2016 sans avoir été utilisé. **2**- La présente loi entre en vigueur le **1er janvier 2017**. »

2) **Art. 21(Règlement (eIDAS))**: « (**Lancement d'un service de confiance qualifié**) **1.** Lorsque des prestataires de services de confiance, sans statut qualifié, ont l'intention de commencer à offrir des services de confiance qualifiés, ils soumettent à l'organe de contrôle

المطابقة الممنوح له من طرف هيئة التّقييم، حيث تقوم هيئة الرّقابة بفحص مدى مراعاة المزوّد(PSC) للشّروط المتعلّقة بمقدّم خدمات الثّقة المؤهّل وبخدمات الثّقة المؤهّلة التي يُتيحها، ففي حالة استيفائها من طرف المُزوّد(PSC)، تُوافق هيئة الرّقابة على مَنْحِهِ للتّأهيل(PSC qualifié) مع إعلامها للّجنة الأوروبيّة بُغية تصنيف المُزوِّد(PSC qualifié) خلال ثلاث(03) أشهر الموالية لإيداع الطّلب، ضمن قوائم الثّقة المُشار إليها في المادة 1/22 من نفس التّنظيم(eIDAS)، التي تقوم الدّولة المعنيّة بتحديثها ونشرها بطريقة مؤمّنة عبر الإنترنت[1]، وفي حالة عدم انتهاء هيئة الرّقابة من عملية الفّحص خلال فترة

---

une notification de leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité.

2. L'organe de contrôle vérifie que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le présent règlement, en particulier les exigences en ce qui concerne les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent. Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier alinéa, l'organe de contrôle accorde le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit et informe l'organisme visé à l'article **22, paragraphe 3**, aux fins de la mise à jour des listes de confiance visées à l'article **22, paragraphe 1**, au plus tard **trois mois** suivant la **notification** conformément au **paragraphe 1** du présent article. Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

3. Les prestataires de services de confiance qualifiés peuvent commencer à fournir le service de confiance qualifié une fois que le statut qualifié est indiqué sur les listes de confiance visées à l'article 22, paragraphe 1. […]. »

1) **Art. 22**(**Règlement (eIDAS)**) : « (**Listes de confiance**) **1.** Chaque État membre établit, tient à jour et publie des listes de confiance, y compris des informations relatives aux prestataires de services de confiance qualifiés dont il est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent.

2. Les États membres établissent, tiennent à jour et publient, de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance visées au paragraphe 1 portant une signature électronique ou un cachet électronique.

3. Les États membres communiquent à la Commission, dans les meilleurs délais, des informations relatives à l'organisme chargé d'établir, de tenir à jour et de publier les listes nationales de confiance, ainsi que des détails précisant où ces listes sont publiées, indiquant les certificats utilisés pour apposer une signature électronique ou un cachet électronique sur ces listes et signalant les modifications apportées à ces listes.

ثلاثة(03) أشهر الموالية لإيداع الطّلب، يجب على تلك الهيئة أن تُعْلِمَ المُزوّد بسبب التّأخر والمدّة الضّروريّة لإنهاء عملية الفَّحْصِ، فبمجرّد إعلان المُزوّد ضمن قائمة الثّقة يُمكنه مزاولة خدمات الثّقة المؤهّلة.

وعليه، فإنّ مزوّد خدمات الثّقة المؤهّل يخضع في كل 24 شهر على الأقّل وعلى نفقاته لتدقيق من طرف هيئة تقييم المطابقة، للتّأكد من مدى مراعاته للشّروط المتعلّقة بخدمات الثّقة المُؤهّلة المُحدّدة بموجب هذا التّنظيم(eIDAS)، حيث يقوم المُزوّد(PSC qualifié) بإرسال تقرير تقييم المطابقة لهيئة الرّقابة خلال ثلاثة أيام الموالية لتاريخ استلامه (Rapport d'évaluation de la conformité)، وفي جميع الظروف، يمكن لهيئة الرّقابة أن تُخْضِعَ المُزوّد المُؤهّل في أيّة لحظة لتدقيق أو تطلب إجراء تقييم المطابقة على نفقاته(المُزوّد) للتّأكد من مدى مراعاته لشروط مزاولة نشاطه، وإذا تبيّن في نتائج التّدقيق عن تواجد إخلال بالمعطيات الشّخصيّة المحميّة تُخطر هيئة الرّقابة الجهات المعنيّة بذلك، وفي حالة إلزام هيئة الرّقابة مزوّد خدمات الثّقة المؤهّل(PSC qualifié) بتصحيح النّقائص التي تمّت معاينتها ولم يَقُمْ بذلك خلال المدّة المُحدّدة، تقوم هيئة الرّقابة بسحب التّأهيل الممنوح للمُزوّد مع إعلام لجنة الاتّحاد الأوروبي، بُغية تحديث قوائم الثّقة المُشار إليها بموجب المادة 1/22 من نفس التّنظيم(eIDAS)[1].

---

4. La Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées au paragraphe 3 sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé. […]. »

[1] **Art. 20(Règlement (eIDAS))**: « (**Contrôle des prestataires de services de confiance qualifiés**) **1.** Les prestataires de services de confiance qualifiés font l'objet, au moins tous les **vingt-quatre mois**, d'un **audit** effectué à leurs frais par un organisme d'évaluation de la conformité. Le but de l'**audit** est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'organe de contrôle dans un délai de trois jours ouvrables qui suivent sa réception.

2. Sans préjudice du paragraphe 1, l'organe de contrôle peut à **tout momen**t, soumettre les prestataires de services de confiance qualifiés à un **audit** ou **demander** à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires

كما نص المشّرع الفيدرالي للكُنفيدِرالية السّويسريّة بموجب المادة 03 من القانون الفيدرالي المؤرخ في 18 مارس 2016، المُتعلّق بخدمات التّصديق في مجال التّوقيع الالكتروني والخدمات الأخرى المتعلّقة بالشّهادات الرّقميّة(LFSCSE du 18 mars 2016)[1]، على شروط الاعتراف بمُزوّدي خدمات التّصديق الإلكتروني، التي من خلالها يجب على كل شخص طبيعي أو معنوي أن يكون لديه سجّل تجاري(الوحدات الإداريّة والمقاطعات

---

de services de confiance qualifiés, aux frais de ces prestataires de services de confiance, afin de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. L'organe de contrôle informe les autorités chargées de la protection des données des **résultats de ses audits** lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées.
3. Lorsque l'organe de contrôle exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues par le présent règlement et que le prestataire n'agit pas en conséquence, et le cas échéant dans un délai fixé par l'organe de contrôle, l'organe de contrôle, tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer à ce prestataire ou au service affecté le statut qualifié et informe l'organisme visé à l'article **22, paragraphe 3**, aux fins de la mise à jour des listes de confiance visées à l'article **22, paragraphe 1**. L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné. […]. »

[1] **Art. 03(LFSCSE du 18 mars 2016)** : « (Conditions de la reconnaissance) **1-** Peuvent être reconnues comme **fournisseurs** les personnes physiques ou morales qui: **a.** sont **inscrites** au **registre** du commerce; **b.** sont en mesure de délivrer et de gérer des certificats **qualifiés** conformément aux exigences de la présente loi; **c.** emploient du **personnel** possédant les connaissances, l'**expérience** et les **qualifications** nécessaires; **d.** utilisent des systèmes et des produits informatiques, notamment des dispositifs de création de **signature** et de **cachet**, qui soient fiables et sûrs; **e.** possèdent des ressources ou des garanties financières suffisantes;
f. ont contracté les assurances nécessaires à la couverture de la responsabilité visée à l'art. 17 et des frais que peuvent entraîner les mesures prévues à l'art. 14, al. 2 et 3; g. assurent le respect du droit applicable, notamment de la présente loi et de ses dispositions d'exécution.
2- Les conditions fixées à l'al. 1 sont applicables également aux fournisseurs étrangers. L'organisme de reconnaissance suisse peut reconnaître un fournisseur étranger qui est déjà reconnu par un organisme étranger s'il est prouvé que: **a.** la reconnaissance a été octroyée conformément au droit de l'État en question; **b.** les règles du droit de l'État étranger applicables à l'octroi de la reconnaissance sont équivalentes à celles du droit suisse; **c.** l'organisme de reconnaissance étranger possède des qualifications équivalentes à celles qui sont exigées d'un organisme de reconnaissance suisse; **d.** l'organisme de reconnaissance étranger garantit sa collaboration à l'organisme de reconnaissance suisse pour la surveillance du fournisseur en Suisse.
3- Les unités administratives de la Confédération, des cantons et des communes peuvent être reconnues comme fournisseurs sans avoir à s'inscrire au registre du commerce. »

والبلديات مَعفية من السّجل التّجاري) مع إصدار شهادات التّصديق الموصوفة وفقا للشّروط المحدّدة بموجب هذا القانون(LFSCSE du 18 mars 2016)، وأن تكون لديه موارد ماليّة وبشريّة ضروريّة لمزاولة خدمات التّصديق الإلكتروني، مع استعمال أنظمة ومعدّات معلوماتيّة مؤمّنة وموثوقة لإحداث التّوقيعات الإلكترونيّة، مع امتلاكه لعقد تأمين لتغطية المسؤوليّة والتّكاليف المترتّبة عن إجراءات إيقاف خدمات التّصديق، كما يجب على المُزوّد احترام أحكام القوانين السّارية المفعول وبالخصوص القانون الفيدرالي المؤرخ في 18 مارس 2016(LFSCSE du 18 mars 2016) مع أحكامه التّنفيذيّة، حيث تُطبّق جميع هذه الشّروط على المزوّد الأجنبي الرّاغب في مزاولة خدمة التّصديق في سويسرا.

وعليه، فإنّ مركز الاعتراف السّويسري يمكن أن يعترف بخدمات المُزوّد الأجنبي المعترف من قِبَلِ مركز الاعتراف الأجنبي، في حالة ما إذا أثبت المزوّد الأجنبي قد تحصّل على الاعتراف وفقا لقانون الدّولة المَانِحَةِ لَهُ إياه، وأنّ قوانين الدّولة الأجنبيّة المتعلّقة بمنح الاعتراف مُطابِقة مع القوانين السّويسريّة، وأن تكون لدى مراكز الاعتراف الأجنبيّة مُؤهّلات مُطابقة لتلك المُؤهّلات التي يَشترِطها القانون السّويسري، وأن يضمن مركز الاعتراف الأجنبي التّعاون مع مركز الاعتراف السّويسري لِمُراقبة نشاطات المُزوّد الأجنبي في سويسرا.

في حالة الإعتراف بـ(م.خ.ت.إ)، تقوم مراكز الإعتراف بإرسال قائمة المزوّدين المُعترَفِ بهم إلى هيئة الإعتماد(SAS) التي تقوم بنشرها عبر موقعها الإلكتروني، حيث كلّف المشّرع الفيدرالي السّويسري بموجب المادة 04 من القانون الفيدرالي المُتعلّق بالتّوقيع الإلكتروني(LFSCSE du 18 mars 2016)، المجلس الفيدرالي كسلطة تنفيذيّة في الكنفيدراليّة السّويسرية، بِمُهمّة تَعيِين هيئة إعتماد مراكز الإعتراف بـ(م.خ.ت.إ)[1]، وفي حالة عدم تواجد

---

1) **Art.04** (**LFSCSE du 18 mars 2016**) : « (**Désignation de l'organisme d'accréditation**) **1-** Le Conseil fédéral désigne l'organisme d'accréditation des organismes de reconnaissance (organisme d'accréditation). **2-** Faute d'organisme de reconnaissance accrédité, le Conseil fédéral désigne comme tel l'organisme d'accréditation ou un autre organisme approprié. »
Art.05 (**LFSCSE du 18 mars 2016**) : « (**Liste des fournisseurs reconnus**) **1-** Les organismes de reconnaissance annoncent à l'organisme d'accréditation les fournisseurs qu'ils

مركز إعتراف مُعتمد، يتوّلى الدّيوان الفيدرالي للاتّصالات (l'Office fédéral de la communication(OFCOM)) وفقا للمادة 2/01 من الأمر الفيدرالي المتعلّق بالتّوقيع الإلكتروني(OSCSE du 23/11/2016)[1]، مهمّة تعيين مراكز الإعتراف بـ(م.خ.ت.إ)، حيث تتمثّل هيئة إعتماد مراكز الإعتراف وفقا للمادة 1/01 من نفس الأمر الفيدرالي (OSCSE 2016)، في مصلحة الإعتماد السّويسرية(Service d'accréditation suisse(SAS)) لدى أمانة الدّولة للإقتصاد، المُفَوَّضَة لاعتماد مراكز الإعتراف بـ(م.خ.ت.إ) وفقا للأمر الفيدرالي المؤرّخ في 17 جوان 1996 المتعلّق بالإعتماد والتّعيين[2].

كما قام المشّرع الجزائري بموجب أحكام المادتين 33 و34 من القانون رقم 15-04 المحدّد للقواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، بإخضاع نشاط التّصديق الالكتروني في المجال الاقتصادي إلى ترخيص تُصْدِرُهُ سلطة ضبط البريد والاتصالات

---

reconnaissent. **2-** L'organisme d'accréditation tient à la disposition du public la liste des fournisseurs reconnus. »

1) **Ordonnance sur la signature électronique, OSCSE** du 23 novembre 2016, RS 943.032(État le 1er janvier 2017).

Art.16 : « Abrogation et modification d'autres actes L'abrogation et la modification d'autres actes sont réglées en annexe. […]. Annexe (art. 16) Abrogation et modification d'autres actes **I** L'ordonnance du 3 décembre **2004** sur la signature électronique est **abrogée**. […]. »

Art.01 : « (Organismes de reconnaissance) **1-** Le Service d'accréditation suisse (**SAS**) du Secrétariat d'État à l'économie accrédite les organismes de reconnaissance des fournisseurs de services de certification conformément aux dispositions de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation.

2- S'il n'existe aucun organisme de reconnaissance accrédité, c'est l'Office fédéral de la communication (**OFCOM**) qui reconnaît les fournisseurs de services de certification (fournisseurs). »

2) **Ordonnance** sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement et d'homologation (Ordonnance sur l'accréditation et la désignation, **OAccD**) du 17 juin 1996, RS 946.512 (État le 20 avril 2016).

Art.02: « But de l'accréditation L'accréditation consiste à reconnaître formellement la compétence d'un organisme de procéder à des essais ou à des évaluations de la conformité conformément aux critères internationaux pertinents. »

Art.05: « **1-** Le Secrétariat d'État à l'économie (**SECO**) gère le Service d'accréditation suisse (**SAS**). **2-** Le **SAS** doit répondre aux critères internationaux pertinents, tels qu'ils sont notamment définis dans les normes figurant dans l'annexe 1. »

الإلكترونية(ARPCE)، وذلك بإعتبارها كسلطة تصديق فرعيّة تابعة للسّلطة الرئيسيّة (ANCE) على مُستوى مرفق المفاتيح العمومية الهرمي(Hyierarchy PKI) في الجزائر، مكلفة بمتابعة ومراقبة نشاطات(م.خ.ت.إ) المتعلّقة بالتوقيع والتصديق الإلكترونيين، حيث تمنح(س.ض.ب.إ.إ) التّرخيص بعد مُوافقة السّلطة الوطنيّة للتّصديق الإلكتروني(ANCE) لأيّ شخص طبيعي أو معنوي، يلتزم باحترام الشّروط التي تُحَدِّدُهَا في مجال إنشاء واستغلال خدمات التّصديق الالكتروني، وبالتالي يُقصد بالتّرخيص وفقا لأحكام نص المادة 10/02 من القانون رقم 15-04 المحدّد للقواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين على أنّه:" **نظام استغلال خدمات التصديق الإلكتروني والذي يتجسد في وثيقة رسمية ممنوحة لمؤدي الخدمات بطريقة شخصية، تسمح له بالبدء الفعلي في توفير خدماته.**"

يجب على كل طالب التّرخيص لمزاولة نشاطات التّصديق التّقيّد بالشّروط الفنيّة والتّقنيّة التي حدّدتها المادة 34 من نفس القانون، كخضوع الشّخص المعنوي للقانون الجزائري أو تمتّع الشّخص الطبيعي بالجنسيّة الجزائريّة، وأن تتوافر القدرة الماليّة الكافية والمؤهّلات والخبرة الثّابتة في ميدان تكنولوجيات الإعلام والاتّصال للشّخص الطّبيعي أو المُسيِّر للشّخص المعنوي، وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاطه.

تجدر الإشارة في هذا السّياق، إلى أنّ الشّخص الطّبيعي أو المعنوي الرّاغب في الحصول على ترخيص لمزاولة خدمات التّصديق الإلكتروني، يجب أن يَتَحَصَّلَ مُسْبَقًا على شهادة تأهيل(Attestation d'éligibilité) لتهيئة الوسائل اللاّزمة لخدمات التّصديق الإلكتروني، مدّة صلاحيتها سنة(01) قابلة للتّجديد مرّة واحدة فقط، التي(الشّهادة) تسمح له وفقا للمادة 51 من نفس القانون، بأن يطلب لدى السّلطة الاقتصادية للتّصديق الإلكتروني(ARPCE) أو لدى مكاتب التّدقيق المعتمدة(Cabinet d'audit accrédité)، بإجراء تدقيق تقييمي(Audit d'évaluation) لمُعدّات وأنظمة أمن تكنولوجيا المعلومات

المُستعملَة في نشاطاته[1]، وبالتّالي فإنّ شهادة التّأهيل لا تسمح لِحَامِلِهَا بِمُزَاوَلَةِ خدمات التّصديق إلاّ بعد حصوله على التّرخيص، الذي يُرْفَقُ بدفتر الشّروط المُحدّد لشروط وكيفيات مزاولة خدمات التّصديق الإلكتروني وكذا شهادة التّصديق الإلكتروني الخاصّة بـ(م.خ.ت.إ) مُوقّعة من طرف السّلطة الاقتصاديّة(ARPCE)، وفي حال رفض منح شهادة التّأهيل والتّرخيص للشّخص المعني، يجب أن يكون قرار الرّفض مُسبّب مع تبليغه مقابل وصل بالاستلام.

فبعدما أن تتأكّد السّلطة الاقتصاديّة(ARPCE) من تَوَافُرِ ومُطابقة الشّروط المحدّدة لدى طالب التّرخيص ومن حصوله على شهادة تأهيل، تُصْدِرُ وفقا للمادة 40 من قانون التّوقيع والتّصديق الإلكترونيين، قرار مُسبّب بمنح التّرخيص مُدّة صلاحيته خمسة(05) سنوات قابلة للتّجديد عند انتهاء تلك المدّة، الذي يُبَلَّغُ(القرار) لصاحب شهادة التّأهيل في خلال شهرين(60 يوم) من تاريخ استلام الطّلب المُثبّت بوصل الاستلام وذلك بمقابل إتاوة يدفعها(م.خ.ت.إ) تُحدَّد عن طريق التّنظيم، وفي جميع الظروف، يخضع(م.خ.ت.إ) أثناء تأديته لنشاطه لمراقبات فجائية وعمليات تدقيق دورية من قِبل السّلطة الاقتصاديّة(س.ض.ب.إ.إ)، من أجل التّحقّق من مدى مراعاته لدفتر الشّروط المُحدّد لشروط وكيفيات تقديم خدمات التّصديق الإلكتروني[2].

---

[1] تنص المادة 51 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" تقوم السلطة الاقتصادية للتصديق الالكتروني، أو مكتب التدقيق المعتمد، وفقا لسياسة التصديق الإلكتروني للسلطة الاقتصادية ودفتر الأعباء الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني، بإنجاز تدقيق تقييمي، بناء على طلب من صاحب شهادة التأهيل قبل منح ترخيص تقديم خدمات التصديق الالكتروني."

[2] تنص المادة 52 من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" تتم مراقبة مؤدي خدمات التصديق الالكتروني من قبل السلطة الاقتصادية، لاسيما من خلال عمليات تدقيق دورية ومراقبات فجائية طبقا لسياسة التصديق للسلطة الاقتصادية ولدفتر الأعباء الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني."

المطلب الثاني

دور شهادات التّصديق الإلكتروني في تأمين مواقع التّجارة الإلكترونيّة

إنّ جدارة الثّقة في مقدّم خدمات التّصديق تكمن في مدى امتثاله للتّأكيدات التي يقدّمها بخصوص السّياسة العامّة المنظّمة لشهادات التّصديق(PC) التي تحدّد تطبيقات الشّهادات وفقا لمقتضيات أمان مُشتركة فيما بينها، والممارسات المتّبعة في إصدار شهادات التّصديق الإلكتروني(DPC) **(الفرع الأول)**، فقد يحدث أن تَفْقِدَ شهادة التّصديق الإلكتروني بعد صدورها صلاحيتها للتّعويل عليها نتيجة عوامل تُثير الشُّبهة فيها، مِمَّا يُجبِرُ الجِّهة المُصدِرة للشّهادة إتّباع إجراءات الأمان اللاّزمة فيها لتفادي الاستعمال التّعسّفي لها**(الفرع الثاني)**، كما أنّ مخططات مرافق المفاتيح العموميّة تعترضها مشاكل تقنيّة تتعلّق بالتّشغيل البِينِي فيما بين هذه المرافق، نتيجة فقدانها لبعض المعايير المُشتركة الأساسيّة بشأن التّكنولوجيات، مما يستوجب إرساء آليات الاعتراف بخدمات جهات التّوثيق الأجنبيّة**(الفرع الثالث)**.

الفرع الأول

البنية التّحتية لمرفق المفاتيح العمومية

يعتبر مرفق المفاتيح العموميّة(PKI) كوسيلة لتوفير الثّقة والأمان في المعاملات الإلكترونيّة وبالخصوص في معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة الإلكترونيّة **(أولا)**، حيث أنّ عملية إحداث مرافق المفاتيح العموميّة بحاجة إلى دراسة مُسبقَة وتنظيم مُحْكَمْ ودقيق منتهج حسب السّياسة الأمنيّة الوطنيّة لكلّ دولة **(ثانيا)**.

أولا– أهداف إنشاء مرافق المفاتيح العموميّة.

للتّحقق من سلامة وصّحة التّوقيع الإلكتروني، يجب أن تَتَوَافَرَ لدى القائم بعملية الفّحص سُبُلِ الوصول إلى المفتاح العام الخاص بالمُوَقِّعِ وأن يكون لديه ما يضمن له تَنَاظُرِهِ مع المفتاح الخاص للمُوقِّع، غير أنه لا توجد علاقة ثقة مُسبقة بين الموقّع ومتلّقي الرّسالة الإلكترونيّة حيث ينبغي أن تتوافر آلية إضافيّة للرّبط على نحو جدير بالتّعويل عليهِ، بين

شخص مُعيّن أو هيئة معيّنة وزوج مفاتيح التّشفير المُصدَرَة في إطار كيان يُشار إليه بمرفق المفاتيح العموميّة، الذي يُعرف على أنّه نظام لإدارة وتسيير المفاتيح العموميّة الذي يسمح بإرساء عناصر الثّقة والأمان اللاّزمة لإجراء المعاملات الإلكترونيّة، كتحديد الهويّة وسريّة وسلامة البيانات الإلكترونيّة مع عدم إنكارها، أو أنّه(PKI) يتضمّن على مجموعة من العناصر والوظائف والإجراءات المتعلّقة بإدارة مفاتيح التّشفير والشّهادات الإلكترونيّة التي ترتكز على آلية التّشفير باستخدام المفتاح العام[1].

وعليه، فإنّ الغاية من إحداث هذه المرافق(PKI) متعدّدة ومتنوّعة والمتمثّلة كالتّالي:

أ)– التّرخيص لسلطات التّصديق الإلكتروني الأخرى لتقديم خدمات التّصديق مُبَاشَرَةً للمُستعملين في إطار مرفق المفاتيح العموميّة، حيث يُرجَّح في هذه الحالة أن تكون سلطات التّصديق(AC) تابعة لسلطات تصديق(AC) أخرى أو يمكن أن تعمل على قَدم المساواة بعضها مع البعض الأخر[2]؛

ب)– التّصديق على تكنولوجيا ومُمارسات جميع سلطات التّصديق الإلكتروني(AC) المُرَخَّصِ لها بإصدار أزواج مفاتيح التّشفير أو شهادات التّصديق المُتعلّقة باستخدام تلك الأزواج من المفاتيح[3]؛

---

[1] **Mustapha BENJADA**, « PKI (Public Key Infrastructure) », p. 01. Article publié le 14 mars 2001, à partir de l'adresse: https://www.securiteinfo.com/cryptographie/pki.shtml, consultée le 07/09/2017.

Yassine CHALLAL, « ICP/PKI: Infrastructures à Clés Publiques (Aspects Techniques et organisationnels) », pp. 11, 12, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, au niveau de l'Hôtel Hilton d'Alger. https://www.arpce.dz

[2] **Mahdi BOUZOUBA**, « Certification électronique et E-Services », pp. 04, 07. (SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, au Cercle National de l'Armée, à Alger. https://www.arpce.dz

[3] تنص **المادة 07** من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001، على ما يلي:"

1– يجوز لـ[أي شخص أو جهاز أو سلطة تعينهم الدولة المشترعة جهة مختصة، سواء أكانت عامة أم خاصة،] تحديد التواقيع الإلكترونية التي تفي بأحكام المادة 6 من هذا القانون.

2– يتعين أن يكون أي تحديد يتم بمقتضى الفقرة 1 متسقا مع المعايير الدولية المعترف بها.

3– ليس في هذه المادة ما يخل بسريان مفعول قواعد القانون الدولي الخاص."

– أنظر كذلك دليل الإشتراع لهذا القانون، ص ص 70، 71.

Arnaud-F. FAUSSE, op.cit., pp. 59- 63.

ج)– إدارة وإصدار مفاتيح التّشفير المُستخدَمة لأغراض التّوقيعات الإلكترونيّة، حيث أن عملية اختيار سلطات التّصديق الإلكتروني(AC) تتوقّف على عدد من العوامل منها قوّة المفتاح العام المستخدم في شهادات التّصديق الإلكتروني؛

د)– التّدقيق في هوّية المستعملين مع التّصديق على أن المفتاح العام يُناظِر بالفعل المفتاح الخاص بالمُوقِّع، ولتيسير التّحقّق من المفتاح العام ومن مناظرته لموقِّع مُعيّن، يجب إتاحة الاطّلاع على شهادة التّصديق الإلكتروني من خلال نشرها عبر قواعد بيانات تتضمّن على معلومات عن الشّهادات ومعلومات أخرى متاحة للاسترجاع والاستخدام في التّحقّق من صّحة التّوقيعات الإلكترونيّة[1]؛

هـ)– نشر المعلومات اللاّزمة المتعلّقة بتعليق شهادة التّصديق الإلكتروني(وقف فترة سريانها مؤقتا) أو إلغائها أي إبطالها بصفة نهائيّة، وفور تعليق الشّهادة أو إلغائها يجب على(م.خ.ت.إ) أن ينشر إشعارا بإلغاء أو تعليق هذه الشّهادات(LCR) التي لا يُمْكِنُ التّعويل عليها من طرف الغير[2]؛

و)– الاعتراف المتبادل لشهادات التّصديق الإلكتروني الأجنبيّة الصادرة من طرف(م.خ.ت.إ) ينتمون إلى مرافق مفاتيح عموميّة أخرى(PKI-ICP-IGC)، حيث يستند الاعتراف المتبادل إلى تَقِيِيم عملية اعتماد مرفق المفاتيح العموميّة الأخر(IGC)، لا إلى تقييم كل(م.خ.ت.إ) بمُفْرَدِهِ مُعتَمَد لدى مرفق المفاتيح العموميّة الأخر، فعندما يَعْتَرِفُ مِرْفَقْ مفاتيح عموميّة(ICP) بمرفق مفاتيح عموميّة مَثِيلْ أخر(ICP)، فهو بالتّالي يَعْتَرِفُ بصفة تلقائيّة بأيّ(م.خ.ت.إ) مُعتَمدين في إطار مخطّط مرافق المفاتيح العموميّة(IGC)، فالمواءمة في السّياسات العامّة المنظّمة لشهادات التّصديق(PC) وبيانات الممارسات المتّبعة في إصدار شهادات التّصديق

---

1) **Y. CHALLAL**, (SICE' 2009 ARPCE), Alger du 08 et 09 décembre 2009, op.cit., p. 13.
2) **Mahdi BOUZOUBA**, (SICE' 2011 ARPCE), Alger du 28, 29 et 30 juin 2011, op.cit., pp. 08-11.

الإلكتروني(DPC)، ضروريّة لضمان التّوافق والتّشغيل البيني فيما بين نطاقات مرافق المفاتيح العموميّة(IGC) [1].

ثانيا– نماذج الثّقة المتّبعة في خدمات التّصديق الإلكتروني.

إنّ إرساء الثّقة والأمان في المعاملات الإلكترونيّة بحاجة إلى تنظيم مُحكم ودقيق لمرفق المفاتيح العموميّة(PKI) المنتهج حسب السّياسة العامّة لكلّ دولة، التي يتعيّن عليها تحديد شكل المرفق وعدد مُستويات سلطات التّصديق الإلكتروني، وإمكانية تفويض هيئات عامّة أو خاصّة "كسلطات تصديق إلكتروني" تُشرف على تنظيم ورقابة نشاطات(م.خ.ت.إ)، يؤكّد من خلاله(م.خ.ت.إ) بأنّ المفتاح العمومي للمُستعمِل(المُوقّع) لم يتعرّض لما يُثير الشُّبهة فيه(لم يُعبث به) وأنّه يناظر بالفعل المفتاح الخاص لذلك المُستعمِل، مع ضمان بأنّ التّقنيات أو المعدّات المستعملة في إحداث التّوقيع الإلكتروني الموصوف مؤمّنة وسليمة، حيث توجد من النّاحية التّقنية أربعة نماذج تنظيميّة لإصدار شهادات التّصديق الإلكتروني وهي على الأشكال التّالية:

أ)– نموذج التّصديق الإلكتروني المُوَّحَدْ(Hierarchy PKI):

يستند هذا النّموذج إلى مستويات هرميّة مختلفة من سلطات التّصديق الإلكتروني، حيث يتضمّن المستوى الأعلى على سلطة تصديق رئيسيّة(Root authority) تقوم بالتّصديق على تكنولوجيا وممارسات جميع الأطراف المُرخَّص لها بإصدار أزواج مفاتيح التّشفير أو شهادات التّصديق الإلكتروني، وكذا تُسجل سلطات التّصديق التّابعة لها(AC)، بينما المستوى الثّاني يشتمل على سلطات تصديق(AC) مختلفة في مرتبة أدنى سلطة التّصديق الرّئيسيّة[2]، حيث

---

[1] **Manel ABDELKADER**, « La Certification Électronique en Tunisie : Expérience et Défis », pp. 07- 09, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, au niveau de l'hôtel Hilton d'Alger. https://www.arpce.dz

[2] تنص **المادة 16** من القانون رقم 15–04، الذي يحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تسمى السلطة الوطنية للتصديق الإلكتروني وتدعى في صلب النص"السلطة". تسجل الإعتمادات المالية اللازمة لسير السلطة ضمن ميزانية الدولة."

تُصدّق على أنّ المفتاح العام لأحد المستعملين يُقابل أو يُناظِر فعلا المفتاح الخاص لذلك المُسْتعمِل ولم يعبث به، أمّا المستوى الثّالث يحتوى على سلطات تسجيل(AE) مختلفة في مرتبة أدنى من مستوى سلطات التّصديق(AC)، حيث تُشرف(AE) على تلّقي الطّلبات من المستعملين للحصول على شهادات التّصديق الإلكتروني وذلك بعد القيام بعملية التّدقيق في هويّتهم.

ومن بين مميّزات مرفق المفاتيح العموميّة الهرمي نجد أنّه يُوَّحِدُ مَسارَات التّصديق في اِتِّجَاهٍ وَاحِدٍ فَقَطْ، أي من الشّهادة الموجودة بحيازة المُستعمِل رجوعا إلى جهة الثّقة[1]، حيث يمكن توسيع نطاق مرفق المفاتيح العموميّة الهرمي بإدماج أو ضّم مرافق عموميّة أخرى(PKI-ICP-IGC)، من خلال قيام سلطة التّصديق الرّئيسيّة[2] بإحداث علاقة ثقة

وتنص **المادة 18** من القانون رقم 15–04، على ما يلي:" تكلف السلطة بترقية استعمال التوقيع والتصديق الالكترونيين وتطويرهما وضمان موثوقية استعمالهما.

وفي هذا الإطار، تتولى المهام الآتية:

1– إعداد سياستها للتصديق الإلكتروني والسهر على تطبيقها، بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة؛

2– الموافقة على سياسات التصديق الصادرة عن السلطتين الحكومية والاقتصادية للتصديق الالكتروني؛

3– إبرام اتفاقيات الاعتراف المتبادل على المستوى الدولي؛

4– اقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الإلكتروني أو التصديق الإلكتروني على الوزير الأول؛

5– القيام بعمليات التدقيق على مستوى السلطتين الحكومية والاقتصادية للتصديق الإلكتروني، عن طريق الهيئة الحكومية المكلفة بالتدقيق؛

تتم استشارة السلطة عند إعداد أي مشروع نص تشريعي أو تنظيمي ذي صلة بالتوقيع أو التصديق الإلكترونيين."

[1] **Arnaud-F. FAUSSE**, op.cit., pp. 124-126.

[2] ينص **الفصل 08** من القانون عدد 2000/83 مؤرخ في 09 أوت 2000، المتعلق بالمبادلات والتجارة الإلكترونية، على ما يلي:" أحدثت مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي أطلق عليها اسم " الوكالة الوطنية للمصادقة الالكترونية" وتخضع في علاقتها مع الغير إلى التشريع التجاري، ومقرها بتونس العاصمة."

وينص **الفصل 09** من القانون رقم 2000/83، على ما يلي:" تتولى هذه المؤسسة القيام خاصة بالمهام التالية:

– منح ترخيص تعاطي نشاط مزود خدمات المصادقة الالكترونية على كامل تراب الجمهورية التونسية؛

– السهر على مراقبة احترام مزود خدمات المصادقة الالكترونية لأحكام هذا القانون ونصوصه التطبيقية؛

بالسّلطة الرّئيسيّة لمرفق المفاتيح العموميّة الجديد(IGC)، التي من خلالها يتّم إدماجها(السّلطة الرّئيسيّة للمجموعة الجديدة) مباشرة في الكيان الرّئيسي لمرفق المفاتيح العموميّة المُستقبِل(IGC)، لتصبح بالتّالي ك(م.خ.ت.إ) تابعا ضمن ذلك المرفق(IGC)، كما يُمكِنها (السّلطة الرّئيسيّة الجديدة) أن تصبح مقدّما لخدمات تصديق تابعا لأحد(م.خ.ت.إ) التّابعين ضمن المرفق القائِم(IGC)، فمن بين الدّول التي طبّقت نموذج التّصديق الهرمي(Modèle Hiérarchique)[1] نجد كل من الجزائر وتونس والمغرب الخ...

فبالرغم من الإيجابيات التي تُتِيحُهَا المرافق الهرميّة إلاّ أنّ لهذه المرافق أيضا سلبياتها لاسيما السّلبيات المُترتّبة عن التّعويل على جهة ثقة وحيدة، فمن الصّعب اختيار كيان واحد ليكون سلطة تصديق رئيسيّة مع فرض تلك البنية الهرميّة على جميع(م.خ.ت.إ) الآخرين، فإذا ضعفت سلطة التّصديق الرّئيسية ضعف مرفق المفاتيح العموميّة المُوّحد بأكمله.

ب)– نموذج التّصديق الإلكتروني المتشابك(Mesh PKI).

يفتقد هذا النّموذج للتّرتيب الهرمي، حيث يمكن لجميع(م.خ.ت.إ) الذين تربطهم علاقة بين أقران أن يكونوا جهات موثوق بها، عن طريق إبرامهم لاتفاقات الاعتراف المتبادل لشهادات التّصديق التي يُصدرها كلّ(م.خ.ت.إ) مع تحديد القيود المفروضة في الشّهادات التي يصدرها لأقرانه، غير أنّ المواءمة بين سياسات التّصديق(PC) تكون هدفا معقدا للغاية

– تحديد مواصفات منظومة إحداث الإمضاء والتدقيق؛

– إبرام اتفاقيات الاعتراف المتبادل مع الأطراف الأجنبية؛

– إصدار وتسليم وحفظ شهادات المصادقة الالكترونية الخاصة بالأعوان العموميين المؤهلين للقيام بالمبادلات الإلكترونية ويمكن أن يتم ذلك مباشرة عبر مزودي خدمات مصادقة إلكترونية عموميين؛

– المساهمة في أنشطة البحث والتكوين والدراسة ذات العلاقة بالمبادلات والتجارة الالكترونية؛

وبصفة عامة كل نشاط أخر يقع تكليفها به من قبل سلطة الإشراف وله علاقة بميدان تدخلها.

وهي تخضع لإشراف الوزارة المكلفة بالقطاع."

[1] أنظر **الملحق رقم (29)**، ص 503.

الشّيء الذي يؤدّي إلى فقدان الثّقة في الخدمات التي تُقدّمها سلطات التّصديق الإلكتروني(PSCE) [1].

ج)– نموذج التّصديق الجّسر(Modèle Bridge).

يتطلّب هذا النّموذج تواجد سلطة تصديق(PSCE) تقوم بإرساء "جسر الثّقة" للشّهادات الإلكترونية المُصدرَة فيما بين مرافق المفاتيح العموميّة(PKI)، التي تسمح للمُستعملِين من التّفاعل فيما بينهم بمستوى ثقة محدّد، مع الإبقاء على جهات الثّقة في التّصديق(PSCE) ضمن كلّ مرفق(PKI)، وبالتّالي فإنّ مقدّم خدمات التّصديق الجّسر(Bridge CA) لا يُصْدِرُ شهادات التّصديق مُبَاشَرَةً إلى المُسْتَعْمِلِينَ، كما هو الحال لـ(م.خ.ت.إ) في مرفق المفاتيح العموميّة المُتشابك(Modèle Maillé)، وكذا لا يعتبر(Bridge CA) كجهة ثقة رئيسيّة على مستوى مرفق المفاتيح العموميّة(PKI)، كما هو الحال لـ(م.خ.ت.إ) الرّئيسي (Autorité Racine)، بل يُعتبر(م.خ.ت) الجّسر كحلقة وصل رئيسيّة في الهيكل التّنظيمي العام لمرافق المفاتيح العموميّة(PKI) سواء على المستوى الدّولي أو الوطني، فبفضل "جسر الثّقة" الذي يَصِلُ مَرْفَقَيْنِ أو أكثر من مَرافِق المفاتيح العموميّة(PKI-ICP-IGC) من خلال علاقتهما المشتركة بـ(م.خ.ت) "الجّسر"، يَتَمَكَّنُ المُسْتَعْمِلُونَ من مجموعات المُستعملِين المختلفة، من التّفاعل فيما بينهم من خلال مقدّم خدمات التّصديق "الجّسر" بمُستوَى ثِقَة مُحَدَّدٍ، لذا تّم اعتماد هذا النّموذج كبنية لإقامة مرفق المفاتيح العموميّة(PKI) للحكومة الفيدراليّة للولايات المتّحدة الأمريكيّة، وفي نظام مرفق المفاتيح العموميّة(PKI) لحكومة اليابان[2].

---

1) **Ahmed BERBAR**, « Certification Électronique en Algérie Situation et Perspectives », p. 09, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, au niveau de l'hôtel Hilton d'Alger. https://www.arpce.dz

أنظر **الملحق رقم (30)**، ص 503.

2) **Arnaud-F. FAUSSE**, op.cit., pp. 127-129.

أنظر **الملحق رقم (31)**، ص 505.

د)– نموذج قائمة الثّقة(Trust List).

يقوم هذا النّموذج على وجود قائمة ثقة(Trust List) وهي عبارة عن وثيقة ينشرها كيان مستقّل، والذي يكون في الغالب كمُنظِّم(Régulateur) لنشاط التّصديق، حيث تتضمّن هذه الوثيقة على قائمة من سلطات التّصديق المُرَخَّصِ لها والمعترف بها، إضافة لمُعَرِّفْ(L'identifiant) مفاتيحها العموميّة، ويقوم نموذج قائمة الثّقة برسم حدود لسلطات التّصديق الإلكتروني[1]، وبالتّالي فهو لا يُوَفِّرُ عملية تصديق إلكتروني موّحدة ومُتقدِّمة، بالقدر الذي يُوَفِّرُهُ نموذج مرفق المفاتيح العموميّة الهرمي، فغياب التّوحيد قد يُسبب مشاكل توافقيّة عِدّة فيما بين(م.خ.ت.إ)، ومن بين مُميّزات نموذج قائمة الثّقة نجد عدم استعانته بسلطة تصديق(AC) تُشرف على رقابة نشاطات(م.خ.ت.إ) المُعْتَرَفِ بِهِمْ، كما أنّ عملية الاعتراف بشهادات التّصديق الأجنبية تستدعي تدّخل سلطة وطنيّة[2] تقوم بِمُهِمَّةِ إبرام

---

1) **Art. 04**(**LFSCSE du 18 mars 2016**) : « (**Désignation de l'organisme d'accréditation**) **1-** Le **Conseil fédéral désigne** l'organisme d'accréditation des organismes de reconnaissance (organisme d'accréditation).
2- Faute d'organisme de reconnaissance accrédité, le Conseil fédéral **désigne** comme tel l'organisme d'accréditation ou un autre organisme approprié. »
Art.05(**LFSCSE**) : « (**Liste des fournisseurs reconnus**) **1-** Les organismes de reconnaissance **annoncent** à l'organisme d'accréditation les **fournisseurs** qu'ils reconnaissent. **2-** L'organisme d'accréditation tient à la disposition du public la **liste des fournisseurs reconnus**. »

2) **Art. 20**(**LFSCSE du 18 mars 2016**) : « 1- Le **Conseil fédéral** peut conclure des conventions internationales pour faciliter l'utilisation et la reconnaissance juridique internationales des signatures électroniques et des autres applications de clés cryptographiques, notamment sur: **a.** la reconnaissance des signatures électroniques, des cachets électroniques et des certificats numériques; **b.** la reconnaissance des fournisseurs et l'accréditation des organismes de reconnaissance; **c.** la reconnaissance des essais et des évaluations de conformité; **d.** la reconnaissance des marques de conformité; **e.** la reconnaissance des systèmes d'accréditation et des organismes accrédités; **f.** l'octroi de mandats de normalisation à des organismes internationaux de normalisation, dans la mesure où la législation renvoie à des normes techniques déterminées ou lorsqu'un tel renvoi est prévu; g. l'information et la consultation concernant l'élaboration, l'adoption, la modification et l'application de prescriptions ou de normes techniques.
2- Il édicte les dispositions nécessaires à l'application des conventions internationales portant sur les domaines énumérés à l'al. 1.
3- Il peut déléguer à des organismes privés des activités relatives à l'information et à la consultation concernant l'élaboration, l'adoption et la modification de prescriptions ou de normes techniques et prévoir une indemnité à ce titre. »

اتفاقيات الاعتراف المتبادل لشهادات التّصديق الإلكتروني، ومن بين الدّول التي أخذت بهذا النّموذج نجد كلٍّ من إسبانيا وسويسرا[1].

الفرع الثاني

إجراءات إصدار وإيقاف وإلغاء شهادات التّصديق الإلكتروني

إنّ جدارة الثّقة في خدمات جهات التّصديق الإلكتروني(PSCE) قد تتوقّف على مجموعة من العوامل منها، قوّة المفتاح العمومي المُستعمَل في إصدار شهادات التّصديق والامتثال لشروط السّياسة العامّة والأمان الصادرة عن السّلطة الرّئيسيّة، أو عن(م.خ.ت.إ) الأعلى درجة، ومدى إنفاذها لمعايير إصدار شهادات التّصديق الإلكتروني وإمكانية التّعويل على الطّريقة المُستخدمة في تحديد الهويّة وتقييمها للبيانات التي تتلقّاها من المُستعمِلين الذين يطلبون إصدار الشّهادات(**أولا**)، فقد يحدث وفقا للظروف أن تَفْقِدَ شهادة التّصديق الإلكتروني جدارتها بالثّقة أو تصبح غير جديرة بالتّعويل عليها، الأمر الذي يدفع بسلطة التّصديق الإلكتروني(PSCE) إلى تعليق العمل بتلك الشّهادة أو حتّى إبطالها بصفة دائمة(**ثانيا**).

أولا– إجراءات إصدار شهادات التّصديق الإلكتروني.

تؤدّي شهادة التّوثيق الإلكترونيّة في إطار التّعاقد الإلكتروني أدوار عديدة كالتّحقّق من هويّة الشّخص المتعاقد، ومن سلطاته وأهليته وأوصافه المهنيّة ومعرفة المفتاح العام الذي من خلاله يتّم التّأكد من المعلومات المُرسلَة، وتُثْبِتُ وجود ارتباط بين زوج المفاتيح(العام والخاص) وبين الشّخص الذي تحقّقت شخصيته، حيث تتلاشى من خلال التّعويل على شهادة التّوثيق الإلكتروني الموصوفة مخاطر إبرام العقد الإلكتروني وتُثبت أنّ بيانات الرّسالة المُوقّعِ عليها صحيحة ولم يشوبها أي تعديل أو تحريف، مع ضمان عدم إنكار أي من

---

1) **Ahmed BERBAR**, (SICE' 2009 ARPCE), Alger du 08 et 09 décembre 2009, op.cit., p.08. أنظر **الملحق رقم (32)**، ص 504.

أطراف الصّفقة الإلكترونيّة لتوقيعه على العقد[1]، وبالتّالي فإنّ عملية إصدار شهادة التّصديق تمرّ بمراحل ضروريّة، حيث يمكن تصنيفها وفقا للواقع العملي لجهات التّوثيق إلى ثلاثة مراحل، والمتمثّلة كالآتي:

أ)– إيداع طلب الحصول على شهادة التّصديق الإلكتروني:

يتعيّن على كلّ من يرغب في الحصول على شهادة تصديق إلكتروني وفقا لمستويات معيّنة من الأمان، أن يقوم في إطار عقد تقديم خدمة التّصديق الإلكتروني بتوجيه طلب بالطّريقة الكتابيّة أو الإلكترونيّة لسلطة التّسجيل(AE) التّابعة لسلطة التّصديق(AC)، أو لأحد وكلاءها المفوّضين لهم وفقا للنّموذج المُعّد مُسبقا المتواجد مجّانًا على مستوى موقعها الإلكتروني، مع إرفاقه عند الاقتضاء بنسخ الوثائق التي تُثبِت صّحة المعطيات المقدّمة في النّموذج، كبطاقة التّعريف الوطنيّة أو جواز، سفر، السّجل التّجاري الخ...[2].

ب)– التّحقق من البيانات المتعلّقة بإصدار شهادة التّصديق الإلكتروني:

تقوم سلطة التّسجيل(AE) بمباشرة إجراءات المرحلة الثّانية المتعلّقة بالتّحقق من البيانات المتعلّقة بإصدار الشّهادة، التي تستلزم عادة الحضور الشّخصي لصاحب طلب إصدار شهادة التّصديق الإلكتروني الموصوفة، من أجل مُباشرة إجراءات التّحقيق في هويّته وأهليته في إبرام التّصرف الإلكتروني بناءا على الوثائق الأصليّة التي يُقدّمها لسلطة التّسجيل[3]،

---

[1] **إيمان مأمون أحمد سليمان**، إبرام العقد الإلكتروني وإثباته(الجوانب القانونية لعقد التجارة الإلكتروني)، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2008، ص ص 367، 368.

[2] **Stéphane LOHIER, Dominique, PRÉSENT**, op.cit., pp. 183- 187, 188- 191.

عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية(دراسة قانونية وتحليلية مقارنة)، دار وائل للنشر والتوزيع، عمان، الأردن، 2003، ص ص 67– 69.

Arnaud- F.FAUSSE, op.cit., pp 164, 165.

[3] أنظر **الملحق رقم (33)**، ص ص 504، 505.

وفي حالة ما إذا كان صاحب الطلب شخص معنوي يتّم التّحقق في هوّية الشّخص الطّبيعي المُمثّل لَهُ قانونيًا، ومدى تمتّعه بأهليّة تسمح له بإبرام التّصرف القانوني إلكترونيًا[1].

ج)– إصدار شهادة التّصديق الإلكتروني:

بعد تحقّق سلطة التّسجيل(AE) من البيانات المتعلّقة بشهادة التّصديق الإلكتروني، تقوم في المرحلة الأخيرة بإرسال طلب إصدار الشّهادة الإلكترونيّة إلى سُلطة التّصديق الإلكتروني(AC)، التي تُباشِر بدورها عملية إصدار زوج مفاتيح التّشفير(العام والخاص) المتعلّقان بالشّهادة الإلكترونيّة وفقا للمواصفات التّقنيّة المعمول بها، حيث يتعيّن عليها أن تُولِي العناية اللاّزمة لضمان دقّة واكتمال كلّ ما تُقدّمه من تأكيدات جوهريّة ذات صلة بالشّهادة في وقت أو قبل إصدارها، مع حفظها في نظام مؤمّن خاص يسمح بالرّجوع إليها عند الحاجة[2]، كما يتعيّن على صاحب الشّهادة أن يقوم بحفظها وتثبيتها في شكلها

---

1) **Art.05**(**OSCSE** du 23 novembre 2016): « Délivrance des certificats réglementés à des personnes physiques **1-** Les **fournisseurs reconnus** doivent exiger des personnes qui demandent un certificat réglementé qu'elles présentent personnellement un passeport, une carte d'identité suisse ou une carte d'identité reconnue pour entrer en Suisse. […].»
Art.06(OSCSE): « Délivrance des certificats réglementés à des entités IDE autres que des personnes physiques **1-** L'identité de la personne qui demande la délivrance d'un certificat réglementé pour une entité IDE qui n'est pas une personne physique doit être vérifiée conformément à l'art. 5, al. 1. Les pouvoirs de représentation de cette personne doivent être justifiés par une procuration écrite, à moins qu'ils ne soient inscrits dans le registre du commerce. […]. »

تنص **المادة 44** من القانون رقم 15–04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" يجب على مؤدي خدمات التصديق الإلكتروني، قبل منح شهادة التصديق الإلكتروني، أن يتحقق من كامل بيانات الإنشاء وبيانات التحقق من التوقيع.

يمنح مؤدي خدمات التصديق الإلكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته، وعند الاقتضاء، التحقق من صفاته الخاصة.

وفيما يخص الأشخاص المعنوية، يحتفظ مؤدي خدمات التصديق الإلكتروني بسجل يدوّن فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني."

2) **Arnaud- F.FAUSSE**, op.cit., p 172.
Art.08 (OSCSE du 23 novembre 2016) : « Copie et conservation de doubles des clés Les fournisseurs reconnus peuvent établir et conserver des doubles des clés cryptographiques

الإلكتروني الأصلي على أيّ حامل تخزين إلكتروني مؤمّن، سواء في مُذّكرة حاسوبه(RAM) أو على أسطوانة مُمَغنطة أو في المفتاح المحمول(Clé USB)، أو في بطاقة الائتمان الذّكيّة(Carte à puce)، وبالمقابل يقوم الطّرف المُعوّل على الشّهادة(المرسل إليه) بحفظ الشّهادة بنفس الكيفيّة على أيّ حامل إلكتروني مؤمّن[1]، وفي جميع الظّروف، يجب على صاحب شهادة التّصديق الإلكتروني التّقيّد بإجراءات السّلامة والأمن المحدّدة من طرف سلطة التّصديق مع إبلاغ هذه الأخيرة عند تعرّض بيانات إحداث توقيعه الإلكتروني لما يثير الشُّبهة فيها أو لانتهاك من طرف الغير[2].

---

privées de leurs clients, **sauf** si celles-ci servent à la signature électronique et sont stockées dans des dispositifs de création de signatures en possession des clients. »

تنص المادة **41** من القانون 15-04 مؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" يكلف مؤدي خدمات التصديق الإلكتروني بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني، وفقا لسياسة التصديق الإلكتروني الخاصة به، التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني."

1) **Maxime WACK et AL**, «certification et archivage légal de dossiers numériques», Revue Document numérique, vol 6, n°1/2002, pp. 152, 153.

2) **Art. 13(OSCSE du 23 novembre 2016)**: « Mesures de sécurité **1-** Le titulaire d'un certificat réglementé doit conserver l'accès exclusif à la clé cryptographique utilisée pour créer une signature ou un cachet électronique. Dans la mesure de ce qui peut être exigé, il doit garder le dispositif de création de signature ou de cachet en sa possession ou le mettre en lieu sûr.

2- En cas de perte ou de vol du dispositif de création de signature ou de cachet, le titulaire d'un certificat réglementé doit demander l'annulation de ce dernier dans les meilleurs délais. Il en va de même pour le titulaire qui sait ou qui a des raisons de croire qu'un tiers a pu avoir accès à la clé cryptographique utilisée pour créer une signature ou un cachet électronique.

3- Les données d'activation du dispositif de création de signature ou de cachet ne doivent pas se référer à des données relatives à la personne ou à l'entité IDE titulaire d'un certificat réglementé.

4- Les transcriptions des données d'activation doivent être conservées en lieu sûr et séparément du dispositif de création de signature ou de cachet.

5- Le titulaire d'un certificat réglementé doit modifier les données d'activation du dispositif de création de signature ou de cachet lorsqu'il sait ou qu'il a des raisons de croire qu'un tiers en a eu connaissance. S'il ne peut pas lui-même modifier les données d'activation, il doit demander l'annulation du certificat dans les meilleurs délais. »

وعليه، فإنّ شهادة التّصديق الإلكتروني تُتيح لأطراف التّعامل الإلكتروني درجة من الثّقة المطلوبة لإجراء معاملات التّجارة الإلكترونيّة، وتضمن سلامة ومِصداقيّة البيانات الإلكترونيّة المتداولة فيما بينهم، فمثلا "مُحَمَّدْ" متعامل اقتصادي يملك موقِع تجاري الكتروني يبيع من خلاله خدمات نقل البضائع(برًّا أو جوًّا أو بحرًا)، و"مُقْرَانْ" يَملِك شركة تجاريّة يَنْوِي تصدير منتجاته من خلال استعمال خدمات النّقل التي يُتيحُها مُحمّد عبر موقعه الإلكتروني، حيث لا يعرف أَحَدْ مِنْهُمَا هوّية الطّرف الأخر لكونهما مُتّصلان عبر شبكة الإنترنت، كما أنّهما يجب أن يتبادلا الرّسائل الإلكترونيّة مع استعمال تقنيّة التّوقيع الالكتروني الموصوف لإجراء عملية البيع والشّراء عبر الإنترنت، وبالتّالي يقوم "مُقْرَانْ" بالاستعانة بخدمات سلطة تصديق(PSCE-AC) معيّنة موثوق بها(AC1) من خلال اللّجوء إلى سلطة التّسجيل(AE1) التّابعة لها مثلا المصرف، لطلب شراء شهادة تصديق إلكتروني مقابل مثلا 100 أورو سنويا[1].

بالمقابل يقوم "مُحَمَّدْ" بِمُبَاشَرَةِ نفس إجراءات الحصول أو شراء شهادة التّصديق أمام سلطة تسجيل(AE2) تابعة لسلطة تصديق إلكتروني أخرى موثوق بها(AC2)، وبعدها تقوم كلّ سلطة تسجيل(AE1+AE2) بإرسال الوثائق مع طلبات الحصول على الشّهادات الإلكترونيّة إلى سلطة التّصديق(AC1+AC2) المعنيّة لكلٍّ منها، بغية إصدار شهادات تصديق مع تسليمها لكل طرف وفقا لصيغ إلكترونيّة تستجيب لمستويات الأمان المطلوبة(Carte à puce, Disquette, Flash disque, etc.).

لذا يُمكن لِمُقْرَانْ بعد حصوله على شهادة التّصديق الاتّصال عبر شبكة الإنترنت بمُحمّد عبر موقعه الإلكتروني لغرض شراء خدمة من خدمات النّقل المتاحة، أين يقوم(مُقْرَانْ) بملء نموذج الشّراء مع توقيعه بالمفتاح الخاص به وإرساله مع شهادة التّصديق مباشرة فيما بعد إلى مُحمّد، فعندما يستقبل هذا الأخير(مُحَمَّدْ) الرّسالة الالكترونيّة المُوقّعة ينبغي أن يتأكّد من مِصداقيّة بيانات شهادة التّصديق الإلكتروني لمُقْرَانْ، والتّحقق من ارتباط التّوقيع الإلكتروني

1) **Arnaud-F. FAUSSE**, op.cit., pp. 24- 28.

بالمحرّر أو الرّسالة الالكترونيّة المعنيّة وأنّ المفتاح العمومي مرتبط بالمفتاح الخاص لصاحب الشهادة(مُقْرَانْ)، حيث يمكن لمُحمَّد في هذه الحالة الاتّصال بسلطة التّصديق التي منح فيها ثقته، بغية التّحقق من أن سلطة التّصديق التي أصدرت الشّهادة لمقران حقًّا موثوق بها حيث يستطيع فيما بعد الحصول على المفتاح العام لمقران لفحص صّحة توقيعه الالكتروني.

لضمان عملية إبرام الصّفقة التّجاريّة عبر الإنترنت يمكن لِمُقْرَانْ الاستعانة بإحدى الخدمات التي يتيحها طرف ثالث موثوق به كوسيط يضمن خدمات الدّفع أو المقاصة فيما بين المصارف باعتباره كجسر الثقة[1]، حيث يقوم المشتري بإرسال أمر الدّفع بعد توقيعه إلكترونيا عبر مُشّغل دفع الكتروني أمن(SPS)، يقبل التّشغيل بإحدى برتوكولات التّشفير الآمنة(SSL/TLS, C-SET, 3-D Secure etc.) على أيّ برنامج مهما كان الجهاز المستعمل، ويعتمد(المشّغل) على بطاقات الائتمان الذّكيّة المحليّة والأجنبيّة (Carte CIB, Master Card, VISA, American Express, etc.)، حيث يقبل محمّد التّعامل معها عبر موقعه التّجاري في إطار العقد المبرم مع مُصدِر هذه البطاقات، في حين يتوّلى المشّغل تشفير الصّفقة المبرمة مع موقِع المتعامل الاقتصادي ومعالجة البيانات المصرفيّة المتبادلة بصفة آمنة مع قبول عملية الدّفع الفّوري وتوفير أقصى مستويات الأمان والثّقة لدى الأطراف[2].

ثانيا– إيقاف وإلغاء شهادات التّصديق الإلكتروني.

يجب على كلّ(م.خ.ت.إ) أن يكون لديه سجّل إلكتروني خاص بشهادات التّصديق الإلكتروني مُتاح على موقعه الإلكتروني عبر شبكة الإنترنت(LCR)، من أجل الإطّلاع عليه من طرف المستعملين بصفة دوريّة ومُستمرّة على المعلومات المُدوّنة فيه، حيث يُبيّن

1) **Arnaud-F. FAUSSE**, op.cit., pp. 29, 30, 258- 261.
2) **Chiheb GHAZOUANI**, op.cit., pp. 150, 151, 160, 161.

فيه جميع شهادات التّصديق الإلكتروني المنتهيّة صلاحيتها، أو التي تّم إخضاعها لإجراءات الإيقاف أو الإلغاء، مع توضيح وقت وتاريخ تعليقها أو إلغاءها عند الاقتضاء[1].

وعليه، فإنّ المشّرع الجزائري اكتفى فقط بالنّص على حالات إلغاء شهادة التّصديق من دون ذكر أو توضيح حالات إيقافها، فوفقا للمادة 45 من القانون رقم 15–04 المُحدّد للقواعد العامّة المُتعلّقة بالتّوقيع والتّصديق الإلكترونيين، فإنّ(م.خ.ت.إ) يُمْكِنُهُ أن يقوم بإلغاء شهادة التّصديق بناء على طلب صاحب شهادة التّصديق أو أنّ هذه الأخيرة(الشّهادة) تّم منحها بناء على معلومات خاطئة أو مزوّرة، أو عدم مطابقة هذه الشّهادة لسياسة التّصديق، وكذا في حالة علم(م.خ.ت.إ) بوفاة الشّخص الطّبيعي أو حل الشّخص المعنوي صاحب الشّهادة، أو في حالة انتهاك سريّة بيانات إحداث التّوقيع الإلكتروني، وبالتّالي يجب

---

[1] ينص **الفصل 14** من القانون عدد 83–2000 المؤرخ في 09 أوت 2000، الذي يتعلق بالمبادلات والتجارة الإلكترونية(تونس) على ما يلي:" على كل مزود خدمات مصادقة إلكترونية مسك سجل إلكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للاطلاع إلكترونيا بصفة مستمرة على المعلومات المدونة فيه.

ويتضمن سجل المصادقة، عند الاقتضاء، تاريخ تعليق الشهادات أو إلغاءها.

ويتعين حماية هذا السجل وشهادة المصادقة من كل تغيير غير مرخص به."

Art.12(LFSCSE, du 18 mars 2016) : « (**Service d'annuaire pour les certificats réglementés**) **1-** Tout fournisseur reconnu garantit aux intéressés de pouvoir vérifier de façon fiable, en tout temps et selon une procédure usuelle, la validité de tous les certificats réglementés qu'il a délivrés.

2- Il peut en outre offrir un service d'annuaire permettant aux intéressés de rechercher et de consulter les certificats réglementés qu'il a délivrés. Un certificat n'est inscrit dans cet annuaire qu'à la demande de son titulaire.

3- Les pouvoirs publics peuvent consulter ces données gratuitement.

4- Le Conseil fédéral détermine la durée minimale pendant laquelle les certificats réglementés qui ne sont plus valables doivent pouvoir continuer d'être vérifiés. »

Voir aussi : Les **Arts. 16**, **17**, **18**, de la **loi(Belge) du 21 Juillet 2016**, mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, MB n° 67478, du 28/09/2016. **(**Dite **Loi « eIDAS » et Archivage électronique.)**

على(م.خ.ت.إ) إبلاغ صاحب شهادة التّصديق الإلكتروني الموصوفة بانتهاء مدّة صلاحيتها في الآجال المُحدّدة في سياسة التّصديق الإلكتروني[1]، وفي حالة إلغاء(م.خ.ت.إ) لتلك الشّهادة يجب إخطار صاحبها مع تسبيب ذلك، حيث يُحتج بالإلغاء لدى الغَيْرِ ابتداء من تاريخ نشر شهادة التّصديق المُلغاة وفقا لسياسة التّصديق الإلكتروني لـ(م.خ.ت.إ)، التي وافقت عليها السّلطة الاقتصادية للتّصديق الإلكتروني(ARPCE)، حيث تَحْتَفِظُ هذه الأخيرة(ARPCE) بجميع المعلومات المتعلّقة بشهادة التّصديق الإلكتروني الموصوفة المُنْتَهِيَةِ صَلاَحِيَتُهَا، وذلك بعد تحويلها من طرف(م.خ.ت.إ)[2].

---

[1] تنص **المادة 45** من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" يلغي مؤدي خدمات التصديق الالكتروني شهادة التصديق الالكتروني في الآجال المحددة في سياسة التصديق، بناء على طلب صاحب شهادة التصديق الالكتروني الموصوفة الذي سبق تحديد هويته.

ويلغي مؤدي خدمات التصديق الإلكتروني أيضا شهادة التصديق الإلكتروني الموصوفة عندما يتبيّن:

1- أنه قد تم منحها بناء على معلومات خاطئة أو مزورة، أو إذا أصبحت المعلومات الواردة في شهادة التصديق الإلكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع،

2- أنها لم تصبح مطابقة لسياسة التصديق،

3- أنّه تم إعلام مؤدي خدمات التصديق الإلكتروني بوفاة الشخص الطبيعي أو بحل الشخص المعنوي صاحب شهادة التصديق الإلكتروني.

يجب على مؤدي خدمات التصديق الإلكتروني إخطار صاحب شهادة التصديق الإلكتروني الموصوفة بإلغاء هذه الأخيرة مع تسبيب ذلك.

يجب على مؤدي خدمات التصديق الإلكتروني تبليغ صاحب شهادة التصديق الإلكتروني الموصوفة بانتهاء مدة صلاحيتها، في الآجال المحددة في سياسة التصديق.

يعتبر إلغاء شهادة التصديق الإلكتروني الموصوفة نهائيا."

[2] تنص **المادة 46** من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ما يلي:" يتخذ مؤدي خدمات التصديق الالكتروني التدابير اللازمة من أجل الرد على طلب الإلغاء وفقا لسياسته للتصديق التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني.

يحتج بالإلغاء تجاه الغير ابتداء من تاريخ النشر، وفقا لسياسة التصديق الإلكتروني لمؤدي خدمات التصديق الإلكتروني."

انطلاقا من ذلك، يعتبر المشّرع التّونسي الأكثر تنظيما وتفصيلا عند تطرّقه لنظام العمل بشهادات التّصديق الإلكتروني في القانون عدد 83– 2000 المتعلّق بالمبادلات والتّجارة الإلكترونيّة[1]، الذي من خلاله ميّز بين نظامين: فالأوّل يتعلّق بحالات تعليق العمل بشهادة التّصديق الإلكتروني التي حدّدها بموجب الفصل 19 من نفس القانون، بينما النّظام الثّاني يتعلّق بحالات إلغاء شهادة التّصديق الإلكتروني المحدّدة في الفصل 20 من نفس القانون، حيث يمكن لـ(م.خ.ت.إ) القيام بإيقاف العمل بشهادة التّصديق الإلكتروني حالا بناء على طلب صاحبها، أو في حالة تسليم الشّهادة وفقا لمعلومات خاطئة أو مزوّرة، أو استعمال الشّهادة لأغراض تدليسيّة، أو تّم تعديل أو تغيير المعلومات الواردة في الشّهادة أو انتهاك منظومة إحداث التّوقيع الإلكتروني، وعليه يقوم(م.خ.ت.إ) حالا برفع حالة الإيقاف إذا تبيّن له صّحة المعلومات المُدوّنة في الشّهادة وأنّ استعمالها قد تّم بصفة شرعيّة[2].

وتنص **المادة 47** من القانون رقم 15–04، على ما يلي:" يجب على مؤدي خدمات التصديق الإلكتروني تحويل المعلومات المتعلقة بشهادة التصديق الإلكتروني الموصوفة بعد انتهاء صلاحيتها، إلى السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها."

[1] **إبراهيم خالد ممدوح**، التوقيع الإلكتروني، دار الجامعية، الإسكندرية، 2010، ص 229.

عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 177.

[2] ينص **الفصل 19** من القانون عدد 83– 2004، الذي يتعلق بالمبادلات والتجارة الإلكترونية، على ما يلي:" يتولى مزود خدمات المصادقة الإلكترونية تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها أو عندما يتبين:

– أن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة،

– أنه تم انتهاك منظومة إحداث الإمضاء،

– أن الشهادة استعملت بغرض التدليس،

– أن المعلومات المضمنة بالشهادة قد تغيرت.

ويتولى مزود خدمات المصادقة الإلكترونية إعلام صاحب الشهادة حالا بالتعليق وسببه.

ويتم رفع هذا التعليق حالا إذا تبينت صحة المعلومات المدونة بالشهادة واستعمالها بصفة شرعية.

ويعارض صاحب الشهادة أو الغير بقرار مزود الخدمات الخاص بتعليق الشهادة من تاريخ نشره بالسجل الإلكتروني المنصوص عليه بالفصل 14 من هذا القانون."

كما يُمكِن لـ(م.خ.ت.إ) أن يقوم بإلغاء شهادة التّصديق الإلكتروني[1] في حالة ما إذا طلب ذلك صاحب شهادة التّصديق أو قيام مقدّم الخدمة بإلغاء الشّهادة التي سبق تعليقها بصفة مؤقّتة بعد كشف معلومات مزوّرة أو غير صحيحة، أو أنّ شهادة التّصديق قد استعملت لغايات تدليسيّة، أو أنّ منظومة إحداث التّوقيع الإلكتروني قد تّم انتهاكها وتّم تغيير البيانات الواردة في الشّهادة الإلكترونيّة، حيث منح المشّرع التّونسي لصاحب الشّهادة أو الغَيْرِ إمكانية الطّعن في قرار إيقاف أو إلغاء الشّهادة من تاريخ نشر أحدهما في السّجل الإلكتروني لشهادات المصادقة المنصوص عليه في الفصل 14 من نفس القانون.

الفرع الثالث

الاعتراف بشهادات التّصديق الأجنبيّة

إنّ انتشار استخدام مرافق المفاتيح العموميّة(PKI–IGC- ICP) كوسيلة توثيق حديثة تُوّفر درجة عالية من الثّقة والأمان واليقين القانوني في إثبات التّصرفات الإلكترونيّة، تعترضها صعوبات رئيسيّة ذات صلة بعدم التّوافق القانوني والتّقني في استخدام طرق التّوثيق، فيما بين مرافق المفاتيح العموميّة نتيجة التّنازع أو التّباين في المعايير أو عدم التّناسق في تنفيذها، وإنكار القوانين الدّاخلية للاعتراف القانوني بالشّهادات والتّوقيعات الإلكترونيّة، وعليه فإنّ الافتقار لمرفق دولي للمفاتيح العموميّة من شأنه أن يُعرقل مبادلات التّجارة الإلكترونيّة ويُحدِث دواعي القلق والشّك بخصوص الاعتراف بشهادات التّصديق من

---

[1] ينص **الفصل 20** من القانون عدد 83– 2000 المتعلق بالمبادلات والتجارة الإلكترونية، على ما يلي:" يلغي مزود خدمات المصادقة الإلكترونية حالا الشهادة في الحالات التالية:

– عند طلب صاحب الشهادة،

– عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي صاحب الشهادة،

– عند القيام باختبارات دقيقة، بعد تعليقها، تبين أن المعلومات مغلوطة أو مزيفة أو أنها غير مطابقة للواقع أو أنه قد تم انتهاك منظومة إحداث الإمضاء أو الاستعمال المدلس للشهادة.

ويعارض صاحب الشهادة أو الغير بقرار مزود الخدمات الخاص بإلغاء الشهادة من تاريخ نشره في السجل الإلكتروني المنصوص عليه في الفصل 14 من هذا القانون."

طرف سلطات تصديق أجنبيّة، الشّيء الذي يستوجب وضع آليات تقنيّة جدّ مُتطوّرة للاعتراف بخدمات التّوثيق الأجنبيّة بصفة عامّة، كما أنّ ضمان شروط الالتحاق بالأسواق العالميّة وتبسيط الإجراءات الخاصّة بخدمات التّصديق فيما بين مرافق المفاتيح العموميّة(PKI–IGC- ICP)، تبدو من بين الأهداف الرّئيسيّة التي تسعى إلى تحقيقها أيّة دولة من العالم.

فكثيرا ما يتّم الاعتراف بشهادات التّصديق الأجنبيّة عن طريق تقنيّة "التّصديق المتبادل"(Certification croisée ou Réciproque)[1]، التي تستوجب تدّخل سلطات التّصديق(PSCE-AC) المتكافئة جوهريا للاعتراف بالخدمات التي تُقدّمها كلّ مِنْهَا، بُغْيَة السّماح للمستعملين التّابعين لكلّ منها، إمكانية التّواصل فيما بينهم بقدرٍ أكبر من الثّقة والأمان تجاه شهادات التّصديق الإلكتروني التي تصدر عنها(PSCE-AC)، حيث تقوم كلّ جهة تصديق رئيسيّة(AC-Racine) في مرفق مفاتيح عموميّة مُعيّن(PKI)، بإصدار شهادة تصديق متقاطعة(Certificat Croisé) التي تسمح لها بالتّوقيع على المفتاح العام، التّابع لجهة التّصديق الإلكتروني المثيلة لها(AC-Racine) في مرفق المفاتيح العموميّة الأخر(PKI)، التي تقوم بدورها(AC-Racine) بإصدار شهادة تصديق مُتقاطعة تُوقّع من خلالها على المفتاح العام التّابع للجهة الأولى، وتتّم نفس العمليّة بالنّسبة لجهات التّصديق الأخرى(AC-Racine) في إطار التّصديق المتبادل فيما بين مرافق المفاتيح العموميّة-PKI) (IGC-ICP، وبالتّالي فإنّ زوج الشّهادات المُصدَرة من طرفهم(Cross-Certificat) يبيّن علاقة الثّقة المتبادلة فيما بين سلطات التّصديق الرّئيسيّة(AC-Racine)، بالشّكل الذي يُؤدّي إلى

---

[1] تنص المادة **01** من القرار الوزاري رقم(1) لسنة 2008 (الإمارات) بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني، على ما يلي:[...]؛" (شهادة المصادقة الالكترونية المتبادلة) شهادات المصادقة الإلكترونية التي تُصدّق بين اثنان أو أكثر من مزودي خدمات التصديق الإلكتروني في عملية تبادلية لبعضهم البعض ويتم تطبيق الاستخدام التبادلي لها وتُصدر عن أيّ منهم. [...]." http://www.government.ae

خلق تكافؤ والتّوازن في السّياسات العامّة(PC+DPC) المُتّبعة في خدمات التّصديق الإلكتروني[1].

انطلاقا من ذلك، فإنّ الاعتراف المتبادل هو ترتيب بشأن قابلية التّشغيل البِينِي من النّاحية التّقنيّة، يحدث عادة على مستوى أعلى في مرافق المفاتيح العموميّة(PKI) وليس على مستوى(م.خ.ت.إ) بمُفرده، فعندما يعترف مرفق مفاتيح عموميّة بمرفق مفاتيح عموميّة آخر بموجب اتّفاقية الإعتراف المتبادل، فيتّم الإعتراف تلقائيا بأيّ(م.خ.ت.إ) يتيح خدمات تصديق ضمن المرفق المعني(PKI-IGC-ICP)، وبالتّالي فإنّ اتّفاقية الاعتراف تستند إلى تقييم عملية اعتماد مرفق مفاتيح عموميّة أخَر، وليس تقييم كلّ(م.خ.ت.إ) بمُفرده معتمد من طرف مرفق مفاتيح عمومية أخَر(PKI)، كما أنّ الاعتراف المتبادل يمكن أن يَنْصَبَّ حول تحديد أصناف معيّنة من شهادات التّصديق، التي يمكن القبول بها لغرض استعمالها فيما بين مرافق المفاتيح العموميّة المعنيّة، في حين يجب أن تكون البرامج التّطبيقية من النّاحية التّقنيّة قادرة على معالجة شهادات التّصديق الأجنبيّة، والدّخول إلى النّظام الدّليلي الحاسوبي لمنطقة مرافق المفاتيح العموميّة الأجنبي(PKI) للتّأكد من صّحة وضعية الشّهادات الأجنبيّة.

إنّ المواءمة بين السّياسات المُنظِّمة للشّهادات وبيانات الممارسات المتّبعة في إصدار شهادات التّصديق الإلكتروني، ضروريّة لضمان الاندماج الكلّي أو الجزئي لنطاقات المرافق العموميّة والاتّفاق فيما بينها ضمن نطاق أكبر حجمًا، فلولا اتفاقية الإعتراف المتبادل المُبْرمة على مستوى أعلى في كلّ مرفق مفاتيح عموميّة، فسيضطّر كلّ(م.خ.ت.إ) بمُفرده التّابع لكلّ مرفق مفاتيح عموميّة(IGC) إلى إبرام عدد لا يُحصى من إتفاقيات التّصديق المتبادل

---

1) **Arnaud-F.FAUSSE**, op.cit., p. 128.

تنص المادة **01** من القرار الوزاري رقم(1) لسنة 2008(الإمارات)، سالف الذكر، على ما يلي:[...]؛"(بيان ممارسة التصديق الإلكتروني) البيان الصادر عن مزود خدمات التصديق الإلكتروني من أجل تحديد الممارسات والإجراءات التي يوظفها مزود خدمات التصديق الإلكتروني في إصدار شهادات المصادقة الإلكترونية والمفتاح الرقمي فيما يتعلق بالتوقيعات الإلكترونية وأية خدمات أخرى مرخص بها. [...]."

مع(م.خ.ت.إ) التّابعين لمرافق المفاتيح العموميّة الأخرى[1](IGC) ، ممّا يخلق صعوبات ومشاكل تقنيّة من حيث قابليّة التّشغيل البِينِي فيما بين مرافق المفاتيح العموميّة، وعدم التّوافق فيما بين السّياسات المُنظِّمَة للشّهادات(PC) وبيانات الممارسات(DPC) المتّبعة في إصدار شهادات التّصديق الإلكتروني، فعن طريق آلية التّصديق المتبادل يتمكّن العملاء المنتمين لكلّ سلطة تصديق ضمن المرفق المعني(IGC) باتفاقيات الإعتراف المتبادل، التّعامل بكلّ ثقة وآمان مع المستخدمين أو المتعاملين الخاضعين لسلطة التّصديق(الأجنبيّة) المنتميّة للمرفق الأخر (IGC)، والقيام بعمليات البيع والشّراء لمختلف المنتجات مع دفع ثمنها بتقنيات مؤمّنة عبر شبكة الإنترنت في أيّ مكان من العالم وفي ظرف وجيز.

إنّ إرساء الثّقة والأمان في المعاملات الإلكترونيّة بحاجة إلى تنظيم مُحكم ودقيق لمرفق المفاتيح العمومية(PKI-IGC-ICP) المنتهج حسب السّياسة العامّة لكلّ دولة، التي يتعيّن عليها تحديد شكل المرفق(ICP) وعدد مستويات سلطات التّصديق(AC)، وإمكانية تفويض هيئات عامّة أو خاصّة كسلطات تصديق(AC-RACINE)، تشرف على تنظيم ورقابة نشاطات مقدّمي خدمات التّصديق الإلكتروني(PSCE-AC)، فبعد الأخذ بعين الاعتبار تجارب مختلف تشريعات الدّول الأجنبيّة والعربيّة في مجال التّصديق الإلكتروني، قام المشّرع الجزائري بانتهاج النّموذج الهرمي في خدمات التّصديق الإلكتروني(Hierarchy PKI) كنموذج تصديق موثوق به لإصدار شهادات التّصديق الإلكتروني في الجزائر.

وعليه، أنشأ المشّرع الجزائري بموجب المادة 16 من القانون رقم 15–04 المحدّد للقواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، "سلطة وطنية للتّصديق الإلكتروني"(ANCE) لدى الوزير الأول تُدعى "**السّلطة**"، وذلك باعتبارها كسلطة تصديق رئيسيّة(AC-Racine) على مستوى أعلى في هرم مرفق المفاتيح العموميّة بالجزائر، تتمتّع

---

1) **Marc LACOURSIÈRE et Édith VÉZINA**, op.cit., pp. 114, 117.

دحماني سمير، "التوثيق في المعاملات الإلكترونية(دراسة مقارنة)"، مذكرة الماجستير في القانون، فرع: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري– تيزي وزو، 2015، ص ص 50، 51، 55، 56.

بالشّخصيّة المعنويّة وذمّة ماليّة مستقلّة، مُكلّفة وفقا للمادة 18 من نفس القانون، بالمهام المتعلّقة بترقية استعمال التّوقيع والتّصديق الإلكترونيين وتطويرهما وضمان موثوقيّة استعمالهما، وبإعداد "سياستها المتعلّقة بالتّصديق الإلكتروني" والسّهر على تطبيقها، بعد الحصول على الرّأي الإيجابي لهيئة الموافقة، المتمثلة في "المجلس الوطني لأمن الأنظمة المعلوماتية"، الذي تم إحداثه بموجب المادة 03 من المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المكلّف(المجلس) بإعداد الإستراتيجيّة الوطنيّة لأمن الأنظمة المعلوماتيّة والموافقة عليها وتوجيهها، إلى جانب المهام الأخرى المنصوص عليها وفقا للمادة 04 من نفس المرسوم[1].

كما تقوم "السّلطة"(ANCE) بالموافقة على سياسات التّصديق الإلكتروني الصادرة عن السّلطتين الفرعيتين "الحكوميّة(AGCE) والاقتصاديّة(ARPCE) للتّصديق الإلكتروني"، مع إبرام اتفاقيات الاعتراف المتبادل على المستوى الدّولي، والمساهمة في اقتراح مشاريع النّصوص التّشريعيّة أو التّنظيميّة ذات صلة بالتّوقيع أو التّصديق الإلكترونيين على الوزير الأول، ويتّم استشارتها عند إعداد أيّ مشروع من هذه القوانين، كما تقوم(ANCE) بعمليات التّدقيق على مستوى السّلطتين "الحكوميّة والاقتصاديّة" عن طريق "الهيئة الحكوميّة المكلّفة بالتّدقيق" التي تشرف بدورها على عملية التّدقيق حتّى على مستوى "السّلطة".

---

[1] تنص المادة 03 من المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، الذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر، على ما يلي:" تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، ما يأتي: مجلس وطني لأمن الأنظمة المعلوماتية يدعى في صلب النص "المجلس"، ويكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها. [...]."

وتنص المادة 04 من نفس المرسوم، على ما يلي:" يتولى المجلس، في إطار إعداد الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتية: [...]، - الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني، [...]."

كانت مهمّة هيئة الموافقة قبل إنشاء "المجلس"(**Conseil**) مُوكلة وفقا لنص **المادة 80** من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، إلى "**مجلس السلطة الوطنية للتصديق الإلكتروني**".

إنّ السّلطة الحكوميّة للتّصديق الإلكتروني(AGCE) المنشأة بموجب المادة 26 من نفس القانون(رقم 15-04)، لدى وزير البريد وتكنولوجيا الإعلام والاتّصال، تتمتّع بالاستقلال المالي والشّخصيّة المعنويّة، مكلّفة(AGCE) وفقا للمادة 28 من نفس القانون، بالمهام المتعلّقة بمتابعة ومراقبة نشاط التّصديق الإلكتروني "للأطراف الثالثة الموثوقة" مع توفير خدمات التّصديق الإلكتروني لفائدة المتدّخلين في الفرع الحكومي، بحيث تقوم السّلطة الحكوميّة(AGCE) بإعداد سياستها المتعلّقة بالتّصديق الإلكتروني وعرضها على "**السّلطة**"(ANCE) للموافقة عليها، وتقوم بنشر شهادة التّصديق الإلكتروني للمفتاح العمومي "للسّلطة" مع إرسال جميع المعلومات المتعلّقة بنشاط التّصديق الإلكتروني إليها دوريا أو بناء على طلب منها(ANCE)، كما تُوافق السّلطة الحكوميّة(AGCE) بدورها على سياسات التّصديق الصادرة عن "الأطراف الثالثة الموثوقة"(TC) مع السّهر على تطبيقها، وكذا تقوم بعمليات التّدقيق على مستوى "الطرف الثالث الموثوق" عن طريق "**الهيئة الحكوميّة المكلّفة بالتّدقيق**" وفقا لسياسة التّصديق، وفي جميع الأحوال تقوم السّلطة الحكوميّة(AGCE) بحفظ شهادات التّصديق الإلكتروني المنتهية صلاحيتها، بغية تسليمها إلى السّلطات القضائيّة المختصّة عند الاقتضاء وفقا للأحكام التّشريعيّة والتّنظيميّة المعمول بها.

أمّا سلطة ضبط البريد والاتصالات الإلكترونيّة(ARPCE)[1] عُيّنت بموجب المادة 29 من نفس القانون، كسلطة اقتصاديّة للتّصديق الإلكتروني مُكلّفة بمتابعة ورقابة مقدّمي

[1] تنص **المادة 189 من** القانون رقم 18-04، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، سالف الذكر، على ما يلي:" تلغى كل الأحكام المخالفة لهذا القانون، لا سيما منها أحكام القانون رقم 2000-03 المؤرخ في 5 جمادى الأولى عام 1421 الموافق لـ 5 غشت سنة 2000 الذي يحدد القواعد المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدل والمتمم، وكذا أحكام المادة 53 من الأمر رقم 10-01 المؤرخ في 16 رمضان عام 1431الموافق لـ 26 غشت سنة 2010 والمتضمن قانون المالية التكميلي لسنة 2010.

غير أنّه، تبقى أحكام النصوص التطبيقية للقانون رقم 2000-03 المؤرخ في 5 جمادى الأولى عام 1421 الموافق لـ 5 غشت سنة 2000، المعدل والمتمم والمذكور أعلاه، سارية المفعول إلى غاية صدور النصوص التنظيمية المتخذة لتطبيق هذا القانون."

خدمات التّصديق الإلكتروني[1]، وبإعداد سياسة التّصديق الخاصّة بها مع عرضها على "السّلطة"(ANCE) لإبداء موافقتها والسّهر على تطبيقها، وتقوم(س.ض.ب.إ.إ) بنشر شهادة التّصديق الإلكتروني للمفتاح العمومي "**للسّلطة**"، وتمنح بعد موافقة هذه الأخيرة(ANCE) التّراخيص لمقدّمي خدمات التّصديق الإلكتروني حيث تُحقّق من مطابقة طالبي التّراخيص مع سياسة التّصديق الإلكتروني سواء بنفسها أو عن طريق مكاتب تدقيق معتمدة، مع التّأكد من مدى مراعاة مقدّمي خدمات التّصديق(PSCE) المرخص لهم للتّأكيدات المقدّمة، في دفتر الشّروط الخاص بمزاولة خدماتهم مع مطالبتهم بأية وثيقة أو معلومة تساعدها أثناء تأدية مهامها الرّقابيّة، حيث يمكن للسّلطة الاقتصاديّة(ARPCE) أن تباشر عمليات المراقبة الفجائيّة أو عمليات التّدقيق الدّوريّة[2] أثناء مباشرة(م.خ.ت.إ) لمهامهم.

كما توافق كذلك السّلطة الاقتصاديّة للتّصديق الإلكتروني(س.ض.ب.إ.إ) على سياسات التّصديق الصادرة عن(م.خ.ت.إ) مع السّهر على حسن تطبيقها[3]، حيث تقوم باتخاذ جميع التّدابير اللاّزمة لضمان استمرارية خدمات التّصديق الإلكتروني في حالة عجز مقدّمي الخدمات عن تقديمها، وفي جميع الظّروف تقوم السّلطة الاقتصاديّة(ARPCE) بإرسال

---

[1] يُقصد بمؤدي خدمات التصديق الإلكتروني وفقا للمادة 12/02 من نفس القانون رقم 15-04، سالف الذكر:" كلّ شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني."

[2] راجع **المادة 52** من القانون رقم 15-04 ، سالف الذكر.

يعني **بالتدقيق** وفقا **للمادة 16/02** من نفس القانون (رقم 15-04): التحقق من مدى المطابقة وفقا لمرجعية ما، وأمّا سياسة التصديق الإلكتروني وفقا للفقرة 15 من نفس المادة (15/02) يقصد بها مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين.

كما تطرق القرار الوزاري رقم(1) لسنة 2008(الإمارات) بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني، سالف الذكر، إلى تعريف **المُدّقق** بموجب **المادة 01** منه، على أنّه:" الجهة أو الشخص الذي يقوم بالتدقيق الفني أو الحسابي على مزودي خدمات التصديق الإلكتروني المُرخص له في الدولة."

[3] تنص المادة 41 من القانون رقم 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيتين، على ما يلي:" يُكلف مؤدي خدمات التصديق الإلكتروني بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني، وفقا لسياسة التصديق الخاصة به، التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني."

جميع المعلومات المتعلّقة بنشاط التّصديق الإلكتروني إلى السّلطة دوريا أو بناء على طلبٍ منها(ANCE)، مع حفظ كافة شهادات التّصديق الإلكتروني المنتهيّة صلاحيتها(LCR)، والبيانات المتّصلة بها لغرض تسليمها بناء على طلبٍ من السّلطات القضائيّة المختّصة، أو تقوم تلقائيا بإعلام أو تبليغ النيابة العامّة في سريّة تامّة عن كلّ فعلٍ إجرامي يُكتشف بمناسبة تأدية مهامها طبقا للأحكام التّشريعيّة والتّنظيميّة المعمول بها.

وتقوم كذلك(س.ض.ب.إ.إ) بإعداد دفتر الشّروط المُحدّد لشروط وكيفيات تأدية خدمات التّصديق الإلكتروني، مع عرضه على "السّلطة"(ANCE) والسّهر على تواجد المنافسة الفعليّة والنّزيهة، من خلال اتّخاذ جميع التّدابير اللاّزمة لترقية أو استعادة المنافسة فيما بين سلطات التّصديق، والتّحكيم في النّزاعات القائمة فيما بينها أو مع المستعملين طبقا للتّشريع المعمول به، وكذا تقوم بإصدار التّقارير والإحصائيات العموميّة والتّقرير السّنوي المتعلّق بوصف نشاطاتها مع احترام مبدأ السّريّة[1].

[1] أنظر **الملحق رقم (34)**، ص 506.

خلاصة الفصل الأول

من خلال الدّراسة السّابقة، نصل إلى أنّ التّغلب على صعوبات الحماية الأمنيّة لمواقع التّجارة الإلكترونيّة من النّاحية التّقنيّة، يستوجب إعداد سياسة أمنيّة مُحْكَمة مدروسة بدقّة من طرف أخصائيين في مجال أمن المعلومات، والعمل على توثيق إجراءات الحماية ومخطّطات الشّبكات وتحديثها بصفة دوريّة، مع السّعي إلى استقطاب كوادر مُؤهّلة من ذوي الخبرة في مجال الحماية الأمنيّة.

وبما أنّ الأمن بصفة نهائية ينعدم بتاتًا في البيئة الإلكترونيّة الافتراضيّة، نتيجة كثرة الأخطار والتّهديدات الإلكترونيّة التي غالبا ما يصعب التّنبؤ بها، فلا بدّ من العمل على تقليل هذه الأخطار من خلال سّد الثّغرات أو الهفوات السّائدة في نظم الحماية الأمنيّة، لكون أنّ جميع مكوّنات الشّبكة تحوي مواطن ضعف قابلة للاستغلال من طرف أهل الاختصاص، الذين يتمتّعون بدراية كافية ومؤهّلات عالية، في مجال اختراق نظم أمن الحماية للمعلومات، الأمر الذي يستوجب بذل الجهود الرّامية إلى توعية وتدريب مُستخدمي الحاسبات الآلية بأهمّية وضرورة تثبيت تحديثات في أنظمة التّشغيل، والبرامج المضّادة للفيروسات والبرامج الخبيثة الضّارة، الخ...

وعليه، يُعتبر المستهلك الإلكتروني الطّرف الأقّل خِبرة ودِراية في مُعاملات التّجارة الإلكترونيّة، التي تتّم في بيئة إلكترونيّة افتراضيّة مملوءة بالمخاطر المتعلّقة بعمليات الاحتيال والتّدليس حول وسائل الدّفع عبر الإنترنت، وانتشار المواقع الإلكترونيّة الوهميّة وسرقة البيانات الإلكترونيّة، وتطوّر أساليب الدّعاية والإعلانات التّضليلية، مما يستوجب على المستهلك اتخاذ الاحتياطات أو التّدابير الأمنيّة اللاّزمة أثناء مباشرته لعمليات التّسويق الإلكتروني، كالتّسوق الآمن عبر الإنترنت والتّوعية بكلّ التّهديدات الإلكترونيّة المحتملة مع الاستعانة بمعايير الحماية الأمنيّة الحديثة، المُستخدمة في تشفير معاملات التّجارة الإلكترونيّة والعمليات المصرفيّة التي تتّم عبر شبكة الإنترنت، وكذا استخدام تقنيّة التّوقيع الإلكتروني الموثوق، كوسيلة أمان حديثة تُحقّق وظائف التّوقيع التّقليدي.

يلعب التّصديق الإلكتروني دورا رئيسيا في منظومة أمن معاملات التّجارة الإلكترونيّة، من خلال قيام (م.خ.ت.إ) الموثوق به بإصدار شهادات تصديق إلكتروني موصوفة تضمن تحديد هوّية أطراف العقد الإلكتروني، وتأكيد سريّة وسلامة البيانات الإلكترونيّة المتداولة، مع ضمان عدم إنكارها من قِبَلِ أطراف التّصرف الإلكتروني، وبالتّالي فإنّ الوظيفة الرّئيسيّة لشهادة التّصديق الموصوفة تكمن في ربط مفتاح عام بصاحب الشّهادة(المُوقّع أو جهة التّوثيق)، حيث تسمح هذه الشّهادة للطّرف المُعوِّل عليها أي متلّقي الرّسالة الإلكترونيّة، استعمال المفتاح العام المذكور فيها، للتّحقّق من أنّ التّوقيع الرّقمي أُنشئ باستخدام المفتاح الخاص المُناظِر له(المفتاح العام)، كما يمكن كذلك التّحقّق من صّحة التّوقيع الرّقمي على الشّهادة من جانب(م.خ.ت.إ) مُصدر الشّهادة، باستخدام المفتاح العام الخاص بـ(م.خ.ت.إ) المبيّن في شهادة أخرى صادرة عن(م.خ.ت.إ) آخر.

إنّ عملية التّصديق الإلكتروني تتطلّب التّنظيم المُحكم والدّقيق لجميع المسائل التّقنيّة المتعلّقة بمرفق المفاتيح العموميّة، حسب ما هو متلائم ومتوافق مع السّياسة العامّة المنتهجة لكلّ دولة، كتحديد شكل مرفق المفاتيح العموميّة وعدد مُستويات السّلطة التي يشملها، وما إذا كان لا يُسمح إلاّ لسلطات تصديق معيّنة تنتمي لمرفق المفاتيح العموميّة بإصدار أزواج مفاتيح التّشفير، أو من المُمكِن أن يُصْدِرُها أطراف التّعامل الإلكتروني بأنفسهم، وتحديد ما إذا كانت سلطات التّصديق الإلكتروني التي تشهد بصّحة أزواج مفاتيح التّشفير ينبغي أن تكون عموميّة أو خاصّة، ومدى خضوعها للتّرخيص أو الاعتماد من طرف الدّولة.

كما أنّ العلاقات المُنْشَئَةِ فيما بين(م.خ.ت.إ) المُنتمِين لأكثر من مرفق مفاتيح عموميّة، تشكّل مصدر قَلَقْ مُهدّد للمعاملات الإلكترونيّة، الشّيء الذي يستدعي النّظر في مدى إمكانية إبرام اتفاقيات التّصديق المتبادل للاعتراف بالمفعول القانوني بالتّوقيعات الإلكترونيّة، وشهادات التّصديق الإلكتروني الموصوفة المُصدرة في إطار كل مرفق مفاتيح عموميّة، فمهما كان نموذج التّصديق الإلكتروني المنتهج في كلّ دولة، فإنّ المواءمة فيما بين سياسات التّصديق، تستدعي تواجد سلطة تصديق رئيسيّة لإبرام اتفاقيات الاعتراف المتبادل فيما بين مرافق المفاتيح العموميّة.

الفصل الثاني

الحماية القانونيّة لمواقع التّجارة الإلكترونيّة

تُعتبر مواقع التّجارة الإلكترونيّة المُحرّك الرّئيسي أو القلب النّابض لمعاملات التّجارة الإلكترونيّة التي تتّم في بيئة إلكترونيّة افتراضيّة، مملوءة بالمخاطر أو الجرائم الإلكترونيّة المُتعلّقة بالخصوص بالتّجسّس الصّناعي أو القرصنة الفكريّة الإلكترونيّة التي تمّس بحقوق الملكيّة الرّقميّة بأصحاب المواقع التّجاريّة، سواء تعلقت بحقوق الملكيّة الأدبيّة والفنيّة(حقوق المؤلّف والحقوق المجاورة)، أو حقوق الملكيّة الصّناعيّة والتّجاريّة، وعليه فإنّ المصّنفات الرّقميّة في صورتها الرّاهنة ظهرت نتيجة التّطوّر العلمي والتّكنولوجي لتقنيات الاتصال التي ساهمت بشكل كبير في انتشار وتنامي تطبيقات التّجارة الإلكترونيّة، حيث فرضت على أرض الواقع تحديات آخرى متعلّقة بالملكيّة الفكريّة الرّقميّة التي تستوجب تدّخل المُشّرع لسّن أنظمة قانونيّة جديدة تضمن الحماية القانونيّة اللاّزمة لها(**المبحث الأول**).

إنّ التّطوّر المُذهِل والمُتسارع لتقنيات شبكة الإنترنت صاحب معه تطوّر رهيب وغير مُتوقَّع لصور الجريمة الإلكترونيّة، التي جعلت منها(الإنترنت) القاعدة الرّئيسيّة أو المكان اللاّئق للمجرمين الذين يستغلّون التّسهيلات المقدّمة من خلال هذه الشّبكة، لتنفيذ مختلف التّهديدات أو الهجمات الإلكترونيّة التي كثرت في الآونة الآخيرة في مجالات التّجارة الإلكترونيّة والعمليات المصرفيّة، حيث فرضت على أرض الواقع إشكالات قانونيّة واقتصاديّة وسّعت من نطاق الحماية الجنائيّة لمواقع التّجارة الإلكترونيّة(**المبحث الثاني**).

المبحث الأول
الحماية القانونية للمصّنفات الرّقميّة عبر الإنترنت

إنّ الملكيّة الفكريّة بمفهومها التّقليدي ترد على أشياء غير ماديّة من إنتاج وابتكار الفكر البشري، فالحقوق الذّهنيّة تشتمل على حقوق المؤلّف والحقوق المجاورة، والملكيّة الصّناعيّة والتّجاريّة المتعلّقة بحقوق المخترع، حيث ساهمت الثّورة الرّقميّة في ظهور مصّنفات رقميّة حديثة لا تختلف في مدلولها أو تكوينها عن المصّنفات التّقليديّة ولم تكن مألوفة ومحميّة في إطار قوانين حقوق الملكيّة الفكريّة، وذلك على غرار المصّنفات الرّقميّة الأخرى التي تّم اِبْتِكَارُهَا أو خلقها عبر الإنترنت أين تتطلّب بدورها الحماية القانونيّة لها(**المطلب الأول**).

إنّ تزايد المنتوج الرّقمي الذي عادة ما يتطلّب مجهودا ذهنيا مميّزا من قِبَلِ المُبْدِع وتوظيف موارد ماليّة وبشرية وتقنيّة ضخمة، وشيوع استخدام مواقع التّجارة الإلكترونيّة التي لا تخلو من نشاط استثماري مباشر وغير مباشر، صاحب معها ارتفاع أعمال التّعدي غير المشروع على المصّنفات الرّقميّة وفقا للإمكانيات التّقنيّة التي تُوفّرها المعلوماتيّة، كالنّسخ والتّحميل من الإنترنت وتقليد العلامات التّجاريّة التي غالبا ما تثير نزاعات حول أسماء مواقع الإنترنت، حيث يتطلّب الأمر توافر مرجعيّة قانونيّة لفّض النّزاعات(**المطلب الثاني**).

المطلب الأول
القواعد المقرّرة لحماية المصّنفات الرّقميّة عبر الإنترنت

إنّ المصّنف الرّقمي مصطلح حديث النّشأة لا يقتصر فقط على برامج الحاسوب وقواعد البيانات وطبوغرافيا الدّوائر المتكاملة المحميّة بموجب قوانين الملكيّة الفكريّة(**الفرع الأول**)، بل يشمل على المصّنفات الرّقميّة التي يتّم خلقها وابتكارها في بيئة الإنترنت كأسماء مواقع الإنترنت ومحتواها(النّشر الإلكتروني)، التي تحتاج هي الأخرى إلى جانب الحماية التّقنيّة إلى حماية قانونيّة فعليّة(**الفرع الثاني**)، التي من خلالها تّم الاتّفاق على إرساء آلية موّحدة لتّسوية نزاعات أسماء الإنترنت(**الفرع الثالث**).

الفرع الأول
المصّنفات الرّقميّة المحميّة عبر الإنترنت

إنّ الملكيّة الذّهنيّة الرّقميّة تنطوي بطبيعتها على حقوق الملكيّة الأدبيّة والفنيّة وحقوق الملكيّة الصّناعيّة والتّجاريّة، التي تعتبر كلّها حقوق فكريّة من نتاج العقل البشري وخلقه وإبداعه[1]، وبالتّالي تنقسم المصّنفات الرّقميّة المحميّة وفقا لتشريعات الملكيّة الفكريّة إلى برامج الحاسوب(**أولا**) وقواعد البيانات(**ثانيا**) وطبوغرافيا الدّوائر المتكاملة(**ثالثا**).

أولا– برامج الحاسوب(Logiciels):

تحتوي شبكات الاتّصال المعلوماتيّة إلى جانب الأجهزة الماديّة(أجهزة الحواسيب، الموّجهات، الموزّعات الخ...)، على كيانات غير ماديّة(البرمجيات) تُشرف على عمليات المعالجة المعلوماتيّة وتشغيل الأجهزة الماديّة وفقا للتّعليمات التي حدّدها المُبرمِج مُسبقا(**1**)، حيث تتمتّع هذه البرمجيات بحماية قانونيّة خاصّة سواء بموجب قانون حق المؤلّف والحقوق المجاورة(**2**)، أو بموجب قانون البراءات(**3**).

1)– أنواع برامج الحاسوب:

تعتبر البرمجيات المعلوماتيّة بمثابة الرّوح في جسد الكائنات الحيّة فبدونها تصبح الأجهزة الماديّة كَكُتل حديديّة وبلاستيكيّة من دون فائدة، حيث تنقسم هذه البرمجيات إلى برمجيات التّشغيل(System software) التي تُعدّ كجزء من الحاسوب أو الشّبكة وليس لها علاقة بالأغراض الخاصّة بالمُستخدمين، حيث تُتيح عمليات التّشغيل والإغلاق لمُكوّنات شبكة الاتّصال والقيّام بوظائف التّحكّم والسّيطرة على مَوَارِدِهَا، أمّا البرمجيات التّطبيقيّة(Application Software) فهي مُخصّصة لمعالجة قضايا أو احتياجات مستخدمي الإنترنت، حيث يتّم خلقها أو ابتكارها لتنفيذ مهام أو غايات مُعيّنة بالمستخدمين ويتم تَثْبِيتُهَا

[1] **رامي إبراهيم حسن الزواهرة**، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف: دراسة مقارنة في القوانين الأردني والمصري والإنجليزي، دار وائل للنشر، عمان، 2013، ص 120.

على مُستوى أجهزة الحاسوب أو الهواتف الذّكيّة، كما تتضمّن هذه البرمجيات كذلك على الأنظمة المُعدّة للصّناعة التي تؤدّي دورا تِقْنِيًا أو صِنَاعِيًا[1].

2)– حماية برامج الحاسوب وفقا لقانون حقوق المؤلّف والحقوق المجاورة له:

أدرجت غالبية التّشريعات الدّولية والوطنيّة برمجيات الحاسوب في مفهوم الإنتاج في المجال الأدبي والعلمي والفني، طبقا لأحكام المادة 02 من اتفاقية برن لعام 1971 المتعلّقة بحماية المصّنفات الأدبيّة والفنيّة، وذلك بالرّغم من عدم إدراج هذه البرمجيات ضمن القائمة الواردة في تلك المادة(02) من نفس الاتّفاقية[2].

حيث أكّدت ذلك أحكام نص المادة 04 من معاهدة الويبو بشأن حق المؤلف لعام 1996 المعروفة بمعاهدة الإنترنت الأولى[3]، التي تنص:" **تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية بمعنى المادة(02) من اتفاقية برن. وتُطبق تلك الحماية على برامج الحاسوب أيّا كانت طريقة التعبير عنها أو شكلها.**"

كما أكدّت ذلك أيضا نص المادة 1/10(الجزء2(القسم1) من الملحق1(ج)) من اتّفاقية الجوانب المتصلة بالتّجارة من حقوق الملكيّة الفكريّة(**TRIPS(ADPIC)**) لعام 1994[4]،

---

[1] **محمد فواز المطالقة**، النظام القانوني لعقود إعداد برامج الحاسوب الآلي، دار الثقافة للنشر والتوزيع، عمان، 2004، ص ص 12، 13.

[2] **Convention de Berne** pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, du 9 septembre 1886, complétée à PARIS le 4 mai 1896, révisée à BERLIN le 13 novembre 1908, complétée à BERNE le 20 mars 1914 et révisée à ROME le 2 juin 1928, à BRUXELLES le 26 juin 1948, à STOCKHOLM le 14 juillet 1967 et à PARIS le 24 juillet 1971 et modifiée le 28 septembre 1979. http://www.wipo.int

[3] **Traité de l'OMPI sur le droit d'auteur (WCT)**, (adopté à Genève le 20 décembre 1996) http://www.wipo.int

Art.4 : « (**Programmes d'ordinateur**) Les programmes d'ordinateur sont protégés en tant qu'**œuvres littéraires** au sens de l'**article 2** de la **Convention de Berne**. La protection prévue s'applique aux programmes d'ordinateur quel qu'en soit le mode ou la forme d'expression. »

[4] **Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce(ADPIC)-Annexe 1C,** signé à Marrakech(Maroc) le 15 avril 1994(l'Accord de Marrakech instituant l'Organisation mondiale de commerce(**OMC**))**.** https://www.wto.org

Art.10.1 : « Les programmes d'ordinateur, qu'ils soient exprimés en code source ou en code objet, seront protégés en tant qu'œuvres littéraires en vertu de la Convention de Berne (1971). »

التي تنص:" **تتمتع برامج الحاسب الآلي(الكومبيوتر)، سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن(1971).**"

كما نص مشّرع الاتّحاد الأوروبي وفقا للمادة 1/01 من التّوجيه رقم 24/2009 المؤرخ في 23 أفريل 2009 المتعلّق بالحماية القانونيّة لبرمجيات الحاسوب[1]، على أنّ برامج الحاسوب تتمتّع بالحماية باعتبارها أعمالا أدبيّة وفقا لمعاهدة برن لعام 1971.

كما أقرّ ذلك أيضا المشّرع الجزائري بموجب المادة 04/(أ) من الأمر رقم 05/03 المؤرخ في 19 جويلية 2003 المتعلّق بحماية حقوق المؤلف والحقوق المجاورة[2]، التي تنص:" **تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:[...]، وبرامج الحاسوب،[...].**"

وعليه، فإنّ حماية برامج الحاسوب بموجب حقوق المؤلف تشمل حقوق التّأليف التي تّم التّعبير عنها بطريقة مُعيّنة على المَوقِع الإلكتروني، ولا تشمل الأفكار أو الإجراءات أو

---

1) **Directive 2009/24/CE** du parlement européen et du conseil du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur, JOUE, n° L 111/16 du 05/05/2009.
Art.01-1 : « - Conformément aux dispositions de la présente directive, les États membres protègent les programmes d'ordinateur par le **droit d'auteur** en tant **qu'œuvres littéraires** au sens de la convention de **Berne** pour la protection des œuvres littéraires et artistiques. Les termes «programme d'ordinateur», aux fins de la présente directive, comprennent le matériel de conception préparatoire.
Art.10 : « La **directive 91/250/CEE**,(du Conseil du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur) telle que modifiée par la directive visée à **l'annexe I, partie A**, **est abrogée**, sans préjudice des obligations des États membres en ce qui concerne les délais de transposition en droit national des directives indiqués à **l'annexe I, partie B**.
Les références faites à la **directive abrogée** s'entendent comme faites à la présente directive et sont à lire selon le **tableau** de correspondance figurant à **l'annexe II**. »

2) مرسوم رئاسي رقم 97–341 مؤرخ في 13 سبتمبر 1997، يتضمن انضمام الجمهورية الديمقراطية الشعبية، مع التحفّظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 09 سبتمبر 1886، والمتممة بباريس في 04 ماي 1896 والمعدلة ببرلين في 13 نوفمبر 1908، والمتممة ببرن في 20 مارس 1914، والمعدلة بروما في 02 جوان 1928، وبروكسل في 26 جوان 1948 واستكهولم في 14 جويلية 1967 وباريس في 24 جويلية 1971، والمعدلة في 28 سبتمبر 1979. ج ر عدد 61 الصادر في 14 سبتمبر 1997.
أمر رقم 03– 05 مؤرخ في 19 جويلية 2003، يتعلق بحماية حقوق المؤلف والحقوق المجاورة، ج ر عدد 44 الصادر في 23 جويلية 2003.

أساليب العمل أو المفاهيم الرّياضيّة في حدّ ذاتها والتي لم يتّم التّعبير عنها بشكل ملموس في الموقِع الإلكتروني[1]، كما أنّ برامج الحاسوب التي تتضمّنها مواقع التّجارة الإلكترونيّة تتمتّع بنفس الحماية المُقرّرة للبرامج التي تم تخزينها على الأقراص المُدمجة.

3)– حماية برامج الحاسوب بموجب قانون براءة الاختراع:

إنّ برمجيات الحاسوب يمكن أن يكون نوعاً منها محميًّا بموجب قوانين براءات الاختراع، في حالة ما إذا كانت مبتكرات جديدة لها مفعول "تقني صناعي أو تجاري" يستوجب الحماية وفقا لنظام براءات الاختراع، حيث ميّز المشّرع الفيدرالي للاتّحاد الأوروبي بموجب المادة 2–1/01 من التّوجيه رقم 24/2009 المتعلق بالحماية القانونيّة لبرمجيات الحاسوب[2]، بين نوعين من الحماية القانونيّة لبرمجيات الحاسوب، فنوع منها محمي بموجب "قانون حماية حق المؤلف" والنّوع الثّاني يكون محمي بموجب "قانون براءة الاختراع" عندما يتعلّق الأمر بالبرمجيات الجديدة القابلة للاستخدام الصّناعي، والجدير بالذّكر أنّ لجنة ومجلس الإتّحاد الأوروبي اقترحا في 2002 توجيه إداري حول منح البراءات للاختراعات التي تمّت بموجب الحواسيب[3]، إلاّ أنّ البرلمان الأوروبي قام في 2006 بإلغاء مُقترح هذا التّوجيه[4] بأغلبية

---

1) **Traité** de l'OMPI sur le droit d'auteur (WCT), adopté à Genève le 20 décembre 1996. http://www.wipo.int

Art.2 : « Étendue de la protection au titre du droit d'auteur La protection au titre du droit d'auteur s'étend aux **expressions** et **non** aux idées, procédures, méthodes de fonctionnement ou concepts mathématiques en tant que tels. »

2) **Directive 2009/24/CE** du parlement européen et du conseil du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur, JOUE, n° L 111/16 du 05/05/2009.

Art.01-2 : « - La protection prévue par la présente directive s'applique à toute **forme d'expression d'un programme d'ordinateur**. Les **idées** et **principes** qui sont à la base de quelque élément que ce soit d'un programme d'ordinateur, y compris ceux qui sont à la base de ses interfaces, ne sont pas protégés par le droit d'auteur en vertu de la présente directive. »

3) **Proposition de directive** du Parlement européen et du Conseil concernant la brevetabilité des inventions mises en œuvre par ordinateur, JOUE, n° C 151 E/129, du 25/6/2002. (Présentée par la Commission le 20 février 2002).

4) **Résolution législative** du Parlement européen relative à la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil concernant la brevetabilité des inventions mises en œuvre par ordinateur (11979/1/2004 - C6-0058/2005 - 2002/0047(COD)), JOUE, n° C 157 E/265, du 6/7/2006.

الأصوات أين أكّد بأنّ براءة الاختراع تمنح فقط للبرمجيات التي تتوافر فيها "شروط منح براءات الاختراع".

انطلاقا من ذلك، فإنّ الملكيّة الصّناعيّة تَرِدُ هي الأخرى على منقول غير مادّي(معنوي) باعتبارها فرع من فروع الملكيّة الفكريّة الرّقميّة، حيث تمنح براءة الاختراع لصاحبها حقّا حصريا لملكية واستغلال اختراعه، وهذا ما أكّدته نص المادة 1/27 من اتفاقية الجوانب المتّصلة بالتّجارة من حقوق الملكيّة الفكريّة(تريبس)، التي تُتيح إمكانية الحصول على براءة الاختراع لأيّ اختراعات جديدة إبداعيّة قابلة للاستخدام الصّناعي سواء كانت منتجات أو عمليات صناعيّة في كافة **ميادين التّكنولوجيا**[1].

وقد استبعد المشّرع الجزائري بموجب المادة 6/07 من الأمر رقم 03-07 المؤرخ في 19 جويلية 2003 المتعلّق ببراءات الاختراع برمجيات الحاسوب من الحماية بالبراءة، وذلك بعدما أن كان قد أخضعها للحماية بموجب براءة الاختراع في ظل المرسوم التّشريعي رقم 93-17 المؤرخ في 07 ديسمبر 1993 المتعلّق بحماية الاختراعات، أين نتساءل عن خلفيات ودوافع حذف أو عدم إدراج برمجيات الحاسوب من قائمة الحماية في حين نجد أنّ التّشريعات الحديثة تسعى إلى منحها الصدارة في قائمة الحماية، وبالتّالي فإنّ الأمر رقم 03-07 المتعلّق ببراءات الاختراع لا يُواكِب التّطوّرات الرّهيبة التي تشهدها تطبيقات التّجارة

1) **Art.27.1** (**ADPIC 1994**): « Objet brevetable Sous réserve des dispositions des paragraphes 2 et 3, un brevet pourra être obtenu pour toute invention, de produit ou de procédé, dans tous les domaines technologiques, à condition qu'elle soit nouvelle, qu'elle implique une activité inventive et qu'elle soit susceptible d'application industrielle. Sous réserve des dispositions du paragraphe 4 de l'article 65, du paragraphe 8 de l'article 70 et du paragraphe 3 du présent article, des brevets pourront être obtenus et il sera possible de jouir de droits de brevet sans discrimination quant au lieu d'origine de l'invention, au domaine technologique et au fait que les produits sont importés ou sont d'origine nationale. […].»

الإلكترونيّة، التي لم يُنَظِّمُهَا المشّرع من النّاحية القانونيّة ولم يتناولها في إطار هذا الأمر، خاصَّةً وأنَّ الجزائرَ بصدد المفاوضات للإنظمام إلى المنظّمة العالميّة للتّجارة(OMC)[1].

تؤدّي برمجيات الحاسوب وظائف تقنيّة مُتعدّدة كمراقبة الآلات أو التّحكّم الصّناعي، أو ترصّد الاتّصالات، الخ...، الأمر الذي يدفع بأصحاب الاختراعات إلى حماية إبداعاتهم البرمجيّة الجديدة بموجب قوانين براءات الاختراع، لكون أنّ قوانين حقوق المؤلّف لا تشمل الحماية سوى "التّعابير الأدبيّة للبرمجيات" سواء كانت بِلُغَةِ المصدر أو بِلُغَةِ الآلة، ولا تمتّد إلى الأفكار أو الإجراءات أو أساليب التّشغيل، ولا لغات البرمجة أو المفاهيم الرّياضيّة(Algorithmes) التي تُستخدم في التّطبيقات الصّناعيّة والتّجاريّة[2].

فلكي يكون البرنامج أهِلاً للحماية بموجب براءة الاختراع يجب أن يكون موضوع الاختراع جديدا قابلا للحماية بموجب البراءة وقابلا للتّطبيق الصّناعي، ينطوي في حدّ ذاته على نشاط ابتكاري ليس بديهي وأن يَسْتَوْفِيَ الاختراع لمعايير شكليّة وموضوعيّة مُحدّدة مُسبقاً، حيث يجب أن تستجيب الاختراعات المرتبطة بالبرمجيات لتلك الشّروط وخاصّة الشّرط المتعلّق بأهليّة الموضوع للحماية بموجب البراءة وشرط النّشاط الابتكاري غير

---

[1] أمر رقم 75–02 مؤرخ في 9 جانفي 1975، يتضمن المصادقة على اتفاقية باريس لحماية الملكية الصناعية المبرمة في 20 مارس 1883، والمعدلة ببروكسل في 14 ديسمبر 1900 وواشنطن في 02 جوان 1911، ولاهاي في 06 نوفمبر 1925 ولندن في 02 جوان 1934 ولشبونة في 31 أكتوبر 1958، واستكهولم في 14 جويلية 1967، ج ر عدد 10 الصادر في 04 فيفري 1975.

أمر رقم 03–07 مؤرخ في 19 جويلية 2003، يتعلق ببراءات الاختراع، ج ر عدد 44 الصادر في 23 جويلية 2003.

المادة 6/07 منه، تنص على ما يلي: "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر:[...] برامج الحاسوب،[...]. "

مرسوم تشريعي رقم 93–17 مؤرخ في 07 ديسمبر 1993 يتعلق بحماية الاختراعات، ج ر عدد 81 الصادر في 24 ديسمبر 1993.

[2] **Sandrine CARNEROLI**, op.cit., pp. 10-14.

أنظر كذلك الموقع الإلكتروني التالي: http://www.wipo.into/news/en/links/index.htm (consulté le 27/02/2019.)

البديهي، أين يُثار الجدل أو التّساؤلات حول الموضوعات الأَهِلة للحماية بموجب براءة الاختراع التي تختلف باختلاف القوانين الوطنيّة لكلّ دولة[1].

حيث ينبغي على صاحب الاختراع التّأكد من أنّ الابتكار المُرتبط ببرنامج الحاسوب يندرج فعلاً في إطار موضوع أهل للحماية بموجب قانون البراءات المعني، وأن يكون الاختراع المُطالب به غير بديهي حيث لا يكفي أن يكون جديدا ومُختلفا عن ما هو موجود في حالة التّقنيّة الصّناعيّة السّابقة، بل يجب أن يكون الفرق بين الاختراع الجديد وحالة التّقنيّة الصّناعيّة السّابقة كبيرا وجوهريا عن الاختراع، فلا يكفي لصاحب اختراع جديد مُرتبط ببرنامج حاسوب يَسْتَبْدِلُ بديهيا الحلول التّقنيّة والماديّة بحلول مُماثِلة باستعمال برامج وأجهزة حاسوبيّة، الخ...، أن يَطْلُبَ حمايته بموجب براءة الاختراع.

لتَيْسِيرِ إيداع طلبات الحصول على البراءات على الصّعيد الدّولي تُتيح معاهدة الويبو للتّعاون بشأن البراءات(PCT)، المُبرمة بواشنطن في 19 جوان 1970 المعدّلة في 28 سبتمبر 1979 وفي 03 فيفري 1984 وفي 03 أكتوبر 2001[2]، نِظام مُوحّد للإيداع الدّولي لتبسيط الإجراءات وخفض تكاليف الحصول على البراءة في الخارج، حيث يمكن للمعني إيداع طلب براءة دولي واحد يكون له نفس الأثر بالنّسبة للطّلبات الوطنيّة المودعة لدى كلّ دولة متعاقدة، حيث صادقت الجزائر بتحفّظ على هذه المعاهدة(PCT) ولائحتها

---

1) **Laure MARINO**, Droit de la propriété intellectuelle, 1er édition, Thémis droit, Paris, 2013, pp. 261- 282.

2) **Traité** de coopération en matière de brevets (**PCT**) fait à Washington le 19 juin 1970, modifié le 28 septembre 1979, le 3 février 1984 et le 3 octobre 2001. http://www.wipo.int
Art.3 : « Demande internationale **1)**- Les demandes de protection des inventions dans tout État contractant peuvent être déposées en tant que demandes internationales au sens du présent traité. **2)**- Une demande internationale doit comporter, conformément au présent traité et au règlement d'exécution, une requête, une description, une ou plusieurs revendications, un ou plusieurs dessins (lorsqu'ils sont requis) et un abrégé. **3)**- L'abrégé sert exclusivement à des fins d'information technique; il ne peut être pris en considération pour aucune autre fin, notamment pour apprécier l'étendue de la protection demandée. **4)**- La demande internationale : **i)** doit être rédigée dans une des langues prescrites; **ii)** doit remplir les conditions matérielles prescrites; **iii)** doit satisfaire à l'exigence prescrite d'unité de l'invention; iv) est soumise au paiement des taxes prescrites. »

التّنفيذيّة، بموجب المرسوم الرّئاسي رقم 99–92 المؤرخ في 15 أفريل 1999 التي دخلت حيّز التّنفيذ في 08 مارس 2000[1].

ثانيا– قواعد البيانات(Database).

تعتبر قواعد البيانات الوعاء الذي يسمح بتخزين واسترجاع ومعالجة العديد من البيانات الإلكترونيّة**(1)**، حيث تتمتّع بحماية قانونيّة بموجب قانون حق المؤلف والحقوق المجاورة**(2)**، أو بموجب القانون الخاص**(3)**.

1)– المقصود بقاعدة البيانات ومكوّناتها:

عرّف مشّرع الإتّحاد الأوروبي قاعدة البيانات بموجب المادة 2/01 من التوجيه رقم 09/96 المؤرخ في 11 مارس 1996 المتعلق بالحماية القانونية لقواعد البيانات[2]، على

---

[1] مرسوم رئاسي رقم 99–92 مؤرخ في 15 أفريل 1999 يتضمن المصادقة بتحفظ على معاهدة التعاون بشأن البراءات، المبرمة في واشنطن بتاريخ 19 جوان 1970 والمعدلة في 28 سبتمبر 1979، وفي 03 فيفري 1984، وعلى لائحتها التنفيذية، ج ر عدد 28 الصادر في 19 أبريل 1999.

Art.59(Traité de coopération en matière de brevets (**PCT**)…) ; « Différends Sous réserve de l'article 64.5), tout différend entre deux ou plusieurs États contractants concernant l'interprétation ou l'application du présent traité et du règlement d'exécution qui ne sera pas réglé par voie de négociation peut être porté par l'un quelconque des États en cause devant la Cour internationale de Justice par voie de requête conforme au Statut de la Cour, à moins que les États en cause ne conviennent d'un autre mode de règlement. Le Bureau international sera informé par l'État contractant requérant du différend soumis à la Cour et en donnera connaissance aux autres États contractants. »

Art.64-5(**PCT**) : « Réserves […], Tout **État** peut **déclarer** qu'il **ne** se considère pas **lié** par l'**article 59**. En ce qui concerne tout différend entre un État contractant qui a fait une telle déclaration et tout autre État contractant, les dispositions de l'**article 59** ne sont pas applicables. […]. »

[2] **Directive 96/9/CE** du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données, JOUE, n° L 077 du 27/03/1996.

Art.01 : « **1-** La présente directive concerne la protection juridique des bases de données, quelles que soient leurs formes.

2- Aux fins de la présente directive, on entend par **«base de données»**: un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière. »

أنّها:" **مجموعة أعمال وبيانات أو أيّ عناصر أخرى مستقلة، مُنظّمة بطريقة منهجية وفردية تُتيح الوصول إليها بوسائل إلكترونية أو أيّ وسيلة أخرى.**" وبالتّالي فإنّ قاعدة البيانات تتألّف من ثلاثة عناصر أساسيّة فالأوّل يشتمل على "البرنامج المعلوماتي" الذي على أساسه تكوّنت هذه القاعدة، والعنصر الثّاني يتمثّل في مضمون ومعالجة البيانات المخزّنة في قاعدة البيانات، أمّا العنصر الثّالث يتمثّل في "قاعدة البيانات" المكوّنة من العنصر "الأوّل" و"الثّاني"، حيث تُشكّل العناصر الثّلاثة مجتمعة جزءا واحد أو مجموعة متكاملة من البيانات تُعْرَفُ بقاعدة البيانات(Base de données)، التي تأخذ أشكالا متعدّدة أو متنوّعة كالموسوعات العامّة والمتخصّصة التي تحتوي على نصوص وأصوات ورسوم بيانية وصور ثابتة ومتحرّكة الخ...

2)– حماية قاعدة البيانات بموجب قانون حقوق المؤلف والحقوق المجاورة:

تعتبر قواعد البيانات القَالِبُ أو الوِعَاءُ الذي يَسْمَحُ بِتَخْزِينِ أو حَفْظِ كميّات هائلة من المعلومات وإدارتها وتعديلها وإلغاءها واسترجاعها، وتشتمل على مجموعة أعمال أدبيّة أو فنيّة أو موسيقيّة أو نصيّة أو صوتيّة أو مجموعة صور أو أرقام أو وقائع أو بيانات الخ...، وبالتّالي فإنّ أساس حماية قواعد البيانات بموجب حقوق المؤلف يتمحور حول الابتكار الفكري وهذا ما عبّرت عنه المادة 05 من اتفاقية الويبو بشأن حقوق المؤلف لعام 1996(معاهدة الإنترنت الأولى)[1] التي تنص:" **تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه، أياً كان شكلها، إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها. ولا تشتمل هذه الحماية البيانات أو المواد في حد ذاتها، ولا تخل بأي حق للمؤلف قائم في البيانات أو المواد الواردة في المجموعة.**"

---

[1] **Art.5 (Traité de l'OMPI sur le droit d'auteur(WCT) 1996**): « Compilations de données (bases de données) Les compilations de données ou d'autres éléments, sous quelque forme que ce soit, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles sont protégées comme telles. Cette protection ne s'étend pas aux données ou éléments eux-mêmes et elle est sans préjudice de tout droit d'auteur existant sur les données ou éléments contenus dans la compilation. » http://www.wipo.int

كما نصت أحكام المادة 2/10 من اتفاقية الجوانب المتّصلة بالتّجارة من حقوق الملكيّة الفكريّة(**TRIPS**) على أنّه[1]:" **تتمتع بالحماية البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آليا أو أي شكل أخر، إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها. وهذه الحماية لا تشمل البيانات أو المواد في حد ذاتها، ولا تخل بحقوق المؤلف المتعلقة بهذه البيانات أو المواد ذاتها.**"

وعليه، فإنّ قواعد البيانات تشتملها الحماية بموجب حقوق المؤلف بشرط أن تُمثّل إبداعات فكريّة، وذلك بصرف النّظر عن الشّكل المقترن بها سواء أكانت في شكل إلكتروني أو عادي، وكذا لا تسري الحماية على البيانات أو المواد نفسها، ولا تخل بحقوق المؤلف المتعلّقة بهذه البيانات أو المواد ذاتها، حيث نص المشّرع الفيدرالي للإتحاد الأوروبي بموجب المادة 1/03 من التّوجيه الأوروبي رقم 09/96 المتعلّق بالحماية القانونيّة لقواعد البيانات، على أنّ هذه الأخيرة تتمتّع بحماية قانون حق المؤلف باعتبارها أعمالا أدبيّة، ولا تشتمِل هذه الحماية على البرمجيات المعلوماتيّة المُستخدمة في صنع أو تشغيل قواعد البيانات التي يُمكِن الوصول إليها بالوسائل الإلكترونيّة المتاحة[2].

كما صنّف المشّرع الجزائري وفقا للمادة 2/5 من الأمر رقم 05/03 المتعلّق بحقوق المؤلف والحقوق المجاورة، قواعد البيانات ضمن المصّنفات الأدبيّة أو الفنيّة المحميّة وفقا

---

1) **Art.10.2** (**ADPIC-Annexe 1C, 1994**) : «Les compilations de données ou d'autres éléments, qu'elles soient reproduites sur support exploitable par machine ou sous toute autre forme, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles seront protégées comme telles. Cette protection, qui ne s'étendra pas aux données ou éléments eux-mêmes, sera sans préjudice de tout droit d'auteur subsistant pour les données ou éléments eux-mêmes.» https://www.wto.org

2) **Art.01-3** (**Directive européenne 96/9/CE…**) **-** La protection prévue par la présente directive ne **s'applique pas aux programmes d'ordinateur** utilisés dans la **fabrication** ou le **fonctionnement** des bases de données accessibles par des moyens électroniques. »
Art.03 (**Même Directive**) : « **1-** Conformément à la présente directive, les bases de données qui, par le choix ou la disposition des matières, constituent une création intellectuelle propre à leur auteur sont **protégées** comme telle par le **droit d'auteur**. Aucun autre critère ne s'applique pour déterminer si elles peuvent bénéficier de cette protection. »

لهذا القانون، حيث تنص:" **تعتبر أيضا مصنفات محمية الأعمال الآتية: –[...] وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، والتي تتأتى أصالتها من انتقاء موادها أو ترتيبها.**"

3)– حماية قاعدة البيانات بموجب القانون الخاص(Droit sui generis):

منح مشّرع الاتّحاد الأوروبي وفقا للمادة 1/03–2 من التوجيه الأوروبي رقم 09/96 المتعلق بالحماية القانونية لقواعد البيانات، حماية قانونية مُزدوجة لقواعد البيانات التي من خلالها يتمتّع البرنامج المعلوماتي المُكوَّنَة مِنْهُ قاعدة البيانات(Le contenant) بالحماية وفقا لقانون حقوق المؤلف في حالة توافر شرط الابتكار، أمّا الحماية الثّانية مَنَحَهَا لِمُحتوى قواعد البيانات(Le contenu) بموجب القانون الخاص(Droit sui generis)، حيث تَشْتَمِلُ هذه الحماية على عنصر الاستثمار الجوهري الذي يتطلّب توظيف موارد ماليّة وبشرية خاصّة، أين يُمكِن للمُستثمِر إثبات مشروعه من خلال رُخص البرمجيات(Licences de logiciels) وعقود المناولة(Sous-traitance)، وعقود العمل(Contrats de travail)، الخ...[1]

وعليه، فإنّ الحماية القانونيّة لقواعد البيانات بموجب حق المؤلف لا تتضمّن على محتواها(Le contenu) كالصّور أو الألحان أو البرامج الخ...، المحميّة بذاتها بموجب حق المؤلف بمعزلٍ عن الحماية القانونيّة لقاعدة البيانات التي تُخزّنها(Le contenant)، حيث تستوجب هذه الحقوق الحصول على ترخيص من صاحب حق المؤلف على العمل المُدخل في قاعدة البيانات قبل إدخاله فيها(قاعدة البيانات)، وبالتّالي فإنّ الحماية القانونيّة لقاعدة البيانات بموجب حق المؤلف تَنْصَبُّ فقط على هيكلتها أو القالب أو الخزّان Le)

---

[1] **Bertrand WARUSFEL,** La protection des bases de données en question : un autre débat sur la propriété intellectuelle européenne, pp. 896, 897. Article disponible à partir de l'adresse: http://www2.droit.parisdescartes.frwarusfelarticlesbasesdonnees_warusfel04.pdf, consulté le 04/01/2019.
Romaine V.GOLA, op.cit., 185-195.

(contenant، الذي تُوضَع فيه المعلومات وعلى العناصر اللاّزمة لتشغيلها أو لاستعمالها ولا تَشْتَمِلُ على مُحْتَوَاهَا(Le contenu)[1].

نظّم مشّرع الاتّحاد الأوروبي الحماية القانونيّة لقاعدة البيانات بموجب القانون الخاص(Droit sui generis) في الفصل الثّالث من نفس التّوجيه(رقم 09/96)، وذلك في حالة ما إذا لم يتوّفر شرط الابتكار في قاعدة البيانات وعدم إمكانية حمايتها بموجب حقوق المؤلف، حيث تستلزم عملية إحداث قاعدة البيانات استثمارا مُهِمًّا من النّاحية الكمّية أو النّوعية في الأموال والتّجهيزات والموارد البشريّة بما فيها الجُهد والوقت والوسائل الماديّة الخ...، وفي هذه الحالة يستفيد مُنتِج أو صَانع قاعدة البيانات من الحماية في إطار القانون الخاص، الذي يحمي الاستثمار الحَاصِل في تجميع معلومات مُحتوى قاعدة البيانات والتّحقق منها وتقديمها، حيث يتحمّل مَخاطِر الاستثمار[2].

فقد يحدث أن تكون قاعدة البيانات مُبتكرة وفي نفس الوقت تَتَطَلَّبُ صِنَاعَتُهَا استثمارات ضخمة، وفي هذه الحالة يُمكِن لصاحبها أن يَتَذَرَّعَ بوسيلة الحماية الأنجع أو اللاّزمة التي يراها ضروريّة، حيث أنّ الحماية بموجب القانون الخاص لقاعدة البيانات (Base de données) لا تَمْنَعُ حماية هذه الأخيرة بموجب حق المؤلف في حال توّفر شرط الابتكار[3]،

---

1) **Art.03-2** (Directive européenne 96/9/CE…) : - La protection des bases de données par le droit d'auteur prévue par la présente directive **ne couvre** pas leur **contenu** et elle est sans préjudice des droits subsistant sur ledit contenu. »
Voir aussi : - **Romaine V.GOLA**, op.cit., pp. 182, 183.

2) **Sandrine CARNEROLI**, op.cit., pp. 30, 31.
Code de la propriété intellectuelle(France) - Dernière modification le 24 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr
Art. L341-1 : « Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel. Cette protection est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs. »

3) **Philippe LE TOURNEAU**, op.cit., pp. 380, 381.

فوفقا للمادة 10 من نفس التّوجيه(رقم 09/96)، فإنّ مدّة الحماية بموجب القانون الخاص تسري منذ انتهاء صُنْعِ قاعدة البيانات وينقضي بعد مرور 15 سنة تُحسب إبتداءا من 01 جانفي الذي يلي تاريخ وضعها تحت تصّرف الجمهور بأيّ طريقة كانت، أو ابتداء من 01 جانفي الذي يلي تاريخ الانتهاء من الصُنْعِ، حيث تتجدّد مدّة الحماية بكلّ تعديل مُهّم على قاعدة البيانات التي تتطلّب أيضا استثمارات مُهمّة جديدة ما دام أنّ سبب الحماية يتعلّق بتواجد الاستثمار، فكلّما تجدّد هذا الأخير تجدّدت مَعَهُ مُدّة الحماية[1].

فوفقا للمادة 07 من التّوجيه الأوروبي رقم 09/96 المتعلّق بالحماية القانونيّة لقواعد البيانات[2]، يمكن لصاحب الحق الخاص منع أي شخص أخر من استخراج(Extraction)

---

[1] **Art.10** (**Directive européenne 96/9/CE…**) : « **1-** Le droit prévu à l'article 7 produit ses effets dès l'achèvement de la fabrication de la base de données. Il expire **quinze ans** après le **1er janvier** de l'année qui suit la date de **l'achèvement**.
2- Dans le cas d'une base de données qui a été mise à la disposition du public de quelque manière que ce soit avant l'expiration de la période prévue au paragraphe 1, la durée de la protection par ce droit expire quinze ans après le **1er janvier** de l'année qui suit la date à laquelle **la base a été mise à la disposition du public** pour la première fois.
3- Toute modification substantielle, évaluée de façon qualitative ou quantitative, du contenu d'une base de données, notamment toute modification substantielle résultant de l'accumulation d'ajouts, de suppressions ou de changements successifs qui ferait considérer qu'il s'agit d'un nouvel investissement substantiel, évalué de façon qualitative ou quantitative, permet d'attribuer à la base qui résulte de cet investissement une durée de protection propre. »

[2] **Art.07** (**Directive européenne 96/9/CE…**): « **1-** Les États membres prévoient pour le fabricant d'une base de données le **droit d'interdire** l'**extraction** et/ou la **réutilisation** de la totalité ou d'une partie substantielle, évaluée de façon qualitative ou quantitative, du contenu de celle-ci, lorsque l'obtention, la vérification ou la présentation de ce contenu attestent un **investissement substantiel** du point de vue qualitatif ou quantitatif. **2-** Aux fins du présent chapitre, on entend par: **a)** «**extraction**»: le transfert permanent ou temporaire de la totalité ou d'une partie substantielle du contenu d'une base de données sur un autre support par quelque moyen ou sous quelque forme que ce soit; **b)** «**réutilisation**»: toute forme de mise à la disposition du public de la totalité ou d'une partie substantielle du contenu de la base par distribution de copies, par location, par transmission en ligne ou sous d'autres formes. La première vente d'une copie d'une base de données dans la Communauté par le titulaire du droit, ou avec son consentement, épuise le droit de contrôler la revente de cette copie dans la Communauté. Le **prêt public** n'est pas un acte d'extraction ou de réutilisation. **3-** Le droit visé au paragraphe 1 peut être transféré, cédé ou donné en **licence contractuelle**. **4-** Le droit visé au paragraphe 1 s'applique indépendamment de la possibilité pour la base de données d'être protégée par le droit d'auteur ou par d'autres droits. En outre, il s'applique indépendamment de la possibilité pour le contenu de cette base de données d'être protégé par le droit d'auteur ou

وإعادة استعمال(Réutilisation) محتوى قاعدة البيانات، حيث يعتبر حق استخراج محتوى قاعدة البيانات أو إعادة استعماله كحق مادّي متعلّق باستثمار قاعدة البيانات، يمكن نقله أو التّنازل عنه أو إعطاؤه للغير بموجب عقد إجازة مُبرم من قِبل صاحب الحق الخاص، في حين يُسمح مبدئيا استخراج أو إعادة استعمال الأجزاء غير المهمّة من قاعدة البيانات، غير أنّه لا يُسمح استخراج أو إعادة استعمال متكرّرة ومنهجية لأجزاء غير مهمّة من محتوى قاعدة البيانات، التي يُفترض على أنّها أعمالا منافية للاستعمال العادي لقاعدة البيانات أو تُسبّب ضررا غير مُبرّر للمصالح المشرُوعة لصانع قاعدة البيانات.

يمكن لمُستعمِل قاعدة البيانات وفقا للمادة 09 من نفس التّوجيه، أن يقوم باستخراج أو إعادة استعمال جزء مهم من محتوى قاعدة البيانات الموضوعة تحت تصّرف الجمهور، من دون الحصول على ترخيص من صَانِعِهَا، وذلك في حالة استخراج محتوى قاعدة بيانات غير إلكتروني لغايات خاصّة، وكذا الاستخراج لأهداف البحث العلمي بشرط ذكر المصدر أو الاستخراج أو إعادة الاستعمال لغاية الأمن العام أو تنفيذ إجراءات إداريّة أو قضائيّة[1].

---

par d'autres droits. La protection des bases de données par le droit visé au paragraphe 1 est sans préjudice des droits existant sur leur contenu. **5-** L'**extraction** et/ou la **réutilisation répétées et systématiques** de parties non substantielles du contenu de la base de données qui supposeraient des actes contraires à une exploitation normale de cette base, ou qui causeraient un préjudice injustifié aux intérêts légitimes du fabricant de la base, ne sont pas autorisées. »
Voir aussi : **- Vincent FAUCHOUX, Pierre DEPREZ**, op.cit., pp. 82- 88.

[1] **Art.09**(**Directive européenne 96/9/CE…**) : « Les États membres peuvent établir que **l'utilisateur légitime** d'une base de données qui est mise à la disposition du public de quelque manière que ce soit **peut**, **sans autorisation du fabricant de la base**, extraire et/ou réutiliser une partie substantielle du contenu de celle-ci: **a**) lorsqu'il s'agit d'une extraction à des fins privées du contenu d'une base de données non électronique; **b**) lorsqu'il s'agit d'une extraction à des fins d'illustration de l'enseignement ou de recherche scientifique, pour autant qu'il indique la source et dans la mesure justifiée par le but non commercial à atteindre; **c**) lorsqu'il s'agit d'une extraction et/ou d'une réutilisation à des fins de sécurité publique ou aux fins d'une procédure administrative ou juridictionnelle. »

ثالثا– طوبوغرافيا الدّوائر المتكاملة(Topographies of Integrated Circuits):

يُعَبَّرُ عن طبوغرافيا الدّوائر المتكاملة من خلال تصميم وخريطة معيّنة يتم التّركيز عليهما في صنع وتكوين مختلف الأجهزة الإلكترونيّة، الخ...**(1)**، حيث حُظِيَتْ بحماية قانونيّة سواء في إطار قواعد حماية الملكيّة الفكريّة الواردة في اتفاقيتي واشنطن لعام 1989 وتريبس لعام 1994**(2)** أو في التّشريعات الوطنيّة المتعلّقة بحماية الملكيّة الصّناعيّة**(3)**.

1)– المقصود بطبوغرافيا الدّوائر المتكاملة:

عرّف مشّرع الاتّحاد الأوروبي المنتوج شبه الموصل(Produit semi-conducteur) بموجب المادة 1/01(a) من التّوجيه الأوروبي رقم 54/87 المؤرخ في 16 ديسمبر 1987 المتعلّق بحماية طوبوغرافيا المنتجات شبه الموصلة[1]، على أنّها:" **كلّ منتوج في شكله النهائي أو في شكله الانتقالي يتكون من دعامة تحتوي على شريحة عناصر شبه موصلة، أو يتكون من شريحة أو عدة شرائح لعناصر شبه موصلة أو منعزلة معدّة وفقا للترتيب الثلاثي الأبعاد، ويكون(المنتوج) مخصص لأداء وظيفة إلكترونية.**"

وتُضيف الفقرة(b) من نفس المادة(1/01) على أنّ التّصميم الشّكلي(Topographie) للمنتوج شبه الموصل يعني:" **سلسلة من الصور المترابطة فيما بينها مهما كانت الطريقة التي تم تثبيتها أو ترقيمها، حيث تُعبِّر(الصور) عن المظهر الثلاثي الأبعاد للشرائح**

---

[1] **Directive 87/54/CEE** du Conseil du 16 décembre 1986 concernant la protection juridique des topographies de produits semi-conducteurs, JOUE, n° L 024 du 27/01/1987.
Art.01: « **1-** Aux fins de la présente directive, on entend par: **a)-** produit semi-conducteur la forme finale ou intermédiaire de tout produit: **i)** composé d'un substrat comportant une couche de matériau semi-conducteur, et **ii)** constitué d'une ou de plusieurs autres couches de matières conductrices, isolantes ou semi-conductrices, les couches étant disposées conformément à une configuration tridimensionnelle prédéterminée, et **iii**) destiné à remplir, exclusivement ou non, une fonction électronique;
b)- topographie d'un produit semi-conducteur une série d'images liées entre elles, quelle que soit la manière dont elles sont fixées ou codées: **i)** représentant la configuration tridimensionnelle des couches qui composent un produit semi-conducteur; **ii)** dans laquelle chaque image reproduit le dessin ou une partie du dessin d'une surface du produit semi-conducteur à n'importe quel stade de sa fabrication. »

المُتكون منها ذلك المنتوج، وتُمثّل كلّ صورة الرسم أو جزء من الرسم على مساحة المنتوج الشبه الموصل مهما كان غرض تصنيعه."

كما عرّفت المادة 1/02 من معاهدة الويبو بشأن الدّوائر المتكاملة المبرمة بواشنطن في 26 ماي 1989، الدّائرة المتكاملة(Circuit intégré)[1] على أنّها:" **منتوج في شكله النهائي أو في شكله الانتقالي يكون أحد عناصره على الأقل عنصرا نشيطا، وكل الارتباطات أو جزءا منها هي جزء متكامل من جسم و/ أو سطح لقطعة من مادة، ويكون مخصصا لأداء وظيفة إلكترونية."**

وتنص الفقرة الثّانية من نفس المادة(2/02) على أنّه يُقصد بالطبوغرافيا(التصميم الشكلي):" **ترتيب ثلاثي الأبعاد مهما كانت الصيغة التي يظهر فيها، لعناصر يكون أحدهما على الأقل عنصرا نشيطا، ولكل وصلات دائرة مُتكاملة أو للبعض منها لمثل ذلك الترتيب الثلاثي الأبعاد المعد لدائرة متكاملة بغرض التصنيع."**

والجدير بالذّكر، أنّ المشّرع الجزائري طبّق حرفيا نص المادة 1/02–2 من معاهدة الويبو بشأن الدّوائر المتكاملة(واشنطن لعام 1989)، بموجب نص المادة 02 من الأمر رقم 08/03 المؤرخ في 2003/07/19 المتعلّق بحماية التّصاميم الشّكلية للدّوائر المتكاملة،

---

[1] **Traité** sur la propriété intellectuelle en matière de circuits intégrés, adopté à Washington le 26 mai 1989. http://www.wipo.

Art.02 : **i)** on entend par «**circuit intégré**» un produit, sous sa forme finale ou sous une forme intermédiaire, dans lequel les éléments, dont l'un au moins est un élément actif, et tout ou partie des interconnexions font partie intégrante du corps et/ou de la surface d'une pièce de matériau et qui est destiné à accomplir une fonction électronique, **ii)** on entend par «**schéma de configuration** (**topographie**)» la disposition tridimensionnelle-quelle que soit son expression-des éléments, dont l'un au moins est un élément actif, et de tout ou partie des interconnexions d'un circuit intégré, ou une telle disposition tridimensionnelle préparée pour un circuit intégré destiné à être fabriqué, **iii)** on entend par «titulaire» la personne physique ou morale qui, selon la législation applicable, doit être considérée comme bénéficiaire de la protection visée à l'article 6, **iv)** on entend par «schéma de configuration (topographie) protégé» un schéma de configuration (topographie) pour lequel les conditions de protection visées dans le présent traité sont remplies. »

وذلك بالرّغم من عدم توقيع وتصديق الجزائر على تلك المعاهدة[1]، ولعلّ أنّ دخول الجزائر في مفاوضات شاقّة بغية الإنظمام إلى المنظّمة العالمية للتّجارة(OMC)، جعلتها تأخذ بعين الإعتبار في تشريعاتها الدّاخليّة أحكام المواد من 35 إلى 38(القسم 06) من اتفاقية تريبس، المُنظِّمَة للرّسومات الطّبوغرافيّة للدّوائر المتكاملة.

2)– حماية طبوغرافيا الدّوائر المتكاملة في إطار الاتفاقيات الدوليّة:

إنّ ضمان الحدّ الأدنى من التّناسق فيما بين تشريعات الدّول في مجال حماية طبوغرافيا الدّوائر المتكاملة، لا يتحقّق إلاّ في إطار اتفاقية الويبو بشأن الدّوائر المتكاملة لعام 1989(أ)، وكذا اتفاقية الجوانب المتّصلة بالتّجارة من حقوق الملكيّة الفكريّة لعام 1994(ب).

أ)– حماية طبوغرافيا الدّوائر المتكاملة في إطار اتفاقية واشنطن لعام 1989:

منحت المادة 12 من هذه المعاهدة الدول المُتعاقِدة إمكانية إقرار الحماية للتّصاميم الشّكلية للدّوائر المتكاملة سواء بموجب أحكام اتّفاقية برن بشأن حقوق المؤلف(معاهدة الإنترنت الأولى لعام1996)، أو أحكام معاهدة باريس لحماية الملكيّة الصّناعيّة[2]، حيث حدّدت المادة 08 من تلك المعاهدة مدّة الحماية المقرّرة للدّوائر المتكاملة بثمانية(08) سنوات على الأقل، وفقا للتّدابير والإجراءات المقرّرة بموجب أحكام المواد من 04 إلى 07 من نفس المعاهدة[3]، والجدير بالذّكر أنّ معاهدة الويبو بشأن الدّوائر المتكاملة لعام 1989

---

[1] أنظر نص **المادة 02** من الأمر رقم 03– 08 المؤرخ في 19 جويلية 2003، الذي يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، ج ر عدد 44، الصادر في 2003/07/23.

[2] **Art.12 (Traité de Washington 1989)** :« Le présent traité **ne** porte pas **atteinte** aux obligations que la Convention de **Paris** pour la protection de la **propriété industrielle** ou la Convention de **Berne** pour la protection des **œuvres littéraires** et **artistiques** peuvent **imposer** aux Parties contractantes. »

[3] **Art.08** (Même traité) : « La durée de la protection est au **moins de huit ans.** »
Art.13 : « Aucune **réserve** ne peut être faite au présent traité. »

لم تَدخُل حيّز التّنفيذ إلى حدّ الآن، حيث لم تُوقِّع عليها سوى ثمانية(08) دول ولم تُصادِق عليها سوى ثلاثة دول من العالم وذلك من دون أيّ تحفّظ على أحكام تلك المعاهدة[1].

ب)– حماية طبوغرافيا الدّوائر المتكاملة في إطار اتّفاقية تريبس لعام 1994:

ألزمت اتّفاقية الجوانب المتّصلة بالتّجارة من حقوق الملكيّة الفكريّة(TRIPS)، بموجب نص المادة 35 منها، الدّول العُضوَة أو التي هي بصدد التّحضير للعضويّة في منظّمة التّجارة العالميّة(OMC)، أن تُوَافِقَ على مَنْحِ الحماية اللاّزمة للتّصميمات التّخطيطية للدّوائر المتكاملة، وفقا لأحكام المواد من 02 إلى 07(باستثناء الفقرة 03 من المادة 06)، وكذا المادتين 12 و03/16 من اتّفاقية واشنطن لعام 1989، وذلك بالإضافة إلى الأحكام الواردة بموجب المواد من 36 إلى 38 من اتّفاقية تريبس.

3)– موقف بعض التّشريعات من حماية التّصاميم الشّكلية للدّوائر المتكاملة:

لحماية طبوغرافيا المنتوج شبه الموصل تشترط فيه المادة 2/02 من التّوجيه الأوروبي رقم 54/87 المتعلق بحماية طوبوغرافيا المنتجات شبه الموصلة، أن يكون نِتاج جُهد فكري أو ذهني لِمُبْتَكِرِهِ وغير شائع في مجال المنتجات شبه الموصلة، ففي حالة ما إذا تَكوَّنت الطّبوغرافيا من عناصر أو أجزاء كانت شائعة ومعروفة، فتستفيد من الحماية إذا كان تجميع عناصرها كمُكوّن واحد مُنْبَثِقًا عن مجهود فكري أو ذهني، وأنّ طريقة تجميع هذه العناصر والمُكَوَّنْ بمُجملِه غير شائعين، حيث تنصّب الحماية القانونيّة فقط على المنتجات شبه الموصلة ويُستثنى منها كلّ مفهوم أو آلية ونظام وتقنيّة ومعلومة مُثْبّتَة مُدخَلة كلّها في الطّبوغرافيا[2].

---

[1] **Traité** sur la propriété intellectuelle en matière de circuits intégrés, adopté à Washington le 26 mai 1989. **Situation le 15 janvier 2019**
Signataires : Chine, Égypte, Ghana, Guatemala, Inde, Libéria, Serbie, Zambie. **Adhésions/Ratifications** : Bosnie-Herzégovine, Égypte, Sainte-Lucie. http://www.wipo.intwipolexartreatiestext.jspfile_id=294977

[2] **Art.02 (Directive 87/54/CEE du Conseil…)** : « **1-** Les États membres protègent les topographies de produits semi-conducteurs en adoptant des dispositions législatives par lesquelles des droits exclusifs sont accordés conformément aux dispositions de la présente directive. **2-** La topographie d'un produit semi-conducteur est protégée dans la mesure où elle

فلكي تستفيد الطّبوغرافيا من الحماية لا بدّ من تسجيلها في خلال السنتين(02) التي تلي أوّل استغلال تجاري لها لدى هيئة "رسميّة" وليست "خاصّة"، فعندما يكون الاستغلال سابق لتاريخ إيداع طلب التّسجيل يمكن إيداع المواد التي تُمثّل الطّبوغرافيا أو تجميعا معيّنا لدى الهيئة الرّسميّة، مع التّصريح عن تاريخ أوّل استغلال تجاري للطّبوغرافيا حيث لا يجوز أصلا للجمهور الاطّلاع على موادها وفقا لمبدأ سريّة الأعمال عند الإيداع، وكاستثناء يمكن للغير الإطّلاع عليها بناء لأمر قضائي أو لأمر سلطة مختصّة في حالات المنازعات[1].

ويُمنح الحق في الحمايةُ لمُبتكري طبوغرافيا المنتوج شبه الموصل أو لصاحب العمل بالنسبة للطّبوغرافيا المُبتكرة من قِبَل موظّف مدفوع الأجر، أو الطّرف في العقد الذي طلب الطّبوغرافيا المُبتكرة بموجب عقد غير عقد العمل وذلك بإستثناء حالة وجود أحكام مُخالفة في

---

résulte de **l'effort intellectuel de son créateur** et **n'est pas courante dans le secteur des semi-conducteurs**. Lorsque la topographie d'un produit semi-conducteur est constituée d'éléments courants dans le secteur des semi-conducteurs, elle est protégée seulement dans la mesure où la combinaison de ces éléments, prise comme un tout, répond aux conditions énoncées ci-avant. »

Art.08 (**Même directive**) : « La protection accordée à la topographie d'un produit semi-conducteur conformément à l'article 2 ne s'applique qu'à la topographie proprement dite, à l'exclusion de tout concept, procédé, système, technique ou information codée incorporés dans cette topographie. »

[1]) **Art.04** (**Même directive**) : **« 1-** Les États membres peuvent disposer que la topographie d'un produit semi-conducteur ne bénéficie pas ou cesse de bénéficier des droits exclusifs accordés conformément à l'article 2, si une demande d'**enregistrement** n'a pas été déposée régulièrement auprès d'un organisme public dans les **deux ans** qui suivent sa **première exploitation commerciale**. Les États membres peuvent exiger, en plus de l'enregistrement, que le matériel identifiant ou représentant la topographie, ou une combinaison quelconque de ces matériels, soient déposés auprès d'un organisme public, de même qu'une déclaration relative à la date de la première exploitation commerciale de la topographie, lorsqu'elle est antérieure à la date du dépôt de la demande d'enregistrement. **2-** Les États membres veillent à ce que le matériel déposé conformément au paragraphe 1 ne soit pas mis à la disposition du public, si ce matériel relève **du secret des affaires**. La présente disposition ne fait pas obstacle à la divulgation de ce matériel suite à une **injonction** d'un tribunal ou d'une autorité compétente à des personnes concernées par des litiges portant sur la validité ou la violation des droits exclusifs visés à l'article 2. **3-** Les États membres peuvent exiger que les transferts de droits relatifs à des topographies protégées soient enregistrées. **4-** Les États membres peuvent **subordonner l'enregistrement et le dépôt** visés aux paragraphes 1 et 3 au **paiement d'une taxe** qui ne peut être supérieure au coût administratif de la procédure. […]. »

عقد العمل أو أي عقد أخر[1]، حيث يحق لمالك الطّبوغرافيا المحميّة منع نسخها وإعادة إنتاجها، أو الاستغلال التّجاري واستيراد طبوغرافيا أو منتوج شبه موصل مُصّنع بواسطتها، في حين تسري هذه الحقوق ابتداء من تاريخ الإستغلال التّجاري الأوّل للطّبوغرافيا أو في تاريخ إيداع طلب تسجيلها أو عند تثبيتها أو ترميزها لأوّل مرّة، حيث تنقضي هذه الحقوق سواء بعد مرور عشرة(10) سنوات تسري من نهاية السّنة التي تم فيها الإستغلال التّجاري للطّبوغرافيا لأوّل مرّة في أيّ بلد، أو عندما لا يتم الاستغلال التّجاري في أيّ بلد في خلال خمسة عشرة(15) سنة تسري من التّاريخ الذي يتّم تثبيتها أو ترميزها لأوّل مرّة[2].

---

1) **Art.03(Même directive)** : **« 1-** Sous réserve des paragraphes 2 à 5, le droit à la protection est accordé aux créateurs des topographies de produits semi-conducteurs. **2-** Les États membres peuvent: **a)** dans le cas d'une topographie créée dans le cadre de **l'emploi salarié du créateur**, disposer que le droit à la protection est accordé à **l'employeur du créateur**, sauf dispositions contraires du contrat de travail; **b)** dans le cas d'une topographie créée au titre d'un **contrat** autre qu'un contrat de travail, disposer que le droit à la protection est accordé à une **partie au contrat** qui a commandé la topographie, sauf dispositions contraires du contrat.[…].»
Voir aussi : **Laure MARINO**, op.cit., pp. 299- 401.

2) **Art.07** (**Même directive**) : « **1-** Les États membres prévoient que les droits exclusifs visés à l'article 2 naissent: **a)** si l'enregistrement est la condition de l'obtention des droits exclusifs conformément à l'article 4, à la première des dates suivantes: **i)** la date à laquelle la topographie a fait l'objet d'une exploitation commerciale pour la première fois où que ce soit dans le monde; **ii)** la date à laquelle la demande d'enregistrement a été déposée en bonne et due forme ou **b)** lors de la première exploitation commerciale de la topographie où que ce soit dans le monde, ou **c)** lorsque la topographie est fixée ou codée pour la première fois. […].
3- Les droits exclusifs viennent à expiration après une période de **dix ans** à compter de la fin de l'année civile au cours de laquelle la topographie a fait l'objet d'une exploitation commerciale pour la première fois, où que ce soit dans le monde, ou, si l'enregistrement est une condition de la naissance ou du maintien des droits exclusifs, après une période de dix ans à compter de la première des dates suivantes: **a)** la fin de l'année civile au cours de laquelle la topographie a fait l'objet d'une exploitation commerciale pour la première fois où que ce soit dans le monde, ou **b)** la fin de l'année civile au cours de laquelle la demande d'enregistrement a été déposée régulièrement. **4-** Lorsqu'une topographie n'a pas fait l'objet d'une exploitation commerciale où que ce soit dans le monde dans un délai de **quinze ans** à partir de la date à laquelle elle est fixée ou codée pour la première fois, tous droits exclusifs existants conformément au paragraphe 1 viennent à expiration et, dans les États membres où l'enregistrement est une condition de la naissance ou du maintien des droits exclusifs, de nouveaux droits exclusifs ne peuvent naître que si une demande d'enregistrement a été déposée régulièrement dans le délai susmentionné. »

أمّا بالنّسبة للمشّرع الجزائري فإنّ مفعول الحماية القانونيّة الممنوحة للتّصميم الشّكلي بموجب المادتين 07 و08 من الأمر رقم 08/03 المتعلّق بحماية التّصاميم الشّكلية للدّوائر المتكاملة، تسري من تاريخ إيداع طلب تسجيله لدى المعهد الوطني للملكيّة الصّناعيّة، أو من تاريخ أول استغلال تجاري له في أي مكان من العالم، حيث يمكن لصاحب الحق إيداع طلب تسجيل واحد لكل تصميم شكلي قبل أي استغلال تجاري له، أو في أجل أقصاه سنتان(02) على الأكثر تسري من تاريخ بداية استغلاله، حيث تنقضي الحماية عند نهاية العشرة سنوات(10) التي تلي تاريخ سريان المفعول القانوني للحماية[1].

الفرع الثاني

المصّنفات الرّقميّة الأخرى التي تتطلّب الحماية في بيئة الإنترنت

إنّ الحماية القانونية للمصّنفات الرّقمية لا تقتصر فقط على ما ذُكِرَ بموجب الأحكام الخاصّة لقوانين حماية حقوق الملكيّة الفكريّة(برمجيات الحاسوب وقواعد البيانات وطبوغرافيا الدّوائر المتكاملة)، بل توجد مصّنفات رقميّة أخرى تّم خَلْقُهَا أو اِبْتِكَارُهَا في بيئة الإنترنت تتطلّب هي الأخرى الحماية القانونيّة لها، والتي سنتطرّق إليها على النّحو التّالي:

أولا– أسماء مواقع الإنترنت(Domaine names):

يَدُلُ اسم نطاق الإنترنت على عنوان رقم بروتوكول(IP) الخادم المُتّصل بشبكة الإنترنت، إذ يعود أوّل استخدام لنظام أسماء النّطاقات إلى عام 1983 على مستوى شبكة الأربنات(ARPANET)، المُستحدثة من طرف الولايات المتّحدة الأمريكيّة في زمن الحرب البّاردة، حيث ظهر هذا النّظام نتيجة التّطوّر اللاّحق على العنوان الرّقمي المُتكوّن من مجموعة الأرقام التي يصعب تخزينها وحفظها على مستوى ذاكرة الإنسان، إذْ جاء لتبسيط وتسهيل الاتّصال بالإنترنت عن طريق ترجمة الحروف المُكوّنة لعنوان(IP) إلى أرقام

[1] للمزيد من المعلومات أنظر نصوص المواد من 07 إلى 25 من الأمر رقم 08/03 المؤرخ في 19 جويلية 2003، الذي يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، سالف الذكر.

باستخدام لغة لا تفهمُها إلاّ الحواسيب، فقبل إنشاء هيئة الآيكان(ICANN) كانت أسماء النّطاقات العليا(TLD) تنحصر فقط في ثمانية(08) أسماء نطاقات عليا عامّة(gTLDs)، تستخدمها الشّركات والمؤسّسات الجامعيّة والمصالح الحكوميّة والعسكريّة التّابعة للولايات المتّحدة الأمريكيّة(«.net», «.org», «.int», «.gov», «.edu», «.com», «.mil», «.arpa»)، حيث ظهرت بعد استحداث تلك الهيئة في 1998 العديد من أسماء النّطاقات العُليا، سواء ضمن النّطاقات العليا العامّة(gTLDs) أو النّطاقات العُليا الوطنيّة(ccTLDs) [1].

إنّ عملية تسجيل اسم النّطاق لدى أحد المسّجلين(Registrar) المعتمدين من طرف هيئة الإنترنت للأسماء والأرقام المخصّصة(ICANN)، تعتبر من بين الخطوات الأساسيّة لإحداث مواقع الإنترنت، حيث يُمكِن تسجيل أسماء النّطاق في أحد النّطاقات العليا(TLD) إذْ يُمكِن أن يَقَعَ الاختيار على تسجيل اسما من النّطاقات العليا المُكوّنة من الأسماء العامّة المفتوحة للتّسجيل مثل(.com, .info, .org, .net, etc.) أو يتم الاختيار على اسم النّطاقات المقيّدة(.aero, .asia, .cat, .coop, .edu, .jobs, .museum, .mobi, etc.) في حالة ما إذا كان صاحبها مؤهّلا لاستخدامها، وكذا يُمكِن أن يتّم تسجيل اسما في إطار النّطاقات العُليا الوطنيّة(ccTLD) ضمن نطاقات المستوى الثاني(SLD) التّابعة لها مثل(.com.dz) للشّركات التّجاريّة، (asso.fr) للجمعيات، (cci.fr) لغرف التّجارة والصناعة الخ...، لذا أسندت إلى هيئة الآيكان(ICANN) مهمّة الإشراف على إدارة وتخصيص أسماء النّطاقات العليا(TLD)، حيث تتّم التّسجيلات في إطار أسماء النّطاقات العليا العامّة(gTLD) لدى مكاتب التّسجيل المُعتمَدة من طرف تلك الهيئة(ICANN)، أمّا التّسجيلات ضمن فئة النّطاقات العليا

---

1) **Philippe BARBET, Isabelle LIOTARD**, « Propriété intellectuelle et régulation des marchés des biens informationnels : le cas du nommage sur l'Internet », Revue d'économie industrielle, n°129-130, 1er et 2e trimestres 2010.
Nathalie DRYFUS, op.cit., pp. 31, 32, 71-73, 85- 87.

الوطنيّة(ccTLD)، تتّم على مستوى هيئة التّسجيل المعيّنة في كلّ نطاق أعلى لرمز البلد المعني التي يُطلق عليها السّجل(Registre)[1].

وعليه، يجب على الشّخص الرّاغب في تسجيل اسم النّطاق أن يتّبِع شروط وإجراءات التّسجيل المحدّدة في ميثاق التّسمية للامتداد المعني، حسب الجِهَةِ التي يجب تسجيل اسم المَوقِع لديها ونوع المَوقِع المرغوب تسجيله، حيث ينبغي عليه أن يأخذ بعين الإعتبار المسائل المتعلّقة بحقوق الملكيّة الفكريّة المحميّة، مع مراعاة مبدأ الأولويّة premier arrivé, » premier servi » أو « First Come First Served » المتّبع في إجراءات تسجيل اسم النّطاق، الذي يكرّس له الحق في استعماله أو استغلاله فعليًا خلال مدّة زمنيّة معيّنة مع الحرص على تجديدها كلما قَرُبَتْ نهايتها، حيث ينبغي التّأكد من عدم تسجيل اسم النّطاق

---

1) La **création** et la **délégation** de la gestion des domaines nationaux est de la responsabilité de l'**Internet Assigned Numbers Authority** (**IANA**). L'IANA est une **composante** de l'ICANN, l'autorité suprême de régulation de l'Internet. https://www.iana.org/domains/root/db
Règlement(CE) n° 733/2002 du parlement européen et du conseil du 22 avril 2002 concernant la mise en œuvre du domaine de premier niveau .eu. JOCE. L113/1 du 30/04/2002.
Art. 04/2-a et b : « […] ; **Le registre**: **a)-** organise, administre et gère le TLD .eu dans l'intérêt général et selon les principes de qualité, d'efficacité, de fiabilité et d'accessibilité;
b)- enregistre dans le **TLD .eu**, via tout **bureau d'enregistrement .eu accrédité**, les noms de domaine demandés par: **i)** toute entreprise ayant son siège statutaire, son administration centrale ou son lieu d'établissement principal dans la Communauté, ou **ii)** toute organisation établie dans la Communauté, sans préjudice du droit national applicable, ou **iii)** toute personne physique résidant dans la Communauté; […]. »
Note : (.eu) est le nom du domaine(**ccTLD**) pour l'**Union européenne**, qui a commencé avec l'adoption de ce règlement (CE) n° 733/2002, il est géré et exploité par un **registre** privé: **EURID**(European Registry of Internet Domain Names) est l'association à but non lucratif de droit belge basée à **Diegem** en **Belgique**, créée le 8 avril 2003 après appel d'offres. Cet organisme s'appuie sur des centaines de **registrars** au sein de l'Union européenne ou à l'extérieur, le domaine « .eu » a été approuvé par l'ICANN le 22/03/2005 et introduit dans la zone racine d'Internet (DNS root zone) le 02/O5/2005, il a été mis en exploitation le 07/12/2005, les sites officiels des institutions intergouvernementales de l'Union européenne ont migré progressivement de **.eu.int** vers « .eu » au cours de l'année 2006. Pour avoir plus d'informations sur ce sujet, veuillez consulter le site: https://eurid.eu/en/about-us/eu-timeline/, consulté le 15/12/2018.

المُراد تسجيله عن طريق البحث في قاعدة بيانات(Whois)[1] للمُسّجل(Registrars)، حيث يُمكِن تقسيم إجراءات تسجيل أسماء المواقع العليا(TLD) على النّحو التّالي:

أ)– إجراءات تسجيل أسماء المواقع العليا العامّة(gTLD): من المُسْتَحْسَنِ على أيّ راغب في تسجيل اسم النّطاق الأعلى العام(gTLD) أن يختار أحد المُسّجلين أو مكاتب التّسجيل المعتمدة من طرف هيئة الآيكان[2] مع التّأكد من نوع الامتداد المُرَادِ تسجيله، حيث ينبغي عليه أن يَتَوَخَّى الحيطة والحذر من مخاطر السّطو أو الاحتيال المُنْبَثِقَةِ من رسائل الاصطياد الخادعة(Le spam, phishing, etc.)، التي تحثّه على تسجيل أو إعادة تسجيل اسم النّطاق(gTLD) أو ضمان وتأكيد تَوَافُرِهِ أو أيّ عرض أخر مُقدّم[3]، وبالتّالي فإنّ شروط وإجراءات تسجيل اسم النّطاق تتّم مُباشرةً عبر المنصّة الإلكترونيّة للمُسّجل في إطار عقد خاص، مُبرَم بين المُسّجل المعتمد(Registraire accrédité) والشّخص(طبيعي أو معنوي) الذي يريد نشر اسم الإنترنت(Requérant)، الذي من خلاله يقوم صاحب طلب التّسجيل بفتح حساب خاص له مع المُسّجل، الذي يُزوّده بمُعرّف((Identifiant (contact ID) ورقم سرّي(Mot de passe)، للتّعريف عن هوّيته لدى خوادم المُسّجل، حيث يتعيّن عليه(Requérant) التّأكد عن طريق قاعدة بيانات(Whois) للمُسّجل من صّحة اختيار اسم

---

1) **Art. 16(Règlement (CE) N° 874/2004** de la commission du 28 avril 2004, établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier niveau **.eu** et les principes applicables en matière d'enregistrement): « **Base de données WHOIS** : La base de données **WHOIS** sert à fournir des informations raisonnablement exactes et actuelles sur les points de contact administratifs et techniques qui gèrent les noms de domaines sous le domaine de premier niveau **.eu**. La base de donnée **WHOIS** contient des informations sur le titulaire d'un nom de domaine, qui sont pertinentes et non excessives par rapport à la finalité de la base de données. Si les informations ne sont pas strictement nécessaires par rapport à la finalité de la base de données et si le titulaire est une personne physique, les informations devant être rendues publiques doivent être soumises au consentement sans équivoque du titulaire du nom de domaine. La fourniture délibérée d'informations inexactes est une raison de considérer que l'enregistrement du nom de domaine n'est pas conforme aux conditions d'enregistrement. »

2) قائمة مكاتب التسجيل المعتمدة من طرف هيئة الآيكان، منشورة على الموقع الإلكتروني التّالي:
https://www.icann.org/en/registrars/accredited-list.html

3) Informez-vous sur les pratiques légales et illégales (Escroqueries dans l'enregistrement de noms de domaine), à l'adresse : http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/ alt084.shtm

الموقِع واثبات عدم مَسَاسِهِ بحقوق الملكيّة الفكريّة المحميّة، وعدم مُخالفته للنّظام والآداب العامّة أو تناقضه مع أيّ نص تنظيمي أو تشريعي ساري المفعول، ليقوم فيما بعد بملء طلب التّسجيل مع إرفاقه بالوثائق اللاّزمة، والموافقة على أحكام اتفاقية تسجيل اسم الموقِع مع دفع تكاليف الخدمة، حيث يقوم المُسّجل إتاحة ملف التّسجيل عبر الإنترنت إلى هيئة التسجيل(Registre)، المسؤولة عن تسجيل اسم الموقِع في قاعدتها المركزيّة للامتداد.

وعليه، يجب على صاحب اسم النطاق أن يقوم بتجديد مدّة تسجيله بصفة دوريّة لدى المُسّجل، والاستجابة لأي إجراء متعلّق بإيقاف أو إلغاء أو تحويل اسم نطاقه تّم وفقا لبنود السّياسة المعتمدة من طرف هيئة(ICANN)، سواء لغرض تصحيح الأخطاء أو في حالة تسوية النّزاع المتعلّق باسم نطاقه، في حين يتمتّع صاحب اسم النّطاق خلال مُدّة التّسجيل بحق استعماله والتّصرف فيه، مع إمكانية نقله أو بيعه لمستخدم أخر أو تحويله من مُسّجل إلى مُسّجل أخر، حيث ينبغي على صاحب اسم الموقِع المُسَجَّلِ(Registrant) أن يَسْتَكْمِلَ فيما بعد خطوات إحداثه وتطويره لاستغلاله فعليًا[1].

ب)– إجراءات تسجيل أسماء النّطاقات العليا المكوّنة من رموز الدّول(ccTLD): إنّ إجراءات تسجيل أسماء النّطاقات العليا الوطنيّة(ccTLD) تختلف حسب الجهة المُشرفة على إدارة وتنظيم اسم النّطاق الوطني لكل دولة، وبالتّالي فإنّ عملية إدارة وتنظيم تسجيلات أسماء النّطاق المُكوَّن من رمز دولة الجزائر(.dz) المَسجَّل لدى هيئة(ICANN) في ماي 1995، كانت بمبادرةٍ من مركز البحث في الإعلام العلمي والتّقني(CERIST)، وذلك تزامنا مع دخول شبكة الإنترنت إلى الجزائر في عام 1994، حيث أُسندت آنذاك عملية إدارة وتنظيم اسم النّطاق(.dz) لمركز أسماء النّطاقات(NIC.DZ)[2] المعتمد من طرف هيئة

---

1) Pour avoir plus d'informations sur la politique de transfert de noms de domaine entre bureaux d'enregistrement(IRTP), vous pouvez visualiser l'adresse: http://icann.org/en/transfers/

2) Dans le **système (DNS)**, un **registre de noms de domaine** est une **base de donnée** contenant des informations sur les sous-domaines (ou **domaine de second niveau**) d'un domaine (.com), (.fr), (.ca), (.org), etc. On appelle aussi **registre** l'**organisation** qui maintient la **base de données** mentionnée au paragraphe précédent, on utilise souvent les

تخصيص أرقام الإنترنت(IANA) في 1995، في حين قام ذلك المركز بِمُبَاشَرَةِ عملية تسجيل اسم النّطاق الثّاني المُكوَّن من رمز دولة الجزائر باللّغة العربية(.الجزائر) في 2011 حيث شرع ذلك المركز (NIC.DZ) في إدارته وتطبيقه في سنة 2012[1].

إنّ إجراءات تسجيل أسماء المواقِع العليا الوطنيّة لا تختلف بكثير عن إجراءات تسجيل أسماء المواقع العليا العامّة(gTLD)، حيث ينبغي على صاحب طلب تسجيل اسم الموقع(ccTLD) أن يختار مُسّجِل معتمد من طرف هيئة تسجيل اسم الموقع الوطني، أين يقوم بالبحث في قاعدة بيانات(Whois) المُسّجِل، للتّأكد من عدم تسجيل اسم المَوقِع من طرف الغير، ليُحال فيما بعد من طرف المُسّجل لخطوات التّسجيل المذكورة سالفا[2]، وبالتّالي فإنّ إجراءات تسجيل اسم الموقع الأعلى الوطني(.الجزائر) أو(.dz)، محدّدة بموجب "ميثاق التّسمية للامتداد .الجزائر" أو(La charte de nommage du .DZ)، حيث تتّم مباشرة عبر المنصّة الإلكترونيّة للمُسّجِل المُعتمد من "مركز أسماء النّطاقات .الجزائر" أو(NIC-DZ)، الذي يجب أن تتواجد الخدمات الرّئيسيّة له بالجزائر (Le serveur DNS primaire du registrar)، حيث يُدير أسماء النّطاقات لحساب مقدّمي الطلبات الخاصين به.

---

termes ***Network Information Center*** ou ***NIC*** pour désigner cette **organisation**. Le **registre** contient la liste des noms de domaine déjà réservés dans un domaine de premier niveau ainsi que l'identification des **serveurs DNS** faisant autorité sur ces domaines, c'est de là que découle le fonctionnement de tous les serveurs DNS dans le monde. L'organisation vend les noms de domaine disponibles aux utilisateurs qui en font la demande, certaines vendent directement aux utilisateurs d'autres ne vendent que par l'intermédiaire de **registrars**. Les **registres** (la majorité le sont, mais pas .com) publient également les informations sociales des utilisateurs : noms, coordonnées des titulaires des domaines et coordonnées des points de contact techniques ou administratifs, cette publication se fait en général par le **protocole whois**.

Source : https://fr.wikipedia.org/wiki/Registre_de_noms_de_domaine/, consulté le 19/02/2019.

1) Voir le site: http://www.nic.dz/(consulté le 02/02/2019.)

2) **Jean-François PILLOU**, « Prendre un nom de domaine », article publié à partir de l'adresse suivante: http://www.commentcamarche.net/ Prendre-un-nom-de-domaine, consultée le 12/06/2018.

لذا يُمكِن الحصول على اسم النّطاق تحت الامتداد(.الجزائر) أو(.dz) من دون أي تكلفة[1]، لجميع الجهات أو الكيانات التي لها مقرّ أو مكتب اتصال في الجزائر أو حاملي وثيقة تُبيّن حقوق ملكية الاسم، حيث ينبغي أن يتضمّن ملف طلب التّسجيل[2] على استمارة تسجيل وفقا للنّموذج الذي أعدّه مركز أسماء النّطاقات(NIC-DZ)، مملوءة ومُوقّعة من طرف المَالِك النّهائي لاسم النّطاق مع إرفاقه بإحدى نسخ الوثائق المُبرِّرة لملكية اسم النّطاق(السّجل التّجاري، أو تسجيل العلامة التّجاريّة لدى(INAPI) أو(OMPI)، أو المرسوم الرّسمي لإنشاء الكيان، أو التّرخيص للجمعيات)، وعند الإقتضاء يجب على صاحب طلب التّسجيل في حالة الإستعانة بوسيط للقيام بإجراءات تسجيل اسم النّطاق (Fournisseur d'Accès à Internet (FAI), Société d'hébergement Web, etc.)، أن يُقدّمَ وكالة(Procuration) يُعَيِّنُ فيها الوسيط المكلّف بعملية تسجيل اسم النّطاق.

فإلى جانب الشّروط الإدارية، يجب على صاحب الطلب مراعاة قواعد صياغة أسماء النّطاق(الشّروط النّحوية) الواردة بموجب المادة 13–1 من ميثاق التّسمية للامتداد(.الجزائر)

---

[1] أنظر المادة 19 من ميثاق التسمية للامتداد(.الجزائر) أو(.dz) المنشورين على الموقع التالي: http://www.nic.dz

[2] أنظر المادتين(08) و(13–2) من ميثاق التسمية للامتداد(.الجزائر) أو(.dz).

Voir aussi : **l'art. 03** (**Règlement (CE) N° 874/2004** de **la commission du 28 avril 2004, […].**) : « La **demande d'enregistrement d'un nom de domaine** doit comporter les éléments suivants: **a)-** le nom et l'adresse de la partie qui introduit la demande;
b)- une déclaration, sous forme électronique, par laquelle la partie qui introduit la demande confirme qu'elle satisfait aux critères d'éligibilité généraux indiqués à **l'article 4, paragraphe 2, point b), du règlement (CE) no 733/2002**;
c)- une déclaration, sous forme électronique, par laquelle la partie qui introduit la demande affirme qu'à sa connaissance la demande d'enregistrement du nom de domaine est faite de bonne foi et n'empiète pas sur des droits détenus par des tiers;
d)- une déclaration, sous forme électronique, par laquelle la partie qui introduit la demande s'engage à respecter toutes les conditions relatives à l'enregistrement, y compris celles relatives à la procédure de règlement extrajudiciaire des litiges prévues au chapitre IV.
Toute inexactitude matérielle dans les éléments indiqués aux points **a) à d)** constitue une violation des conditions d'enregistrement. La vérification par le **registre** de la validité des demandes d'enregistrement est effectuée après l'enregistrement à l'initiative du registre ou dans le cadre d'un litige relatif à l'enregistrement du nom de domaine en question, sauf pour les demandes reçues pendant le déroulement de la procédure d'enregistrement par étapes telle que prévue aux articles 10, 12 et 14. »

أو(dz.)، حيث ينبغي عليه التّقيّد بالحروف والرّموز المسموح استخدامها في كتابة اسم النّطاق التي حدّدها المركز(NIC-DZ) عبر موقعه الإلكتروني، واحترام القواعد الخمسة المتعلّقة بكتابة اسم النّطاق كعدم استعمال حركة التّشكيل أو الشّدة حيث لا تُقبل كتابة(سَجّل.الجزائر) بينما يُسمح بكتابة(سجل.الجزائر)، وعدم دمج الحروف العربيّة والأجنبيّة(Wissal.الجزائر) الخ...[1]، مع تفادي كتابة الأسماء الممنوعة التي حدّدتها المادة 3/13 من ميثاق التّسمية(الدول، المدن، المهن، الأسماء العامّة، الأشخاص، والشّخصيات).

فبعد استيفاء الشّروط النّحوية والإداريّة يقوم المسّجل(Registrar) بعرض ملف طلب التّسجيل عبر الإنترنت لمركز التّسجيل(NIC-DZ) الذي يقوم بالتّحقّق من صّحة الملف، فإذا اكتشف عدم اكتماله أو تواجد معلومات ناقصة أو خاطئة في استمارة التّسجيل أو عدم موافقة اسم النّطاق لمواصفات ميثاق التّسمية، أو عدم عضوية المُمثّل الإداري للكيان، فإنّ طلب التّسجيل يُرْفَضُ، وفي الحالة العكسيّة يقوم المركز(NIC-DZ) بتسجيل المعلومات عن مالك اسم النّطاق في قاعدته الأصليّة(.الجزائر) أو(dz.) خلال مدّة أقصاها يومين تسري من تاريخ تقديم ملف طلب التّسجيل، مع تسليم شهادة تسجيل اسم النّطاق لصاحبه، الذي يمكن له أن يطلب في أيّ وقت تعديلات يراها ضروريّة على اسم النّطاق، بينما يحتفظ المركز بحقّه في إتاحة المعلومات للجمهور عبر قاعدة بيانات(Whois)[2].

في كلّ الظروف، يمكن للمركز(NIC-DZ) إلغاء اسم النّطاق من سجّل أسماء النّطاقات(.الجزائر) أو(dz.)، بناء على طلب من المُسّجل أو أمرٍ من محكمة أو إدارة أو وفقا لقرار إلغاء صادر من قِبَلِ لجنة تسوية النّزاعات لأسماء النّطاقات(.الجزائر)، أو(dz.) حيث حدّدت المادة 16 من ميثاق التّسمية للامتداد(.الجزائر) أو(dz.) على سبيل الحصر الحالات التي يمكن إلغاء تسجيل اسم النّطاق، التي تنطوي على حالة عدم التّبليغ عن

---

[1] للإطّلاع على قواعد صياغة اسم النطاق(.الجزائر) أنظر الموقع الالكتروني: http://www.nic.dz/

[2] أنظر المادتين 15 و17 من ميثاق التسمية للامتداد(.الجزائر) أو(dz.).

تغييرات لمعلومات مُصرّح بها أو الاستخدام غير المشروع لاسم النّطاق، أو يكون الإلغاء بقرار من لجنة تسوية النّزاعات لأسماء النّطاقات(.الجزائر) أو(dz.).

ثانيا– النّشر الإلكتروني(Electronic publication):

يعتبر النّشر الإلكتروني من بين إفرازات الثّورة الرّقميّة في مجال الإعلام والاتّصالات، إذ يشتمل على نشر مصنّفات الملكيّة الفكريّة باستخدام الوسائل الإلكترونيّة الحديثة، حيث يمكن أن تنصّب تقنيّة النّشر الإلكتروني على أسلوب النّشر التّقليدي للمصّنفات التي سبق نشرها ورقيًا ويتّم إعادة نشرها إلكترونيًا فيما بعد، إذ يُعرف هذا النّوع بالنّشر الإلكتروني المُوازي الذي لا يستّقل كليّة عن النّشر الورقي[1].

أمّا النّوع الثّاني من النّشر الإلكتروني يكون خالص ومُستقّلا عن النّشر التّقليدي، حيث تُنشر من خلاله المصّنفات لأوّل مرّة بطريقة إلكترونية على إحدى الوسائل الإلكترونيّة(DVD, CD ROM, MP3,MP4, etc.)، أو مباشرة عبر الإنترنت عن طريق روابط الإحالة(Liens hypertextes) المستعملة لنشر المصّنفات الرّقميّة عبر صفحات الويب ومحرّكات البحث، والإعلانات التّجاريّة، وكذا الوسائط الإلكترونيّة المتعدّدة(Multimedia) التي تنوّعت على نحو سريع ومُتنامي في محتوى مواقع الإنترنت، حيث تُستخدم لتَمَثِيل المعلومات باستخدام أكثر من نوع من الوسائط، مثل النّص(Text) الصّوت(Sound) والصّورة(Image) والحركة(Animation) والفيديو(Video) أو أيّ مُؤثّر آخر، مع إمكانية

---

[1] **إبراهيم الدسوقي أبو الليل**، "النشر الإلكتروني وحقوق الملكية الفكرية"، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية– الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، المجلد الثاني، ص ص 150، 151.

ربحي مصطفى عليان، إيمان السامرائي، النشر الالكتروني، الطبعة الثانية، درا صفاء للنشر والتوزيع، عمان، الأردن، 2014، ص ص 39– 46.

خالد عبده الصرايره، النشر الإلكتروني وأثره على المكتبات ومراكز المعلومات، دار كنوز المعرفة العلمية للنشر والتوزيع، عمّان، الأردن، 2008، ص 101.

يونس عرب، "نظام الملكية الفكرية للمصنفات المعلوماتية"، ص 22، مقال منشور عبر الموقع الإلكتروني التالي: https://www.arablawinfo.com

المزج بين هذه العناصر(نص وصورة وصوت وحركة وفيديو...) وتَفَاعُلِهَا معًا في وقت واحد عن طريق برنامج معلوماتي، حيث يتّم تسويقها تجاريا في وسائل الكترونية (VLC, PotPlayer, VegasPro, etc.) تُتيح إمكانية توزيعها وتحميلها وتعديلها مباشرة عبر الإنترنت[1].

وعليه، فإنّ محتوى مواقع التّجارة الإلكترونيّة يثير جدال وتحديّات حول تكييفها وإعطاؤها الوصف القانوني الملائم، ومدى القدرة على حمايته بموجب حقوق المؤلف والحقوق المجاورة له، أو بموجب الحق الخاص في حالة ما إذا تضمّنت على قاعدة بيانات أو تتّم حمايته(المحتوى) وفقا لأحكام قوانين الملكيّة الصّناعيّة والتّجاريّة، وبالتّالي فإنّه لا يُثار أيّ إشكال عندما يتضمّن محتوى الموقع الإلكتروني على مصّنف محمي بموجب قوانين حقوق الملكيّة الفكريّة، التي تُطبّق أحكامها على سبيل القياس على الأعمال الرّقميّة الإلكترونيّة أو على مُكوّنات مِنْهَا، وذلك وفقا للوَصْفِ القانوني المُمْكِن إعطاؤه لها، أو لكلّ مُكوّن منها.

حيث يتّم عادة التّأشير بحفظ حقوق المؤلف على نُسخ المصنّف الرّقمي أو في أسفل صفحات ويب الأصليّة، بصيغة دائرة تتضمّن في دَاخِلها على الحرف الأبجدي © الذي يُشير إلى مصطلح(Copyright)، وبيان السّنة التي تّم فيها نشر المصنّف لأوّل مرّة مع عبارة " جميع الحقوق محفوظة" أو "حقوق الطّبع"، التي يمكن كتابها بأيّة لغة أجنبيّة آخرى، وبالتّالي يعتبر نظام التّأشير بحقوق المؤلف معمول به دوليا ومن الإجراءات الضّروريّة التي "تُساعد" المؤلف على حماية مصنّفه المنشور عبر الإنترنت، وتُوّفر العِلم اليَقين لدى مُستخدم الإنترنت بأنّ هذا المصنّف محمي بموجب قوانين حق المؤلف[2].

---

[1] **أحمد عبد الله مصطفى**، "حقوق الملكية الفكرية والتأليف في بيئة الإنترنت"، مجلة الكترونية محكمة في المكتبات والمعلومات(Cybrarians journal)، عدد 21، ديسمبر 2009، ص ص 05، 09. https://www.cybrarians.info/journal/no21/searchengines.htm

[2] **Mickaël LE BORLOCH**, « L'application du droit d'auteur aux hyperliens analyse de droit Français et de droit américain », Thèse de doctorat en droit privé, Université Panthéon-Sorbonne - Paris I, France, 2016, pp. 25-30.

ولكن الإشكال، يُثار في حالة ما إذا كان محتوى الموقِع الإلكتروني التّجاري يتضمّن على مواد سمعية ومرئية وعلامات وأشكال ورسومات وتصميمات، تّم خَلقُها أو إبداعها لأوّل مرّة عبر الإنترنت، كاسم موقع الإنترنت وعناصر تصميمه وإعلانات روابط الإحالة، والوسائط الالكترونية المتعدّدة الخ...، التي لا تجد وسيلة للنّشر إلاّ عبر الإنترنت، حيث تستوجب هي الأخرى الحماية بموجب القانون، كما أنّها محل بحث ودراسة من قِبَلِ المختّصين والخبراء في مجال قوانين الملكيّة الفكريّة[1].

المطلب الثاني

القواعد المقرّرة لحماية أسماء مواقع الإنترنت

منذ ظهور هيئة الآيكان في عام 1998 أصبحت تتولى مسؤوليّة إدارة نظام أسماء مواقع الإنترنت التي انتشرت بسرعة في الآونة الأخيرة، حيث ظهرت أسواق تنافسيّة لتسجيلات أسماء المواقع التي تتّم من خلالها عمليات بيع وشراء وتحويل أسماء النّطاقات العليا العامّة(gTLD)، حيث ازدادت عمليات الاحتيال والسّطو على العلامات التّجاريّة المشهورة للشّركات التي ترضخ عادة إلى طلبات القراصنة التي تهدف إلى دفع مبالغ ماليّة كبيرة مقابل التّنازل عن أسماء المواقع المحتويّة لعلاماتها التّجاريّة، الأمر الذي دفع بمنظمتي الويبو والآيكان إلى إيجاد وإرساء آلية مُشتركة(« UDRP + Les « règles ») لتّسوية المنازعات المتعلّقة بأسماء المواقع الإلكترونيّة عبر الإنترنت(**الفرع الأوّل**)، حيث يمكن للطرف المتضّرر من النّزاع اللّجوء إلى إحدى آليات تسوية نزاعات أسماء مواقع الإنترنت، كالجهات المعتمدة من طرف هيئة الآيكان لحل نزاع أسماء المواقع وفقا للسّياسة الموّحدة

نواف كنعان، حق المؤلف: النماذج المعاصرة لحق المؤلف ووسائل حمايته، الطبعة الثالثة، دار الثقافة للتوزيع والنشر، عمان، 2000، ص ص 439، 440.

محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص 317.

[1] **يونس عرب**، "التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية"، مجلة العربية 3000، عدد 2003/1، النادي العربي للمعلومات، سوريا، ص ص 171–172.

وقواعدها، أو الجهات المسؤولة عن تسجيل أسماء المواقع الوطنيّة أو اللّجوء إلى المحاكم(**الفرع الثاني**).

الفرع الأوّل
الإطار الموّحد لتسوية نزاعات أسماء مواقع الإنترنت

يَطْرَحُ نظام أسماء المواقِع مجموعة من التّحدّيات المُتعلّقة بحماية حقوق الملكيّة الفكريّة عبر الإنترنت، الأمر الذي يستوجب إرساء سياسة موّحدة لتسوية نزاعات أسماء المواقع مع العلامات(**أوّلا**)، التي تستدعي مراعاة مجموعة من الشّروط والإجراءات الشّكلية المتعلّقة بالنّزاع، حيث يتّم على إثرها إصدار قرار تحكيمي لصالح أحد الأطراف المتنازعة(**ثانيا**).

أولا)– نشأة الإطار الموّحد لتسوية نزاعات أسماء مواقع الإنترنت ومجال تطبيقه.

إنّ مبادئ وقواعد السّياسة الموّحدة لتسوية نزاعات أسماء المواقِع أملتها ظروف اقتصاديّة ذات صلة بتطوّرات الاقتصاد الرّقمي(**1**)، الذي شهد عدّة نزاعات بشأن أسماء المواقِع(**2**).

1)– نشأة مبادئ وقواعد السّياسة الموّحدة لتسوية نزاعات أسماء النّطاقات(UDRP):

اعتمدت هيئة الإنترنت للأسماء والأرقام المُخصّصة(ICANN) مبادئ السّياسة الموّحدة لتسوية نزاعات أسماء مواقِع الإنترنت(UDRP)[1]، بناء على توصيات منظّمة الويبو في إطار مشروعها الأول بشأن أسماء مواقِع الإنترنت التي قامت بعرضه للهيئة(ICANN) في أفريل 1999[2]، حيث وافق مجلس إدارتها على التّوصيات المُقدّمة في إطار الجلسات

---

[1] En Anglais: "Uniform Domain Name Dispute Resolution Policy(UDRP)".
En français : Principes directeurs de règlement uniforme des litiges relatifs aux noms de domaine.

[2] التقرير النهائي لمشروع الويبو الأوّل بشأن أسماء الحقول على الإنترنت، منشور الويبو رقم 439:
http://www.wipo.int/amc/en/processes/process1/report
أنظر كذلك تقرير مشروع الويبو الثاني بشأن أسماء الحقول على الإنترنت، منشور الويبو رقم 843، الإقرار بالحقوق والانتفاع بالأسماء في نظام أسماء الحقول على الإنترنت، عبر الموقع التالي:
http://www.wipo.int/amc/en/processes/process2/report

المُنعقِدة بسانتياغو الشيلية(Santiago (Chili)) يومي 25–26 أوت 1999، كما صادق مجلس إدارة الهيئة(ICANN) على إجراءات السّياسة المُوّحدة لتسوية نزاعات أسماء المواقِع (les « Règles »)[1] في 24 أكتوبر 1999، المُعدّلة في 30 أكتوبر 2009 وفي 28 سبتمبر 2013[2]، وبالتّالي يجب أن تكون القواعد التّكميليّة(Règles supplémentaires) للمراكز المعتمدة لتسوية نزاعات أسماء المواقِع وفقًا للسّياسة الموّحدة(UDRP) التي تَبَنَّتْهَا هيئة(ICANN) وأن لا تتعارض مع قواعد لائحة إجراءاتها(Les « règles »)، ففي حال تعارضها(القواعد الإضافيّة) مع إجراءات السّياسة الموّحدة فتُطبّق هذه الأخيرة.

2)– مجال تطبيق إجراءات السّياسة الموّحدة لتسوية نزاعات أسماء المواقِع:

إنّ التّطبيق الإلزامي للسّياسة المُوّحدة يقتصر على أسماء المواقِع العليا العامّة(gTLDs)، وبعض أسماء المواقِع العليا الوطنيّة(ccTLDs) التي تشرف عليها هيئات التّسجيل التي قَبِلَتْ بمحض إرادتها إجراءات السّياسة الموّحدة لتسوية نزاعات أسماء المواقِع (Procédures(UDRP))[3]، وبالتّالي فإنّ هذه الإجراءات تُطبّق على النّزاعات النّاشئة فيما بين مُسَجِّلِي أسماء المواقِع ومالِكي العلامات(التّجاريّة أو الخدمة) أو أيّ عنصر أخر مُميّز(Autre signe distinctif) مملوك للغير، وليس النّزاعات النّاشئة فيما بين أسماء المَواقِع بِحَدِّ ذَاتِهَا[4]، لذا يجب على كلّ كيان(Registres et Bureaux d'enregistrements) معتمد من طرف هيئة(ICANN)، التّقيّد بإجراءات السّياسة الموّحدة لتسوية النّزاعات في إطار اتفاقيات التّسجيل المُبرمة مع أصحاب طلبات تسجيل أسماء المواقِع[5].

---

1) En Anglais: "Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules")"

2) **Nathalie DRYFUS**, op.cit., pp. 108- 110.
Voir aussi : Guide de l'OMPI relatif aux Principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine (Principes UDRP). http://www.wipo.intamcfrdomainsgtld.html

3) **Loïc ANDRÉ**, Le droit des marques à l'heur d'internet, Gualino éditeur, Paris, 2012, pp. 62, 63.

4) **Vincent FAUCHOUX, Pierre DEPREZ**, op.cit., pp. 33, 34.
Philippe BARBET et Isabelle LIOTARD, op.cit., pp. 133- 136.

5) **Nathalie DRYFUS**, op.cit., pp. 59, 60, 61.

ثانيا)– إجراءات السّياسة الموّحدة(Procédures(UDRP)).

حدّدت السّياسة الموّحدة(UDRP) النّزاعات التي تخضع للإجراء الإداري الإلزامي، الذي يسمح لأطراف النّزاع إتّباع إجراءات السّياسة الموّحدة(Procédures(UDRP)) التّالية:

1)– شروط اللّجوء إلى إجراء السّياسة الموحّدة(Procédure(UDRP)): يجب على أطراف النّزاع(Requérant-Défendeur) الإمتثال لمبادئ السّياسة الموّحدة (Principes(UDRP)) ولائحة إجراءاتها(Règles(UDRP))، التي تبنّتها هيئة(ICANN)، وكذا القواعد الإضافيّة لمركز تسوية النّزاعات المُعتمد التي يجب أن لا تتعارض Règles) supplémentaires) مع مبادئ وقواعد السّياسة الموّحدة، حيث حدّدت المادة(04) فقرة(a) من "السّياسة"[1] النّزاعات التي تخضع للإجراء الإداري الإلزامي Procédure) administrative obligatoire) لدى أيّ مركز تسوية مُعتمَد، الذي من خلاله يجب على المُدَّعِي(Requérant) أن يُثبت وفقا لقواعد السّياسة[2]، إحدى الحالات التّالية:

---

[1] **U**niform **D**omain name **D**ispute **R**esolution **P**olic**y (UDRP).**
https://www.icann.org/resources/pages/policy-2012-02-25-fr
« **Politique** » désigne : la politique uniforme de règlement de litiges relatifs aux noms de domaine(**UDRP**) qui est **annexée** et **intégrée** au **contrat d'enregistrement.**
Remarques : […], Ces principes directeurs constituent une **convention** entre le **registraire** (ou tout autre organisme d'enregistrement dans le cas d'un domaine national de premier niveau) et **son client** (le titulaire ou le registrant du nom de domaine). C'est pourquoi les principes édictés utilisent « **nous** », « **notre** » et « **nos** » pour se **référer** au **registraire** et « **vous** », « **votre** » et « **vos** » pour se **référer** au **titulaire du nom de domaine**.

[2] UDRP et « Règles » : https://www.icann.org/resources/pages/udrp-rules-2015-03-12-fr
Art. 4 (Principes UDRP) : « Procédure administrative obligatoir. Ce paragraphe stipule les litiges pour lesquels vous devez vous soumettre à une procédure administrative obligatoire. Ces procédures seront conduites par-devant l'un des prestataires de services de règlement de litiges administratifs répertoriés sur: http://www.icann.org/en/dndr/udrp/approved-providers.htm (chacun, un « prestataire »).
a)- Litiges concernés. Vous devez vous soumettre à une procédure administrative obligatoire dans le cas où un tiers (un « **plaignant** ») fait valoir au prestataire applicable, en **conformité avec les règles de procédure**, **(i)** que **votre** nom de domaine est identique à, ou d'une similitude prouvant prêtée à confusion avec une marque commerciale ou une marque de service dans laquelle le plaignant a des droits ; et **(ii)** que **vous** n'avez aucun droit ou intérêt légitime au regard du nom de domaine ; et **(iii)** que **votre** nom de domaine a été enregistré et est utilisé de mauvaise foi. Au cours de la procédure administrative, le plaignant doit prouver la véracité de chacune de ces assertions. »

– أنّه يَمْلِكُ علامة تجاريّة أو خدمة مُطابقة أو متشابهة بشكل يؤدّي إلى اللّبس مع اسم الموقِع المُسجَّل؛ أو

– أنّه ليس لدى مُسّجِل(Défendeur) اسم الموقِع المتنازع عليه أيّ حق أو مصلحة مشروعة على اسم الموقِع المُسجَّل؛ أو

– أنّ المُسّجِل لاسم الموقِع قام بتسجيل واستغلال موقعه بسوء نيّة وبطريقة تعسّفيّة.

2)– إيداع الدعوى: يجب أن تنحصر طلبات المدّعي أمام الهيئة(Panel) التي ستفصل في النّزاع، حول تحويل اسم الموقِع المُسجَّل إليهِ أو طلب إلغاءه[1]، وأن يختار إحدى مراكز التّسوية المعتمدة من طرف هيئة آيكان، وفي حال تعدّد النّزاعات يُمكن لأحد أطراف النّزاع أن يطلب لدى الهيئة(Panel) الأولى التي تّم تعيينها للبّت في النّزاع بدمج النّزاعات أمام هيئة واحِدة[2]، كما يجب على المُدّعِي دفع مصاريف الإجراءات الأوّلية لمركز تسوية النّزاع خلال العشرة(10) أيّام الموالية لتاريخ استلام المركز للدّعوى، على أن يقوم المركز عند الإقتضاء في حال تعيين الهيئة بردّ جُزء من المصاريف للمُدَّعِي وفقا للقواعد الإضافيّة له، وفي حال عدم تلّقي مركز التّسوية للمصاريف يقوم بسحب الدّعوى وإنهاء الإجراءات[3].

---

1) **Art.04-(i) (Principes (UDRP)) :** « Voies de droit. Les voies de droit à la disposition d'un plaignant à la suite d'une procédure par-devant une commission administrative sont **limitées** à exiger l'**annulation** de votre nom de domaine ou le **transfert** de l'enregistrement de votre nom de domaine au plaignant. »

2) **Art.04/d-f (Principes (UDRP))** : « Choix du prestataire. **(d)-** Le plaignant doit sélectionner le prestataire parmi ceux agréés par l'ICANN en déposant la plainte auprès du prestataire. Le prestataire choisi aura la charge d'administrer la procédure, sauf dans les cas de regroupement tels que décrits au paragraphe 4(f). **(f)- Regroupement.** En cas de litiges multiples entre vous et un plaignant, l'un de vous peut demander de regrouper les litiges par-devant une seule commission administrative. Cette requête doit être soumise à la **première** commission administrative désignée pour instruire un litige en cours entre les parties. La commission administrative peut regrouper une partie ou l'ensemble des litiges sur lesquels elle a à statuer, à son entière discrétion, sous réserve que les litiges regroupés sont régis par ces principes directeurs ou une version ultérieure de ceux-ci adoptée par l'ICANN. »

3) **Art.19 (Règles (UDRP))** : « **(a)-** Le plaignant devra payer au fournisseur les frais initiaux fixés conformément aux règles supplémentaires du fournisseur, dans le délai et le montant requis. Un défendeur qui choisit, conformément au paragraphe **5(b)(iv)**, que le litige soit arbitré par un panel de trois membres plutôt que par un panel d'un seul membre choisi par le plaignant, il devra payer au fournisseur la moitié des frais fixés pour un panel de trois

وعليه، يجوز لأيّ شخص أو ممثّله المُخوّل إيداع دعوى بطريقة إلكترونيّة وفقا للسّياسة وقواعدها، لأيّ مركز تسوية مُعتمد من قبل هيئة(ICANN)، تتضمّن على البيانات الواردة بموجب المادة 03-(b) من قواعد السّياسة((Règles(UDRP)، مع إرفاقها بنسخ المُستندات المُثبِتة لذلك، كالبيانات الشّخصيّة للمُدّعِي والمُدّعَى عليهِ أو بيانات المُمثّل المُخوَّل لمباشرة إجراءات التّسوية وتحديد طريقة الاتصال بالمُدّعَى عليهِ، مع إبراز مَوْقِفِهِ بشأن أعضاء الهيئة(خَبير أو (03) خُبراء) التي تفصل في النّزاع، وكذا تحديد المُسّجِل واسم أو أسماء المواقع المتنازع عليها وأصحابها، وتقديم عرض مُفصَّل لوقائع القضية مع تحديد طلباته وإرفاقها بأيّ وثيقة تبرّر ذلك(نسخة من السيّاسة أو العلامة...)، مع توضيح أيّ إجراءات قانونيّة قد تّم البدء فيها أو إنهائها ذات صلة باسم الموقِع، وفي الأخير يجب على المُدّعِي أو مُمَثِّلُهُ المُخوَّل أن يُوقِّع إلكترونيا على الدّعوى بعد اختتامها بالبيان الختامي المحدّد بموجب الفقرة الفرعيّة(13) من نفس المادة (03-(b))[1].

لذا حدّدت المادة(b/04) من السّياسة الموّحدة(UDRP) على سبيل المثال الحالات التي يمكن للمُدّعِي إثبات سوء نيّة المُسّجِل(Défendeur) لاسم الموقِع، كقيام هذا الأخير بتسجيل اسم موقِع لغرض البيع والإيجار لمالك العلامة(التّجاريّة أو الخدمة)، أو لأحد منافسيه(المُدّعي) مُقابل قيمة ماليّة مُرتفعة تتجاوز تكاليف التّسجيل Débours) (documentés، أو قيام المُدّعَى عليهِ(Défendeur) بتسجيل اسم الموقِع لغرض مَنْعِ مالك العلامة من تسجيلها كاسم موقِع، أو قيامه بتسجيل اسم الموقِع لهدف تعطيل عمل أحد

---

membres. Voir paragraphe 5(c). Dans tous les autres cas, le plaignant devra supporter tous les frais du fournisseur, **sauf** les cas de figure prescrits au **paragraphe 19(d)**. Après la **nomination** du panel, le fournisseur devra, s'il y a lieu, **rembourser** au plaignant la part correspondante des frais initiaux tel que cela est établi dans les règles supplémentaires du fournisseur. **(b)**- Le fournisseur devra s'abstenir de toute action concernant une plainte tant qu'il n'aura pas reçu de la part du plaignant les frais initiaux conformément à ce établi dans le paragraphe **19(a)**.

(c)- **Si** le fournisseur n'avait pas reçu les frais dans les **dix (10)** jours civils suite à la réception de la plainte, celle-ci devra être réputée retirée et la procédure administrative sera close. […].»

[1] Voir l'**Art.03/(B)-(xii) et (ix), (Règles (UDRP)).**

المنافسين، أو استخدام اسم الموقِع المُسجَّل لِجَذْبِ الزّبائن وجعلهم يعتقدون بأنّ هناك علاقة تربط المُسّجِل لاسم الموقِع مع مالك العلامة التّجارية أو الخدمة[1].

3)– فحص وتبليغ الدّعوى من قِبلِ مركز التّسوية: بعد تلقي مركز التّسوية للدّعوى يطلب من مكتب التّسجيل إجراء تحقيق لغرض وضع القفل على اسم الموقِع(Verrouillage)، الذي يقوم في خلال يومين(02) من تاريخ استلام الطلب بتقديم كل المعلومات المتعلّقة بالمُدّعَى عليهِ مع تأكيد تطبيق إجراء القفل، كما يقوم المركز بمُراجعة الدّعوى من أجل الإمتثال للإجراء الإداري وفقا للسّياسة وقواعدها، فإذا كان الأمر بذلك يُرسِل بطريقة إلكترونيّة الدّعوى بمُلحقاتِها إلى المُدّعَى عليهِ ومكتب التّسجيل[2]، على أن يتّم التّبليغ في ظرف ثلاثة(03) أيّام التّالية لتاريخ استلام مصاريف الإجراءات التي دفعها المُدّعِي، فإذا رأى المركز أيّ نقائص يُخطِر أطراف النّزاع على الفور بذلك، وفي حال تصحيحها يقوم المركز على الفور بإخطار أطراف النّزاع ومكتب التسجيل وهيئة(ICANN) بتاريخ بداية إجراءات التسوية[3].

4)– مذكرة ردّ المُدّعَى عَليهِ(Défendeur): يجب على المُدّعَى عليهِ أن يُقَدِّمَ ردًّا بطريقة إلكترونيّة إلى المركز في مدّة عشرين(20) يوم مع إمكانية طلب تمديدها بأربعة(04) أيام تسري من تاريخ بدء الإجراءات الإداريّة، حيث يجب أن يتضمّن الرّد على جميع البيانات الواردة في المادة 05–(c) من قواعد السّياسة((Règles(UDRP)، وأن يَنْصَّبَ فقط على طلبات الدّعوى مع إثبات غير ذلك بأيّة وثيقة، مع تحديد بياناته الشّخصيّة أو مُمثّله وأيّ إجراءات قانونيّة تَّم البدء فيها بشأن اسم الموقِع، وكذا إبراز مَوْقِفِهِ بشأن أعضاء الهيئة(Panel) التي سَتَفْصِلُ في النّزاع، حيث يجب على المُدّعىَ عَليهِ التّوقيع إلكترونيا على مذّكرة الرّد مع اختتامها بالبيان الوارد في الفقرة الفرعيّة(c/8) من نفس المادة(05)[4]، ويجوز للهيئة(Panel) البَّت في النّزاع بناء على ما وُرد في الدّعوى في حالة عدم الرَّدِ عَنْهَا.

---

1) Voir l'**Art. 04- b (Principes (UDRP)).**
2) Voir l'**Art. 02-a (Règles (UDRP)).**
3) Voir **l'Art.04/a-b-c-d-e-f-g(Règles (UDRP))**.
4) Voir l'**Art.05/c(viii), (Règles (UDRP))**.

وعليه، يمكن للمُدّعَى عليهِ(Défendeur) دَحْضِ إدّعاءات المُدّعِي بالاستناد إلى إحدى الحالات المحدّدة بموجب المادة(c/04) من السّياسة(UDRP)[1]، كاستخدام اسم الموقِع بنيّة حسنة لبيع السلع أو الخدمات، أو أنّه(Défendeur) معروفا عموما باسم الموقِع الذي سجّله حتّى ولو لم تَكُنْ لديه علامة(تجاريّة أو خدمة)، أو أنّه يستخدم اسم المَوقِع بطريقة قانونيّة غير تجاريّة ولا ينوي من خلال استخدامه تحقيق مكاسب تجارية لتضليل المُستهلكين، أو الإساءة لسمعة مالك العلامة التّجاريّة أو الخدمة.

5)– تسوية النّزاع بالتّراضي: يمكن لأطراف النّزاع الاتفاق بينهم حول تسوية النّزاع بالتّراضي سواء قَبْلَ مُباشرةِ إجراءات التّسوية أمام الهيئة، أو أثناء وقَبْلَ صدور قرار الهيئة(Panel) بشأن النّزاع، حيث يجب عليهم تقديم طلب خطي أمام مركز التّسوية وفقا لأحكام المادة(17/(a)) من قواعد السّياسة المُوّحدة، لتعليق الإجراءات الإداريّة ومُباشرَةِ إجراء تسوية النّزاع بالتّراضي، حيث يقوم المركز بِمُجَرَّدِ اِستلامهِ للطلب إخطار الأطراف ومكتب التّسجيل بطلب التّعليق ومدّتهِ المُتوقَّعة، وفي حال توصّل الأطراف إلى حلٍّ بشأن النّزاع يجب عليهم تسليم المركز لنموذج عن اتّفاق التّسوية(Formulaire d'accord)، ومُلخّص(Formulaire d'accord standard) عن شروط ذلك الاتّفاق إلى جانب القواعد التّكميليّة لمركز التّسوية، على أن يلتزم هذا الأخير بمنح نسخ من اتّفاق التّسوية لأطراف النّزاع مع إخطار مكتب التّسجيل بتنفيذ بنود الاتّفاق، الذي يقوم في خلال يومين(02) من استلامه الإخطار بإزالة قفل اسم الموقِع(Déverrouillé)، حيث يجب على المُدَّعِي أن يُؤَكِدَ لمركز التّسوية بأنّ الاتّفاق بشأن اسم المَوقِع تمّ تَنفيذهِ وفقا للإجراءات الإضافيّة له[2].

6)– كيفية تعيين أعضاء الهيئة الإداريّة(Membres du panel): يجب على كلّ مركز مُعتمد لتسوية نزاعات أسماء مواقع الإنترنت، أن يَقُومَ بتحديث ونشر قائمة من الخبراء مع مؤهّلاتهم عبر موقعه الإلكتروني، الذين يختارهم حسب شُهرَتهم وحِيادِ أو استقلاليّة كلّ

---

1) Voir l'**Art. 04/c** (**Principes (UDRP)**).

2) Voir **l'Art. 17(a) (Règles(UDRP))**: **Accord ou autres motifs de résiliation.**

عضو(Impartial et Indépendant) وكذا الخبرة المُكتسبة لكلّ واحد منهم، وبالتّالي فإنّ إجراءات تعيين الخبراء تتّم عبر الخطوات التّالية:

– إذا لم يختار كلّ من أطراف النّزاع هيئة من ثلاثة خبراء يقوم مركز التّسوية، خلال خمسة(05) أيّام التّالية لتاريخ استلام الرّد أو انقضاء مدّة تقديمه، تحديد خبير(01) في قائمة الخبراء المنشورة عبر منصّته الإلكترونيّة، حيث يتحمّل المُدّعِي تكاليف الإجراءات[1].

– إذا أراد أطراف النّزاع الفصل فيه من خلال هيئة تتكوّن من ثلاثة خبراء، يقوم المركز في خلال خمسة(05) أيام بتعيينها وفقا لإجراءات المادة 06/(e) من قواعد السّياسة (Règles(UDRP))، التي من خلالها يقوم الأطراف باختيار الخبراء الثلاثة ضمن قائمة خمسة(05) الخبراء المقترحة من طرف المركز، فإذا لم يختاروا الخبير الثالث يقوم المركز بتعيينه حيث يترّأس الهيئة، وفي حال عدم تلّقي المركز لأيّ رّد من قِبَلِ أطراف النّزاع، يقوم بتعيِين خبير ضمن القائمة المُقترَحَة من طَرَفِ المُدّعِي والمُدّعَى عليهِ، وخبيران ضِمْنَ قائمة الخُبرَاء المُقترحة من طرَفِهِ(المركز)، وبالتّالي فإنّ مصاريف الإجراءات تكون على عاتق المُدّعِي في حال ما إذا طلب تعيين هيئة من ثلاثة خبراء، أمّا إذا طلب المُدّعَى عليهِ هيئة من ثلاثة خبراء فيتّم تَقَاسُمِ المصاريف أمام الهيئة بالتّساوي بين أطراف النّزاع[2].

---

[1] **Art.06/a-b(Règles(UDRP)): Nomination du panel et délais de la décision.**
« **(a)** Chaque fournisseur mettra à jour et publiera une liste des membres du panel et de leurs qualifications. **(b)** Si ni le plaignant ni le défendeur n'ont opté pour un panel de trois membres (**paragraphes 3(b)(iv) et 5(b)(iv)**), le fournisseur devra nommer un seul membre du panel issu de sa liste dans les cinq (5) jours civils suivant la réception de la réponse par le fournisseur ou l'expiration du délai pour la présentation de la réponse. Les **frais** pour un panel d'un seul membre devront être entièrement réglés par le **plaignant**.»

[2] **Art.06/(c-d-e) (Règles (UDRP)): Nomination du panel et délais de la décision.** « **(c)** Si le plaignant ou le défendeur souhaitent que le litige soit arbitré par un panel de trois membres, le fournisseur devra nommer trois membres conformément aux procédures identifiées dans le paragraphe 6(e). Les frais correspondants à un panel de trois membres seront réglés intégralement par le plaignant, sauf si c'est le défendeur qui a opté pour un panel de trois membres, auquel cas les frais applicables seront partagés à parts égales entre les deux parties.
(d) Sauf s'il a déjà choisi un panel de trois membres, le plaignant devra, dans les cinq (5) jours ouvrables suivant la communication de la réponse dans laquelle le défendeur choisit un panel de trois membres, présenter au fournisseur les noms et les coordonnées des trois candidats

فحسب الخبيرة في مسائل تسوية نزاعات أسماء المواقِع(Nathalie DREYFUS)، فإنّ أغلبية القرارات تُصدَر من طرف خبير واحد يُشرف على الهيئة(Panel)، أمّا القرارات الصادرة من طرف هيئة تضّم ثلاثة خبراء تتصّب حول الحالات التي يكون فيها موضوع النّزاع معقّد أو أنّ حيثياته تستدعي الاستعانة برأي أكثر من خبير واحد للفصل فيه[1].

7)– فصل الهيئة الإداريّة(Panel) في موضوع النّزاع: بِمُجرّد تَعيِّين الهيئة(Panel) يقوم مركز التّسوية إحالة ملف النّزاع إليها في أقرب وقت مُمكِن، حيث يجب عليها(Panel) البّت في النّزاع خلال أربعة عشرة(14) يوم التّالية لتاريخ تعيِينها، وفقا للبيانات والوثائق المُقدّمة لها أو التي تَطْلُبُهَا من الأطراف والاستناد إلى أيّة مبادئ قانونيّة تراها قابلة للتّطبيق، أو إلى أحكام القانون الوطني لأطراف النّزاع ذوي نفس الجنسيّة أو الإقامة[2]، وكذا يُمكن للهيئة أن تُقرر عند الإقتضاء عقد جلسات الاستماع الفرديّة عبر الإنترنت لأطراف النّزاع (Téléconférences, Conférences Web, Vidéoconférences.)، أين يتعيّن عليهم دفع الرّسوم الإضافيّة للمركز[3]، حيث تقوم الهيئة إصدار قرار التّسوية(Décision(UDRP)).

---

proposés comme membres du panel. Ces candidats pourraient être tirés au sort dans la liste de membres du panel du fournisseur approuvée par l'ICANN.

(e) Au cas où ni le plaignant ni le défendeur ne choisiraient un panel de trois membres, le fournisseur s'efforcera de nommer un membre du panel parmi la liste de candidats fournie par le plaignant et le défendeur. Au cas où, dans le délai de cinq(5) jours civils, le fournisseur serait incapable de nommer un membre du panel issu de la liste de candidats des parties, le fournisseur devra faire son choix parmi les candidats de sa propre liste. Le troisième membre du panel sera nommé par le fournisseur à partir d'une liste de cinq candidats qu'il présentera aux parties, la sélection entre les cinq candidats étant effectuée par le fournisseur de façon à équilibrer raisonnablement les préférences des deux parties qui peuvent les signaler au fournisseur dans les cinq(5) jours civils après la présentation de la liste. »

1) **Nathalie DREYFUS**, op.cit., pp. 167, 168.

2) Ibid., pp. 169, 170.

3) **Art. 13(Règles d'application(UDRP))** : « **Audiences en personne.** Il n'y aura aucune **audience en personne** (y compris des téléconférences, vidéoconférences et conférences Web) à moins que le **panel** ne décide, à sa seule discrétion et à titre exceptionnel, qu'une telle audience est nécessaire pour prendre une décision à propos de la plainte. »

Art. 19/d(Règles d'application(UDRP)) : « **Frais.** […], (**d**)- Dans des circonstances exceptionnelles, par exemple lorsqu'il y a une **audience en personne**, le fournisseur devra exiger aux parties le **règlement des frais supplémentaires** qui seront déterminés en accord avec les parties et le panel. »

يجب أن يكون قرار التّسوية مكتوب ومُسبّب يحتوي على تاريخ الإصدار مع اسم الخبير أو أسماء الخبراء الثلاثة للهيئة أين يُتّخذ القرار فيها بالأغلبية، وفي حال وجود رأي مُخالف لأحد الخبراء أثناء البّت في النّزاع، يجب على الهيئة الإشارة إلى رأيه على هامش القرار من دون أيّ تأثير على مَنْطُوقِ قرار التّسوية، الذي يُمكِن أن يَصْدُرَ لمصلحة المُدّعِي صاحب العلامة مَرْفُوقاً بأمر تحويل اسم الموقِع إليه، أو بأمر إلغاءه، كما يُمكِن أن يَصْدُرَ ذلك القرار لمصلحة المُدّعَى عَلَيْهِ صاحب الحق أو المصلحة المشروعة في اسم المَوقِع، أو أنّ النّزاع لا يُراعِي شروط اللّجوء إلى الإجراء الإداري الإلزامي(Procédure(UDRP))، أو أنّ الدّعوى تم إيداعها "بسوء نيّة" من خلال الاستخدام التّعسّفي للإجراء الإداري، بُغْيَة سرقة اسم الموقِع(Reverse Domain Nam Hijacking)، أو إهانة مُسجِّل اسم الموقِع (Défendeur)[1].

8)– تنفيذ قرار التّسوية(Décision(UDRP)): يجب على الهيئة(Panel) التي فصلت في النّزاع أن تُرسِلَ قرار التّسوية إلى المركز الذي يُبَلِّغُهُ بدوره في خلال ثلاثة(03) أيّام التّالية لتاريخ الاستلام، إلى أطراف النّزاع ومكاتب التّسجيل وهيئة الآيكان، حيث يقوم كلّ مكتب تسجيل وفقا "للسّياسة"، بتبليغ تاريخ تنفيذ القرار إلى هؤلاء في مدّة ثلاثة(03) أيّام المواليّة

---

[1] **Art. 15**(**Règles d'application(UDRP)**) : « **Décision du panel**. **(a)**- Un panel devra décider d'une plainte en se basant sur les déclarations et les documents présentés et conformément à la politique, à ces règles et à toute règle et principe juridique réputés applicables. **(b)**- En l'absence de circonstances exceptionnelles, le panel devra transmettre sa décision sur une plainte au fournisseur dans les quatorze (14) jours suivant sa nomination conformément au paragraphe 6. **(c)**- Dans le cas d'un panel de trois membres, la décision du panel sera prise à la majorité. **(d)**- Le panel devra présenter sa décision par **écrit**, exposer les **éléments** qui l'ont **motivée**, indiquer la **date** à laquelle elle a été prise et mentionner le **nom** du ou des **membres** du **panel**. **(e)**- Les décisions du panel et toute opinion divergente devront normalement respecter les lignes directrices quant à la longueur énoncées dans les règles supplémentaires du fournisseur. Toute opinion divergente devra accompagner la décision de la majorité. Si le panel estimait que le litige ne rentre pas dans la portée du paragraphe 4(a) de la politique, il devra l'indiquer ainsi. Si après avoir examiné les soumissions le panel estimait que la **plainte** a été déposée de **mauvaise foi**, par exemple pour l'utilisation frauduleuse du nom de domaine ou pour harceler le titulaire du nom de domaine, le **panel** devra **déclarer** dans sa décision que la plainte a été déposée de mauvaise foi et qu'elle constitue un **abus** de la procédure administrative. »

لتاريخ استلامه للقرار، حيث يمكن للمركز عند الإقتضاء نشر القرار كامِلاً مع تاريخ تنفيذه عبر منصّته الإلكترونية، في حين يتمتّع قرار التّسوية بحجيّة الشّيء المقضي فيه مع سهولة تنفيذه في أيّ بلد، وذلك بالمقارنة مع ما تتطلّبه إجراءات تنفيذ أحكام التّحكيم أو الأحكام الأجنبيّة فيما بين الدّول، حيث يتّم تنفيذ القرار مُباشرةً من طرف مكتب التّسجيل، وبالتّالي تفادي مسألة تنفيذ الأحكام الأجنبيّة(L'exequatur des titres étrangers) وما تتطلّبه من إجراءات الحصول على الصيغة التّنفيذيّة(La grosse) في البلد المعني[1].

وعليه، فإنّ مكتب تسجيل اسم الموقِع لا يَجْرُأُ على تنفيذ القرار إلاّ بعد مرور العشرة(10) أيّام الموالية لتاريخ تبليغه للقرار من قبَلِ المركز، فمن خلال هذه المدّة يستطيع الطرف الصادر ضِدَّهُ القرار، إرسال أيّ وثيقة تُثبِت لمكتب التّسجيل رفع الدّعوى أمام القضاء ضد الطرف الذي صُدِرَ لِمَصْلَحَتِهِ القرار، حيث يَتوقَّف المكتب عن تنفيذ ذلك القرار ويَمتنِع عن اتّخاذ أيّ إجراء أخر، حَتَّى يَسْتَلِمَ مَا يُثبِتُ سواء وجود حلّ بين الطرفين أو أنّه قد تّم التّنازل عن الدّعوى القضائيّة وسحبها، أو عدم الاستمرار في استخدام اسم الموقِع المتنازع عليه.

---

[1] **Art. 16 (Règles d'application(UDRP)) : « Communication de la décision des parties.**
(a)- Dans les trois (3) jours civils après réception de la décision du panel, le fournisseur devra communiquer le texte complet de la décision à chaque partie, au(x) bureau(x) d'enregistrement concerné(s) et à l'ICANN. Dans les trois (3) jours ouvrables suite à la réception de la décision du fournisseur, le ou les bureaux d'enregistrement concernés doivent communiquer immédiatement à chaque partie, au fournisseur et à l'ICANN la date d'exécution de la décision conformément à la politique. **(b)-** Sauf décision contraire du panel (voir **paragraphe 4(j)** de la **politique**), le fournisseur devra publier la décision complète et sa date d'exécution sur un site web accessible au public. Dans tous les cas, la partie de la décision déterminant qu'une plainte a été déposée de mauvaise foi (voir paragraphe 15(e) de ces règles) devra être publiée. »
Voir aussi : **Nathalie DRYEFUS**, op.cit., pp. 192, 231.

الفرع الثاني
آليات تسوية نزاعات أسماء مواقع الإنترنت

يعتبر مبدأ الأسبقيّة في تسجيل أسماء مواقع الإنترنت كعامل مُحفّز للقراصنة لتبرير عمليات السّطو الإلكتروني(Cybersquatting)، وتسجيل وإعادة بيع اسم الموقِع للمالك الشّرعي له أو لأحد منافسيه، الخ...، حيث تثير هذه الأفعال نزاعات مع عناصر الملكيّة الفكرية(العلامات، الأسماء التّجاريّة، الخ...)، التي تدفع بالمُتضّرر الاستعانة بإجراءات السّياسة الموّحدة((Procédures(UDRP)**(أوّلاً)**، أو يتّم اللّجوء إلى الجهات المسؤولة عن تسجيل أسماء المواقِع**(ثانياً)**، أو إلى المحاكم الوطنيّة المختصّة**(ثالثاً)**.

أوّلا– اللّجوء إلى الجهات المعتمدة لتسوية نزاعات أسماء المواقع وفقا لإجراءات السّياسة المُوّحد((Procédures(UDRP).

يُمكِن لأطراف النّزاع بشأن اسم موقِع الإنترنت اللّجوء إلى إحدى مراكز التّسوية المعتمدة من طرف هيئة الآيكان للفصل في النّزاع وفقا لإجراءات السّياسة الموّحدة((Procédures(UDRP)، فمن بين هذه المراكز [1] نجد:

أ)– مركز الويبو للتّحكيم والوساطة WIPO Arbitration and Mediation Center) (WAMC: يعتبر مركز الويبو للتّحكيم والوساطة كأوّل مركز لتسوية نزاعات أسماء المواقِع الذي إعتمدته هيئة(ICANN) في 19 نوفمبر 1999، حيث أنشأ هذا المركز (WAMC) في عام 1994 من طرف منظّمة الويبو (OMPI)، لتسوية نزاعات التّجارة الدّوليّة عبر الآليات التّسوية البديلة((Alternative Dispute Resolution(ADR)، كالوساطة(Médiation) أو التّحكيم(Arbitrage)، والتّحكيم السّريع(Arbitrage accéléré) أو الخبرة(Expertise)، فمعظم قضايا التّحكيم والوساطة للمركز تتعلّق بالملكيّة الفكريّة[2].

---

[1] أنظر الموقع التالي: https://www.icann.org/resources/pages/providers-2012-02-25-fr

[2] **Patrick THIEFFRY**, Commerce électronique: droit international et européen, édition litec, Paris, 2002, p. 225. **Nathalie DRYFUS,** op.cit., p. 112.

وعليه، يُمْكِنُ لأطراف النّزاع أن يَقَعَ اختيارهم على إحدى الإجراءات البديلة لتسوية النّزاعات باعتباره خيارا قائما بذاته لتسوية المنازعات، أو تستند على جميع هذه الإجراءات للفصل الأفضل للقضيّة، فإجراء الوساطة يعتمد فيه الأطراف على وسيط مُحايِد للتَّوَصُلِ إلى حلّ مُنَاسِبٍ لأطراف النّزاع الذين يتمتّعون بِكَامِلِ الحرّية في قُبُولِهِ أو من عَدَمِهِ، أمّا إذا اتفق الأطراف حول عرض النّزاع إلى مُحكِم واحد أو أكثر للنّظر فيه، فإنّ قرار التّحكيم الذي يُصْدَرُ يكون نِهائياً ومُلزِماً ما لم يتّفق أطراف النّزاع على خلاف ذلك، حيث اعتمد مركز الويبو للتّحكيم والوساطة في أوّل مارس2010، منظومة إجراءات التّسوية الإلكترونيّة للنّزاعات التي من خلالها يتّم إرسال الطلبات والوثائق عبر الإنترنت[1]، إذْ يُعتبر قرار التّحكيم الصادر في 09 ديسمبر1999 الأوّل في إطار إجراءات السّياسة المُوّحدة(Procédures(UDRP))، حيث أشرف المركز منذ تلك الفترة على أكثر من27500 قضية، في حين يُتيح المركز عبر موقعه إحصائيات آنية للقضايا المُعالجة[2].

فمن بين النّزاعات التي عالجها مركز الويبو للتّحكيم والوساطة[3] (Centre d’arbitrage et de médiation de l’OMPI)، نجد قضية شركة(Christian Dior) التي صدر في حقّها قرار في 29 جانفي 2000، على أساس الحالة الأولى المحدّدة وفقا للمادة (i)a/04)) من السّياسة(UDRP)، الذي تقرّر من خلاله تحويل أسماء المواقع(diorcosmetics.com) و(diorfachions.com) المُماثِلة أو المشابهة للعلامات المملوكة لتلك الشّركة[4]، كما عالج ذلك المركز العديد من القضايا ذات صلة بالحالة الثانية من نفس المادة(ii)a/04)) المتعلّقة

---

1) Procédures/Décisions des litiges: http://www.wipo.int/amc/en/domains/search/index.html
Règles supplémentaires: http://www.wipo.int/amc/en/domains/rules/

2) أنظر الموقع الإلكتروني التالي: http://www.wipo.int/amc/en/domains/statistics (consulté le 27/02/2019.)

3) للتعرف أكثر حول قرارات مركز الويبو في إطار السياسة الموحدة أنظر الموقع الإلكتروني التالي: http://www.wipo.int/cgi-bin/domains/search/legalindex

4) Centre d’arbitrage et de médiation de l’OMPI, 29 janvier 2000, décision n° D 2000-0022, Dior. http://www.wipo.int/(consulté le 29/01/2016.)

بالمساس بحقوق أو مصالح مشروعة للغير من طرف مُسّجِل اسم الموقِع، سواء تعلق ذلك بالأسماء التّجاريّة، أو مؤلفات أدبيّة، أو بعلامة مشهورة[1] الخ...

ب)– مُجمَّع التّحكيم الوطني(National Arbitration Forum NAF): أُسْتُحْدِثَ هذا المُجمَّع في عام 1986 بالولايات المتّحدة الأمريكيّة كمحكمة تحكيم معتمدة من طرف هيئة الآيكان(ICANN) في 23 ديسمبر 1999، لتسوية نزاعات أسماء المواقِع العليا للدّولة الفيدرالية(.us) وفقا لإجراء التّسوية(USDRP-Dispute Resolution Policy)، التي تعتمد على تقنيّة الاتّصالات الإلكترونيّة[2].

ج)– المركز الآسيوي لِحَلِّ مُنازعات أسماء المواقع (Asian Domain Name Dispute Resolution Center (ADNDRC): اعتمدت هيئة الآيكان(ICANN) هذا المركز في 28 فيفري 2002 لتسوية نزاعات أسماء المواقع العليا العامّة(gTLDs)، وأسماء المواقع العليا الوطنيّة الأسيويّة وفقا لإجراءات السياسة الموّحدة((Procédures(UDRP)، حيث يتضمّن(ADNDRC) على أربعة مراكز للتّسوية كلجنة التّحكيم الصينيّة للإقتصاد العالمي والتّجارة(CIETAC)، ومركز التّحكيم الدولي لهونكونج(HKIAC)، واللّجنة الكوريّة للتّسوية الوديّة لنزاعات عناوين الإنترنت(KIDRC)، ومركز التّحكيم الجهوي لماليزيا(KLRCA)[3].

د)– مركز محكمة التّحكيم التشيكيّة لنزاعات الإنترنت (Czech Arbitration Court, Arbitration Center for Internet Disputes(CAC)): أُستحدث هذا المركز(CAC) في عام 1949 في هيئة جمعية ذات طابع غير ربحي مُلحقة بغرفتي الإقتصاد والزّراعة

---

1) Centre d'arbitrage et de médiation de l'OMPI, 1er mars 2000, décision n° D 2000-0008, Digitronic Inventioneering Corporation c/ Six Net Registred. http://www.wipo.int/ (consulté le 02/02/2016.)
Centre d'arbitrage et de médiation de l'OMPI, 23 juin 2000, décision n° D 2000-410, Religious Technology Center c/ Freie Zone. http://www.wipo.int/ (consultée le 03/02/2016.)
Centre d'arbitrage et de médiation de l'OMPI, 20 mai 2000, décision n° D 2000-0204, Penguin c/ Katz Family. http://www.wipo.int/ (consulté le 05/02/2016.)

2) Procédures/Décisions des litiges: http://domains.adrforum.com/decision.aspx
Règles supplémentaires:
http://domains.adrforum.com/users/icann/resources/UDRP%20Supplemental%20Rules%20eff%20March%201%202010.pdf

3) Procédures/Décisions des litiges: https://www.adndrc.org/hk/case_decision.php
Règles supplémentaires: https://www.adndrc.org/hk_supplemental_rules.html

للجمهوريّة التشيكيّة، وتحوّلت في جانفي2008 إلى مركز مُعتمد من طرف هيئة الآيكان لتسوية نزاعات أسماء المواقع(Procédures(UDRP))، حيث اعتمد المركز في 21 ماي 2009 على منظومة التّوقيع الإلكتروني الموثوق لغرض توثيق المستندات والرّسائل الخ...، وتسوية القضايا مباشرة عبر الإنترنت [1].

هـ)– معهد تسوية النّزاعات(Institute For Dispute Resolution(CPR)): أُنشأَ هذا المركز بالولايات المتّحدة الأمريكيّة في عام 1979 الذي إعتمدته هيئة الآيكان(ICANN) في 15 ماي 2000 كمركز لتسوية نزاعات أسماء المواقع وفقا لإجراءات السّياسة المُوّحدة، حيث يعتمد المركز على خبراء في مجال الملكيّة الفكريّة وقضاة ومحامين وممثّلين لمكاتب التّسجيل، بغية النظر في منازعات أسماء مواقع الإنترنت[2]، حيث توقّف هذا المركز (CPR) عن تقديم خدماته في جانفي2007 بعد تَعَرُّضِهِ للإفلاس(Faillite)[3].

ثانيا– اللّجوء إلى الجهات المسؤولة عن تسجيل أسماء المواقع الوطنيّة(Registres).

يُمكِن لأطراف نزاعات أسماء مواقِع الإنترنت اللّجوء إلى هيئات التّسجيل الوطنيّة(Registres) لتسوية النّزاع وفقا للقوانين المحليّة، التي قد لا تتّبع إجراءات السّياسة المُوّحدة(Procédures(UDRP)) المعتمدة من طرف هيئة آيكان(ICANN)، حيث سنتطرّق إلى بعض هذه الإجراءات على النَّحْوِ التّالي:

1)– إجراءات تسوية أسماء النطاقات وفقا لسياسة هيئة التّسجيل(AFNIC).

بعد صدور القانون رقم 2011–302 المؤرخ في 22 مارس 2011[4]، الذي يتضمّن الأحكام المختلفة لتكييف التّشريع مع قانون الاتّحاد الأوروبي في موضوع الصّحة والعمل والاتّصالات الإلكترونيّة، قامت هيئة التّسجيل(AFNIC) المسؤولة عن تسجيل أسماء المواقع

---

1) Procédures/Décisions des litiges: http://udrp.adr.eu/adr/decisions/index.php
Règles supplémentaires:http://udrp.adr.eu/arbitration_platform/udrp_supplemental_rules.php
2) Procédures /Décisions des litiges :
http://cpradr.org/FileaCase/CPRsNeutrals/DomainNameICANNDisputes.aspx
3) **Nathalie DRYFUS**, op.cit., p. 113.
4) **Loi n° 2011-302** du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques, JORF n° 0069 du 23/03/2011. **(**Chapitre III : Dispositions relatives aux communications électroniques).

العليا الوطنيّة والأقاليم التّابعة لفرنسا، بإحداث نظام داخلي لتسوية نزاعات أسماء المواقع العليا الوطنيّة، الذي دخل حيّز التّنفيذ في 22 مارس 2016 بعدما أن وافق عليه وزير الاقتصاد والصّناعة، حيث تضمّن النّظام على نوعين من الإجراءات، فالأولى تتعلّق بنظام تسوية النّزاعات(Syreli) بينما الثّانية تتعلّق بإجراءات التّسوية(PARL EXPERT).

أ)– **نظام تسوية النّزاعات(SYRELI):** أصبحت إجراءات نظام تسوية النّزاعات((SYstème de RÉsolution de LItiges(Syreli) منذ 06 ديسمبر 2011، تُطبّق على جميع أسماء المواقع العليا التي تُديرها هيئة التّسجيل(AFNIC)[1]، حيث يمكن لأيّ شخص يُثْبِتُ المساس بأحد حقوقه المحميّة وفقا للحالات التي أشارت إليها أحكام المادة(L45) مكرر02 من تقنين البريد والمواصلات الإلكترونيّة[2]، أن يطلب بطريقة

---

1) **Loïc ANDRÉ**, op.cit., pp. 66- 68.
Charte de Nommage de l'Association Française pour le Nommage Internet en Coopération(AFNIC).
https://www.afnic.frmediasdocumentsCadre_legalCharte_de_nommage_22032016_VF.pdf
Art. 01-1§3 : « La présente charte de nommage définit les conditions d'attribution et de gestion des noms de domaine dont la **centralisation** est assurée par l'**AFNIC** en sa qualité d'**Office d'enregistrement**, à savoir : (.fr) France métropolitaine et Corse, (.re) la Réunion, (.yt) Mayotte, (.pm) Saint-Pierre et Miquelon, (.wf) Wallis-et-Futuna, (.tf) Terres australes et antarctiques Françaises. **-§4** : Sauf décision contraire, la présente charte s'applique pour toute nouvelle extension dont la centralisation serait confiée à l'AFNIC. **-§5** : La présente charte de nommage ne s'applique pas aux noms de domaine de premier niveau autres que ceux prévus au présent article et **notamment** : Aux noms de domaine de premier niveau géographique (**ccTLD**) ; Aux noms de domaine de premier niveau générique (**gTLD**) ; Aux noms de domaine pour lesquels l'AFNIC pourra assurer un rôle de prestataire technique (back end registry). »

2) **Loi n° 2011-302** du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques. (Chapitre III- Dispositions relatives aux communications électroniques- Article.19)
Art. L. 45-2 (Code des postes et des communications électroniques): « Dans le respect des principes rappelés à l'article L. 45-1, l'enregistrement ou le renouvellement des noms de domaine peut être refusé ou le nom de domaine supprimé lorsque le nom de domaine est : **1-** Susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ; **2-** Susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi ; **3-** Identique ou apparenté à celui de la République française, d'une collectivité territoriale ou d'un groupement de collectivités territoriales ou d'une institution ou service

إلكترونيّة وفقا لنص المادة(L45) مكرر06 من نفس التّقنين، إلغاء أو تحويل اسم النّطاق المتنازع عليه لدى هيئة التّسجيل(AFNIC)، التي تقوم بتعيين مُقرِّر(Rapporteur) لفحص الطلب مع الوثائق المرفوقة به، مع إخطار المدّعي في خلال خمسة عشرة(15) يوم من تاريخ استلامه للطلب لغرض تصحيح النّقائص المتواجدة في الملف[1].

في حال إتمام وثاق الملف ودفع مصاريف الإجراءات يطلب المقرّر لدى مكتب التّسجيل إجراء تجميد اسم الموقِع[2]، وذلك بعد تبليغ كلّ من المُدّعِي(Requérant) ومكتب التّسجيل

---

public national ou local, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi. Le **décret en Conseil d'État** prévu à l'article L. 45-7 et les règles d'attribution de chaque office d'enregistrement définissent les éléments permettant d'établir un usage de **mauvaise foi** et l'absence d'**intérêt légitime**.[…].»

Art. L. 45-6(code des postes et des communications électroniques) : « Toute personne démontrant un intérêt à agir peut demander à l'office d'enregistrement compétent la suppression ou le transfert à son profit d'un nom de domaine lorsque le nom de domaine entre dans les **cas** prévus à l'article **L. 45-2**. L'office statue sur cette demande dans un délai de **deux mois** suivant sa réception, selon une procédure contradictoire fixée par son règlement intérieur qui peut prévoir l'intervention d'un tiers choisi dans des conditions transparentes, non discriminatoires et rendues publiques. Le règlement intérieur fixe notamment les règles déontologiques applicables aux tiers et garantit le caractère impartial et contradictoire de leur intervention. « Le règlement intérieur de l'office est approuvé par arrêté du ministre chargé des communications électroniques. Les décisions prises par l'office sont susceptibles de recours devant le juge judiciaire. »

1) **Art. II- v et vi (Règlement SYRELI (Partie I)).** Sur la **réponse du tutilaire** et **Décision**.

2) **Art. II- iii (Règlement SYRELI (Partie I)) : « Gel des opérations sur le nom de domaine**. Dès l'ouverture de la Procédure, le Rapporteur **gèle** les opérations sur le nom de domaine objet du litige, pour la durée de la Procédure ainsi que, le cas échéant, au-delà de la durée de la Procédure, conformément à l'article (**II**) (**viii**) du présent Règlement. Le Gel des opérations sur un nom de domaine s'effectue conformément aux termes de la **Charte de nommage.** »

Art. 06.2 (Carte de Nommage(AFNIC)) : « **Gel de nom de domaine**. Un nom de domaine fait l'objet d'une procédure de gel dans les cas suivants : **1-** une décision de justice ordonnant le gel du nom de domaine et répondant aux conditions prévues par l'article (Procédure judiciaire) ; **2-** À l'**ouverture** d'une Procédure Alternative de Résolution de Litiges **gérée** par l'**AFNIC** ; **3-** À l'ouverture d'une procédure de vérification telle que visée à l'article (Pouvoirs de l'Office d'enregistrement). Aucune demande de gel ne pourra être traitée en dehors des cas visés ci-dessus. Le gel d'un nom de domaine peut annuler l'ensemble des opérations en cours de traitement par l'AFNIC et les tickets correspondants et empêcher toute demande d'opération à venir sur le nom de domaine. »

والمُدّعَى عليهِ(Titulaire) بالبدء في إجراءات التّسوية وأنّ هيئة التّسجيل(AFNIC) ستفصِل في موضوع النّزاع في ظرف شهرين(02)، حيث يجب على المُدَّعَى عليه الرّد في خلال مُدّة(21) يوم على الطلبات أمام الهيئة(Collège)(تتكوّن من ثلاثة أعضاء مُعيّنين من قِبَلِ هيئة(AFNIC))، التي تفصل في النّزاع خلال مدّة(21) يوم التّالية لتاريخ نهاية مدّة الرّد، بقرار مكتوب مُسبّب ومؤرّخ يتضمّن إمّا تحويل اسم الموقع أو إلغاءه أو رفض الطلب[1].

وعليه، يقوم المُقرِّر بتبليغ منطوق القرار بطريقة إلكترونيّة أو عادية إلى أطراف النّزاع ومكتب التّسجيل، حيث لا يتّم تنفيذ القرار إلاّ بعد مرور مدّة خمسة عشرة(15) يوم التّالية لتاريخ التّبليغ، التي من خلالها يمكن للمدّعي أو المدّعَى عليهِ رفع دعوى أمام الجهة القضائيّة المختصّة مع إعلام هيئة(AFNIC) بما يثبت القيام بذلك، حيث تتوّقف هيئة التّسجيل(AFNIC) عن تنفيذ القرار وتَمْتَنِعُ عن اتّخاذ أيّ إجراء أخر، حتى تَسْتَلِمَ ما يُثبِت وجود حلّ بين الطرفين أو أنّه قد تّم التّنازل عن الدّعوى القضائيّة أو سحبها، أو عدم الجدوى في استمرار استخدام اسم الموقع المتنازع عليه، فإذا لم يقم الطرف الذي صُدِر لمصلحته القرار بتنفيذه خلال مدة ستين(60) يوم، يمكن لهيئة التّسجيل(AFNIC) أن تقوم بإلغاء اسم الموقع، أو تنفيذ القرار وفقا للحالات المُحدّدة بموجب المادة 06 مكرر5 من ميثاق التّسمية المتعلّقة بالتّحويل الإجباري(Transmission forcée) لاسم المَوقِع[2].

---

[1] **Art. II- v et vi (Règlement SYRELI (Partie I)).** Sur la **réponse du tutilaire** et **Décision**.

[2] **Art. II- vii, viii, ix (Règlement SYRELI (Partie I)).** Sur **la Notification de la décision** et **l'exécution, publication de la décision.**

Art. 06-5(Carte de Nommage(AFNIC)) : « **Transmission forcée.** L'AFNIC procède aux transmissions forcées de nom de domaine faisant suite : - À une décision de transmission prise dans le cadre d'une Procédure Alternative de Résolution de Litiges gérées par l'AFNIC ;
- À une décision de justice ordonnant la transmission forcée de nom de domaine et répondant aux conditions prévues par l'article « Procédure judiciaire » ; - À une opération de patrimoine (fusion, scission etc.) dès lors que le titulaire d'origine ne dispose plus de la capacité à procéder à une transmission volontaire ; - À une situation où le titulaire d'origine ne dispose plus de la capacité à procéder à une transmission volontaire et qu'un lien juridique ou commercial est démontré entre ce dernier et le nouveau titulaire. […]. »

ب)– الإجراءات البديلة لتسوية النّزاعات(PARL EXPERT): إنّ الإجراءات البديلة لتسوية النّزاعات(Procédures Alternatives de Résolution des Litiges(PARL))، كانت تتّم عبر مركز الويبو للتّحكيم والوساطة إلى أن تّم إيقاف العمل بها منذ 15 أفريل2011[1]، حيث كانت تلك الإجراءات قبل تلك الفترة تُطبّق على نزاعات أسماء المواقع مع العلامات والحقوق الأخرى المحميّة بموجب القوانين الفرنسيّة، وبالخصوص تلك المتعلّقة بحقوق الملكيّة الفكريّة والمنافسة غير المشروعة والأسماء أو الأسماء المستعارة(Pseudonyme) للأشخاص، وبالتّالي يمكن لأطراف النّزاع الاستعانة بإجراءات تسوية النّزاعات(PARL) أمام مركز الوساطة والتّحكيم لباريس (Centre de Médiation et d'Arbitrage de Paris(CMAP))، لتسوية نزاع اسم الموقِع مباشرة عبر الإنترنت عن طريق إجراء الوساطة أو المصالحة، الذي من خلاله يتّفق الأطراف حول وسيط(Tiers aviseur) مُحايِد ومُستقّل للفصل في القضيّة خلال مدّة ستة عشرة(16) يوم، التي من خلالها يُصدَر قرار حول دفع مبلغ مُعيَّن لإصلاح الضّرر أو بإلغاء أو تحويل اسم موقِع الإنترنت لصاحبه، حيث يمكن للأطراف اللّجوء إلى القضاء المختص[2].

2)– إجراءات تسوية نزاعات أسماء النّطاقات لدى هيئة التّسجيل(Nominet).

إنّ الإجراءات البديلة لتسوية نزاعات أسماء المواقع العليا الوطنيّة لإنجلترا تُديرها هيئة التّسجيل(Nominet)، حيث قامت منذ سبتمبر2001 بتعديل هذه الإجراءات من خلال إحداث نظام وساطة وتحكيم للنّزاعات(Dispute Resolution Service(DRS))، التي اختلفت مع إجراءات السّياسة الموّحدة في بعض الأمور، حيث أَنَّ هذه الأخيرة تُطبّق على نزاعات أسماء المواقِع مع العلامات وتشترط على المُدّعِي إثبات سوء نيّة المُدَّعَى عَليهِ، بينما إجراءات التّسوية(Nominet) يمكن تطبيقها على العلامات والحقوق الأخرى إذً تشترط فقط إثبات التّعسّف في تسجيل اسم الموقِع، حيث تتيح هذه الإجراءات(Nominet) تسوية معظم النّزاعات عن طريق إجراء الوساطة وذلك على خلاف إجراءات السّياسة الموّحدة، كما أنّ

1) **Nathalie DRYEFUS**, op.cit., pp. 174, 175.
2) Ibid. pp. 176, 177.

الخبراء لا يتم تعيِينُهم بنفس الطّريقة وأنّ الطّعن في القرار الصادر بالاستئناف مُمكِن في إجراءات(Nominet) على عكس إجراءات السّياسة الموّحدة[1].

وعليه، يُمكِن لأيّ شخص إيداع دعوى أمام هيئة التّسجيل(Nominet) عبر الإنترنت يثبت من خلالها أنّه(Requérant) صاحب حق على اسم الموقع أو علامة محميّة بموجب القانون الإنجليزي، حيث يمكن أن تتعلّق هذه الحقوق بعنوان مقّر اجتماعي أو علامة أو اسم تجاري أو اسم شخص، مع إقامة الدّليل بأنّ المدّعَى عليهِ(Défendeur) قام بتسجيل اسم المَوقِع تَعسُّفيا لغرض إيجاره أو إعادة بيعه للمُدّعِي بسعر مُرتفِع، أو أنّ اسم الموقِع المُسجَّل تَعسُّفيا يُثير خطر الخلط في ذهن الجمهور في حالة مُطابقته أو تشابهه مع اسم تجاري مُنافس له أو اسم شركة معروفة أو علامة تجاريّة أو خدمة، حيث تقوم الهيئة(Nominet) بعد تلّقي الدّعوى بفحصها من النّاحية الشّكليّة مع تبليغها في خلال ثلاثة(03) أيام إلى المُدَّعَى عَلَيْهِ، الذي يجب عليه الرّد على الطلبات في خلال خمسة عشرة(15) يوم من تاريخ استلامه للدّعوى، وفي حال الرّد يتّصل الوسيط هاتفيا بالأطراف لغرض تسوية النّزاع بالتّراضي حيث تتّم الوساطة عادةً في مدة أربعة عشرة(14) يوم.

فإذا لم يتّم التّوصّل إلى حلّ النّزاع عن طريق الوساطة يُمْكِنُ للمُدَّعِي أن يَطْلُبَ من الهيئة(Nominet) تعيين خبير مُحايد ومُستقّل لتسوية النّزاع، التي تقوم بذلك عبر إحدى الخطوات التّالية: – إمّا أن تقوم الهيئة(Nominet) بتعيين الخبير المُتواجِد في المرتبة الأولى في قائمة الخبراء التي نَشَرَتْهَا، على أن لا تكون لديه مصلحة في النّزاع(Conflit d'intérêt) حيث تقوم الهيئة بعد تعيينه(الخبير) بإعادة تصنيفه في المرتبة الأخيرة من نفس القائمة؛
– إذا عَايَنَت الهيئة(Nominet) لدى الخبير تواجد مصلحة في النّزاع فلا تقوم بتعيينه بل تُعيّن الخبير المُتواجَد في المرتبة الثّانية له من القائمة الذي لا تكون لديه مصلحة في النّزاع،

1) **Nathalie DRYEFUS**, op.cit., p. 182.

في حين يَحْتَفِظُ الخبير غير المُعيَّن(Expert écarté) بمرتبته الأولى في القائمة ويتّم الاتّصال به أوّلاً في النّزاع المطروح مُستقبلاً لدى هيئة التّسجيل(Nominet)[1].

وفي حالة عدم رد المُدَّعَى عليه على الدّعوى، يمكن للمُدَّعِي أن يطلب من الخبير إصدار قرار ولو لم يكن مُسبّب مقابل دفع قيمة بسيطة من مصاريف الإجراءات، أين يتّم النّص في مَتْنِهِ تحويل اسم المَوقِع إلى المُدّعِي، فإذا قام المُدّعَى عَليهِ بالرّد على الطلبات يجب على المُدَّعِي دفع جميع مصاريف الإجراءات للخبير، الذي يقوم في خلال العشرة(10) أيام الموالية لتاريخ تَعْيِينِهِ، بالفصل في موضوع النّزاع وفقا للحجج وأدّلة الإثبات المُقدّمة سَلَفاً من الأطراف من دون تقبّل أيّ مُستندات جديدة، حيث لا يُصْدِرُ الخبير قراره بشأن النّزاع إلاّ إذا تّم إعادة النّظر فيه وقِراءته من طرف أحد فريق الخبراء (Expert Review Group) الذي يقوم سواء بتعديل القرار أو نشره على حالته، حيث يُشْرِفُ كذلك هؤلاء الخبراء على مُهمّة اختيار أعضاء هيئة الإستئناف(Panel d'appel)، وفي حالة استئناف القرار من طرف المُستأنِف(Appelant) في خلال العشرة(10) أيام التّالية لتاريخ إصداره، يجب على هيئة الإستئناف المُكوَّنة من ثلاثة خبراء البّت في القضيّة خلال ثلاثين(30) يوم، بموجب قرار يتم نَشْرُهُ مع القرار الأوّل المُسْتَأْنَفِ عبر المنصّة الإلكترونيّة للهيئة(Nominet).

ثالثا– اللّجوء إلى المحاكم الوطنيّة.

تعتبر أسماء مَواقِع الإنترنت من بين المصّنفات الرّقميّة التي تستوجب الحماية بموجب القوانين الخاصّة بها(**1**)، حيث تنفرد إجراءات السّياسة الموّحدة لتسوية نزاعات أسماء المَواقِع بخصائص تُميِّزها عن إجراءات التّحكيم العادي(**2**)، في حين يُمكِن لأطراف النّزاع بشأن اسم المَوقِع اللّجوء إلى القضاء المختص لإعادة الفصل في موضوع النّزاع(**3**).

1)– الطبيعة القانونيّة لاسم الموقِع: إنّ عقد تسجيل اسم الموقِع يمنح لصاحبه فقط حق استعماله خلال فترة تسجيله ولا يحق له ملكيته، حيث ينبغي عليه تجديد مدّة التّسجيل كُلّما

1) **Nathalie DRYEFUS**, op.cit., p. 180-182.

قربت نهايتها وإلاّ سيفقد الأسبقيّة في استعماله، في حين يُمْكِنُ أن يَكُونَ اِسْمُ المَوقِع "أثناء مدّة تسجيله" محلّ حق ملكيّة يمنح لصاحبه حق التّصَرُفِ فيه والتمتّع بثماره ومُلحقاته، إذْ يصلح بحكم القانون أن يكون محل حق مالي(Droit patrimonial) لصاحبه[1]، حيث يُمْكِنُ أن يُسْتَخْدَمَ اسم الموقِع لتمييز سلع وخدمات جديدة أو لتسجيل أسماء الأشخاص، أو الشّخصيات المشهورة أو المدن وأسماء الهيئات العموميّة والجماعات المحليّة[2]، الخ...

إنّ غياب النّصوص القانونيّة الخاصّة بتنظيم المسائل المتعلّقة بأسماء المواقِع لم يمنع القضاء الفرنسي، من تطبيق أحكام قوانين الملكيّة الفكريّة على سبيل القيّاس مع إعطاء الوصف القانوني المُلائم لاسم المَوقِع، باعتباره كرمز مميّز(Signe distinctif) يستوجب الحماية في حال توافر الشّروط الضّروريّة المطلوبة لحمايته[3]، أو حتى الاستناد إلى أحكام التّقنين المتعلّق بالبريد والمواصلات الإلكترونيّة، أو القواعد العامّة للمسؤوليّة على أساس المادتين 1382 و1383 من التّقنين المدني، فلكي يتمتّع اسم مَوقِع الإنترنت بالحماية القانونيّة يشترط القضاء الفرنسي على صاحبه إثبات الشّروط الثلاثة التّالية[4]:

أ)– الحصول بطريقة مشروعة على اسم الموقِع: يجب أن يقع الاختيار على تسجيل اسم الموقِع الذي لا يُشكّل تعدّياً على الحقوق المُكتسبة من طرف الغَيْرِ، وأن يكون جديد ومشروع ومُميّز للسّلعة أو الخدمة المُتاحة على النّحو الذي يسمح بتحديدها والتّعريف بها للمستهلك.

ب)– أسبقيّة استعمال اسم الموقِع: يجب على مُسّجِل اسم موقِع الإنترنت أن يقوم باستغلاله فِعْلِيًّا باعتباره كشرط ضروري لحمايته وإلاّ سيفقد الحقّ في استعماله.

---

1) **Nathalie DRYFUS**, op.cit., pp. 237, 238. Et **Loïc ANDRÉ**, op.cit., pp. 45, 46.
2) **Laure MARINO**, op.cit., pp. 341- 342.
3) **Nathalie DRYFUS**, op.cit., pp. 236, 237.
4) Cour d'appel de Paris, 4e Ch, 18 octobre 2000, Virgin interactive Entertainment Ltd et Virgin interactive Entertainment Sarl c/ France Télécom et BDDP-TBWA. https://www.legifrance.gouve.fr(consulté le 13/12/2018.)

ج)– وجود خطر الخلط في الأذهان بسبب تطابق أو تشابه الأسماء: إذا كان الغرض من تسجيل العلامة تفادي الخلط في ذهن الجمهور بين الخدمات والسّلع المماثلة أو المرتبطة معها، فإنّ ذلك ينطبِق على اسم الموقِع المُسَجَّلِ والمُستَغَّلِ فعليا من طرف صاحبه.

2)– الطبيعة القانونيّة لإجراء السّياسة الموّحدة(Procédure(UDRP)): إجراء تحكيم(Arbitrage) أم إجراء من نوع خاص(Sui generis): إنّ الإطار الموّحد لتسوية نزاعات أسماء المواقِع تبنّته جميع هيئات التّسجيل(Registres) ومكاتب التّسجيل المعتمدة من طرف هيئة(ICANN)، ويتّم إدماجه تلقائيا في أحكام عقد تسجيل اسم الموقِع المُبرَم بين مكتب التّسجيل مع صاحب اسم الموقِع(Titulaire)، حيث يُمكِن تصنيف ذلك العقد ضمن عقود الإذعان(Contrats d'adhésion)، التي لا تقبل المُساومة ولا التّفاوض حول أحكامها المحرّرة مُسبقًا من طرف هيئة التّسجيل(Registre)، حيث لا تُعطِي لصاحب اسم الموقِع كطرف ضعيف في العقد حرّية الاختيار والتّفاوض حول أحكامه، وبالتّالي الامتثال لإجراءات السّياسة الموّحدة في حالة نشوب نزاع بشأن اسم المَوقِع المُسَجَّلِ[1].

إنّ التّحكيم يُمكِن أن يَرِدَ كشرط في العقد(La clause compromissoire) حول إحالة المنازعات المستقبليّة التي تثور بشأن العقد للتّحكيم، أو يكون في صورة مُشارطة التّحكيم التي ترد في شكل اتفاق يَقْبَلُ بموجبه أطراف العقد الأصلي، بعد وقوع النّزاع بشأنه(العقد) على عرض النّزاع للتّحكيم(Le compromis)، كما يمكن لأطراف العقد الأصلي أن يشيروا في وثيقة أخرى إلى التّحكيم(بالإحالة)[2]، فمن بين الشّروط الموضوعيّة لِلُّجُوءِ إلى التّحكيم

---

[1] **Romain V.GOLA**, op.cit., p. 577.

[2] قانون رقم 08–09 مؤرخ في 25 فيفري 2008 يتضمن قانون الإجراءات المدنية والإدارية.

المادة 1007: " شرط التحكيم هو الاتفاق الذي يلتزم بموجبه الأطراف في عقد مُتّصِل بحقوق متاحة بمفهوم المادة 1006 أعلاه، لعرض النزاعات التي قد تُثار بشأن هذا العقد على التحكيم."

المادة 1008: " يُثبَت شرط التحكيم، تحت طائلة البطلان، بالكتابة في الاتفاقية الأصلية أو في الوثيقة التي تستند إليها. يجب أن يتضمن شرط التحكيم، تحت طائلة البطلان، تعيين المحكم أو المحكمين، أو تحديد كيفية تعيينهم."

المادة 1011:" اتفاق التحكيم هو الاتفاق الذي يقبل الأطراف بموجبه عرض نزاع سبق نشوؤه على التحكيم."

نجد ضرورة توافق إرادتي أطراف النّزاع حول اتخاذ التّحكيم كوسيلة لحل النّزاع القائم أو المُحتمل إثارته مُستقبلا، الأمر الذي يستوجب توافر الرِضَا وصّحته من عيوب الإرادة، أمّا في إجراء السّياسة الموّحدة يتم اللّجوء إليه بموجب شرط يُدرج مُسبقا في عقد تسجيل اسم الموقِع، أين يُفرض على الطرف الأخر (Titulaire) لحلّ أي نزاع يثور بشأنه مُستقبلا[1].

انطلاقا من ذلك، يجب أن يتضمّن كلّ من شرط التّحكيم (La clause compromissoire) واتفاق أو مُشارطة التّحكيم (Le compromis) تحت طائلة البطلان على تحديد كيفية تعيِين المُحكِم أو المُحكِمين، في حين نجد أنّ شرط التّحكيم في إطار إجراء السّياسة الموّحدة لا ينطبق مع شرط التّحكيم الوارد في إطار اتفاقيات التّحكيم، سواء من حيث طريقة تبادل إرادة الأطراف بشأن التّحكيم في النّزاع أو من حيث كيفية تعيين المحكمين (Arbitres-Experts)[2]، وبالتّالي فإنّ أعضاء الهيئة الإداريّة (Panel) لا يتّم تعيِينهم مباشرة بموجب شرط التّحكيم بل يُعيّنهم مركز التّسوية المُعْتَمَد ضمن قائمة الخبراء المؤهّلين، التي أعدَّها مُسبقًا لتسوية نزاعات أسماء المواقِع وفقا لإجراءات السّياسة، وفي حالة نشوب نزاع بشأن اسم الموقِع فإنّ المُدّعِي يفرض هؤلاء الخبراء على المُدّعَى عليهِ (Défendeur) الذي لا يملك خيار أخر سِوَى تقديم رأيه حول الخبراء الذين يتّم تعيِينُهم من طرف مركز تسوية النّزاع.

كما أنّ المُدّعَى عَليهِ مُلزَم بالخضوع إلى إجراءات السّياسة الموّحدة بمجرّد استلامه للدّعوى من طرف مركز التّسوية، أين تتحقّق إرادة أطراف النّزاع بصفة آَجِلَة حول شرط التّحكيم لتسوية نزاع اسم المَوقِع (« Échange de consentement différé »)، كما أنّ الإجراء الإداري يختلف عن التّحكيم أيضا من حيث حجيّة الحُكم أو القرار الصادر في

المادة 1012: " يحصل الاتفاق على التحكيم كتابيا. يجب أن يتضمن اتفاق التحكيم، تحت طائلة البطلان، موضوع النزاع وأسماء المحكمين، أو كيفية تعيينهم. إذا رفض المحكم المعين القيام بالمهمة المسندة إليه، يستبدل بغيره بأمر من طرف رئيس المحكمة المختصة."

1) **Chiheb GHAZOUANI**, op.cit., pp. 411, 412.
2) Ibid.

إطارهما، فإذا كان حكم التّحكيم يقتصر أثره على أطرافه فقط، ولا يَمْتَدُّ إلى الغيرِ الخارج عن الاتّفاق، فإنّ قرار الإجراء الإداري لا يُنَفَّذُ من جانب "أطرافه" بل من جانب "الغَيْرِ"، وبمعنى أخر، فإنّ القرار الصادر حول إلغاء اسم الموقِع أو نقله من المُدّعِي إلى المُدّعَى عليهِ أو بقاءه مِلْكاً للمُدّعِي، لا يُخَاطِبُ سوى هيئة التّسجيل(Registre) التي تقوم بالنّقل أو الإلغاء بالرّغم من أنّها لم تَكُنْ طَرَفاً في الدّعوى[1].

وعليه، فإنّ اتفاق أطراف النّزاع باللّجوء إلى إجراء السّياسة الموّحدة لتسوية نزاع اسم الموقِع، لا يكفي لإضفاء أو تكييف إجراء السّياسة((Procédure(UDRP) على أساس اتفاقية التّحكيم(Convention d'arbitrage)، ولا تنتمي إلى أيّة طرق أخرى بديلة لتسوية النّزاعات(الصلح والوساطة)، حيث يمكن بالمقابل اعتبار هذه الإجراءات ((Procédures(UDRP) على أنّها إجراء من نوع خاص(Procédure sui generis)[2]، تّم إحداثها وتطويرها لغرض التّأقلم والتّكيّف مع تطبيقات التّجارة الإلكترونيّة، والاستعمال الكثيف والمُتسارع لشبكة الإنترنت والتّقنيات التّكنولوجيّة الحديثة المنبثقة عن الثّورة الرّقميّة.

3)– عرض نزاعات أسماء المواقِع أمام الجهة القضائيّة المختصّة: إنّ إجراءات السّياسة المُوّحدة، لا تَمْنَعُ أيِّ طرف من تقديم النّزاع إلى القضاء للتّوصّل إلى تسوية مستقّلة سواء قبل البدء فيها أو بعد إنهائها، حيث يتعيّن على الطرف الذي بادر بإجراءات قانونيّة قبل أو أثناء فترة إجراءات التّسوية أن يُخطر الهيئة(Panel) ومركز التّسوية على الفور بذلك، حيث يجب على الهيئة أن تُقرِّرَ ما إذا كان سيتّم تعليق أو إنهاء الإجراءات الإداريّة أو إصدار أي قرار أخر[3]، غير أنّه في حال صدور قرار من طرف الهيئة ضدّ مُسجِّل اسم الموقِع حول

---

1) **Romain V.GOLA**, op.cit., pp. 578, 579.
2) Ibid.
Nathalie DREYFUS, op.cit., pp. 187- 189.
CA de Paris, 1er ch., sect. C, 17 juin 2004, Michel Le P., L'association Internationale des concours de beauté pour les Pays francophones (Miss francophonie) c/ La société Miss France, l'association Comite Miss France, Miss Europe, Miss Univers. https://www.legifrance.gouve.fr(consulté le 03/03/2017.)
3) **Art. 18 (Règles d'application(UDRP)) : « Effet des procédures judiciaires.**

إلغاء اسم الموقِع أو نقله إلى المُدّعِي ، يجب على المُسّجِل أن يقوم خلال عشرة(10) أيام المُوالية لتاريخ عِلْم مكتب التّسجيل بالقرار، برفع دعوى قضائيّة ضّد الطرف الذي صدر في حقّه القرار "لإعادة" الفصل من جديد في موضوع النّزاع وليس لغرض "إلغاء" قرار التّسوية((Décision(UDRP)، لتفادي رفض الدّعوى من القضاء بِدَاعِي أنّ قرار التّسوية لا يُعتبر كحكم تحكيمي(Sentence arbitrale) وفقا للأحكام القانونيّة باتفاقيات التّحكيم[1].

تقتصر سلطة الهيئة(Panel) في الفصل في النّزاع وفقا لإجراءات "السّياسة"، فقط حول رفض الدّعوى أو إلغاء اسم الموقِع أو تحويل تسجيله إلى مالك العلامة، في حين يُمكِن أن تتعدّد الطلبات أمام القضاء أَيْنَ يُمْكِنُ لِلطَّرَفِ الذي صَدَرَ لمصلحتهِ القرار، اللّجوء إليه في حالة إثبات ضرر مُترتّب عن تسجيل اسم موقِع لأحد عناصر الملكيّة الفكريّة المحميّة، أو يقوم الطرف الذي صُدِر ضِدّه القرار برفع دعوى قضائيّة في حال تواجد غموض بشأن وقائع القضيّة، الأمر الذي يستدعي إعادة النّظر فيها وإعطاءها التّكييف القانوني الصّحيح وفقا للمستندات والوثائق المُتوفِّرة، لذا منحت إجراءات السّياسة الموّحدة لمُسجِّل اسم المَوقِع، إمكانية رفع الدّعوى القضائيّة سواء أمام محكمة المقّر الرّئيسي لمكتب التّسجيل، أو أمام المحكمة الذي يَقَعُ في دائرة اختصاصها عنوان مُسّجِل اسم المَوقِع المُبَيَّنِ في قاعدة بيانات"Whois" وقت تقديم الدّعوى لمركز التّسوية المعتمد[2].

---

a)- En cas de **procédures judiciaires** commencées **avant** ou **pendant** une procédure administrative concernant un litige sur un nom de domaine faisant l'objet de la plainte, le **panel** devra décider à sa discrétion s'il faut suspendre ou clore la procédure administrative, ou bien s'il faut prendre une décision.

b)- Au cas où une partie entamerait une procédure judiciaire **pendant** une procédure administrative en instance concernant un litige sur un nom de domaine faisant l'objet de la plainte, elle devra notifier le panel et le fournisseur dans les plus brefs délais. Voir le paragraphe 8 ci-dessus. »

1) **Nathalie DREYFUS**, op.cit., p. 190.

Voir aussi : l'**Art.04-(k)(Principes UDRP):** Possibilité d'engager des poursuites judiciaires.

2) **Art. 01(Règles d'application(UDRP))** : « Juridiction compétente. désigne un tribunal situé soit **(a)** au **siège principal du bureau d'enregistrement** (pourvu que le titulaire du nom de domaine soit soumis, en vertu de son contrat d'enregistrement, à cette juridiction pour le règlement judiciaire de litiges concernant ou découlant de l'utilisation du nom de domaine),

يتّم الفصل في النّزاعات النّاشئة فيما بين أسماء المواقع عادةً وفقا لمبدأ الأولويّة في التّسجيل « First Come First Served » المتّبع في إجراءات تسجيل أسماء المَواقِع، إلاّ أنّ ذلك لا يَمْنَعُ من النّاحية العمليّة تسجيل اسم مَوقِع مُماثِل أو مُشابِه لاسم موقع أخر وفقا لامتداد معيّن، الذي من خلاله يجب على مُسّجِل اسم الموقِع إثبات الصِّفة المُميِّزة لاسم موقعِه(Nom de domaine distinctif)، الذي ينبغي أن يكون مُميِّزا لما يَعرِضُهُ من سلع أو خدمات وقادرا على التَّعريف بها، حيث فصلت محكمة استئناف باريس وفقا لذلك بموجب القرار الصادر في 25 ماي 2005 في القضية التي جَمعت بين شركة (Société d'économie mixte des pompes funèbres de la ville de Paris) مع شركة (Société OGF)، أين قامت الشّركة الأولى في عام 2000 بتسجيل اسم الموقع (servicesfuneraires.fr)، بينما الشّركة الثّانية قامت في عام 2004 إيداع اسم موقِع مشابه للموقِع الأوّل المُسَجَّلِ(services-funeraires.fr)، حيث اعتبر قضاة الموضوع أنّه لا يحق لأيّ طرف في النّزاع طلب شطب أو تحويل اسم الموقِع من خَصْمِهِ، لكون أنّ خطر الخلط في الأذهان يتحقّق في اسم المَوقِع المُميِّز (Distinctif) وليس الوَصْفِي(Descriptif)[1].

وعليه، يجب التّمييز بين النّزاعات بشأن العلامات المُسجَّلة(Marques antérieures)، مع أسماء المواقِع المُسجَّلة لاَحِقًا(Postérieurs)، أين تُطبَّق في هذه الحالة الأحكام الواردة في قوانين الملكيّة الفكريّة ما دَامَ أنّ العلامة المَحميّة قد سبق تسجيلها لدى المصلحة المختصّة، أمّا إذا كان اسم المَوقِع قد تّم تَسْجِيلُهُ وفقا لمبدأ الأسبقيّة في التّسجيل بالمقارنة

---

soit **(b)** à **l'adresse du titulaire du nom de domaine** indiquée pour l'enregistrement du nom de domaine dans la base de données Whois du bureau d'enregistrement au moment où la plainte est déposée auprès du fournisseur. »

1) **CA de Paris**, 25 mai 2005, S.A. OGF, son Président du Conseil d'Administration et Directeur Général c/ S.A. d'économie mixte des pompes funèbres de la ville de Paris-services funéraires de Paris. Disponible sur les sites: https://www.legifrance.gouve.fr et https://www.doctrine.fr (consultés le 09/07/2016.)

CA de Douai, 1er chambre, 09 septembre 2002, Michel P, Société Codina c/ Association le Commerce du bois. Disponibles sur le site: https://www.legifrance.gouve.fr et https://www.doctrine.fr (consultés le 10/07/2016.)

مع العلامة المُسجَّلة لاَحِقًا، فيتّم إلغاء هذه العلامة لعدم تَوَافُرِ العناصر المُمَيِّزَةِ لها مع انتهاك حق مُكتسب، حيث أكدّت ذلك محكمة لومان الفرنسية (Tribunal de grande instance le Mans) بموجب الحكم الصادر في 29 جوان 1999، في القضية التي جمعت بين شركة(Oceanet) مُزوّد خدمات الإنترنت مع شركة(Microcaz) المختصّة في بيع المعدّات المعلوماتيّة وخدمات الإنترنت والشّبكات[1]، حيث قامت شركة(Oceanet) بِتَسْجِيلِ اسم الموقِع(www.oceanet.fr) في منتصف جويلية 1996 مع إيداع علامتها(Oceanet) في 17 سبتمبر 1996، وبالمقابل قامت شركة(Microcaz) في 02 سبتمبر 1996 إيداع علامتها(OCE@net) لدى مصلحة(INAPI)، حيث قرّر القضاة إلغاء علامة شركة(Microcaz) وفقا لمبدأ الأولويّة في التّسجيل وعدم توافر الصّفة المميّزة لها عند الإيداع، وبالتّالي عدم مراعاة نص المادة(L.711-4) من تقنين الملكيّة الفكريّة.

يُمكن لمُسّجِل اسم الموقِع أن يَفْقِدَ الحق في استعماله إذا لم يَقم باستغلاله فعليًا(Exploité de manière effective)، وهذا ما أكّده حُكم محكمة باريس الصادر في 09 جويلية 2002، في قضية(Looxor) التي جمعت بين شركة بيجو(Peugeot) مع شركة شيرلوكوم(Sherlocom)، أين قامت شركة(Peugeot) في 31 أوت 2000 إيداع علامة(Looxor) لدى المصلحة المختصّة للتّعريف بمنتوج جديد(Scooter)، مع التّرويج له عبر المنصّة الإلكترونيّة(www.peugeotlooxor.com)، لكن شركة(Sherlocom) سجّلت اسم الموقِع(www.looxor.com) في 26 جوان 2000، حيث طلبت من المحكمة إلغاء علامة(Looxor) من شركة(Peugeot) لكونها(Sherlocom) السّباقة في تسجيلها ضمن اسم الموقِع، لكن المحكمة رفضت طلبها بِدَاعِي أنّ اسم الموقِع المُسَجَّلِ لم يُستعمَل بطريقة فِعليّة قَبْلَ إيداع وتسجيل شركة(Peugeot) لعلامة(Looxor) لدى المصلحة المختصّة[2].

---

1) **TGI Le Mans**, 29 juin 1999, SARL Microcaz c/ SARL Oceanet. Disponible sur les sites: https://www.legifrance.gouve.fr et https://www.juriscom.net/txt/jurisfr/ (consultés le 15/07/2016.)

2) **TGI Paris**, 3ème ch, 3ème sect, 09 juillet 2002, SA Peugeot Motocycles c/ M. Guy C., SA société Sherlocom. Disponible sur les sites: https://www.legifrance.gouve.fr et https://www.juriscom.net/txt/jurisfr/ (consulté le 18/07/2016.)

المبحث الثاني
الحماية المدنيّة والجزائيّة لمواقع التّجارة الإلكترونيّة

ساهمت الثّورة الرّقميّة في انتشار مختلف البرمجيات والتّطبيقات المعلوماتيّة وسيطرة تقنيّة الخوارزميات على نمط إدارة وتنظيم وسير جميع المعاملات، وبالخصوص الإداريّة والتّجارية والماليّة والملكيّة الفكريّة الرّقميّة الخ...، حيث تزايد الاهتمام بمنهجيات وتقنيات لغة برمجة مواقع التّجارة الإلكترونيّة بشكل غير مسبوق وبروز مصنّفات رقميّة لا يمكن إحداثها إلاّ عبر شبكة الإنترنت أو الموقِع الإلكتروني، كعناصر وشكل تصميم الموقِع والعلامات والرّسومات ولغات البرمجة والخوارزميات وروابط الإحالة، التي تسمح بعرض السّلع والخدمات عبر صفحات ويب مواقع التّجارة الإلكترونيّة، الخ...، التي تستوجب الحماية القانونيّة اللاّزمة لها(**المطلب الأول**).

إنّ تعميم استخدام شبكة الإنترنت ساهم بشكل كبير في انتشار المتاجر الافتراضيّة وتنامي فكرة الانفتاح على الإقتصاد الرّقمي وتشجيع استخدام تطبيقات التّجارة الإلكترونيّة، ومختلف التّقنيات والخدمات التي تفرض على المستهلك حتميّة الاستعانة بمقدّمي خدمات الإنترنت أو الوسطاء في خدمات الإنترنت، بحسب تنوّع نشاطاتهم وتعدّد أدوارهم التي تستوجب بالمقابل تتبّع النّشاط المعلوماتي غير المشروع وكشفه لتكييف مسؤوليّة كلّ مزوّد، حيث أنّ معاملات التّجارة الإلكترونيّة تتم في بيئة افتراضيّة مملوءة بالمخاطر والتّهديدات التي تمّس بأمن وسلامة البيانات الإلكترونيّة المتداولة عبر المتاجر الافتراضيّة، الأمر الذي يتطلّب الاستعانة بالأحكام الجزائيّة الرّدعيّة كضمانات قانونيّة لمَواقِع التّجارة الإلكترونيّة(**المطلب الثاني**).

المطلب الأول
الحماية المدنيّة والجزائيّة للمصّنفات الرّقميّة

إنّ الانتشار الكثيف والمُتزايد لمواقع التّجارة الإلكترونيّة صاحب معه ظهور العديد من المنازعات المتعلّقة بأسماء مواقِع الإنترنت، نتيجة التّسارع الكبير حول تسجيل أسماء المواقِع وفقا لمبدأ الأسبقيّة أو الأولويّة في التّسجيل الذي يسمح لصاحبه باستعماله أوّلاً، في حين تُشكّل المُمارسات التّجارية غير النّزيهة تعدّيًا أو تجاوزًا على حقوق صاحب المصنّف الرّقمي حيث يُنْظَرُ على أنّها أفعالا غير مشروعة مُخالفة للقواعد المنظّمة للمُمارسات التّجاريّة، وهذا ما يَدْفَعُ بالطرف المُتضرّرِ إلى طلب التّعويض في إطار إجراءات رفع الدّعوى المدنيّة أمام الجهات القضائيّة المُختصّة(**الفرع الأوّل**).

كما أنّ تعميم الرّقمنة وانتشار البرامج والتّطبيقات صاحبت معها ظهور وانتشار تقنيات جدّ مُتطوّرة في تنفيذ التّهديدات وارتكاب الجرائم الإلكترونيّة، من أبرزها جريمة التّقليد التي تمّس بالمُصّنفات الرّقمية أين يتحمّل الفاعِل المسؤوليّة الجزائيّة على أساس جُنحة التّقليد المُعاقب عليها وفقا للقوانين الخاصّة بحماية حقوق الملكيّة الفكريّة، فإذا كانت أعمال المُنافسة في الأصل مشروعة بالرّغم من طابعها الضّار بِالْغَيْرِ، فإنّ الإسراف في استعمال هذه الحريّة أو التّعسّف فيها يُشكل بالتّالي الفِعْلُ الوَحيد الذي يُجَرِّمُهُ القانون، وذلك مَا دَامَ أنّ المُنافسة تتضمّن عادةً في طبيعتها إلحاق الضرر عَمْداً بالغير، الأمر الذي يَدْفَعُ بالمُتضّرر الاستعانة بالأحكام الجزائيّة المزدوجة لأعمال المنافسة غير المشروعة(**الفرع الثاني**).

الفرع الأول
الحماية المدنيّة للمصّنفات الرّقميّة

تعدّ حقوق الملكيّة الفكريّة الرّقميّة نتاج القدرات الإبداعيّة لصاحبها التي تتطلّب إجراءات وشروط متقاربة لإضفاء الحماية القانونيّة عليها، حيث يُعتبر التّسجيل كشرط جوهري لتحديد نوع الحماية القانونيّة لأسماء مواقع الإنترنت(**أوّلا**)، في حين تشترك عادةً حقوق الملكيّة الفكريّة الرّقميّة المُسجَّلة وغير المُسجَّلة في الحماية المدنيّة من خلال رفع دعوى المنافسة

غير المشروعة(**ثانيا**) أو عن طريق مُباشرة إجراءات رفع دعوى المسؤولية التّقصيرية أمام المحكمة المختصّة(**ثالثا**).

أولا– أهميّة التّسجيل في تحديد نوع الحماية القانونيّة لأسماء مواقع الإنترنت.

إذا كان شرط التّسجيل مطلوب لحماية كلّ من حقوق المؤلف والحقوق المجاورة أو حقوق الملكيّة الصّناعيّة والتّجاريّة، فإنّ أسماء مواقع الإنترنت تعتمد هي الأخرى على إجراءات التّسجيل وفقا لمبدأ الأسبقيّة أو الأولويّة في التّسجيل[1]، الذي يكرّس الحماية القانونيّة لأصحاب المواقِع أثناء فترة مدّة التّسجيل مع السّهر على تجديدها كلّما قربت مدّة نهايتها، وبالتّالي منح المشّرع الفرنسي حماية خاصّة لأسماء المواقع العليا الوطنيّة الفرنسيّة، بموجب القانون رقم 2011–302 المؤرخ في 22 مارس 2011 الذي يتضمّن الأحكام المختلفة لتكييف التّشريعات الخاصّة بالصّحة والعمل والاتّصالات الإلكترونيّة مع قانون الاتّحاد الأوروبي[2]، الذي من خلاله قام بتعديل بعض أحكام تقنين البريد والمواصلات الإلكترونيّة المتعلّقة بأسماء المواقع الوطنيّة الفرنسيّة، فبالرجوع إلى نص المادة(L45) مكرر2 من نفس التّقنين وكذا المادة 02 مكرر4 من ميثاق التّسمية لهيئة

---

[1] **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007، ص ص 287– 294.

[2] **Loi n° 2011-302** du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de […], et de communications électroniques.

Art. L. 45-2 : « […], L'enregistrement ou le renouvellement des noms de domaine peut être refusé ou le nom de domaine supprimé lorsque le nom de domaine est : **1-** Susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ; **2-** Susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi ; **3-** Identique ou apparenté à celui de la République française, d'une collectivité territoriale ou d'un groupement de collectivités territoriales ou d'une institution ou service public national ou local, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi.[…]. »

Art. L. 45-3 : « Peuvent demander l'enregistrement d'un nom de domaine, dans chacun des domaines de premier niveau : – les personnes physiques résidant sur le territoire de l'Union européenne ; – les personnes morales ayant leur siège social ou leur établissement principal sur le territoire de l'un des États membres de l'Union européenne. »

التّسجيل(AFNIC)[1]، فإنّ عملية تسجيل أسماء المواقِع لدى الهيئة(AFNIC) تخضع لمجموعة من الشّروط التي من خلالها يجب على أيّ شخص طبيعي أو معنوي بمفهوم المادة(L45) مكرر3 من نفس التّقنين، أن يتقدّم بطلب أمام مكتب التّسجيل المعتمد لتسجيل اسم مَوقِع الإنترنت أو تجديد مدة تسجيله، أن يضمن تحت مسؤوليّته ما يلي:

– أنّ الغرض من تسجيل اسم الموقِع لا يتعلّق بالمساس بالنّظام العام أو الآداب العامّة أو إنتهاك حقوق مضمونة بموجب الدّستور أو القانون؛

– عدم انتهاك الحقوق المتعلّقة بالملكيّة الفكريّة أو بالأشخاص؛

– أن يكون اسم الموقِع غير مُتشابه أو مُتطابق مع اسم الجمهوريّة الفرنسيّة أو أسماء ذات صلة بالجماعات الإقليميّة والمحليّة أو بمؤسّسة أو مرفق عام، إلاّ إذا أثبت صاحب الطلب(Demandeur) تواجد حسن النّية والمصلحة المشروعة في تسجيل اسم مَوقعِه.

يتمتّع اسم مَوقِع الإنترنت المُسجَّل لدى مكتب التّسجيل المعتمد من طرف هيئة التّسجيل(AFNIC)، وفقا لهذه الشّروط، بحماية قانونية خاصّة خلال المدّة القانونيّة لتسجيله، سواء بموجب أحكام التّقنين المتعلّق بالبريد والمواصلات الإلكترونيّة أو أحكام تقنين الملكيّة الفكريّة التي من خلالها، يُمكِن لصاحب اسم الموقِع المُسجَّل في حالة النّزاع مع علامة تجاريّة أو خدمة، أن يُثِيرَ أحكام نص المادة(L711) مكرر4 من تقنين الملكيّة الفكريّة الفرنسي[2]، ما دَامَ أنّ هذه المادة لم تُحدِّد على سبيل الحصر الحقوق السّابقة التي يجب

---

1) **Art. 2-4 (Charte de nommage(AFNIC)) :** « Noms de domaine soumis à examen préalable. […] ; Pour obtenir l'enregistrement d'un terme soumis à examen préalable, le demandeur doit s'assurer que le nom de domaine : - N'est pas susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ; - N'est pas susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité ou n'est pas identique ou apparenté au nom de la République Française ou d'une collectivité territoriale ou d'un groupement de collectivités territoriales ou d'une institution ou service public national ou local sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi. - Il est fait application des dispositions du Code des postes et communications électroniques, pour caractériser l'existence d'un « intérêt légitime » et de la « mauvaise foi ». […]. »

2) **Code de la propriété intellectuelle**(France) - Dernière modification le 24 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr

عدم المساس بها أثناء القيام بتسجيل العلامة لدى المصلحة الرّسميّة المختصّة، حيث ينبغي في هذه الحالة على صاحب اسم الموقِع المُتنازع عليه، أن يُثْبِتَ للقضاء المختّص أنّ اسم موقعِه المُسجَّلِ قد تمّ اكتسابه بطريقة مشروعة وقانونيّة، ويتمتّع بصفة مُميِّزة عن غَيْرِهِ لما يَعْرِضُهُ وقادرا على التّعريف بِهِ، مع أسبقية الاستغلال الفِعْلِي لاسم مَوقِعِهِ المُسجَّلِ، بالمقارنة مع اسم المُصنّف محلّ النّزاع، وكذا تواجد خطر الخلط في ذهن الجمهور من جرّاء التّشابه أو التّطابق مع الاسم المتنازع عليه الذي يؤدّي إلى تضليل الجمهور أو إيقاعه في الغلط[1].

لذا يعتبر التّسجيل كعنصر جوهري لحماية اسم الموقِع المُسجَّل لدى هيئة التّسجيل(Registre) المسؤولة عن تسجيل أسماء المواقِع العليا للدّولة المعنيّة، حيث يضمن لصاحب الحق الحماية أثناء مباشرة إجراءات رفع الدّعوى القضائيّة(المدنيّة أو الجزائيّة) أمام المحكمة المختصّة، وعليه فإنّ التّساؤلات لا تُثار عندما تتضمّن أسماء مواقع التّجارة الإلكترونيّة على مُصنّف مميّز(Signe distinctif) أو أيّ عنصر من عناصر الملكيّة الفكريّة المحميّة كالعلامات، أو البرمجيات وقواعد البيانات الخ...، التي تُحظى بواحد أو أكثر من تشريعات الحماية سواء في إطار الملكيّة الفكريّة أو القوانين الخاصّة[2]، بينما تُثار الإشكالية

Art. L711-4 : « Ne peut être adopté comme marque un signe portant atteinte à des droits antérieurs, et **notamment** : **a)** A une marque antérieure enregistrée ou notoirement connue au sens de l'article 6 bis de la convention de Paris pour la protection de la propriété industrielle ; **b)** A une dénomination ou raison sociale, s'il existe un risque de confusion dans l'esprit du public ; **c)** A un nom commercial ou à une enseigne connus sur l'ensemble du territoire national, s'il existe un risque de confusion dans l'esprit du public ; **d)** A une appellation d'origine protégée ou à une indication géographique ; **e)** Aux droits d'auteur ; **f)** Aux droits résultant d'un dessin ou modèle protégé ; **g)** Au droit de la personnalité d'un tiers, notamment à son nom patronymique, à son pseudonyme ou à son image ; **h)** Au nom, à l'image ou à la renommée d'une collectivité territoriale. »

1) **Thibault VERBIEST, Maxime LE BORNE**, « Le fonds de commerce virtuel : une réalité juridique? », Journal des tribunaux, 23 février 2002, 121e année- N° 6044, p. 148. Article disponible sur le site: https://www.droit-technologie.org, consulté le 04/05/2016.
Nathalie DREYFUS, op.cit., pp. 220- 226, 236.
Voir aussi : l'Art. **L711-4** du code de la de la propriété intellectuelle(France).

2) **Grégoire LOISEAU**, « Nom de domaine et Internet : turbulence autour d'un nouveau signe distinctif », Recueil Dalloz, n° 23/ 1999, pp. 247- 250.

حول مدى القدرة على حماية المصّنفات الرّقميّة الأخرى عبر شبكة الإنترنت التي لا يكون وجودها إلاّ عبر الموقِع الإلكتروني، ولا تَشْتَمِلُهَا الحماية من خلال إجراءات تسجيل أسماء المواقِع، كعناصر وشكل تصميم الموقِع والعلامات والوسائط المتعددة، وروابط الإحالة التي تسمح بعرض السّلع والخدمات على صفحات ويب مواقِع الإنترنت الخ...

وعليه، فإنّ معظم المنازعات النّاشئة مع أسماء المواقع تتمحور حول المستوى الثّاني (SLD) الذي يُمثِّل القيمة الماليّة الأكبر للشركات، حيث يجب على الراغب في إحداث موقع تجاري تفادي اختيار اسم تجاري مُسّجل أو علامة محمية أو حتى الأسماء الأخرى المُثيرة للجدل، مثل المصطلحات الجغرافيّة، أو أسماء المشاهير أو أسماء الأدويّة النوعيّة وأسماء المنظّمات الدّوليّة الخ...، التي تتداخل مع أنظمة حماية حقوق الغَيْرِ أو أنظمة الحماية الدوليّة، ولتفادي عمليات السّطو الإلكتروني على العلامات قامت المنظّمة العالميّة للملكيّة الفكريّة(WIPO) بإحداث بوابة إلكترونيّة[1]، تُتيح إمكانية النّفاذ إلى قاعدة البيانات الخاصة بالعلامات للمُساعدة على إجراءات البحث.

إنّ غياب التّشريعات المُنظّمة لأسماء مواقع الإنترنت وكثرة الإشكالات القانونيّة التي تتطلّب تحديد حقوق الملكيّة الرّقميّة عبر الإنترنت، واستقصاء الحماية القانونية اللاّزمة لها، لا تزال تُثير إلى حدّ الآن التّساؤلات والجدال ومحلّ بحث من جانب الفقهاء وخبراء القانون، ولعلّ ما تقوم به المنظّمة العالميّة للملكيّة الفكريّة(OMPI) من حلّ النّزاعات بشأن أسماء مواقع الإنترنت مع العلامات، عبر مركز التّحكيم والوساطة المعتمد من طرف هيئة الآيكان(ICANN)، وفقا لإجراءات السّياسة الموّحدة(Procédures(UDRP) كآلية مُشتركة بين الويبو والآيكان، يبدو أنّه اتجاه نحو إرساء نظام قانوني لحماية أسماء مواقع الإنترنت.

ديالا عيسى ونسه، حماية حقوق التأليف على شبكة الإنترنت، منشورات صادر الحقوقية، لبنان، 2002، ص ص 54، 55.

1) https://www.ecommerce.wipo.int/databases/trademark/index.html

ثانيا– حماية المصّنفات الرّقمية بدعوى المنافسة غير المشروعة.

تتمثّل المنافسة غير المشروعة، وفقا للمادة 10 مكرّر من اتّفاقية باريس لحماية الملكيّة الصّناعيّة، في تلك المنافسة التي تتعارض مع العادات الشّريفة في الشّؤون الصّناعيّة أو التّجاريّة، حيث تشتمل على كافة الأعمال التي من طبيعتها أن تحدث بأية وسيلة كانت لُبْسًا من شركة أحد المنافسين أو منتجاته أو نشاطه الصّناعي أو التّجاري، أو تنطوي على استخدام إدّعاءات مُخالفة للحقيقة في مزاولة التّجارة التي من طبيعتها نزع الثّقة عن شركة أحد المنافسين أو منتجاته أو نشاطه التّجاري أو الصّناعي، كما يمكن أن يكون الهدف من المنافسة غير المشروعة استعمال البيانات أو الإدّعاءات في التّجارة لتضليل الجمهور حول طبيعة السّلع أو طريقة تصنيعها أو خصائصها أو صلاحيتها للاستعمال أو كمّيتها[1].

وعليه، فإنّ الحماية المدنيّة بموجب دعوى المنافسة غير المشروعة (Action en concurrence déloyale)، تعتبر بمثابة المِظَلّة التي تَسْتَظِلُّ بها جميع الحقوق الأخرى أيّا كان نوعها، وما بَالُكَ بالمصّنفات الرّقميّة التي تحتاج للحماية القانونيّة عبر الإنترنت، حيث يمكن للمُتضّرر صاحب الحق على أحد المصّنفات الرّقميّة المُميّزة(Signes distinctifs) مُبَاشرَة إجراءات رفع دعوى المنافسة غير المشروعة، في حالة عدم إمكانية مباشرة إجراءات

---

1) **Art.10bis (Convention de Paris** pour la protection de la propriété industrielle du 20 mars 1883 révisée à[…], et modifiée le 28 septembre 1979) : « [**Concurrence déloyale**]
1) Les pays de l'Union sont tenus d'assurer aux ressortissants de l'Union une protection effective contre la concurrence déloyale.
2) Constitue un acte de **concurrence déloyale** tout acte de concurrence contraire aux usages honnêtes en matière industrielle ou commerciale.
3) Notamment devront être interdits : **1-** tous faits quelconques de nature à créer une confusion par n'importe quel moyen avec l'établissement, les produits ou l'activité industrielle ou commerciale d'un concurrent;
2- les allégations fausses, dans l'exercice du commerce, de nature à discréditer l'établissement, les produits ou l'activité industrielle ou commerciale d'un concurrent;
3- les indications ou allégations dont l'usage, dans l'exercice du commerce, est susceptible d'induire le public en erreur sur la nature, le mode de fabrication, les caractéristiques, l'aptitude à l'emploi ou la quantité des marchandises. »

الدّعوى الجزائيّة المتعلّقة بجُنحة التّقليد التي يعتبر فيها تسجيل العلامة كإجراء شكلي ضروري لقبول الدّعوى أمام الجهة القضائيّة المختصّة.

لذا يُمكن رفع دعوى المنافسة غير المشروعة بصفة مستقّلة عن دعوى التّقليد أو رفعها بجانب هذه الأخيرة، كدعوى فرعيّة أمام المحكمة الجزائيّة التي تفصل في دعوى التّقليد بشأن احد عناصر الملكيّة الفكريّة المحميّة، وبالتّالي فإنّ الحماية القانونيّة الممنوحة للشّخص الذي قام بتسجيل أحد عناصر الملكيّة الفكريّة، تختلف عن الحماية الممنوحة لصاحب الحق على المصنّف الرّقمي الذي تتوافر فيه شروط الحماية القانونيّة الخاصّة، حيث يحقّ للأوّل الحصول على الحماية الجنائيّة في حالة التّقليد، بينما لا يجوز للشّخص الثّاني سوى مباشرة دعوى المنافسة غير المشروعة للحماية المدنيّة[1].

إنّ دعوى المنافسة غير المشروعة يمكن مباشرتها كاستثناء على دعوى التّقليد لحماية حقوق المصّنفات الرّقميّة غير المُسّجلة، التي كفلتها جميع التّشريعات المقارنة، حيث سمح المشّرع الجزائري لأصحاب المصّنفات الرّقميّة غير المُسّجلة التي تعرّضت إلى مختلف الاعتداءات، إمكانية رفع دعوى المنافسة غير المشروعة وتأسيسها وفقا لأحكام المادة 124 من التّقنين المدني أو الأحكام الواردة في قوانين الملكيّة الفكريّة، أو عند الاقتضاء أحكام القانون رقم 04-02 المتعلق بالقواعد المُطبّقة على الممارسات التّجاريّة، وعلى العموم تخضع دعوى المنافسة غير المشروعة إلى جانب الشّروط العامّة المتعلّقة بتواجد الخطأ والضّرر والعلاقة السّببية[2]، إلى مجموعة من الشّروط الأخرى التي من خلالها يجب على

---

[1] **سمير جميل حسين الفتلاوي**، الملكية الصناعية وفقا للقوانين الجزائرية، ديوان المطبوعات الجامعية، الجزائر، 1988، ص ص 395، 397.

شريف محمد غنام، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني(Domain Name)، مرجع سابق، ص ص 162، 163.

[2] **زواوي الكاهنة**،" المنافسة غير المشروعة في الملكية الصناعية"، شهادة دكتوراه في العلوم، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر– بسكرة، 2015، ص ص 163-175.

المُتضّرر أن يُثبتَ وفقا لأحكام قانون الملكيّة الفكريّة الخاص بالعلامات، الصّفة المُميّزة لمصنّفه الرّقمي وأسبقيّة حقّه بالمقارنة مع العلامة التّجاريّة أو الخدمة المتنازع عليها، وإثبات تواجد خطر الخلط في ذهن الجمهور، حيث يملك قاضي الموضوع السّلطة التّقديريّة في تحديد عُنصر المنافسة غير المشروعة[1].

انطلاقا من ذلك، تعتبر روابط الإحالة(Liens hypertextes) بمثابة الطّاقة المُحرِّكَة لشبكة الإنترنت وبالخصوص مُعاملات التّجارة الإلكترونيّة، حيث أثارت هذه الرّوابط في الآونة الأخيرة نقاشات قانونيّة عِديدة بشأن الطّريقة التّقنيّة المُستخدمة في عرض أو الوصول إلى المصّنفات الرّقميّة عبر الإنترنت، التي تؤدّي عادة إلى المساس بحقوق أصحاب الملكيّة الفكريّة الأدبيّة أو الصّناعيّة والتّجاريّة، أو حتّى خرق قواعد المنافسة المشروعة، في حين لا يوجد أيّ نص قانوني مُنظّم لروابط الإحالة، بل تُرِك الأمر للاجتهاد القضائي للفصل في النّزاعات التي تُثيرها هذه الرّوابط بشأن المصّنفات الرّقميّة عبر الإنترنت[2].

وعليه، فإنّ مواقع التجارة الإلكترونية تتضمّن على العديد من روابط الإحالة التي تسمح للمستهلك بالتّعرف على منتجاتها والوصول إليها بكل حريّة، حيث لا يوجد ما يمنع أصحاب هذه المواقع من إعتماد روابط الإحالة التي تّم إحداثها بطريقة مألوفة ومشروعة، غير أنّ بعض مواقع الإنترنت لديها نظام خاص بكيفية إحداث روابط الإحالة إليها، حيث تقوم في إطار "الشّروط العامّة للاستعمال"(Conditions générales d'utilisation) المُعلَن عليها عادة في أسفل صفحة الويب، بفرض شرط الحصول على التّرخيص لكل عملية إنشاء لرابط إحالة نحو الموقِع الإلكتروني، حيث اعتبرت محكمة النّقض الفرنسيّة بموجب قرارها الصادر بتاريخ 31 أكتوبر 2012[3]، بأنّ الشّروط العامّة للاستعمال المشار إليها في أسفل صفحة

---

1) **Laure MARINO**, op.cit., pp. 376- 378.

2) **Lionel THOUMYRE**, « De la responsabilité arachnéenne sur Internet : Quelle issue pour les tisseurs de liens en France », pp. 05, 06. Lex Electronica, vol. 10, n°1, Hiver 2005.
علي كحلون، مرجع سابق، ص ص 158–160، 223– 229.

3) Arrêt de la Cour de cassation, 1ère ch. civile, du 31 octobre 2012, Groupe M6 c/ Société SBDS, n° 11-20480. Disponible sur : https://www.legifrance.gouve.fr(consulté le 11/12/2018.)

الويب، لا يمكن تكييفها على أساس التزام تعاقدي مفروض على المستخدم في إطار الخدمات المتاحة، لكون أنّ عملية الوصول إلى صفحة الاستقبال الأصليّة للموقع ومحتواه تتّم بكل حريّة وبصفة مُباشِرة من دون الأخذ بعين الاعتبار بالشّروط العامّة للاستعمال.

إنّ روابط الإحالة السّطحيّة(Lien en surface) التي تسمح بمجرّد النّقر عليها بعرض المصّنفات الرّقميّة عبر صفحات الاستقبال الأصلية للمواقِع المُحالَة إليها، قد وَقَعَ الإجماع عليها من جانب الفقه والقضاء بشأن مشروعيّة استخدامِهَا[1]، لكون أنّ نظام تشغيل شبكة الإنترنت يعتمد مبدئياً مُنْذُ نَشْأَتِهَا على روابط الإحالة التي تسمح بالتنّقل بحريّة من صفحة ويب إلى آخرى، حيث تحتويها(Liens hypertextes) جميع مواقع الإنترنت لتمكين المستخدم بعرض المصّنف المَنشور مُسبقاً عبر الإنترنت، كما أنّ عملية الإحالة السّطحيّة إلى موقع آخر لا تُعدّ من بين أعمال إعادة النّقل للمصّنف[2].

«[…]. qu'un usage à des fins privées est incompatible avec la nature même d'une entreprise commerciale, et qu'il est pour le moins paradoxal d'accorder à une société une autorisation de référencement et en même temps de lui opposer des conditions générales lui imposant un usage à titre privé et non commercial. […]. tout **contrat** exige la rencontre d'une **offre** et d'une **acceptation**, laquelle n'est pas démontrée en l'espèce, les sociétés du groupe M6 ne produisant aucun document manifestant l'accord de la société SBDS sur les conditions générales invoquées. […], qu'en jugeant néanmoins que la société **SBDS n'**était pas un **utilisateur** des services M6 replay et W9 replay, au sens de leurs **conditions générales d'utilisation**, au motif qu'elle ne procède pas au **visionnage** des programmes disponibles sur lesdits sites, mais se borne à les **mettre** à la **disposition** de ses internautes, pour les **juger inopposables** à cette dernière, les juges du fond ont **violé** l'article 1134 du Code civil. […], qu'en jugeant néanmoins les conditions générales d'utilisation des services M6 replay et W9 replay inopposables à la société SBDS faute de preuve qu'elle les ait formellement acceptées, la Cour d'appel a violé l'article 1134 du Code civil. […]. »
Voir aussi : **Mickaël LE BORLOCH**, op.cit., pp. 315-332.

1) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., pp. 25, 26.

2) **Arrêt** de la C.J.U.E (4ème ch.), du 13/02/2014, Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd c/ Retriever Sverige AB, (Affaire C-466/12). https://www.curia.europa.eu/juris/document/(consulté le 03/01/2018.)
« […].Par ces motifs, la Cour (quatrième chambre) dit pour droit:
1) L'article 3, paragraphe 1, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, doit être interprété en ce sens que ne constitue pas un acte de communication au public, tel que visé à cette disposition, la fourniture sur un site Internet de liens cliquables vers des œuvres **librement** disponibles sur un autre site Internet.

حيث أكّد ذلك قاضي الاستعجال للمحكمة التّجاريّة بنانتير(T.Com de Nanterre) بتاريخ 08 نوفمبر 2000، بصدد القضية التي جمعت بين شركة(Sarl Stepstone France) مع شركة(Sarl Ofir France)[1]، التي من خلالها قامت الشّركة الثانية عبر موقعها الإلكتروني تنظيم قائمة لمناصب عمل شاغرة تتضمّن على روابط إحالة نحو الموقع الأصلي لشركة(Stepstone France) الذي يُتيح عروض حول إعلانات مناصب العمل، حيث طلبت هذه الأخيرة من رئيس المحكمة(بتاريخ 30 أكتوبر 2000)، إصدار أمر يُلزِم شركة(Ofir France) تحت الغرامة التّهديديّة(**jour** par 600 000F)، بإلغاء محتوى مواقعها الإلكترونية التي تتضمن على جميع المعلومات ou Annonces, CV, informations) (autres الواردة في الموقع الإلكتروني الأصلي(Stepstone France)، مع إدانتها بدفع غرامة مالية تقدّر بـ(30 000 F) إلى جانب دفعها للمصاريف القضائية.

لذا لم يرى قاضي الاستعجال في طريقة الإحالة أيّ ضرر مُسّبب لشركة Stepstone) (France على مستوى حقوق الملكية الفكرية، أو ناتج عن عمل منافسة غير مشروعة، أو تشويه لصُورة الموقع الأصلي، وذلك لكون أنّ شركة(Ofir France) لا تقترح إعلانات التّشغيل الواردة في الموقِع الأصلي(Stepstone France)، بل قائمة مناصب عمل تحتوي على روابط إحالة تُساعِد مُستخدم الإنترنت من الوصول إلى قاعدة بيانات الموقع الأصلي، للحصول على المعلومات الكاملة المتعلّقة بإعلانات التّشغيل التي تَهُمُّهُمْ، حيث أكّد القاضي الإستعجالي بأنّ روابط الإحالة من مبادئ نظام عمل الإنترنت وتُستعمل بكل حريّة.

---

2) L'article 3, paragraphe 1, de la directive 2001/29 doit être interprété en ce sens qu'il s'oppose à ce qu'un État membre puisse protéger plus amplement les titulaires d'un droit d'auteur en prévoyant que la notion de **communication au public** comprend davantage d'opérations que celles visées à cette disposition. »

1) **T.com de Nanterre**, Ordonnance de référé du 8 novembre 2000 Sarl Stepstone France c/ Sarl Ofir France. https://www.legalis.net(consulté le 22/03/2018.)

« […]; Que la raison d'**être d'Internet** et ses principes de **fonctionnement** impliquent nécessairement que des liens hypertextes et intersites puissent être effectués **librement**, surtout lorsqu'ils ne se font pas, comme en l'espèce, directement sur les pages individuelles du site référencé ;

Que la société **Ofir France** ne porte atteinte à **aucun** droit de propriété intellectuelle, et n'exerce aucun acte de concurrence manifestement **déloyale** ou donnant une image **négative** du site sur lequel le lien est effectué, actes qui pourraient justifier les demandes de la société Stepstone France ; […]. »

فإذا كانت طريقة الرّوابط السّطحيّة(Lien en surface) لا تُثير جدلا كبيرا، فإنّ بقيّة تقنيات روابط الإحالة على غرار الرّوابط الآليّة(Lien automatique) والإطاريّة (Le cadrage) والعميقة(Liens profonds)، تؤدّي في معظم تطبيقاتها إلى الاعتداء على حقوق الملكيّة الفكريّة، والمساس بالممارسات التّجارية المشروعة[1]، كتقليد العلامة واستخراج وجمع البيانات بصفة جزئيّة أو كليّة من مضمون قاعدة البيانات من دون أي ترخيص من أصحابها، حيث يعدّ ذلك اعتداء على العلامة وقاعدة البيانات المحميّة وفقا لقوانين الملكيّة الصّناعيّة[2]، أو الاعتماد في رابط الإحالة على اسم موقِع يتضمّن على علامة تجاريّة محميّة، ممّا يُشّكلُ اعتداء على حقوق الملكيّة الصّناعيّة، أو اعتماد موقِع تجاري على روابط عميقة(Deep links) من دون المرور عبر صفحة الاستقبال للموقع التّجاري المحَال إليه(Site relié)، أو يكون الغرض من وراء استعمال رابط الإطار(Framing) عدم استهداف الإعلانات الإشهاريّة التي تمّت عبر الموقِع المُحَال إليهِ، فلا شّك أن من بين هذه الأفعال ما يُعد من قَبِيلِ المنافسة غير المشروعة، حيث يمكن للطرف المُتضّرر مباشرة إجراءات دعوى المنافسة غير المشروعة أمام القضاء المختص.

---

1) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., pp. 19-27.

2) **TGI** de Paris, 3ème ch, 1ère section, 5 septembre 2001, SA Cadremploi c/ SA Keljob et Sté Colt Télécommunications France. https://www.juriscom.net/txt/jurisfr/ ou https://www.legifranec.gouve.fr(consultés le 10/05/2017.)

« […]. Attendu qu'en reproduisant ainsi **sans autorisation**, dans le cadre de son service de sélection d'offres d'emploi, la **marque** dont la société CADREMPLOI est titulaire, la société KELJOB commet des actes de **contrefaçon** prohibés par l'article L 713- 2 du Code de la propriété intellectuelle ; que cette exploitation est bien effectuée à des fins commerciales, et non dans le seul but désintéressé d'informer l'utilisateur ; que la société KELJOB tire ainsi profit de la réputation de sérieux de la marque CADREMPLOI; […]. Attendu qu'il résulte de ces éléments que la société KELJOB **extrait** et **réutilise** quotidiennement une partie qualitativement substantielle de la **base de données** de la société CADREMPLOI, **sans** l'**autorisation** de cette dernière ; […]. Attendu que la société KELJOB, en agissant **ainsi**, porte **atteinte** aux droits de la société CADREMPLOI sur sa **base de données**, et tire profit des investissements considérables effectués par cette dernière pour la constituer et la mettre à jour ; qu'elle s'approprie **indûment** le travail et les efforts de la demanderesse en réutilisant à son profit une partie substantielle de cette base ; […]. »

وفي هذا الصدد، اعتبرت المحكمة التّجارية لباريس في 26 ديسمبر 2000 بمناسبة القضية التي جمعت بين محرّك البحث(SA Keljob) مع شركتي (SNC Havas Numérique et SA Cadres on Line)، أنّ الرّوابط العميقة من شأنها أن تؤدّي إلى المنافسة غير المشروعة وتطبيقها يُعد عملا مخّلا بقواعد العرض السّليم للمصّنف الرّقمي، حيث نُسِبَ إلى مُحرّك البحث تعمّده تعديل أو تغيير وسوم أو أكواد لغة برمجة صفحات الويب، وإخضاعها للرّوابط العميقة مع عدم الكشف عن عناوينها الأصليّة(Cadresonline.com)، وبالمقابل ردّت شركة(Keljob) بأنّه لا توجد قاعدة قانونيّة تُلْزِمُ بأن يكون صاحب الموقع الإلكتروني على عِلم أو دِراية بهذا التّرابط، حيث عادت المحكمة إلى أحكام قانون الملكيّة الفكريّة التي أكّدت بأنّ عرض المصّنف من دون إذن صاحبه يعتبر عملا مُضرّرًا، وأنّ حُسن استغلال المواقع الإلكترونيّة يتطلّب إعلام أصحابها، وتُضيف المحكمة بأنّه إذا حصل الإجماع حول استعمال الرّوابط السّطحيّة وفقا للموافقة الضّمنيّة لأصحاب مواقع الويب، فإنّ إخضاع المواقع للرّوابط العميقة بدون المرور عبر صفحة الاستقبال يُعدّ عمل غير مشروع.

وفي النّهاية حدّد القاضي الفرنسي الحالات التي يُعتبر فيها رابط الإحالة من قَبِيلِ المنافسة غير المشروعة ويمّس بالحقوق المملوكة للغَيْرِ:

– احتواء أو تشويه محتوى أو صورة الموقع الإلكتروني المُحَال إليهِ؛

– بعث الاعتقاد حول ملكيّة الموقِع الإلكتروني المُحَال إليهِ من دون الإشارة إلى مصدره وإخفاء عنوانه الأصلي، مع إظهار عنوان الموقِع الإلكتروني الذي أنشأ رابط الإحالة.

– عدم إعلام مستخدم الإنترنت بطريقة واضحة وسليمة بحقيقة الموقِع موضوع الزّيارة، وعدم الإشارة بصفة مكتوبة وواضحة إلى مرجع وعنوان الموقِع الإلكتروني المُستهدف.

والجدير بالذّكر، أنّ قاضي الموضوع لم يستجب لكامل طلبات المُدّعي (Cadres on line) الذي أسّسها وفقا للمنافسة غير المشروعة وتدليس علامة الصّنع، بل اكتفى بإلزام المُدّعَى عليهِ(Keljob) بإنهاء المنافسة غير المشروعة[1].

---

[1] **T.Com** de Paris, réf., 26 décembre 2000, SNC Havas Numérique et Sté Cadres On Line c/ SA Keljob. https://www.juriscom.net/txt/jurisfr/(consulté le 16/05/2017.)

ثالثا– حماية المصّنفات الرّقميّة بدعوى المسؤوليّة عن الفعل الشّخصي.

تعتبر المسؤوليّة التّقصيريّة(La responsabilité délictuelle) فرع من المسؤوليّة المدنيّة حيث تنشأ عن الإخلال بالتزام فرضه القانون، من خلال تعويض الضّرر المرتكب من دون تواجد علاقة عقديّة بين المسؤول عن هذا الضّرر وبين الشّخص المتضّرر، وذلك على عكس المسؤوليّة العقديّة التي تترتّب عن عدم تنفيذ الإلتزام النّاشئ عن العقد، في حين تعّد المسؤوليّة عن الأعمال الشّخصيّة نوع من أنواع المسؤوليّة التّقصيريّة التي قسّمتها الإرادة التّشريعيّة لمختلف الدّول وفقا للأحكام العامّة للمسؤوليّة المدنيّة[1]، حيث تقوم المسؤوليّة عن الفعل الشّخصي على أساس إثبات الخطأ، وهذا ما أكّده المشّرع الجزائري بموجب المادة 124 من التّقنين المدني[2] التي تنص:" **كل فعل أيّا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض.**"

« […]. Que, par ailleurs, le **bon usage** des possibilités offertes par le réseau Internet **commanderait**, pour le moins, de **prévenir** le propriétaire du site cible ; Que si la pratique des liens hypertextes peut favoriser le développement du réseau Internet, c'est à la condition **sine qua non** du **respect** incontournable des lois et règlements qui régissent le droit de la propriété intellectuelle;

Attendu, au surplus, que **s'il est admis** que l'établissement de liens hypertextes **simples** est censé avoir été implicitement **autorisé** par tout opérateur de site Web, il **n'en va pas** de même pour ce qui concerne les liens dits "**profonds**" et qui renvoient directement aux pages secondaires d'un site cible, sans passer par sa **page d'accueil** ;

Attendu, en conséquence, que toute **création** d'hyperliens entre les sites du réseau Internet, quelle que soit la méthode utilisée et qui aurait pour conséquence : - de détourner ou dénaturer le contenu ou l'image du site cible vers lesquels conduit le lien hypertexte,

- faire apparaître ledit site cible comme **étant le sien**, sans mentionner la **source**, notamment en ne laissant pas apparaître l'adresse URL du site lié et, de plus, en faisant figurer l'adresse URL du site ayant pris l'initiative d'établir ce lien hypertexte,

- de **ne pas signaler** à l'internaute, de façon **claire** et sans **équivoque**, qu'il est dirigé vers un site ou une page Web extérieur au premier site connecté, la référence du site cible devant obligatoirement, clairement et lisiblement être indiquée, notamment, son adresse URL,

Sera considérée comme une **action déloyale**, **parasitaire** et une appropriation du travail et des efforts financiers d'autrui même si, dans le cas d'espèce, la société **Keljob**, simple moteur de recherche sur Internet, déclare ne pas exercer la même activité que la société **Cadres on Line**, et ainsi ne pas être en concurrence avec elle ; […].».

[1] **عايد رجا الخلايلة**، مرجع سابق، ص ص 67، 68.

[2] أمر رقم 75– 58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، المعدل والمتمم بموجب القانون رقم 05– 10 المؤرخ في 20 جوان 2005، ج ر عدد 44 الصادر في 26 جوان 2005.

كما نص المشّرع الفرنسي على ذلك، بموجب المادتين 1382 و1383 من التّقنين المدني، التي من خلالها ألزم كلّ مرتكب لخطأ، سبّب في حدوث ضرر للغير، بالتّعويض ويتحمّل المسؤوليّة سواء كان الخطأ عمدي أو بسبب الإهمال وعدم توّخي الحذر[1].

بالإضافة إلى ذلك، ألزم المشّرع الفيدرالي السّويسري بدوره بموجب المادة 1/41–2 من تقنين الالتزامات، الشّخص الذي ألحق بطريقة غير مشروعة ضررا للغير، بالتّعويض سواء كان ذلك عمدا أو بالإهمال أو عدم الاحتياط[2].

انطلاقا من ذلك، يُمكن للطرف المتضّرر من تسجيل أحد عناصر الملكيّة الفكريّة المحميّة في صورة اسم موقع، مُباشَرة إجراءات رفع دعوى المسؤوليّة التّقصيريّة بمجرّد ثبوت توافر أركانها الثلاثة(الخطأ، الضّرر والعلاقة السّببية بينهما)[3]، حيث يعتبر صاحب الموقع الأصلي المسؤول الرّئيسي عن المحتوى والتّطبيقات التي ينظِّمُها(على عِلمِهِ) بالموقِع التّابع له دون غيره، في حين لا يُمكن أن يُسأل صاحب الموقع الأصلي عن محتوى لم يَقِفْ على فَحْوَاهُ أو لم يتمكّن من معرفة ما يتضمّنه، فإذا كانت عملية الإحالة نحو موقع إلكتروني آخر تعتبر مشروعة بشرط عدم "عِلم" صاحب الموقِع الذي قام بالإحالة، بأنّ الموقع الإلكتروني المُحال إليهِ يحتوى بطريقة غير مشروعة على مصّنفات رقمية محميّة، فإنّ القضاء اعتبر معيار العِلم بالمحتوى غير المشروع على أساس "الافتراض" في حالة ما إذا كان الموقِع

---

1) **Code civil(France)** - Dernière modification le 23 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr
Art.1382: « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. »
Art.1383 : « chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »

2) **Loi fédérale** complétant le Code civil suisse (**Livre cinquième**: Droit des obligations) du 30 mars 1911, RS 220 (État le 1er novembre 2019).
Art.41: « 1- Celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer .
2- Celui qui cause intentionnellement un dommage à autrui par des faits contraires aux mœurs est également tenu de le réparer. […].»

3) **شريف محمد غنام**، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني (Name Domain)، مرجع سابق، ص ص 164– 169.

الإلكتروني الذي قام بالإحالة ذات طابع ربحي، وهذا ما أكّدته محكمة العدل الأوروبية بموجب قرارها الصادر بتاريخ 08 سبتمبر 2016[1]، الذي من خلاله اعتبرت معيار العِلم بالمحتوى غير المشروع "مُفترض" بالنّسبة لصاحب الموقِع الإلكتروني ذات الطّابع الرّبحي، الذي أنشأ روابط إحالة نحو موقع إلكتروني يتضمّن على محتوى غير مشروع، حيث لم تُميّز المحكمة الأوروبية في قرارها بين روابط الإحالة(Liens hypertextes).

فإذا كان صاحب الموقع الإلكتروني الأصلي يعتبر المسؤول الرئيسي عن المحتوى غير المشروع الذي يُنظّمه بالموقع التّابع له دون غيره، فإنّه يمكن إمداد المسؤوليّة لأصحاب المواقِع الذين أنشئو الإرتباط نحو المُحتوى غير المشروع، ما دامَ أنّه لا يوجد ما يَمْنَعُ من مُساءلتِهم على أساس "المشاركة" إذا تحقّقت شروط المسؤوليّة المدنيّة أو الجزائيّة[2].

حيث مدّد القضاء البلجيكي مفهوم المشاركة إلى تطبيقات الإحالة لغرض تَتبُّع صاحب الموقِع الذي أَوْرَدَ روابط الإحالة، وذلك بمناسبة القضية التي طُرحت بتاريخ 21 ديسمبر 1999 أمام قاضي الاستعجال البلجيكي للمحكمة الابتدائيّة (Le tribunal de première instance d'Anvers, statuant en référé)، التي جمعت بين شركة(I.F.P.I) مع الطالب الجامعي(Beckers W.)، الذي أتاح عبر موقِعه الإلكتروني بطريقة غير قانونية روابط إحالة

---

1) **Arrêt** de la C.JU.E (2ème ch.), du 08/09/2016, GS Media BV c/ Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker, (Affaire C-160/15). https://www.curia.europa.eu/juris/document/(consulté le O6/01/2018.)

« […]. Par ces motifs, la Cour (deuxième chambre) dit pour droit :

L'article 3, paragraphe 1, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, doit être interprété en ce sens que, afin d'établir si le fait de placer, sur un site Internet, des **liens hypertexte** vers des œuvres protégées, librement disponibles sur un autre site Internet **sans** l'autorisation du titulaire du droit d'auteur, constitue une « **communication au public** » au sens de cette disposition, il convient de déterminer **si** ces liens sont fournis sans **but lucratif** par une personne qui **ne connaissait** pas ou **ne** pouvait raisonnablement pas connaître le caractère **illégal** de la publication de ces œuvres sur cet autre site Internet **ou si**, **au contraire**, lesdits **liens** sont fournis dans un **tel but**, hypothèse dans laquelle cette connaissance doit être **présumée**. »

2) **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., pp. 27- 33.

علي كحلون، مرجع سابق، ص ص 191– 195.

نحو مواقع إلكترونية تتضمّن على مصّنفات موسيقيّة محميّة، لتَمْكِينِ مُستخدمي الإنترنت بتحميلها بصيغة(MP3) ومن دون دفع الحقوق المكتسبة لصاحبها(I.F.P.I).

لذا أمر القاضي المدّعَى عليهِ(Étudiant) بغلق موقعه الإلكتروني الذي يتضمّن على أكثر من 25,000 رابط إحالة نحو مصّنفات رقميّة غير مشروعة، وأكّد(القاضي) على أنّ روابط الإحالة ليست ببساطة كمراجع في أسفل صفحة الويب(Note de bas de page)، فبمجرّد النّقر على الرّابط يتحقّق الوصول إلى الموقع الإلكتروني، الذي لا يمكن الوصول إليه إلاّ بتحديد عُنوانُه مع النّقر على رابط الإحالة، الذي تم إحداثه لهدف تقديم المُساعدة وتوفير المفتاح الأساسي للتّحميل بطريقة غير مشروعة، وهذا المفتاح هو العنصر الأساسي في ارتكاب الجريمة، ويجعل صَاحبَه(Étudiant) مَسْئُولاً[1].

كما أكّدت محكمة الاستئناف(CA d'Aix-en-Provence) في قرارها الصادر بتاريخ 10 مارس 2004، حُكم المحكمة الابتدائية(T corr. de Draguignan) الصادر بتاريخ 18 أفريل 2002، الذي حكم على المتّهم(A. Emmanuel) في القضية التي جمعته مع الشركات (SA Atari, SA Infogrammes Europe, SA Take two, et autres.)، على أساس المشاركة في تقليد المصّنفات الرّقميّة المحميّة، الذي من خلاله قام المتّهم عبر موقعه

---

[1] **Tribunal** de Première Instance d'Anvers (référé), 21 déc. 1999, I.F.P.I. Belgium c/ Beckers Werner Guido, (R.G. 99/594/C). Décision confirmée en appel le 21 juin 2001, (R.G. 99/23830/C). Disponible sur le site: http://www.droittechnologie.org, [rubrique jurisprudence], (consulté le 13/01/2019.)

« […]. qu'un hyperlien n'est pas simplement une note de bas de page. En activant un lien de cette nature, un accès est donné à un site. Pour obtenir un accès à un site, il doit être possible de le localiser et de l'activer. Créer un hyperlien a précisément pour but de fournir ce service à l'utilisateur potentiel. En l'espèce, le défendeur a, sciemment et en pleine connaissance de cause, établi des liens vers des sites qui permettent de télécharger de manière illicite de la musique, c'est-à-dire sans payer les droits requis. »

Voir aussi : **Thibault VERBIEST et Etienne WÉRY**, « La responsabilité des fournisseurs de services Internet : derniers développements jurisprudentiels », Journal des tribunaux, 17 février 2001, 120e année - N° 6000, p. 171. Disponible sur le site: http://www.droittechnologie.org, consulté le 11/01/2019.

الالكتروني(www.disco.fr) الذي أنشأه في سبتمبر 2000، بإحداث روابط إحالة نحو مواقع إلكترونية آخرى تُتيح إمكانية تحميل برمجيات الألعاب المقلّدة بكل سهولة [1].

الفرع الثاني
الحماية الجزائيّة للمصنّفات الرّقميّة

يُعتبر الاعتداء على أحد حقوق الملكيّة الفكريّة الصّناعيّة جنحة تقليد معاقب عليها بموجب القوانين المتعلّقة بحماية الملكيّة الصّناعيّة(**أولا**)، حيث يمكن رفع الدّعوى الجزائيّة وتأسيسها وفقا للأحكام الواردة بموجب القانون رقم 04–02 المتعلّق بالقواعد المُطبّقة على الممارسات التّجاريّة(**ثانيا**).

أولا– حماية المصنّفات الرّقميّة بدعوى التّقليد.

يعتبر التّسجيل كشرط أساسي لحماية المصنّفات الرّقميّة بدعوى التّقليد فبمجرد إثبات وتكييف الفعل المشّكل لجنحة التّقليد، يحقّ للطرف المتضّرر في رفع دعوى المسؤوليّة الجزائيّة أمام الجهة القضائيّة المختصّة على أساس جنحة التّقليد، حيث لا تقتصر جريمة التّقليد على الحقوق الأدبيّة للمؤلف والحقوق المجاورة له، بل تمّس كذلك الحقوق الماليّة المتعلّقة بالملكيّة الصّناعيّة والتّجاريّة، وفي كلّ الظروف، يجب على القاضي الجزائي مراعاة مبدأ الشّرعية في فرض العقاب(Principe de légalité pénale)، حيث لا يُمكن مُعاقبة أيّ

---

1) **CA d'Aix-en-Provence**, 5ème Ch, 10 mars 2004, A. Emmanuel c/ S.E.V., SA INFOGRAMMES EUROPE, SA TAKE TWO, et Autres, Arrêt n° 04/192. Disponible sur les sites : https://www.doctrine.fr et https://www.legalis.net(consultés le 15/01/2019.)
« […].Que les premiers juges ont également relevé que, si A Emmanuel ne proposait pas aux internautes le téléchargement direct de logiciels de jeux contrefaits, il faisait néanmoins apparaître sur son site des **liens** renvoyant à d'autres **sites** proposant **le téléchargement illégal** de tels jeux; qu'ils ont justement retenu que cette **mise** à disposition de **liens hypertexte** devait s'analyser en une **complicité de contrefaçon** par fourniture de moyens;
Attendu qu'il convient de confirmer purement et simplement le jugement déféré du chef de la culpabilité; […].
Réformant sur la peine, Condamne A Emmanuel à une amende de 5,000 € avec sursis.
L'avertissement prévu à l'article 132·29 du code pénal n'ayant pu être donné au condamné en raison de son absence. Ordonne la publication du présent arrêt par extraits, aux frais du condamné, dans le journal Var Matin. […].Confirme le jugement déféré en toutes ses dispositions civiles. […]. »

شخص عن فعلٍ أيًا كان لم يُجَرِّمُهُ القانون أو لم يُعاقب عليه، وبالتّالي فإنّ العقاب يتطلّب ارتكاب الشّخص للفعل المجرم على أساس النّص القانوني الذي يعاقب على ذلك الفعل[1]، فمباشرة الدّعوى العموميّة على أساس جنحة التّقليد، تستوجب توافر الركنان الأساسيان في الجريمة، والمتمثّلان في الركن المادي والمعنوي للجريمة[2].

فالرّكن المادي للجريمة لا يتعلّق فقط بارتكاب سلوك إجرامي وحدوث نتيجة معيّنة، بل يستوجب كذلك توافر العلاقة السّببية بين الفعل والنتيجة، حيث يجب أن يكون الفعل الإجرامي هو الذي أدّى إلى تحقيق النتيجة وحدوثها، في حين نجد أنّ القانون لا يعاقب على مجرّد النّوايا أو التّصميم على ارتكاب الجرائم، بل يتطلّب تطبيق هذه الأفكار والنّوايا وإخراجها إلى حيّز المادّيات، فجريمة التّقليد إذاً تقع ولو لم يحقّق المجرم أرباحا من وراء اعتدائه على الحقوق المحميّة، فلكي يتحقّق الرّكن المادي في جريمة التّقليد يجب توافر الشّروط التّالية[3]:

1- أن يكون الشيء الذي تعرّض للتّقليد محل الحماية بموجب القانون: حيث ينبغي أن يقع الاعتداء خلال الفترة القانونيّة للحماية، وليس بعد نهايتها من دون تجديدها، أو إبطالها في حالة عدم استعمال المصّنف المحمي خلال المدّة المحدّدة قانونا، أو في حالة عدم تسديد

---

[1] راجع أحكام المواد من 151 إلى 160 من الأمر رقم 03- 05 المؤرخ في 19 جويلية 2003، الذي يتعلق بحقوق المؤلف والحقوق المجاورة، سالف الذكر،

راجع أحكام المادة 26 من الأمر رقم 03-06 المؤرخ في 19 جويلية 2003، الذي يتعلق بالعلامات، ج ر عدد 44 الصادر في 23 جويلية 2003.

راجع أحكام المواد من 56 إلى 61 من الأمر رقم 03-07 المؤرخ في 19 جويلية 2003، الذي يتعلق ببراءات الاختراع، سالف الذكر.

راجع أحكام المواد من 35 إلى 41 من الأمر رقم 03-08 المؤرخ في 19 جويلية 2003، الذي يتعلق بالتصاميم الشكلية للدوائر المتكاملة، سالف الذكر.

[2] **شريف محمد غنام**، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني Name Domain)، مرجع سابق، ص ص 158، 159.

[3] **زواوي الكاهنة**، مرجع سابق، ص ص 200- 203.

رسوم الإبقاء أو التّجديد الموافقة لتاريخ الإيداع، أو بناءً على حكم أو قرار صادر من الجهة القضائيّة المختصّة سواء كان ذلك بأثر رجعي أم لا، وبالتّالي انتقال الحقوق المحميّة للملك العام، أو تدخل في إطار الإباحات والرخص العامّة.

2- يجب أن يكون الحق المعتدى عليه متعلّقا بملك الغير: حيث يُشترط في جريمة التّقليد أن يكون المصّنف المحمي قد تعرّض لاعتداء من جانب الغير، وذلك من دون أيّ ترخيص من طرف صاحب الحق مَحَل الحماية.

3- أن يقع اعتداء مباشر أو غير مباشر على الحق المحمي: يُشترط كذلك في تحقّق الرّكن المادي لجريمة التّقليد قيام المعتدي مباشرة باصطناع حق من حقوق الملكيّة الفكريّة في صورة مطابقة تماما أو مُشابهة لما هو موجود في الحق الأصلي المحمي، حيث تكفي عملية النّقل الكليّة أو الجزئيّة لإبراز تواجد التّقليد، كما يمكن أن يقع الاعتداء بصورة غير مباشرة على حق مملوك للغير من خلال استغلاله لغرض الإيجار أو التّقليد أو البيع الخ...

وعليه، فإنّ الرّكن المادي للجريمة لا يكفي لوحده لقيام جريمة التّقليد، بل يُشترط أن يصدر الفعل المادي عن إرادة سليمة لشخص مُدرِك لأفعاله، حيث تشّكل الإرادة والإدراك الرّكن المعنوي للجريمة العمديّة وغير العمديّة، فجريمة التّقليد كغيرها من الجرائم العمديّة، يجب أن يتوافر فيها القصد الجنائي بنوعيه العام أو الخاص[1]، حيث يعني بالقصد الجنائي العام ارتكاب جريمة التّقليد وفقا لإرادة مُرتكبها، مع علم هذا الأخير بتوافر أركان الجريمة وفقا لما يتطلّبه القانون، بينما القصد الجنائي الخاص يعني السّبب والمصلحة الدّافعة إلى ارتكاب جريمة التّقليد، حيث أنّ الباعث يتغيّر ويختلف من جريمة إلى أخرى، أمّا القصد العام يبقى واحد لا يختلف من جريمة إلى أخرى، في حين نجد أنّ القانون يكتفي بتواجد القصد العام لقيام الجريمة في معظم جرائم التّقليد ولا يهتّم بالباعث إلى ارتكابها، بينما يُعتبر

[1] **أحسن بوسقيعة**، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر، الطبعة 10، الجزائر، 2011، ص ص 120، 121، 128، 129.

الباعث في بعض جرائم التّقليد عنصرا إضافيا لقيام الرّكن المعنوي، حيث أنّ غياب الباعث لا يكتمل الرّكن المعنوي ولا تقوم جريمة التّقليد.

انطلاقا من ذلك، أصبحت عمليات التّقليد غير المشروعة في عصرنا الرّقمي تُرتكب من طرف أشخاص ذوي كفاءات عالية، ويتقنون استعمال لغات البرمجيات وتعديلها أو تغييرها بما يتوافق مع تقنيات روابط الإحالة، على غرار الرّوابط العميقة أو الإطاريّة أو الآلية، المستعملة بطريقة غير مشروعة في ارتكاب جرائم التّقليد على أحد عناصر الملكيّة الفكريّة المحميّة بموجب القوانين الخاصّة بها، إذ يمكن لإحدى الشّركات المنافسة أن تقوم بطريقة غير مشروعة اعتماد اسم موقع إلكتروني كمُصوّب(Pointeur)[1] يتضمّن على اسم علامة أو اسم تجاري محمي، لغرض جذب الزّائرين وتحقيق مكاسب وأرباح على حساب الموقِع الإلكتروني المُحَال إليهِ، فبِمُجرّد قيام المستهلك بالنّقر في صفحة الويب على المُصوّب تتّم عملية الإحالة مُباشرة إلى صفحات الموقِع المُحَال إليهِ، من دون عِلْمِ المُستهلك بالعنوان الأصلي لصفحة ويب المفتوحة على شاشة حاسوبه(Framing)، أو يتّم الوصول إلى تلك الصّفحة من دون المرور عبر الصّفحة الأصليّة للموقِع المُحال إليهِ(Deep linking)، أو يتّم ذلك بطريقة آلية من دون تدّخل المستهلك أو عِلمه بالعنوان الإلكتروني لصفحة الويب المفتوحة(Inlining)، حيث تُكَيَّفُ كلّ هذه الأفعال على أساس جريمة تقليد يُعاقب عليها وفقا للقوانين المتعلّقة بحماية حقوق الملكيّة الفكريّة.

فإذا كانت طريقة تنظيم المُصوّب(Pointeur) المُلحقَة بنظام الإحالة لا تمّس "مَبدئيًا" بحقوق الملكيّة الفكريّة، حيث يمكن لصاحب الموقِع الإلكتروني أن يُورِدَ عبر محتوى صفحات الويب لعناوين المواقع المحالَة إليها من دون الحصول على التّرخيص المُسبق من أصحابها، ما دَامَ أنّ روابط الإحالة السّطحيّة لا تمّس بحقوقهم المحميّة وتُستعمل بطريقة

---

1) La commande HTML de base utilisée est : <A REF="URL de la page sur laquelle on fait un lien">pointeur</A>. - **Alain STROWEL, Nicolas IDE**, (2ème partie: la responsabilité en matière d'hyperliens), op.cit., p. 07.

مشروعة عبر الإنترنت، وهذا ما أقرّه القضاء في أكثر من مناسبة[1]، فإنّ بعض تقنيات روابط الإحالة المستعملة تؤدّي إلى الاعتداء على حقوق الملكيّة الفكريّة المحميّة، حيث أكّدت ذلك المحكمة البريطانية بمناسبة القضية التي جمعت بين شركة(Shetland News) مع جريدة (The Shetland Times)، التي من خلالها قامت الشّركة الأولى عبر موقعها الإلكتروني بتقليد عناوين المقالات المنشورة لجريدة(The Shetland Times) بنسختها الورقيّة، حيث أنّ هذه الأخيرة لا تحقّق أرباح عن طريق الإشهار، وذلك بالمقارنة مع شركة(Shetland News) الذي يتوافر موقعها الإلكتروني على إعلانات (Bannières publicitaires)، فبمجرّد قيام المستهلك بالنّقر على عناوين المقالات المقلّدة، يتّم إحالته إلى صفحة موقع جريدة(The Shetland Times) من دون أن يُدركَ عنوان صفحة الإحالة.

لذا أكّد القاضي بموجب الأمر الصادر في 24 أكتوبر 1996، أنّه من المُحتملِ أن تكون بعض عناوين المقالات المقلّدة محميّة بموجب قانون حق المؤلف (Copyright, Design and Patent Act de 1988)، وأنّه من الضّروري أن تقع الإحالة عبر صفحة الاستقبال الأصليّة التّابعة للموقع المُحَال إليهِ(The Shetland Times)، حيث انتهت القضية أثناء جلسة النّظر في الموضوع بصلح بين الأطراف، الذي من خلاله يحتفظ موقِع شركة(Shetland News) بروابط الإحالة باستعمال عناوين المقالات كمُصوّب، بشرط احترام حقوق المؤلف المحميّة المملوكة لجريدة(The Shetland Times)[2].

كما قضت المحاكم الفرنسية على أساس جنحة التّقليد في عمليات الإحالة إلى المصّنفات الرّقميّة المحميّة، التي تمّت من دون الحصول على ترخيص مُسبق من المؤلف، حيث حكمت المحكمة الابتدائية لـ(TGI, de Saint-Étienne) بتاريخ 06 أكتوبر 1999، وفقا لهذا

---

1) **Alain STROWEL, Nicolas IDE,** (2ème partie: la responsabilité en matière d'hyperliens), op.cit., pp. 09- 12.

2) Ibid., pp. 15, 16.
Shetland Times Ltd v. Dr. Jonathan Wills, Court of Session: Outer House, (1996) Outer House Cases, 24 oct. 1996. Disponible sur les sites: https://www.lectlaw.com/files/elw10.htm ou http://www.netlitigation.com/netligation/cases/shetland.htm (consultés le 19/12/2018.)

الأساس على كل من المتّهم(F. Battie et V. Roche) بصدد القضية التي جمعتهم مع الشّركات(SACEM/SDRM et S.C.P.P. et autres.)، التي من خلالها قام المتّهمان عبر الموقع الالكتروني(MP3-Albums) الذي أحدثه السّيد(V.R) في شركة (NET SYSTEM FRANCE ©) التي كان يعمل فيها، بإحداث روابط إحالة بطريقة غير قانونية نحو مصّنفات رقميّة مُتواجدة في مواقع إلكترونية تّم إيواءها مجانياً لدى شركة(GEOCITIES) بالولايات المتّحدة الأمريكيّة، تُتيح(Liens) لكل زائر للموقِع(MP3-Albums) إمكانية تحميل هذه المصّنفات بصيغة(MP3) بسهولة، ومن دون الحصول على أيّ ترخيص مُسبق من أصحاب حقوق المؤلف، حيث حَكَمَ القاضي على المتّهمين بجنحة التّقليد على أساس المادتين(L 335-2 et L 335-4) من تقنين العقوبات إلى جانب الحبس مع دفع الغرامات المالية، في حين لم يُوضّح في حُكْمِهِ طبيعة حق المؤلف المُعتدَى عليهِ[1].

ثانيا– الحماية الجزائيّة المزدوجة لأعمال المنافسة غير المشروعة.

يمكن أن يترتّب عن أفعال الاعتداء على إحدى حقوق صاحب الملكيّة الفكريّة تحمّل مرتكبها المسؤوليّة الجزائيّة، إلى جانب المسؤولية المدنية المترتبة عن أعمال المنافسة غير المشروعة، حيث حكمت على هذا الأساس محكمة الاستئناف بباريس بمناسبة القضية التي جمعت بين شركة الإذاعة(NRJ) والسّيد(Jean-Paul B.) مع شركة (Europe 2 Communication)، التي من خلالها يملك السّيد(Jean-Paul B.) علامة خدمة (NRJ (n°

---

1) **TGI de Saint-Étienne**, 3ème ch, 6 décembre 1999, SACEM/SDRM et S.C.P.P. et Stuffed Monkey et S Sony Music et S Island et S Warner et X Recording Corporation, c/ M. V.V R et M. F. B, n° 99007491. Disponible sur le site : https://www.doctrine.fr(consulté le 21/12/2018.)
« […].Attendu qu'en reproduisant, en diffusant et en mettant à la disposition des utilisateurs du réseau Internet, futce à titre gratuit, des phonogrammes numérisés sans l'autorisation des cessionnaires des droits de reproduction, V R et F B se sont rendus coupables des délits de contrefaçon prévus par les articles L 335-2 et L 335-4 du **Code Pénal**. […]. »
Voir aussi : **TGI d'Épinal**, 24 octobre 2000, S.C.P.P c/ M. C S, n° 00006350. https://www.doctrine.fr(consulté le 21/12/2018.)
« […]. Attendu qu'en mettant à la disposition des utilisateurs du réseau INTERNET, même à titre gratuit, des phonogrammes numérisés sans l'autorisation des artistes et des producteurs, Monsieur S c s'est rendu coupable du délit de contrefaçon prévu par les articles L.335-2 et L.335-4 du **Code de la Propriété Intellectuelle**. […]. »

((1.206.811 تخص اتصالات السّمعي البصري، المودعة لدى المصلحة الرّسميّة المختصّة بتاريخ 17 جوان 1982، والتي استغلتها فِعليًا شركة الإذاعة(NRJ) بترخيص من مالكها، حيث قامت شركة(Europe 2) المنافسة لشركة الإذاعة(NRJ) بتقليد علامة الخدمة عبر موقعها الالكتروني بصيغة(Anti-NRJ)، مع إنشاء رابط إحالة مباشرة إلى صفحة موقع إلكتروني سويدي تّم من خلاله إطلاق عبارات حقد وكراهية لإهانة وتشويه شركة(NRJ).

لذا قام الأطراف المتضّررة برفع دعوى قضائية ضّد شركة(Europe 2) أمام المحكمة الابتدائيّة باريس(TGI de Paris)، التي أصدرت حكم بتاريخ 30 جوان 1999، يقضي بأنّ إستعمال شركة(Europe 2) لمصطلح(Anti-NRJ) عبر موقعها، يُشَّكِلُ تقليد لعلامة الخدمة المملوكة للسّيد(.Jean-Paul B)، وأنّ المصطلح المستعمل يعتبر كمنافسة غير مشروعة لشركة(NRJ)، لكن المحكمة لم تُدِين شركة(Europe 2) على أساس المحتوى غير المشروع.

وبعد استئناف القضية من قِبَلِ الأطراف(.NRJ et Jean-Paul B) أمام محكمة الاستئناف بباريس(بتاريخ 04 أكتوبر 1999)، أصدرت هذه الأخيرة قرار بتاريخ 19 سبتمبر 1999 يقضي بأنّ شركة(Europe 2) ارتكبت أعمال تقليد للعلامة المملوكة للسّيد(.Jean-Paul B)، التي من خلالها تُؤسَّس أعمال التّشويه كمنافسة غير مشروعة بالنّسبة لشركة(NRJ)، وأنّ استعمال شركة(Europe 2) مصطلح(Anti-NRJ) في موقعها الإلكتروني، يُشّكلُ فعل تقليد بالنّسبة لمالك علامة(NRJ)، وأنّ فعل التّقليد المُرتكب يُشّكلُ تشويه ويُؤسّس كمنافسة غير مشروعة بالنّسبة لشركة الإذاعة(NRJ)، والمُلفت للانتباه، أنّ محكمة الاستئناف لم تُدين شركة(Europe 2) على أساس المحتوى غير المشروع لموقعها الالكتروني، بل ألزمتها فقط بإصلاح الضّرر مع تحمّل مصاريف نشر القرار والإجراءات القضائيّة [1].

---

1) **CA** de Paris, 4ème ch, 19 septembre 2001, NRJ et Jean-Paul B. c/ SA Europe 2 Communication. https://www.legalis.net(consulté le 22/02/2019.)

« […].dit qu'en reproduisant la mention "anti-NRJ" dans son propre site et en créant de manière délibérée un lien hypertexte avec la page d'un site suédois comportant la reproduction de la marque figurative n° 1.206.811 et(un texte dénigrant les prestations de la radio NRJ, la société Europe 2 Communication a commis des actes de contrefaçon de marque aux dépens de Jean-Paul B., lesquels sont constitutifs de concurrence déloyale à l'encontre de la société NRJ, et des actes de dénigrement constitutifs de concurrence déloyale aux dépens de la société NRJ ; confirme le jugement entrepris en

انطلاقا من ذلك، فإنّ الأصل في تأسيس دعوى المنافسة غير المشروعة وفقا للقواعد العامّة الواردة في التّقنين المدني الجزائري، كان على أساس الخطأ التّقصيري الذي نصت عليه المادة 124 من نفس التّقنين، غير أنّه بعد صدور القانون رقم 04–02 المتعلّق بالقواعد المُطبّقة على الممارسات التّجارية، أصبح هذا القانون المرجع الرئيسي لتأسيس دعوى المنافسة غير المشروعة، كما منح للمتضّرر (العون الاقتصادي) من الفعل الإجرامي إمكانية رفع الدّعوى الجزائيّة وتأسيسها وفقا لأحكام القانون رقم 04–02، سالف الذكر[1].

وعليه، تعتبر المخالفات والجنح الأكثر انتشارا في مجال الممارسات التّجارية غير النّزيهة، حيث تطبّق عليها، إلى جانب الحق في التّعويض عن الأضرار الماديّة والمعنويّة التي مسّت بالمُتضّرر، عقوبات أخرى تتراوح ما بين الحبس والغرامات الماليّة، والمصادرة، وبعض التّدابير التّحفظيّة الأخرى، كالحجز على المنتجات أو إتلافها أو غلق الموقِع التجاري الإلكتروني، أو الحكم بتعليق ونشر الحكم بالإدانة، حيث يُمْكِنُ لقاضي الموضوع المختص أن يحكم بناءً على القواعد الخاصّة بحماية حقوق الملكيّة الفكريّة، وذلك في حالة ما إذا كانت الحقوق مُودعة ومُسجَّلة، أو يعتمد على الأحكام الواردة في القانون رقم 04–02 المعدّل والمتمم المتضمّن القواعد المطبّقة على الممارسات التّجاريّة، الذي وضع حماية

---

ce qu'il a retenu que la mention "anti-NRJ" reproduite par la société Europe 2 Communication sur son site constituait à l'égard de Jean-Paul B. un acte de contrefaçon de marque; dit que cet acte de contrefaçon constitue un acte de concurrence déloyale aux dépens de la société NRJ et un acte de dénigrement; condamne la société **Europe 2** Communication à payer à Jean-Paul B. et à la société NRJ la somme de 250 000 F à chacun en réparation et celle de 25 000 F à chacun au titre de l'article 700 du nouveau code de procédure civile pour leurs frais irrépétibles en cause d'appel;
autorise Jean-Paul B. et la société NRJ à faire publier dans deux revues de leur choix aux frais de la société Europe 2 Communication le présent arrêt, dans les limites d'une somme de 50 000 F HT par insertion; confirme pour le surplus le jugement entrepris; rejette toute autre demande plus ample ou contraire; condamne la société Europe 2 Communication aux dépens et dit que ceux-ci pourront être recouvrés conformément aux dispositions de l'article 699 du nouveau code de procédure civile. »

[1] **حسين نوارة**، "الحماية القانونية للمستثمر الأجنبي في الجزائر"، رسالة دكتوراه في العلوم، تخصص: القانون، كلية الحقوق، جامعة مولود معمري– تيزي وزو، 2013، ص ص 465، 466.

قانون رقم 04–02 مؤرخ في 23 جويلية 2004 يحدد القواعد المطبقة على الممارسات التجارية، ج ر عدد 41 الصادر في 27 جويلية 2004، المعدل والمتمم.

جنائيّة مُزدوجة، وذلك في حالة ما إذا وقعت أفعال التّعدي على حقوق غير مُسجّلة أو وقعت قبل نشر تسجيلها، أو حتى الاستناد إلى أحكام القانون رقم 18–05 المؤرخ في 10 ماي 2018 المتعلّق بالتّجارة الإلكترونيّة، ما دام أنّ المُورّد الإلكتروني يَخْضَعُ للتّشريع والتّنظيم المتعلّق بالأنشطة التّجارية وحماية المستهلك[1].

1)– الجزاءات المفروضة في إطار القانون رقم 04–02 المتعلق بالقواعد المطبقة على الممارسات التجارية.

نص المشّرع الجزائري في إطار هذا القانون، على مجموعة من الجزاءات المطبّقة على المُمارسات التّجارية غير النزيهة، والتي يمكن تقسميها إلى العقوبات الأصليّة(**أ**)، والعقوبات التّكميليّة والتّدابير الاحترازيّة والتّحفظيّة(**ب**).

أ– **العقوبات الأصليّة:** تتمحور العقوبات الأصليّة في الحبس والغرامة الماليّة.

أ–**1**– **الحبس:** فوفقا للمادة 47 من القانون رقم 04–02 المعدل والمتمم بموجب القانون رقم 10–06 المؤرخ في 15 أوت 2010، المتضمّن القواعد المطبّقة على الممارسات التّجارية، فإنه في حالة ارتكاب العون الاقتصادي لإحدى الممارسات التّجارية غير النّزيهة المذكورة بالخصوص بموجب أحكام المادة 27 من نفس القانون[2]، كقيام العون الاقتصادي بتشويه سمعة عون اقتصادي منافس، عن طريق نشر معلومات سيئة تمّس بشخصه أو بمنتوجاته أو خدماته، أو تقليد علامات مميّزة لعون اقتصادي آخر منافس، أو تقليد منتوجاته أو خدماته أو الإشهار لغرض جذب وكسب زبائن هذا العون، من خلال زرع الشّكوك والأوهام في أذهان المستهلكين، كما تنصّب كذلك الممارسات التّجارية غير النّزيهة حول استغلال مهارة تقنيّة أو تجارية مميّزة من دون أي ترخيص من صاحبها أو الاستفادة من

---

[1] تنص **المادة 35** من القانون رقم 18–05 مؤرخ في 10 ماي 2018، الذي يتعلق بالتّجارة الإلكترونية، على ما يلي: " يخضع المورد الإلكتروني للتشريع والتنظيم المعمول بهما المطبقين على الأنشطة التجارية وحماية المستهلك."

[2] قانون رقم 04–02 مؤرخ في 23 جويلية 2004 يحدد القواعد المطبقة على الممارسات التجارية، ج ر عدد 41 الصادر في 27 جويلية 2004، المعدل والمتمم بموجب القانون رقم 10–06 المؤرخ في 15 أوت 2010، ج ر عدد 46 الصادر في 18 أوت 2010.

الأسرار المهنيّة، بصفة أجير قديم أو شريك للتّصرف فيها قصد الإضرار بصاحب العمل أو الشّريك القديم، في حين يمكن للعون الاقتصادي أن يقوم بإحداث خلل في تنظيم العون الاقتصادي المنافس له، من خلال استعمال طرق غير نزيهة لغرض تحويل زبائنه وتبديد أو تخريب وسائله الإشهاريّة واختلاس البطاقات أو الطّلبيات وإحداث اضطراب في شبكته للبيع والقيام بالسّمسرة غير القانونيّة الخ...، يُمكن لقاضي الموضوع المختص أن يَحْكُمَ إلى جانب العقوبات المسّلطة، بعقوبة الحبس من ثلاثة(03) أشهر إلى خمس(05) سنوات.

أ–2– الغرامة: يعاقب وفقا للمادة 37 من نفس القانون، على الممارسات التّجاريّة التّدليسيّة المذكورة في أحكام المادتين 24 و25 من ذلك القانون، بغرامة من ثلاثمائة ألف دينار(300.000 دج) إلى عشرة ملايين دينار(10.000.000 دج)، وتُضيف المادة 38 من نفس القانون على أنّه يُعاقب على الممارسات التّجارية غير النّزيهة والممارسات التّعاقديّة التّعسّفية المذكورة في المواد 26 و27 و28 و29 من نفس القانون، بغرامة من خمسين ألف دينار(50.000 دج) إلى خمس ملايين دينار(5.000.000 دج)[1].

ب– العقوبات التّكميليّة والتّدابير الاحترازيّة والتّحفظيّة: يمكن للقاضي الجزائي أن يحكم إلى جانب الجزاءات المفروضة بإحدى العقوبات الإضافيّة التّالية:

ب–1– الحجز: فوفقا لنص المادة 39 من نفس القانون، يمكن أن تتّم عملية حجز البضائع التي هي موضوع المخالفات المنصوص عليها بموجب أحكام المواد 4 و5 و6 و7 و8 و9 و10 و11 و12 و13 و14 و20 و22 و22 مكرر و23 و24 و25 و26 و27/2–7 و28 الواردة في ذلك القانون، أيا كان مكان وجودها، كما يمكن حجز العتاد والتّجهيزات التي استعملت في ارتكابها مع مراعاة حقوق الغير حسن النّية، حيث يمكن أن يكون الحجز في المخالفات التي تشكل منافسة غير مشروعة، إما حجزا عينيا أو ماديا السّلع موضوع المخالفة، أو حجزا اعتباريا في حالة كون هذه السّلع معنوية لا يمكن للمخالف تقديمها، كالحجز على بعض الأسرار التّجارية أو الصّناعيّة المتعلّقة بحقوق الملكيّة الصّناعيّة والتّجاريّة.

---

[1] قانون رقم 04–02 مؤرخ في 23 جويلية 2004 يحدد القواعد المطبقة على الممارسات التجارية، معدل ومتمم.

ففي حالة الحجز العيني تتّم عملية تشميع المواد المحجوزة بالشّمع الأحمر من طرف الأعوان المؤهّلين، حيث توضع تحت حراسة مُرتكب المخالفة في حالة امتلاكه لمحلاّت تخزين، وفي الحالة العكسيّة أي (عدم امتلاكه لمحلات تخزين) يخول الأعوان المؤهّلين مهمّة حراسة المواد المحجوزة إلى إدارة أملاك الدّولة التي تقوم بتخزينها في أي مكان تختاره لهذا الغرض، ففي كلتا الحالتين تكون المواد المحجوزة تحت مسئولية حارس الحجز إلى غاية صدور قرار العدالة، حيث تكون التّكاليف المتعلّقة بعملية الحجز على عاتق مُرتكب المخالفة، فإذا تجاوز إيداع المواد المحجوزة مدّة ستة(06) أشهر من دون أن يصدرَ حكم من العدالة، يمكن لإدارة أملاك الدولة بيعها بالمزاد العلني بموجب أمر من رئيس المحكمة المختصة، أين يُصّب ثمن البيع في حساب مؤقت إلى غاية صدور الحكم القضائي[1].

فعندما يقع الحجز على سلع أو مواد سريعة التلف أو تقتضي ذلك حالة السوق أو لظروف خاصّة، يجوز للوالي المختّص إقليميا، بناءًا على اقتراح المدير الولائي المكلّف بالتّجارة، وبعد قيام مصالح الولاية المختصة بالمراقبة الصحيّة للمواد المحجوزة، أن يقرّر(الوالي) من دون المرور بالإجراءات القضائيّة المسبقة، البيع الفوري للمواد المحجوزة أو تحويلها من طرف محافظ البيع، ومن طرف مدير أملاك الدولة الولائية إذا اقتضى الأمر ذلك، أو تحويلها مجانا إلى الهيئات والمؤسّسات ذات الطّابع الاجتماعي، وعند الاقتضاء يمكن إتلاف هذه المواد المحجوزة التي تضّر بالصّحة أو لكونها مغشوشة، بشكل يجعلها غير قابلة للاستعمال، حيث يودع المبلغ الناتج عن عملية البيع في خزينة الولاية إلى غاية صدور قرار العدالة[2].

---

[1] راجع أحكام المادة 41 من القانون رقم 04-02 المؤرخ في 23 جويلية 2004، الذي يحدد القواعد المطبقة على الممارسات التجارية، المعدل والمتمم، بموجب القانون رقم 17-11 المؤرخ في 27 ديسمبر 2017، الذي يتضمن قانون المالية لسنة 2018 ، سالف الذكر.

[2] راجع أحكام المادة 43 من القانون رقم 04-02 المؤرخ في 23 جويلية 2004، الذي يحدد القواعد المطبقة على الممارسات التجارية، المعدل والمتمم، بموجب القانون رقم 17-11 المؤرخ في 27 ديسمبر 2017، الذي يتضمن قانون المالية لسنة 2018، سالف الذكر.

أما في حالة الحجز الاعتباري، فإنّ قيمة المواد المحجوزة تُحدّد على أساس سعر البيع المطبّق من طرف مرتكب المخالفة، أو بالاعتماد على سعر السّوق، حيث يُدفع المبلغ النّاتج عن بيع السّلع المحجوزة إلى الخزينة العموميّة، في حين يُطبّق نفس الإجراء في حالة الحجز العيني عندما لا يتمكّن مرتكب المخالفة تقديم المواد المحجوزة الموضوعة تحت الحراسة[1].

ب–2– المصادرة: يمكن للقاضي أن يحكم، زيادة إلى العقوبات الماليّة المنصوص عليها بموجب أحكام القانون رقم 04–02 المتعلّق بالقواعد المطبّقة على الممارسات التّجاريّة، بمصادرة السّلع المحجوزة، وفي حالة ما إذا كانت المصادرة تتعلّق بسلع كانت موضوع الحجز العيني، فيتّم تسليم هذه المواد إلى إدارة أملاك الدّولة التي تقوم ببيعها وفق الشّروط المنصوص عليها في التّشريع والتّنظيم المعمول بهما، أمّا في حالة الحجز الاعتباري فإنّ المصادرة تقع على قيمة الأملاك المحجوزة بكاملها أو على جزء منها، فعندما يحكم القاضي بالمُصادرة يصبح مبلغ بيع السلع المحجوزة مكتسبا للخزينة العموميّة[2].

ب–3– غلق المؤسّسة أو المحّل التّجاري: إنّ تسليط عقوبة غلق المؤسّسة أو المحّل التّجاري تدخل ضمن سلطات الضّبط الإداري التي منحها القانون للوالي المختّص إقليميا، الذي يقوم بناءً على اقتراح من المدير الولائي المكلّف بالتّجارة، بإصدار قرار غلق المحّل التّجاري لمدة أقصاها ستون(60) يوم، وذلك في حالة مخالفة أحكام المواد 4 و5 و6 و7 و8 و9 و10 و11 و13 و14 و20 و22 و22 مكرر و23 و24 و25 و26 و27 و28 و53 الواردة في ذلك القانون[3]، حيث يمكن لقاضي الموضوع الحكم بهذه العقوبة وفقا لقاعدة الخاص يقيّد العام، أو يستعين بالأحكام الواردة ضمن قانون العقوبات[4]، في حين

---

[1] راجع أحكام المادة 42 من القانون رقم 04–02، الذي يحدد القواعد المطبقة على الممارسات التجارية، سالف الذكر.

[2] راجع أحكام المادة 44 من القانون رقم 10–06 المؤرخ في 15 أوت 2010 المعدل والمتمم للقانون رقم 04–02 المؤرخ في 23 جويلية 2004، الذي يحدد القواعد المطبقة على الممارسات التجارية، سالف الذكر.

[3] راجع المادة 46 من القانون رقم 04–02، سالف الذكر.

[4] أمر رقم 66–156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، معدل ومتمم بموجب القانون رقم 04–15 المؤرخ في 10 نوفمبر2004، ج ر عدد 71 الصادر في 10 نوفمبر 2004، المعدل والمتمم بموجب القانون رقم 06–23 المؤرخ في 20 ديسمبر 2006، ج ر عدد 84 الصادر في 24 ديسمبر 2006.

يمكن أن يكون قرار الغلق محل طعن أمام المحكمة الإدارية المختصّة في البّث في النّزاع، فإذا حكمت بإلغاء القرار، يمكن للعون الاقتصادي المتضّرر طلب التّعويض عن الضّرر الذي ألحق به أمام العدالة.

ب–4– نشر الحكم: يعتبر نشر الحكم أو القرار عقوبة تكميليّة مترتّبة عن الممارسات التّجارية غير المشروعة، حيث سمحت المادة 48 من القانون رقم 04–02 المتضمّن القواعد المطبّقة على الممارسات التّجاريّة[1]، لكل من الوالي المختّص إقليميا والقاضي أن يأمر على نفقة مرتكب المخالفة أو المحكوم عليه بصفة نهائيّة، بنشر خلاصة من قراراتهما أو كاملة في الصّحافة الوطنيّة، أو يتّم لصقها بأحرف بارزة على مستوى البلديات والسّاحات العموميّة أو الأماكن العموميّة الأخرى، لغرض إعلام الجمهور بمُرتكبي جرائم الممارسات التّجاريّة غير المشروعة.

2)– الجزاءات المفروضة في إطار القانون رقم 18–05 المتعلق بالتّجارة الإلكترونية:

يمكن للقاضي الاستعانة بأحكام الباب الثالث من القانون رقم 18–05 المتعلّق بالتّجارة الإلكترونيّة، التي نصت على مجموعة من الجزاءات المتمثّلة فيما يلي:

أ)– تعليق تسجيل اسم موقِع المورّد الإلكتروني: كل شخص طبيعي أو معنوي مُقيم في الجزائر يقترح توفير سلع أو خدمات عن طريق الإنترنت من دون التّسجيل المُسبق في السّجل التّجاري، يتّم تعليق اسم موقعه الإلكتروني فورا من طرف الهيئة المؤهّلة لمنح أسماء المواقِع في الجزائر، حيث يبقى هذا التّعليق ساري المفعول إلى غاية تسوية وضعيته، وفي حالة ارتكاب المورّد الإلكتروني أثناء ممارسة نشاطه لمخالفات تكون تحت طائلة عقوبة غلق المحل التّجاري، بمفهوم التّشريع المتعلّق بممارسة الأنشطة التّجاريّة، يتّم تعليق تسجيل اسم موقِع المورّد الإلكتروني بشكل تحفّظي من طرف تلك الهيئة، بناءً على مقرّر من وزارة التّجارة، حيث لا يمكن أن تتجاوز مدّة التّعليق التّحفظي لاسم النّطاق ثلاثين(30) يوما[2] .

---

[1] قانون رقم 04–02 مؤرخ في 23 جويلية 2004، يحدد القواعد المطبقة على الممارسات التجارية، سالف الذكر.

[2] المادتين 42 و43 من القانون رقم 18–05 الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

ب)– عرض أو بيع سلع وخدمات محظورة: كل مورّد إلكتروني يَعْرِضُ أو يَبِيعُ عن طريق الاتّصال الإلكتروني لسلع وخدمات ممنوعة، يُعاقب بغرامة تتراوح من مائتي ألف دينار(200.000) إلى مليون دينار(1.000.000)، حيث يمكن للقاضي أن يأمر بغلق الموقِع الإلكتروني لمدة تتراوح من شهر(01) إلى ستة(06) أشهر، كما يُمنع التّعامل عن طريق الاتّصالات الإلكترونيّة في العتاد والتّجهيزات والمنتجات الحسّاسة المحدّدة عن طريق التّنظيم المعمول به، وكذا كل المنتجات أو الخدمات الأخرى التي من شأنها المساس بمصالح الدّفاع الوطني والنّظام والأمن العموميين، حيث يمكن للقاضي في هذه الحالة، أن يأمر بغلق الموقع الإلكتروني والشّطب من السّجل التّجاري[1] .

ج)– مخالفة المتطلبات المتعلّقة بالعرض التّجاري الإلكتروني والطلبيّة: كل مورّد إلكتروني لا يستجيب لأحد التزامات العرض التّجاري الإلكتروني المنصوص عليها في المادة 11 من القانون رقم 18–05 المتعلّق بالتّجارة الإلكترونيّة، وكذا مخالفته المراحل الإلزاميّة الثلاثة التي تتطلّبها طلبيّة منتوج أو خدمة التي نصت عليها المادة 12 من نفس القانون، يُعاقب بغرامة ماليّة تُقدّر بخمسين ألف دينار(50.000) إلى خمسمائة ألف دينار(500.000)، حيث يجوز للجهة القضائيّة التي تفصل في النّزاع أن تأمر بتعليق نفاذ المورّد الإلكتروني إلى جميع منصّات الدّفع الإلكتروني لمدّة لا تتجاوز ستة(06) أشهر[2] .

د)– الإخلال بالالتزامات المتعلّقة بالإشهار الإلكتروني: كل مورّد إلكتروني يخالف الالتزامات المتعلّقة بالإشهار الإلكتروني، يُعاقب بغرامة ماليّة تتراوح من خمسين ألف دينار(50.000) إلى خمسمائة ألف دينار(500.000)، وذلك دون المساس بحقوق الضحايا في طلب التّعويض[3].

هـ)– مخالفة التزامات البيع بالفاتورة وحفظ وإرسال سجّلات المعاملات التّجاريّة: كل بيع لسلعة أو خدمة يتّم عبر الإنترنت من دون إعداد وتسليم فاتورة للمستهلك الإلكتروني، بطريقة

---

[1] المادتين 37 و38 من القانون رقم 18–05، الذي يتعلق بالتجارة الالكترونية، سالف الذكر

[2] المادة 39 من القانون رقم 18–05، سالف الذكر.

[3] المادة 40 من القانون رقم 18–05، سالف الذكر.

إلكترونيّة أو بشكلها الورقي وفقا لمقتضيات المادة 20 من القانون رقم 18–05 المتعلق بالتّجارة الإلكترونيّة، يُعَاقَبُ المورّد الإلكتروني طبقا لأحكام القانون رقم 04–02، الذي يُحدّد القواعد المُطبّقة على المُمارسات التّجارية، المعدل والمتمم، وفي حالة عدم قيام المُورّد بحفظ سجّلات المعاملات التّجارية المُنجزة وتواريخها مع إرسالها بطريقة إلكترونيّة إلى المركز الوطني للسّجل التّجاري، يعاقب بغرامة ماليّة تتراوح من عشرين ألف دينار(20.000) إلى مائتي ألف دينار(200.000)[1].

يمكن للإدارة المُكلّفة بحماية المستهلك أن تباشر إجراءات غرامة الصّلح مع الأشخاص المتابعين بمخالفة أحكام القانون رقم 18–05 المتعلق بالتّجارة الإلكترونيّة، حيث يجب على أعوان الرّقابة، المنصوص عليهم في المادة 36 من نفس القانون اقتراح غرامة الصّلح على المورّد الإلكتروني، وفقا للمادة 1/45–2 من نفس القانون، وفي حالة قبول هذا الأخير(المورّد الإلكتروني) تقوم الإدارة المؤهّلة بإقرار تخفيض مبلغ غرامة الصلح قدره 10%، ففي حالة عدم دفع ذلك المبلغ أو لم يمتثل المُخالِف للأحكام التّشريعيّة والتّنظيميّة المعمول بهما في أجل(45) يوم من تاريخ استلامه لأمر الدفع المُرسَل من طرف المصالح التّابعة للتّجارة، يتّم إرسال محضر المخالفة إلى الجهة القضائيّة المختصّة، وإذا قام المخالف بتكرار نفس الجريمة خلال مدة لا تتجاوز(12) شهرا من تاريخ تنفيذه للعقوبة المتعلّقة بالجريمة السّابقة، فإنّ مبلغ الغرامة يُضاعف، وفي جميع الأحوال لا يمكن إجراء غرامة الصّلح في حالة العُودِ(Récidive) أو عندما يتعلّق الأمر بالمخالفات المنصوص عليها في المادتين 37 و38 من القانون رقم 18–05 المتعلّق بالتّجارة الإلكترونيّة[2].

[1] المادة 41 من القانون رقم 18–05، الذي يتعلق بالتجارة الالكترونية، سالف الذكر.

[2] المواد 45 و46 و47 و48 من القانون رقم 18–05، سالف الذكر.

المطلب الثاني
المسؤوليّة المدنيّة والجزائيّة لمزوّدي خدمات الإنترنت

إنّ التّعامل مع الخدمات التي يتيحها(م.خ.إ) يجب أن يتّم في إطار ضوابط عقديّة وقانونيّة تُحدِّد حقوق والتزامات كل طرف في النّشاط المعلوماتي، التي من خلالها يتحمّل كل طرف منهم المسؤوليّة المدنيّة عمّا يُرتكب من مخالفات عبر شبكة الإنترنت بمجرّد توافر أركانها(**الفرع الأول**)، كما أنّ الطّابع التّقني والفنّي المُعقّد لشبكة الإنترنت جعلت المخالفات المرتكبة تأخذ تكييفات وأسس قانونيّة مختلفة، كانتهاك حقوق الملكيّة الفكريّة الرّقميّة، أو إفشاء الأسرار المهنيّة، أو المساس بحرمة الحياة الخاصّة أو البيانات الشّخصيّة، الخ...، التي من خلالها يتحمّل (م.خ.إ) للمسؤوليّة الجزائيّة(**الفرع الثاني**).

الفرع الأول
المسؤوليّة المدنيّة لمزوّدي خدمات الإنترنت

قد يحدث أن يقوم (م.خ.إ) بنشر مضمون إلكتروني غير مشروع نتيجة الإخلال بالتزام عقدي أو قانوني، ممّا يدفع بالشّخص المتضرّر(المستهلك) إلى طلب التّعويض استنادا إلى قواعد المسؤوليّة المدنيّة بشّقيها العقدي أو التّقصيري.

أولا)– المسؤوليّة العقديّة لمزوّدي خدمات الإنترنت.

إنّ تنوّع الخدمات المتاحة عبر الإنترنت تدفع بالمستهلكين إلى إبرام مجموعة من العقود مع مزوّدي الخدمات، التي تتميّز بخصوصيات قانونيّة وتقنيّة تتعلّق بنمط ومستوى كلّ خدمة مُتاحة(**أ**) حيث يمكن لمزوّد خدمات الإنترنت أن يتحمّل المسؤوليّة العقديّة(**ب**).

أ– طبيعة الخدمات المتاحة من طرف المزوّدين:

إنّ الخدمات التي يتيحها(م.خ.إ) للمستهلكين تدخل في نطاق الأحكام المنظّمة للتّجارة الإلكترونيّة، وهذا ما أقرّه المشّرع الفرنسي بموجب أحكام المادة 14 من القانون رقم 2004–575 المؤرخ في 21 جوان 2004 المتعلّق بالثّقة في الاقتصاد الرّقمي(LCEN)، التي من خلالها صنّف خدمات المزوّدين(توريد المعلومات، الاتّصال، البحث، الدّخول واسترجاع

البيانات الالكترونيّة، الدّخول إلى شبكة اتّصال، أو إيواء المعلومات)، ضمن نشاطات التّجارة الإلكترونيّة حتّى ولو كانت الخدمات المتاحة من دُونِ مُقَابِلٍ[1].

أ–1– مزوّد الدّخول(Fournisseur d'accès à internet(FAI)): يلتزم مزوّد الدّخول في إطار عقد الدّخول إلى الشّبكات العامّة أو الخاصّة ببذل العناية اللاّزمة في وضع الخوادم أو الموّزعات على ذمّة المستهلك على امتداد كامل السّاعات والأيّام، وتوفيرهم للوسائل التّقنيّة التي تُمكّنهم من تحديد أو تضييق النّفاذ إلى بعض خدمات الإنترنت[2]، حيث لا يضمن المزوّد خلال فترات الصّيانة سريان المعدّات المعلوماتيّة أو تَوقُّفها لسبب كثافة المبادلات الإلكترونية أو خلل فُجائي، كما يُعفى المزوّد من المسؤوليّة عن جرّاء الاستعمال غير المشروع أو الأضرار اللاّحقة بمُعدّات المُستهلك، الذي يلتزم بدوره بضمان أمن وسلامة معدّاته وحماية أنظمته من مختلف البرمجيات الخبيثة، فكل استعمال غير مشروع للشّبكة العامّة أو الخاصّة يتحمّل المُستهلك تبعات فسخ العقد من جانب واحد[3].

أ–2– مزوّد الإيواء(Hébergeur): يلتزم مزوّد الإيواء في إطار عقد الخدمة ببذل العناية اللاّزمة بوضع الخوادم أو الموزّعات تحت تصرف المورد الإلكتروني طيلة أيّام الأسبوع وكامل السّاعات، حيث يبقى المُزوّد مسؤولا تجاه التزامه التّعاقدي في حالة عدم تنفيذه كليًا أو جزئيًا، وتَقِفُ مسؤوليّته التّعاقديّة عند خروج المَعلومة من المُعدّات التّابعة له، ولا يضمن

---

1) **Loi n° 2004-575** du 21 juin 2004 pour la confiance dans l'économie numérique(LCEN), J.O.R.F, n° 143 du 22 juin 2004.

Art. 14 : « […]. Entrent également dans le **champ** du **commerce électronique** les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent.[…].»

2) **Art.6-I.1(LCEN)** : « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens. »

3) **علي كحلون**، مرجع سابق، ص ص 210، 211.

Philippe LE TOURNEAU, op.cit., p. 433.

سُرعة الخدمات وسلامة المواقع الإلكترونيّة من الإتلاف أو التّغيير[1]، حيث يجب على المورّد الإلكتروني الالتزام في إطار عقد الإيواء احترام المتطلّبات الفنيّة في الإيواء، وتأمين وحماية موقعه الإلكتروني من مخاطر الشّبكة، مع احترام ميثاق الإنترنت وحقوق الغير المتعلّقة بالتّجارة الإلكترونيّة والملكيّة الفكريّة والمعطيات الشّخصيّة الخ...[2].

أ–3– مزوّد البحث(Fournisseur de recherche): إنّ المتجر الافتراضي الذي لا يُتِيحُ للمستهلك إمكانية الوصول إليه عبر الإنترنت، لا جدوى منه، لذا يسعى صاحبه إلى إبرام عقد الإحالة(Contrat de référencement) مع مُزوّد البحث، لغرض إدراج وقبول المتجر الافتراضي في فضاء مُحرّكات البحث أو الفهارس المعلوماتيّة، حيث يتّم إذعان صاحب الموقِع بشروط ومُتطلّبات ذات صلة بعنوان وموضوع الموقِع وبمُحتواه مع عدم مخالفة الجانب القانوني، في حين يلتزم مُزوّد البحث في إطار العقد ببذل العناية اللاّزمة بالإشارة إلى الموقِع الإلكتروني في محرّك البحث مع تصنيفه ضمن المرتبة اللاّئقة فيه[3].

أ–4– مزوّد النّقل(Transmetteur): يتمثّل نَاقِلُ المعلومات في كل شخص طبيعي أو معنوي يقوم بنقل أو إيصال المادّة المعلوماتيّة إلى الجمهور، حيث يلتزم في إطار عقد نقل المعلومة بتقديم الوسائل التّقنيّة والفنيّة اللاّزمة لعملية النّقل المادّي للمضمون المعلوماتي، مع إيصاله إلى الجمهور والحفاظ على سريّته عبر شبكته والحياد تِجاه المادة المعلوماتيّة المنقولة، مع الالتزام بعدم الاطّلاع على مُضْمُونِهَا[4].

أ–5– مورّد المعلومات(Fournisseur du contenu): يتمثّل في الطرف المُنشئ للمعلومة وله علاقة بمحتواها، فقد يكون صاحب موقع إلكتروني أو مُنتجه أو مُشارك في حلقة الحوار والنّقاش(Forum)، أو مزود خدمات، أو يكون مجرد شخص يباشر المعالجة الالكترونية للمعلومات في إطار عمله أو نشاطه المنزلي، حيث يلتزم مُورّد المعلومات في إطار عقد

---

1) **Vincent FAUCHOUX, Pierre DEPEREZ**, op.cit., pp. 270, 271.

2) **Michel VIVANT**, Les contrats du commerce électronique, Litec, France, 1999, p. 29.
Lionel BOUCHURBERG, op.cit., p. 44.

3) **Romain V.GOLA**, op.cit., pp. 444- 447 .

4) **محمد حسين منصور**، مرجع سابق، ص 197.

توريد المعلومات، بتوريد أو نشر المادّة المعلوماتيّة المشروعة والحقيقيّة، والكشف على جميع هوّية القائمين على المضمون المعلوماتي، مع وضع تحت تصرّف الجمهور جميع المعلومات التي تعرّف بهويّته وهوّية النّشاط الإلكتروني الذي يشرف عليه، فإذا كان مورِّد المعلومات شخص طبيعي يجب عليه تحديد بياناته الشّخصيّة(الاسم واللّقب، العنوان، رقم الهاتف والسّجل التّجاري)، أمّا إذا كان شخص معنوي فيلتزم بتحديد اسمه، ونشاطه، ومقرّه الرّئيسي، ورقم هاتفه وسّجله التّجاري، ويتعيّن على مورّد المعلومات كذلك ذكر اسم مدير النّشر أو رئيس التّحرير عند الاقتضاء، وكذا اسم ولقب مُتعهّد الإيواء أو عنوانه ومقرّه الرّئيسي، في حين يُمْكِنُ للمُورّد(النّاشر غير المهني) أن يضع فقط تحت تصرّف الجمهور المعلومات المتعلّقة بتحديد هوّية متعهّد الإيواء، في حال عدم رغبته الكّشف عن المعلومات المذكورة أعلاه للجمهور، بشرط أن يتيح بياناته الشّخصيّة لمتعهّد الإيواء[1].

وعليه، يلتزم مورّد المعلومات بضرورة تأمين الوسائل التّقنيّة اللاّزمة التي تتيح للشّخص المضرور إمكانية مباشرة حق الرّد عن كل انتهاك يمّس بأحد حقوقه المحميّة، مع تمكينه من مطالبة تصحيح أو شطب المعلومة غير المشروعة عبر صفحات الويب، حيث ينبغي على الشّخص المضرور وفقا للمادة 4/06 من القانون رقم 2004-575 المتعلّق بالثّقة في

---

1) **Art. 6. III.1 et 2(LCEN) : « -1** Les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert : **a)** S'il s'agit de personnes physiques, leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ; **b)** S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ; **c)** Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 précitée ; **d)** Le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du prestataire mentionné au 2 du I.
2. Les **personnes éditant** à titre **non professionnel** un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur **anonymat**, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.»
Voir aussi : **Vincent FAUCHOUX, Pierre DEPEREZ**, op.cit., pp. 239, 240.

الإقتصاد الرّقمي(LCEN)، أن يقدّم طلب الرّد إلى مدير النّشر في مدة ثلاثة(03) أشهر تسري من تاريخ علم الجمهور بمضمون رسالة الرّد[1].

أ–6– مُقدّم خدمة التّصديق الإلكتروني: يلتزم (م.خ.ت.إ) في إطار عقد تقديم الخدمة بمنح وإصدار شهادات التّصديق الإلكتروني، بعد التّأكد من هوّية صاحبها وصّحة المعلومات الواردة في الشّهادة، وإيقافها أو إلغائها عند الاقتضاء، مع الالتزام بالسّر المهني أثناء تأديته لخدمة التّصديق الإلكتروني، وكذا الالتزام بحفظ شهادات التّصديق، الخ...، وبالمقابل يعتبر صاحب الشّهادة المسؤول الوحيد عن سريّة بيانات توقيعه الإلكتروني، مع التّقيّد بالأغراض التي أُصدرت من أجلها الشّهادة واحترام مدّة صلاحيتها، مع الإلتزام بإخطار سلطة التّصديق الإلكتروني عند تعرّض أداة إحداث التّوقيع الإلكتروني لما يُثير الشُّبهة الخ...[2].

ب– نطاق المسؤوليّة العقديّة لمزوّدي خدمات الإنترنت:

إنّ نطاق المسؤوليّة العقديّة تُحدّد وفقا للقواعد العامّة بالعلاقات النّاشئة عن عقد صحيح قائم بين المسؤول والمضرور، وتحقّق الضّرر النّاتج عن الإخلال بالإلتزامات المفروضة

---

1) **Art. 6. IV.(LCEN)** « – Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un **droit de réponse**, sans préjudice des **demandes** de correction ou de suppression du message qu'elle peut adresser au service, [**Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004**]. La demande d'exercice du droit de réponse est adressée au directeur de la publication ou, lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée au 2 du I qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois mois à compter de [**Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004**] la mise à disposition du public du message justifiant cette demande. Le directeur de la publication est tenu d'insérer dans les trois jours de leur réception les réponses de toute personne nommée ou désignée dans le service de communication au public en ligne sous peine d'une **amende de 3 750 €**, sans préjudice des autres peines et dommages-intérêts auxquels l'article pourrait donner lieu. Les conditions d'insertion de la réponse sont celles prévues par l'article 13 de la loi du 29 juillet 1881 précitée. La réponse sera toujours gratuite. Un décret en Conseil d'État fixe les modalités d'application du présent article. »
Voir aussi : - **Romain V.GOLA**, op.cit., pp. 467, 468.

2) **دحماني سمير**، مرجع سابق، ص ص 133– 149، 157– 162.

بموجب ذلك العقد، فبِغَيْرِ هذا العقد لا يمكن تصوّر قيام مسؤوليّة عقديّة وبانتفائه تختفي معه المسؤوليّة العقديّة[1]، وبالتّالي يجب أن يكون الضّرر نتيجة عدم تنفيذ إلتزام تعاقدي سواءا كان إلتزاما رئيسيا أو ثانويا أو فرضته نصوص قانونيّة أو أوجدته بنود أو أحكام العقد، غير أنّه يقع على عاتق قاضي الموضوع الذي يفصل في النّزاع واجب القيام بتفسير الإرادة المُشتركة لأطراف العلاقة العقديّة، حتّى يُحيط نفسه عِلماً بمضمونه من أجل تحديد الإلتزامات النّاشئة عنه حيث تُثار المسؤوليّة العقديّة في حالة الإخلال بها، فلكي تتحقّق المسؤوليّة العقديّة لـ(م.خ.إ) لا بدّ من توافر وتحقّق الشّروط الثّلاثة المتمثّلة في الخطأ العقدي(Faute contractuelle) والضرر(Le Dommage) والعلاقة السّببية بالخطأ والضّرر(Un lien de causalité)، والتي سنتطرّق إليها على النّحو التّالي:

ب–1– الخطأ العقدي(Faute contractuelle): إنّ المسؤوليّة العقديّة النّاتجة عن الخطأ لا تعدو أن تكون إلاّ تنفيذاً بمُقابل للالتزام الثّابِت في العقد، ما دام أنّ الخطأ في الميدان العقدي لا يُنشئ التزاماً جديداً وإنّما هو أثر "لإلتزام قائم"، فإسناد الخطأ العقدي لمزوّد خدمات الإنترنت مرهون بعدم تحقّق الغاية المرجوة من الإلتزام، إلاّ إذا أثبت أنّ عدم تنفيذ الإلتزام يرجع إلى فعل المضرور(المستهلك) أو إلى أيّ سبب أجنبي لا يد له فيه، وبالتّالي فإنّ الخطأ العقدي للمُزوّد يتحقّق بِمُجَرَّدِ إثبات المُستهلك لعدم بذل العناية الكافية في تحقيق الإلتزام المفروض عليه بموجب أحكام عقد تقديم الخدمة، وفي حال ما إذا كان الإلتزام يتعلّق بتحقيق النّتيجة(Obligation de résultat) المطلوبة، كالإلتزام بسريّة البيانات الإلكترونيّة، أو تعليق وإلغاء الشّهادات بطَلَبٍ من صاحب الشّهادة، أو عدم إعلام مُزوّد النّقل لعملائه بالوسائل التّقنيّة لمنع الدّخول إلى بعض خدمات الإنترنت، أو عدم التزام مزوّد الاتّصال

1) **Patrice JOURDAIN**, La Distinction des Responsabilités Délictuelle et Contractuelle : État du Droit Français, pp. 05-10. Article disponible sur le site: http://www.grerca.univ-rennes1.fr/, consulté le 14/02/2019.

بتقديم خدمة الإنترنت بالسّرعة أو الجودة المتّفق عليها الخ...، فيتحقّق بالتّالي الخطأ العقدي لمزوّد الخدمة بمُجرّد إثبات المستهلك لعدم تحقيق النتيجة المطلوبة[1].

ب–2– الضّرر (Le Dommage): إنّ الأخطاء التي تقع قبل إبرام العقد أو بعد انحلاله تُسْتُبْعَدُ من المسؤوليّة العقديّة، ولتحقّق الضّرر يجب أن يقع أو يحدث أثناء سريان أو قِيام عقد تقديم الخدمة عبر الإنترنت وأن يكون ناتج عن إخلال مزوّد الخدمة بالتزام ناشئ عن العقد، وأن يُصيب الضّرر الطرف المُتعاقِد الآخر (المستهلك)، فإذا كان الضّرر ناتج عن عدم قيام مزوّد المعلومات بالكشف عن هويّة النّاشرين للمعلومات، أو عدم إتاحة مزوّد النّقل للوسائل التّقنيّة اللاّزمة لعملية النّقل المادّي للمعلومة أو انتهاكه لسريّتها، أو انقطاع خدمة الإنترنت ورداءتها بسبب خطأ مزوّد الخدمة وما ينجم عنها من تعطيل لخدمات مواقع التّجارة الإلكترونيّة(شركات الطّيران، المصارف، أسواق الأوراق الماليّة(البورصات)...)، وإلحاقها أضرار تجاريّة واقتصاديّة فادحة في حالة ما إذا استمّر الانقطاع لفترة طويلة، الخ...، فتُثار بالتّالي المسؤوليّة العقديّة لمزوّد خدمة الإنترنت التي لا تتحقّق إلاّ بتواجد العلاقة السّببية بين الخطأ المرتكب والضّرر الذي أُلْحِقَ بالمضرور الذي يقع عليه عبئ الإثبات.

ب–3– علاقة السّببية بين الخطأ والضّرر (Un lien de causalité): إنّ توافر ركني الخطأ العقدي والضّرر لوحدهما لا يكفي لإسناد أو تحقق المسؤوليّة العقديّة لمزوّد الخدمة، التي تستوجب وجود العلاقة السّببية بين الخطأ العقدي المنسوب للمزوّد والضّرر المُسّبب للمضرور (المستهلك)، حيث يُعْفَى مزوّد الخدمة من مسؤوليته العقديّة في حالة ما إذا أثبت انتفاء علاقة السّببية بين الخطأ والضّرر لسبب أجنبي خارج عن إرادته، يعود إلى قوّة قاهرة أو حادث فجائي أو أيّ سبب مشروع أخر، كأن يتّم حجب خدمة الإنترنت عن المورّد

---

[1] **باسم السيد**، "النظام القانوني لمزودي خدمة الإنترنت في سورية"، مجلة جامعة البعث، المجلد 39، العدد 50، 2017، ص ص 76، 77.

الإلكتروني لمخالفته للقوانين المُنظّمة للمُمارسات التّجارية، أو توقّف خدمة الاتّصال بالإنترنت نتيجة الضّرر الذي سبّبته سفينة معيّنة لكابل الإنترنت في البحر، الخ...[1].

تجدر الإشارة، إلى أنّ آثار العقد لا تنصرف وفقا للأصل العام إلاّ على الأطراف المتعاقدة ولا تنصرف إلى غيرهم، لكن كاستثناء من ذلك يجوز للمتعاقدين الاتّفاق على إفادة شخص ثالث ليس طرفا في العقد من أحكام العقد، الذي يكتسب(الغير) حقًّا مباشرا من العقد، حيث تثار في هذه الحالة المسؤوليّة العقديّة عن الأضرار المُلحقَة بالْغَيْرِ وفقا لقواعد الإشتراط لمصلحة الغير، ويتحقّق ذلك عندما يشترط صاحب الموقع التّجاري الإلكتروني(صاحب شهادة التّصديق الموصوفة) على مزوّد خدمة التّصديق الإلكتروني(م.خ.ت.إ)، أن يضمن تُجَاهَ الغير(المستهلك) الأضرار التي تُلحقه نتيجة تعويله على شهادة التّصديق، فعندئذ يُنشِئُ العقد إلتزاما قانونياً لصالح الغَيْرْ يَتَحَمَّلُهُ(م.خ.ت.إ)[2].

ثانيا– المسؤوليّة التّقصيريّة لمزوّدي خدمات الإنترنت.

---

[1] **Code civil(France)** - Dernière modification le 23 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance.gouve.fr
Art. 1148 : « Il n'y a lieu à aucuns dommages et intérêts lorsque, par suite d'une force majeure ou d'un cas fortuit, le débiteur a été empêché de donner ou de faire ce à quoi il était obligé, ou a fait ce qui lui était interdit. »

[2] أمر رقم 75– 58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، المعدل والمتمم.
تنص **المادة 113** على ما يلي: "لا يرتب العقد التزاما في ذمة الغير، ولكن يجوز أن يكسبه حقا."
تنص **المادة 118** على ما يلي:" يجوز في الاشتراط لمصلحة الغير أن يكون المنتفع شخصا مستقبلا أو هيئة مستقبلة كما يجوز أن يكون شخصا أو هيئة لم يعينا وقت العقد متى كان تعيينهما مستطاعا في الوقت الذي يجب أن ينتج العقد فيه أثره طبقا للمشارطة."
إبراهيم الدسوقي أبو الليل، "توثيق التعاملات الإلكترونية و مسؤولية جهة التوثيق تجاه الغير المضرور"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و 12 ماي 2003، المجلد الخامس، ص 1887.
Bernard BRUN, Nature et impacts juridiques de la certification dans le commerce électronique sur Internet, P. 50. Article disponible à partir de l'adresse: http://www.signelec.comcontentsearticlesarticle_bernard_brun_html, consultée le 25/02/2019.

يعتبر الإلتزام القانوني المصدر الرّئيسي لقيام المسؤوليّة التّقصيريّة التي تتحقّق بمجرّد توافر أركانها الثلاثة(الخطأ والضّرر والعلاقة السّببية بينهما)[1]، حيث يُمكن لمزوّد خدمة الإنترنت أن يتحمّل تلك المسؤوليّة عن فعله الشّخصي أو عن فعل الغير أو عن الأشياء.

أ)– المسؤوليّة عن الفعل الشّخصي(La responsabilité du fait personnel):

إنّ المسؤوليّة عن الأعمال الشّخصيّة وفقا للأحكام العامّة المنظّمة للمسؤوليّة المدنيّة قائمة على أساس إثبات الخطأ، حيث نص المشّرع الجزائري بموجب المادة 124 من التّقنين المدني[2] على أنّه كل شخص يرتكب بفعله خطأ سبّب أو أحدث ضررا للغير، يلتزم بتعويض هذا الأخير، ومن هنا يجب أن يتحقّق إلى جانب عنصر الخطأ ركن الضرر لإسناد المسؤوليّة عن الفعل الشّخصي لـ(م.خ.إ)، وذلك باعتباره(الضّرر) المِحور الأساسي الذي تدور حوله المسؤوليّة بوجه عام، حيث يجب على المضرور إثبات العلاقة السّببية بين الخطأ التّقصيري المُرتكب من طرف مقدّم الخدمة نتيجة عدم بذله العناية اللاّزمة من الحيطة والتبّصر لتفاديه، والضّرر الذي ألحق بمصلحته المشروعة(المضرور).

وعليه، يجب على (م.خ.إ) الالتزام بواجب الحذر أو الحيطة والتبّصر في سلوكه المهني تُجاه الغير حتى لا يُلحقه أضراراً، والالتزام هنا هو إلتزام ببذل العناية وليس تحقيق النّتيجة، حيث يتحمّل(م.خ.ت.إ) المسؤولية التّقصيريّة عن الضّرر المسبّب للطرف المُعوِّل على(صاحب المتجر الافتراضي) على شهادة التّصديق الموصوفة، نتيجة عدم التّحقّق في هوّية صاحب الشّهادة وكذا عدم صّحة ومطابقة البيانات الواردة في شهادة التّصديق وقت إصدارها، أو إخلاله بالتزام إلغاء الشّهادة بعد ثبوت دواعي ذلك، حيث تنتفي مسؤوليّته

---

[1] **محمد صبري السعدي**، شرح القانون المدني الجزائري (مصادر الإلتزام – الواقعة القانونية)، الطبعة الثانية، دار الهدى، الجزائر، 2004، ص ص 27، 28.

عبد الرزاق السنهوري، الوسيط في شرح القانون المدني (نظرية الالتزام– الإثبات)، الطبعة الثالثة، الجزء الثاني، دار النهضة العربية، القاهرة، 1981، ص 1083.

[2] أمر رقم 75– 58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، المعدل والمتمم.

التّقصيريّة(م.خ.ت.إ) في حالة إثبات أنّه لم يرتكب أيّ إهمال، أو في حالة تجاوز حدود إستعمال الشّهادة، أو القيمة المُحدّدة فيها[1].

بالإضافة إلى ذلك، نصت المادة 14 من التوجيه الأوروبي رقم 2000–31 المؤرخ في 08 جوان 2000 المتعلق بالتجارة الإلكترونية، والمادة 06–I/2 من القانون رقم 2004–575 المؤرخ في 21 جوان 2004 المتعلق بالثّقة في الإقتصاد الرقمي(LCEN)، على تحمّل متعهّد الإيواء للمسؤوليّة التّقصيريّة في حالة إثبات علمه الفِعْلِي بالمضمون الإلكتروني غير المشروع، ومع ذلك لم يَتَّخِذْ الإجراءات اللاّزمة لشطبه أو منع الوصول إليه[2]، كما تُضيف المادة 12 من نفس التّوجيه، أنّ مزوّد نقل المعلومة ومزوّد الدّخول إلى الشّبكة

---

[1] راجع نصوص المواد من 53 إلى 57، من القانون رقم 15–04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر.

Voir aussi : l'**Art. 33** (**LCEN n° 2004-575**).

2) **Directive 2000/31/CE** du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JOUE n° L 178 du 17/07/2000.

Art. 14 : « (Hébergement) 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que: a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.[…].»

Art. 06.I-2(LCEN) : « Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, **le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature** fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles **n'avaient** pas effectivement **connaissance** de leur caractère **illicite** ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour **retirer** ces données ou en rendre **l'accès impossible**. L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa. »

يتحمّلون المسؤوليّة التّقصيريّة عن المضمون الإلكتروني المُرسل، في حال ما إذا قاموا بأنفسهم إرسال المعلومة وتحديد الشّخص المُرسَل إليهِ مع الاطّلاع وتعديل مضمون المعلومة المُرسلة، حيث تنتفي مسؤوليّة كل مزوّد في حالة إثبات عكس ذلك، وأنّ أعمالهما لم تَتجاوَز خِدمة النّقل والدّخول[1].

والجدير بالذّكر، أنّ المشّرع الفيدرالي للاتّحاد الأوروبي قام في إطار أحكام التّوجيه الأوروبي رقم 2000–31 المتعلّق بالتّجارة الإلكترونيّة(المواد 12، 13، 14 منه) بإسناد المسؤوليّة فقط لمزوّدي خدمات الوصول والإيواء ونقل المعلومات، ولم يذكر على سبيل الحصر المزوّدين الآخرين على غرار مزوّد البحث، ومزوّد المعلومات، الخ...، الذين يُمكن مساءلتهم مدنيا(أو حتّى جزائيا) في حالة عِلمِهم بوجود معلومة إلكترونية غير مشروعة واكتفوا بالمَوقِف السّلبي تجاهها، أو في حالة ما إذا تجاوزوا حدود خدمتهم[2].

حيث يمكن أن يُسأل مُزوّد البحث تقصيرياً كمزود إيواء في حالة جمع معلومة مع إدراكه بمحتواها غير المشروع، أو في حدود "أعمال البحث" في إطار روابط الإحالة التي تُمكّن المستعمل من الوصول إلى المعلومات غير المشروعة المنشورة عبر مختلف المواقع الإلكترونيّة، وبالتّالي يتحمّل مُزوّد البحث المسؤولية التّقصيريّة في حالة علمه بالمحتوى غير المشروع لصفحات الويب ولم يُبادر بقطع روابط الإحالة مع هذه المواقع، وتنتفي مسئوليته

---

1) **Art. 12(Directive 2000/31/CE sur le commerce électronique) : « Simple transport («Mere conduit»)** 1- Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire: a) ne soit pas à l'origine de la transmission; b) ne sélectionne pas le destinataire de la transmission et . c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission. […]».
Voir aussi : **Alain STROWEL, Nicolas IDE**, (Actualités législatives et Jurisprudentielles), op.cit., pp.21-25.

2) **Thibault VERBIEST, Etienne WÉRY**, La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés, p.05. Article publié le 10/09/2002 sur le site: https://www.droit-technologie.org, consulté le 05/01/2019.
Philippe LE TOURNEAU, op.cit., p. 463.

في حالة إثبات عكس ذلك، وفي جميع الظروف، يجب التّمييز بين روابط الإحالة التي يستعملها مُحرّك البحث في حدود أعمال البحث، والرّوابط التي يتّم إحداثها من طرف أصحاب المواقِع الالكترونية، لتكييف الوقائع على الأساس القانوني اللاّزم لإسناد المسؤوليّة لكل طرف بمجرّد تحقّق أركانها[1].

كما يُسأل مزوّد المعلومة تقصيرياً عن محتوى معلوماته في علاقته مع الغير، بوصفه مُؤلّفا ومُوزّعا لمحتوى المعلومة عبر مواقع الانترنت أو مِنصّات التّواصل الاجتماعي، حيث يعتبر المسئول الأوّل عن المحتوى غير المشروع المنشور مهما كان سند المتابعة، إذْ يمكن متابعة المُستعمل "كمُشارك" في حالة ما إذا قام بدوره بنشر هذا المُحتوى وألحق أضرار بالحقوق المُكتسبة للغير، كالمساس بحقوق الملكية الفكرية أو المعطيات الشّخصيّة والحياة الخاصّة، الخ...، حيث لا يوجد ما يمنع الاجتهاد القضائي من تطبيق الأحكام المتعلّقة بمزوّد الدّخول أو الإيواء على مزود المعلومة في حالة تجاوزه لحدود خدمته [2].

---

1) **Mickaël LE BORLOCH**, op.cit., pp. 117-122, 135- 146, 171, 172, 177-180.

للمزيد من المعلومات حول الموضوع، أنظر كذلك الأحكام والقرارات القضائية التالية:

TGI Nanterre, réf, 28/02/2008, Olivier D. c/ Éric D. https://www.juriscom.net (consulté le 11/09/2018.)

TGI Paris, réf, 28/02/2008, Olivier D. c/ Sté Ad Soft Com. https://www.juriscom.net (consulté le 11/09/2018.)

TGI Paris, 3ème ch, 3ème sect, 24/06/2009, Jean-Yves Lafesse et A. c/ Google et A. https://www.juriscom.net(consulté le 12/09/2018.)

2) **CA Paris**, 14ème ch, 29/11/2009, Jean-Yves Lafesse c/ My Space. https://www.juriscom.net (consulté le 07/09/2018.)

TGI Paris, 3ème ch, 2ème sect, 19/10/2007, Google c/ Zading Productions. https://www.juriscom.net(consulté le 07/09/2018.)

TGI Paris, 4ème ch, 2ème sect. A, 06/05/2009, Dailmotion c/ Nord Ouest Production et A. https://www.juriscom.net(consulté le 09/09/2018.)

TGI Paris, réf, 07/01/2009, Jean-Yeves Lafesse et A. c/ Youtube Inc. https://www.juriscom.net (consulté le 09/09/2018.)

TGI Paris, 3ème ch, 1ère sect, 22/09/2009, Adami, Omar, Fred et A. c/ Sté Youtube. https://www.juriscom.net(consulté le 10/09/2018.)

وفي مجال حماية المعطيات الشّخصيّة للأفراد، قضت محكمة العدل الأوروبيّة في مناسبتين[1]، على أنّ صاحب صفحة فايس بوك(Administrateur) أو موقع تجاري إلكتروني يحتوي على صيغة الإعجاب(J'aime) لصفحة(Facebook)، للترويج بخدمة أو سلعة معيّنة، يتحمّل المسؤوليّة "مع" شركة(Facebook) على أساس "المشاركة"، عن الضّرر المترتّب في نفس النّشاط المتعلّق بالمعالجة الآلية للمعطيات الشّخصيّة للأفراد، التي من خلالها "شارك" في عملية جمع ومعالجة المعطيات الشّخصيّة لكل زَائِر قام بالضّغط على صيغة الإعجاب، مع إرسالها مباشرة(المعطيات) إلى موقع فرع شركة(Facebook) المُقيم في ألمانيا أين تّم فيه إيواء المعطياتِ الشّخصية.

حيث لم تُقرّر المحكمة(CJUE) على أساس أحكام المسئولية عن فعل الغير-Ni Sous) traitant, ni Tiers au traitement)، بحُكمِ العلاقة العقدية التي ربطت بين شركة الأم(Facebook Inc) مع فرعها(Facebook Ireland)، أو مع صاحب صفحة فايس بوك(Wirtschaftsakademie) أو الموقع الالكتروني(Fashion ID) كمسئولين عن المعالجة.

لذا أكدّت المحكمة(CJUE) أنّ عملية جمع ومعالجة المعطيات الشّخصيّة للأفراد تمّت لتحقيق أغراض تجاريّة، التي تتطلّب الحصول المُسبق على الموافقة الصّريحة للمعني بمعالجة معطياته الشّخصيّة، مع وضع تحت تصرّفه المعلومات المتعلّقة بهوية القائم بالمعالجة والغاية التي جُمعَت من أجلها تلك المعطيات[2].

---

1) **Arrêt de la C.J.U.E** (Grande ch.), 5 juin 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, (Affaire C-210/16). http://curia.europa.eu/juris/document/(consulté le 10/07/2018.)

Arrêt de la C.J.U.E (2ème ch.), 29 juillet 2019, Fashion ID GmbH & Co. KG contre Verbraucherzentrale NRW, (Affaire C-40/17). http://curia.europa.eu/juris/document/(consulté le 02/08/2019.)

2) **Etienne WÉRY**, « Celui qui a une page Facebook est-il un « responsable de traitement » ? », Article publié le 13/11/2017, sur le site: https://www.droit-technologie.or, consulté le 18/02/2018.

Bojana SALOVIC, Etienne WÉRY, Thierry LÉONARD, «Celui qui a une page Facebook est coresponsable du traitement des données visiteurs ». Article publié le 05/06/2018, sur le site: https://www.droit-technologie.org, consulté le 17/06/2018.

والجدير بالذكر، أنّ المحكمة(CJUE) فصلت في وقائع القضيتين على أساس أحكام التوجيه الأوروبي رقم 46/95 المؤرخ في 24 أكتوبر 1995، المتعلق بحماية المعطيات الشخصية للأشخاص الطبيعيين مع حرية تنقل هذه المعطيات، الساري المفعول آنذاك، وليس وفقا لأحكام التنظيم الأوروبي رقم 679/2016 المتعلق بحماية المعطيات الشّخصية(RGPD)، الذي دخل حيّز التّنفيذ في 25 ماي 2018[1].

ب)– المسؤوليّة عن فعل الغير(La responsabilité du fait d'autrui):

نظّمت مختلف التّشريعات الوطنيّة الأحكام العامّة للمسؤوليّة عن عمل الغير وبالخصوص مسؤوليّة المتبوع عن أعمال تابعه على غرار المشّرع الفرنسي، الذي ألزم بموجب المادة 5/1384 من التّقنين المدني الفرنسي الرّؤساء والمتبوعون، بتحمّل مسؤوليّة الأضرار المرتكبة من طرف تابعهم أثناء تأدية وظائفهم[2]، وكذا المشّرع الجزائري الذي نص بموجب المادتين 136 و137 من التّقنين المدني على أنّ المتبوع، يكون مسؤولا عن الضّرر

Bojana SALOVIC, Thierry LÉONARD, Etienne WÉRY, « Bouton "J'aime" de Facebook: voici le verdict final de la CJUE ». Article publié en ligne le 29/07/2019, sur le site: https://www.droit-technologie.org, consulté le 17/08/2019.

1) **Directive 95/46/CE** du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. J.O.U.E, n° L 281/31 du 23/11/1995.(**Abrogé par (RGPD)**).

Art 94(RGPD) : « **Abrogation de la directive 95/46/CE 1.** La directive 95/46/CE est abrogée avec effet au **25 mai 2018**. […]. »

Art 99(RGPD) : « **Entrée en vigueur et application 1.** Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

2. Il est applicable à partir du **25 mai 2018**.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre. »

2) **Art.1384- 5 (Code civil(France)** - Dernière modification le 23 octobre 2019 Legifrance): « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde,[...] Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés. » http://www.legifrance.gouve.fr/

Philippe MALINVAUD, Dominique FENOUILLET, Droit des Obligations, 11e édition, Litec, France, 2010, pp. 462, 463 et s.

الذي أحدثه تابعه بسبب فعله الضّار الذي وقع منه في حالة تأدية وظيفته أو بسببها أو بمناسبتها، حيث تتحقّق علاقة التّبعية بين المتبوع وتابعه الذي يعمل لحساب المتبوع حتى ولو لم يكن هذا الأخير(المتبوع) حرّا في اختياره(تابعه)، في حين يُمكِن للمتبوع الرّجوع على تابعه في حالة ارتكابه لخطأ جسيم[1].

وعليه، فإنّ مسؤوليّة المتبوع عن أعمال تابعيه تتحقّق بمجرّد توافر شرطين: فالشّرط الأوّل يتعلّق بقيام رابطة التّبعية(Lien de préposition) التي تنشأ عادة عن عقد عمل أو عقد المناولة(La sous-traitance) أو أي سند قانوني أخر، الذي من خلاله يجب على المتبوع أن يُحسِن في اختيار تَابِع جدير بالثّقة يتمتّع بالكفاءات والخبرات المهنيّة والتّقنيّة المؤهّلَة له للقيام بمسؤولياته وواجباته المهنيّة، وأن يتصّرف(التّابِع) وفقا لإذن والتّعليمات الصّادرة من المتبوع[2]، بينما الشّرط الثّاني يتعلّق بخطأ التّابع(Le Préposé) حال تأدية الوظيفة أو بسببها أو بمناسبتها، كأن يقوم التّابع بإفشاء أو تعديل البيانات الشّخصيّة المتعلّقة بأصحاب شهادات التّصديق، أو يعرقل سير مبادلات التّجارة الإلكترونيّة، أو لا يحترم الواجبات والمتطلّبات والمعايير المحدّدة بموجب عقد تقديم الخدمة، الخ...

---

[1] أمر رقم 75– 58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، المعدل والمتمم، سالف الذكر.

تنص **المادة 136** على ما يلي:" يكون المتبوع مسؤولا عن الضرر الذي يحدثه تابعه بفعله الضار متى كان واقعا منه في حالة تأدية وظيفته أو بسببها أو بمناسبتها. وتتحقق علاقة التبعية ولو لم يكن المتبوع حرّا في اختيار تابعه متى كان هذا الأخير يعمل لحساب المتبوع."

وتنص المادة **137** على ما يلي:" للمتبوع حق الرجوع على تابعه في حالة ارتكابه خطأ جسيما."

[2] تنص **المادة 39** من القانون رقم 18–07 المؤرخ في 10 جويلية 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، على ما يلي: "عندما تجرى المعالجة لحساب المسؤول عن المعالجة، يجب على الأخير، اختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها. تنظم عملية المعالجة من الباطن بموجب عقد أو سند قانوني يربط المعالج من الباطن بالمسؤول عن المعالجة. وينص خصوصا على أن لا يتصرف المعالج من الباطن إلاّ بناء على تعليمات من المسؤول عن المعالجة وعلى تقيده بالالتزامات المنصوص عليها في المادة 38، أعلاه."

انطلاقا من ذلك، نص مشّرع الاتّحاد الأوروبي بموجب الفقرة الثانية من المادة 14 من التّوجيه الأوروبي رقم 2000–31 المتعلّق بالتّجارة الإلكترونيّة، على أنّ متعهّد الإيواء باعتباره كمتبوع يتحمّل المسؤوليّة التّقصيريّة عن الضّرر الذي أحدثه تابعه للغير، بسبب فعله الضّار، سواء كان المَتبوع لا يعلم أو يدري بالمحتوى غير المشروع أو عدم قيام التّابع بعد إخطاره من طرف المتبوع بسحبه أو جعل الوصول إليه غير مُمكِن، حيث أقّر المشّرع الفيدرالي بعدم تطبيق أحكام الفقرة الأولى من نفس المادة(14–1) الخاصّة بإعفاء متعهّد الإيواء من المسؤوليّة، وذلك بمجرّد تحقّق علاقة التّبعية بين المتبوع والتّابع[1].

والجدير بالذكر، أنّ المُورّد الإلكتروني يتحمّل المسؤوليّة التّقصيريّة عن فِعل الغَيْرِ بصفتهِ كمتبوع، عن الأضرار المترتّبة عن عدم تنفيذ الالتزامات من طرف مؤدّي خدمات آخرين تابعين للمورّد الإلكتروني، حيث يحق لهذا الأخير الرّجوع ضدّهم عند الإقتضاء، كما يمكنه(المورّد) التنّصل من كامل مسؤوليّته التّقصيريّة في حالة ما إذا أثبت أنّ عدم تنفيذ الالتزام يعود إلى المستهلك الإلكتروني أو إلى قوّة قاهرة[2].

ج)– المسؤوليّة النّاشئة عن الأشياء غير الحيّة (La responsabilité du fait des choses inanimées):

نص المشّرع الجزائري على أحكام المسؤوليّة النّاشئة عن الأشياء غير الحيّة بموجب المادة 138 من التّقنين المدني، التي من خلالها يكون الشّخص مسؤولا عن الضّرر الذي يُحْدِثُهُ الشّيء الذي تَوَلَى حِراستهِ، ما دام يتمتّع بِقُدرة الاستعمال والتّسيير والرّقابة عليهِ، حيث يُعفى حارس الشّيء من مسؤوليّته في حالة ما إذا أثبت أنّ ذلك الضّرر حدث بسبب لم يكن يَتَوَقَعُهُ مثل عمل الضّحية، أو عمل الغير، أو الحالة الطّارئة، أو القوّة القاهرة، ومن هُنا فإنّ أساس المسؤوليّة عن حراسة الشّيء قائم على أساس خطأ مُفترض وقوعه من حارس

---

1) **Art. 14-2(Directive 2000/31/CE sur le commerce électronique) : « (Hébergement)** […le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :…]. 2- Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'**autorité** ou le **contrôle** du prestataire. […]»

2) راجع نص المادة 18 من القانون رقم 18–05، الذي يتعلق بالتجارة الإلكترونية، سالف الذكر.

الشّيء، نَاتِج عن فُقدانِه للسّيطرة الفعليّة على ذلك الشّيء، إلاّ إذا أَثْبَتَ الحَارِسُ أنّ وقوع الضّرر نَاتِج عن سبب أجنبي لا يَدَ له فيهِ[1].

إنّ المسؤوليّة النّاشئة عن الأشياء غير الحيّة تتحقّق بمجرّد توافر شرطان: حيث يتعلّق الشّرط الأوّل بتواجد شيء في حراسة شخص يملك السّيطرة الفعليّة عليه، مع التّصرف فيه في الاستعمال والتّوجيه والرّقابة باعتباره أداة لتحقيق غرض مُعيّن، وأمّا الشّرط الثاني، يتمثّل في أن يتسبّب الشّيء المحروس في حدوث ضرر للغير الذي يجب عليه إثبات علاقة السّببية بين الضّرر وبين تدخّل الشّيء الإيجابي[2]، وبالتّالي تتحقّق المسؤوليّة التّقصيريّة لـ(م.خ.إ) بمجرّد توافر الأركان الثّلاثة(الخطأ والضّرر والعلاقة السّببية بينهما)، حيث يمكن أن يتعلّق الخطأ في تقصير(م.خ.إ) في اتّخاذ إجراءات تأمين مواقع التّجارة الإلكترونيّة، أو إدراج مَوْقِع إلكتروني غير موثوق ضمن قائمة المواقِع الالكترونية المحميّة، الخ...

وعليه، ذهب جانب من الفقه إلى إسناد المسئولية عن الأشياء لبعض(م.خ.إ) على غرار مزوّد البحث ومورّد المعلومة، على أساس الخطأ المُفترض وقوعه من حارس الشّيء نتيجة فقدان السّيطرة الفعليّة على الشّيء، وقد تكون العلاقة السّببية بين الضّرر وتدخّل الشّيء الإيجابي غير قابلة للدّحض أو إثبات العكس، بحُكمِ الإمكانيات التّقنيّة المتوّفرة لديهم وأنّ المعدّات المعلوماتية ليست في نهاية الأمر إلاّ شيء تستوجب الحِراسَة، حيث أخذت بعض الدّعاوى من هذه المسؤوليّة كأساس قانوني لها أمام القضاء[3]، ولعلّ أنّ الحديث على

---

1) **Lionel THOUMYRE**, « L'échange des consentements dans le commerce électronique », pp. 20, 21. Lex Electronica, vol. 05, n°1, Printemps 1999.

علي كحلون، مرجع سابق، ص ص 250، 251.

2) **محمد صبري السعدي**، مرجع سابق، ص ص 217– 227.

عايد رجا الخلايلة، مرجع سابق، ص ص 244– 252.

3) **Cyril ROJINSKY**, « Sens interdit – La responsabilité du créateur de lien hypertexte du fait du contenu illicite du site cible », pp. 03, 04, article publié le 17 décembre 2002, sur le site : https://www.juriscom.net(consulté le 18/11/2018.)

علي كحلون، مرجع سابق، ص ص 246، 250، 251.

المسئولية عن الأشياء في ظلّ المعاملات الالكترونية لا يزال يُثير العديد من النّقاشات في وسط رجال الفقه والقضاء، نظرا لحداثتها واحتكامها لأصول فنيّة معقّدة ومُتشّعبة وغامضة، وأنّ إسناد المسئولية لحارس الأشياء على أساس خطأ مُفترض لا يقبل إثبات العكس، لا يتلاءم مع طبيعة تدخّل كل(م.خ.إ)، وأنّ أحكام وشروط هذه المسئولية نادرا ما تتحقّق تجاه المحتوى غير المشروع بحكم صعوبة إثبات الضّرر على أنّه ناتِج عن الفعل المُستقّل للشّيء[1]، وبالتّالي لم يخرج الحديث عن إطار الخطأ الشّخصي في مجملهِ.

ثالثا– التّعويض في المسؤولية المدنية.

يعتبر التّعويض كجزاء مدني يقضي بضرورة تعويض الضّرر المُتسبّب للمضرور بفعل المسؤول الذي أخلّ بالتزاماته العقديّة أو القانونيّة، حيث تركت التّشريعات المُنظّمة لقواعد المسؤوليّة المدنيّة طريقة تحديد وتقدير التّعويض الواجب مَنْحِهِ أو دَفْعِهِ من طرف المسؤول عن الضّرر، سواء إلى المتعاقدين الذين قاموا بتحديده مُسبقاً في أحكام العقد أو في اتّفاق لاحِق، أو إلى قاضي الحكم الذي يفصل في موضوع النّزاع في حالة عدم اتّفاق الأطراف حول تحديد التّعويض اللاّزم مُسبقا في أحكام العقد أو في اتّفاق لاحق، حيث اشترطت مختلف التّشريعات الوطنيّة والأجنبيّة أن يكون التّعويض عادل ومنصف، يشمل الضّرر المادّي أو الضّرر المعنوي في حالة المساس بالحريّة أو الشّرف أو السّمعة[2].

---

1) **TGI Paris**, ord. réf., 31 juillet 2000, Bertrand Delanoé c/ Alta Vista Company, Kohiba Multimédia, Kohiba Productions, Objectif Net. Disponible sur le site : https://www.juriscom.net(consulté le 20/11/2018.)
Voir aussi: **Lionel THOUMYRE**, « L'échange des consentements dans le commerce électronique », op.cit., pp. 20, 21.

2) **Loi fédérale** complétant le Code civil suisse (Livre cinquième: Droit des obligations) du 30 mars 1911, RS 220 (État le 1er novembre 2019)**.**
Art.42 : « **1-** La preuve du dommage incombe au demandeur. **2-** Lorsque le montant exact du dommage ne peut être établi, le juge le détermine équitablement en considération du cours ordinaire des choses et des mesures prises par la partie lésée. »
Art.43/1-2 : « **1-** Le juge détermine le mode ainsi que l'étendue de la réparation , d'après les circonstances et la gravité de la faute. **2-** Des dommages-intérêts ne peuvent être alloués sous forme de rente que si le débiteur est en même temps astreint à fournir des sûretés. »

إذا لم يتّم تحديد التّعويض بموجب القانون أو العقد يَتَوَّلَى قاضي الحكم تحديده على أن يشمل التّعويض ما لحق للدّائن(المضرور) من خسارة وما فاتحه من كسب، بشرط أن يكون الضّرر المُتَسَبَّبِ ناتِج عن عدم الوفاء بالإلتزام أو التّأخر في الوفاء به، مع عدم إمكانية الدّائن أن يتفاداه ببذل جُهد معقول، فإذا كان العقد مصدر الإلتزام فلا يلتزم المدين(المسؤول عن الضّرر) الذي لم يرتكب غشًّا أو خطأ جسيم إلاّ بتعويض الضّرر المُمكِن تَوقُّعِهِ "وقت التّعاقد"، فإذا لم يقدّر القاضي أثناء الحكم قيمة التّعويض بصفة نهائيّة، يجب أن يَحْتَفِظَ للمضرور الحق في أن يطلب النّظر من جديد في تقدير قيمة التّعويض[1].

فإذا تجاوز الضّرر قيمة التّعويض المحدّد في الاتفاق أو العقد، يجوز للدّائن(المضرور) أن يُطالب بأكثر من هذه القيمة إذا أثبت أنّ المدين(المسؤول) قد ارتكب غشًّا أو خطأً جسيماً، غير أنّه في حال ما إذا أثبت المدين أنّه لم يلحق أيّ ضرر للدّائن فإنّ التّعويض المحدّد في الاتّفاق لا يكون مُستحقاً، وكذا يُمكِن للقاضي أن يُخَفِّضَ مبلغ التّعويض إذا أثبت المدين أنّه قد نفّذ جزء من الإلتزام الأصلي أو أنّ تقدير التّعويض كان مُفرِطا، ويجوز له كذلك إنقاص مِقدار التّعويض، أو لا يحكم بالتّعويض إذا كان الدائن(المضرور) قد اشترك بخطئه في إحداث الضّرر أو زاد فيه[2]، كما يمكِن للقاضي تحديد طرق تقدير التّعويض تِبَعاً للظّروف، فقد يكون التّعويض مُقسطاً أو في شكل إيراداً مُرَتَباً مع إلزام المدين في كلتا

راجع كذلك نص المادتين 182 و183 من الأمر رقم 75– 58 المؤرخ في 26 سبتمبر 1975 الذي يتضمن القانون المدني، المعدل والمتمم، سالف الذكر.

[1] تنص **المادة 131** من الأمر رقم 75– 58، على ما يلي:" يقدر القاضي مدى التعويض عن الضرر الذي لحق المصاب طبقا لأحكام المادتين 182 و182 مكرر مع مراعاة الظروف الملابسة، فإذا لم يتيسر له وقت الحكم أن يقدر مدى التعويض بصفة نهائية، فله أن يحتفظ للمضرور بالحق في أن يطالب خلال مدة معينة بالنظر من جديد في التقدير."

[2] راجع نصوص المواد **177، 184، 185**، من الأمر رقم 75– 58 الذي يتضمن القانون المدني، سالف الذكر.

الحالتين بأن يقدّر تأمينا، ويجوز للقاضي بناءا على طلب المضرور أن يأمر بإعادة الحالة إلى ما كانت عليه، أو أن يحكم ببعض الإعانات التي تتّصل بالفعل غير المشروع[1].

الفرع الثاني

المسؤوليّة الجزائيّة لمزوّدي خدمات الإنترنت

يُمكِن أَنْ يُكَيَّفَ الفعل غير المشروع الذي يرتكبه(م.خ.إ) على أساس جريمة يُعاقب عليها بموجب أحكام قانون العقوبات، كالمساس بالحياة الخاصّة، أو بأحد حقوق الملكيّة الفكريّة، أو تبييض الأموال عبر الإنترنت، الخ...، حيث يتحمّل الشّخص المعنوي بدوره المسؤوليّة الجزائيّة عن الجرائم المرتكبة لحسابه من طرف الأشخاص الذين يعملون لحسابه، وفقا لمبدأ الشّرعية الجزائيّة [2].

أولا– الأساس القانوني لجرائم مزوّدي خدمات الإنترنت.

إنّ إسناد المسؤوليّة الجزائيّة لـ(م.خ.إ) يتّم وفقا للتّكييف القانوني للجريمة المرتكبة عبر الإنترنت، فوفقا للمادة 6-I/3 من القانون رقم 2004-575 المتعلّق بالثّقة في الإقتصاد الرّقمي(LCEN)، والمادة 14 من التّوجيه الأوروبي رقم 2000-31 المتعلّق بالتّجارة الإلكترونيّة، فإنّ متعهّد الإيواء يتحمّل المسؤوليّة الجزائيّة بمُجرّد إثبات عِلْمِهِ بالفعل أو

---

[1] راجع نص المادة **132** من الأمر رقم 75- 58 الذي يتضمن القانون المدني، المعدل والمتمم، سالف الذكر.

[2] أمر رقم 66- 156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004، ج ر عدد 71 الصادر في 10 نوفمبر 2004.

تنص **المادة 51 مكرر** منه، على ما يلي:" بإستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه عندما ينص القانون على ذلك. إنّ المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال."

وتنص **المادة 01** على ما يلي:" لا جريمة ولا عقوبة أو تدابير أمن بغير قانون."

Code pénal (suisse) du 21 décembre 1937, RS 311.0 (État le 1er novembre 2019).

Art.1 : « Une peine ou une mesure ne peuvent être prononcées qu'en raison d'un acte expressément réprimé par la loi. »

المعلومة الإلكترونية غير المشروعة، ومع ذلك لم يتّخذ الإجراءات اللاّزمة لسحب المحتوى غير المشروع مع جعل إمكانية الوصول إليه غير مُمْكِناً[1]، حيث يمكن مساءلة مزوّد البحث كمزوّد إيواء وفقا لهذه الضوابط في حالة علمه بالمحتوى غير المشروع لصفحات الويب ولم يُبادر على سحبها، أو قطع الرّوابط(Liens hypertextes) نحو محتوى غير مشروع لمواقع بعد أن عَلِمَ به، ولعلّ أنّ خدمات مُزوّدي البحث تكون عُرضة للمساءلة الجزائيّة نظرا للنّزاعات التي تثيرها روابط الإحالة، بشأن الإضرار بحقوق الملكيّة الأدبيّة والصّناعيّة أو بقواعد المنافسة المشروعة أو بكرامة وحُرمة الحياة الخاصّة للأفراد[2].

كما أنّ مُزوّد الدّخول إلى الشّبكة أو مُزوّد نقل المعلومة(النّاقل)، يتحمّل كل واحد منهم المسؤولية الجزائية وفقا للمادة 12 من نفس التّوجيه(رقم 2000–31)، في حالة ما إذا تم إثبات أنّه مصدر المعلومة غير المشروعة، وقام بتحديد هوّية المُرسَل إليه مع تعديل محتوى المعلومة المُرسلَة[3]، أمّا في حالة قيامهم بأعمال الحفظ أو الخزن الآلية والوقتيّة وفي حدود

---

1) **Art.6.I-3(LCEN) :** « Les personnes visées au **2 ne** peuvent voir leur **responsabilité pénale engagée** à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible. L'alinéa précédent ne s'applique pas lorsque le destinataire du service **agit** sous l'**autorité** ou le **contrôle** de la personne visée audit alinéa. »

2) **Tribunal** de Première Instance de Bruxelles, 05/09/2006, S.A.R.L COPIEPRESS c/ S Google Inc. Disponible sur : https://www.juriscom.net(consulté le 12/01/2019/)

Voir aussi: **Thibault VERBIEST, Etienne WÉRY, «** La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés », op.cit., pp. 06,12- 15.

Maurizio DE ARCANGELIS, « La responsabilité des « fournisseurs d'hébergement » - Étude de droit comparé entre la France et l'Italie », pp. 16, 17. Article publié le 07 novembre 2001 sur le site : http://www.droit-technologie.org, consulté le 06/01/2019.

Mickaël LE BORLOCH, op.cit. pp. 68- 75.

3) **Art.12(**Directive européenne n° 2000/31/CE sur le commerce électronique) : « **Simple transport ("Mere conduit")** 1- Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire: **a)** ne soit pas à l'origine de la

الوساطة(Caching)، لنسخة عن كل معلومة إلكترونيّة(صفحة ويب)، لغرض نقلها لاَحِقاً على سبيل السُّرعة إلى طالبيها من المستخدمين(مثل خدمة البريد الإلكتروني...)، فيتحمّل كل واحد منهم(مزوّد الدّخول والنّاقل) المسؤوليّة الجزائيّة وفقا للمادة 13 من نفس التّوجيه، في حالة ما إذا تّم تعديل أو تغيير المعلومة الإلكترونية المخزّنة وعدم مراعاة الشّروط المتعلّقة بالنّفاذ، والحصول على بيانات استعمال المعلومة، أو عرقلة إجراءات تحديثها، أو لم يقم النّاقل أو مزوّد الدّخول بسحب المعلومة المُخزّنة، وجعل الوصول إليها غير مُمكِناً بالرّغم من علمهِ بعدم مشروعيتها أو لم يقم بذلك وفقا لأمر صادر من سلطة إداريّة أو قضائيّة[1].

لذا حثّ مشرع الاتّحاد الأوروبي بموجب المادة 1/15 من التوجيه رقم 2000–31 المتعلّق بالتّجارة الإلكترونيّة، دول الاتّحاد على عدم إلزام(م.خ.إ) برقابة المعلومات المُرسَلة أو التي تمّ حِفظها، أو البحث عن الأفعال غير المشروعة أو ظروف حدوثها، لكن بالرّجوع

---

transmission; **b)** ne sélectionne pas le destinataire de la transmission; et **c)** ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent **le stockage automatique, intermédiaire et transitoire des informations transmises**, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission. […]. »

1) **Art. 13**(Directive n° 2000/31/CE) : « **Forme de stockage dite "caching"** 1- Les États membre veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que: **a)** le prestataire ne modifie pas l'information; **b)** le prestataire se conforme aux conditions d'accès à l'information; **c)** le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises; **d)** le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information; et **e)** le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible. »

Voir aussi : - **Romain V.GOLA**, op.cit., pp. 488, 489.

إلى أحكام الفقرة الثّانية من نفس المادة(2/15)، نجد أنّه يمكن لدول الاتّحاد إلزام(م.خ.إ) بإعلام السّلطات العامّة المختصّة لكل دولة عن أيّ نشاطات أو معلومات غير مشروعة، وكذا تزويدها بمعلومات عن صاحب المحتوى غير المشروع، وهذا يعني أنّ(م.خ.إ) يلتزم بمُمارسة الرّقابة اللاّحقة على المحتوى غير المشروع، حيث يُسأل جزائياً في حالة علمه به ولم يقم بسحبه ومنع الوصول إليه، أو عرقلته للتّحريات القضائيّة أو أيّ إجراء آخر[1].

---

1) **Art.15** (**Directive 2000/31/CE**) : « (**Absence d'obligation générale en matière de surveillance**) **1-** Les États membres ne doivent pas imposer **aux** prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de **surveiller les informations** qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des **activités illicites**.
2- Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, **l'obligation d'informer promptement** les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de **communiquer aux autorités compétentes**, à **leur demande**, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement. »
Art.12 (**Directive 2000/31/CE**) : « (**Simple transport "Mere conduit"**) **1-** Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, […] ; **3-** Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation. »
Art.13 (**Directive 2000/31/CE**) : « (**Forme de stockage dite "caching"**) […] ; **2-** Le présent article n'affecte pas la possibilité, pour une **juridiction** ou une **autorité administrative**, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation. »
Art.14 (**Directive 2000/31/CE**) : « (**Hébergement**) […] ; **3-** Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible. » - Voir aussi : **Art.6.I-7 et 8(LCEN n° 2004-575).**
Voir aussi: Christophe **VERDURE**, « Les hébergeurs de sites web : victimes ou régulateurs de la société de l'information? », DCCR, n° 68/ 2005, pp. 40, 41, 42. Article disponible sur le site: https://www.droit-technologie.org, consulté le 08/01/2019.

وعليه، فإنّ(م.خ.إ) ملزمون بإخطار السّلطات القضائيّة عن كل فعل ذي طابع جزائي يتّم كشفه أثناء مزاولة النّشاط، ويمكن للسّلطة القضائيّة في حالة الاستعجال أو بناء لدعوى قضائيّة، أن تأمرهم بإتخاذ أيّ إجراء لمنع وقوع الضّرر أو إيقافه[1]، فوفقا للمادة 24 من القانون رقم 20–05 المؤرخ في 28 أفريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، يمكن للجهة القضائية أن تأمر(م.خ.إ) تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول، بالتّدخل الفوري لسحب أو تخزين المحتويات التي يُتيح الاطّلاع عليها، أو جعل الدّخول إليها غير ممكن، عندما تُشكِّل جريمة من الجرائم المتعلّقة بالتّمييز وخطاب الكراهيّة، المنصوص عليها في أحكام الفصل الخامس من نفس القانون[2].

وفي هذا السّياق، ألزمت المادة 10 من القانون رقم 09–04، الذي يتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، (م.خ.إ)، بتقديم يَدِ المُساعدة للسّلطات القضائيّة المكلّفة بالتّحريات القضائيّة لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، وإتاحتهم للمعطيات التي يتعيّن عليهم حفظها وفقا للمادة 11 من نفس القانون، مع التّقيد بالسريّة في العمليات التي ينجزونها بطلب من المُحققين، حيث يسألون جزائياً في حالة عرقلة التّحريات القضائيّة أو إفشاء أسرار التّحقيق[3].

كما يلتزم كذلك (م.خ.إ) وفقا لنص المادة 12 من القانون رقم 09–04، المذكور أعلاه، بالتّدخل الفوري لسحب المحتويات التي يتيحون الاطّلاع عليها، بمجرد عِلْمِهِم بطريقة مباشرة

---

[1] راجع المادة 3/30 من قانون رقم 15–04، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سالف الذكر.
Voir : Les **Arts.12/2** et **13(e)/2** et **14/3**(Directive n° 2000/31 sur le commerce électronique.)

[2] راجع نص المادتين 23 و24 من القانون رقم 20–05 المؤرخ في 28 أفريل 2020، الذي يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج ر عدد 25 الصادر في 29 أفريل 2020.

[3] راجع نص المادتين 10 و11 من القانون رقم 09–04، سالف الذكر.

أنظر كذلك في هذا الشأن: **زيبحة زيدان**، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار هدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص ص 153– 156.

أو غير مباشرة بمُخالفتها للقوانين، وتخزينها أو جعل الدّخول إليها غير مُمكِن، وكذا وضع ترتيبات تقنيّة تسمح بحصر إمكانية الدّخول إلى الموزّعات التي تَحْوِي معلومات مخالفة للنظام العام والآداب العامة، مع إخبار المشتركين لديهم بتواجدها[1].

ثانيا– الجزاءات المتعلّقة بمزوّدي خدمات الإنترنت.

يترتّب عن المسؤوليّة الجزائيّة لـ(م.خ.إ) مجموعة من الجزاءات الواردة بموجب قانون العقوبات(**أ**)، حيث يمكن للقاضي تطبيق الجزاءات المتعلّقة بالتّوقيع والتّصديق الإلكترونيين(**ب**)، أو النّطق بالجزاءات المتعلّقة بالمعطيات الشّخصيّة للأفراد(**ج**).

أ– الجزاءات الواردة في قانون العقوبات:

نص المشرع الجزائري في أحكام الأمر رقم 66–156 المؤرخ في 08 جويلية 1966 المتضمن لقانون العقوبات، المعدل والمتمم بموجب القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004،[2] على مجموعة من الجزاءات المتعلّقة بالجرائم الإلكترونية، والمتمثّلة في:

أ–1– الدخول غير المشروع إلى منظومة المعالجة الآلية للمعطيات: كلّ من يدخل أو يبقى عن طريق الغش في كلّ أو جزء من منظومة المعالجة الآلية للمعطيات أو يُحاول ذلك، يُعاقب وفقا للمادة 394 مكرر من نفس القانون، بالحبس من ثلاثة(03) أشهر إلى سنة(01)، وبغرامة من خمسين ألف دينار(50.000) إلى مائة ألف دينار(100.000)، وتُضاعف العقوبة في حالة ما إذا ترتب عن ذلك حذف أو تغيير معطيات المنظومة، وإذا ترتّب عن هذه الأفعال تخريب نظام تشغيل منظومة المعالجة الآلية، تكون العقوبة الحبس من ستة(06) أشهر إلى سنتين(02)، وغرامة ماليّة من خمسين ألف دينار(50.000) إلى مائة وخمسين ألف دينار(150.000).

---

[1] راجع نص المادة 12 من القانون رقم 09–04، سالف الذكر.

[2] أمر رقم 66– 156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، المعدل والمتمم بموجب القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004، ج ر عدد 71 الصادر في 10 نوفمبر 2004.

وكلّ من أزال أو عدّل أو أدخل بالغش مُعطيات في نظام المعالجة الآلية، يُعاقب وفقا للمادة 394 مكرر1 من نفس القانون، بالحبس من ستة(06) أشهر إلى ثلاث(03) سنوات وبغرامة من خمسمائة ألف دينار(500.000) إلى مليوني دينار(2.000.000).

أ–2– استخدام المعطيات المعالجة أو المخزنة في ارتكاب الجرائم: كلّ من يقوم عمداً وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مُخزنة أو معالجة، أو مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو إستعمال لأيّ غرض يُمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، يعاقب وفقا للمادة 394 مكرر2 من نفس القانون، بالحبس من شهرين(02) إلى ثلاث(03) سنوات وبغرامة من مليون دينار(1.000.000) إلى خمسة ملايين دينار(5.000.000)، ويمكن أن تُضاعف عليه وفقا للمادة 394 مكرر3 من نفس القانون[1]، العقوبات المنصوص عليها في القسم السابع مكرر1 من قانون العقوبات، في حالة ما إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام وذلك دون الإخلال بعقوبات أشدّ.

وكلّ مُشارك في مجموعة أو في إتفاق تألّف لغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا التحضير مجسّدا بفعل أو عِدَّةِ أفعال مادية، يُعاقب وفقا للمادة 394 مكرر5 من نفس القانون، بالعقوبات المُقرّرة لذات الجريمة، ويُعاقب وفقا للمادة 394 مكرر4 من نفس القانون، الشخص المعنوي المرتكب لإحدى جرائم القسم السابع مكرر1، بغرامة تُعادل خمس(05) مرّات الحدّ الأقصى للغرامة المُقررة للشخص الطبيعي.

أ–3– استخدام المعدّات والمواقع في ارتكاب الجرائم: يمكن للقاضي الجزائي أن يَحْكُمَ وفقا للمادة 394 مكرر6 من نفس القانون، بمُصادرة المعدّات المُستخدمَة مع إغلاق المَوَاقِعْ التي تكون محلاً لجريمة مُعاقب عليها وفقا للقسم السابع مكرر1 من قانون العقوبات، وإغلاق المحلّ الذي ارتُكبت فيه الجريمة بِعِلْمِ مالكها مع الإحتفاظ بحقوق الغير حسن النيّة.

---

[1] أمر رقم 66– 156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، معدل ومتمم، سالف الذكر.

أ–4– استخدام العملات الإفتراضية كعائدات إجرامية: يُعتبر تبييضا للأموال وفقا للمادة 389 مكرر من قانون العقوبات، كلّ الممتلكات المُكتسبة أو التي تم حيازتها أو المُستخدمة التي تُشكّل بِعِلْمِ الفاعل أو شريكه كعائدات إجرامية يُعاقب عليها القانون، ويقوم المُجرِم بتحويلها أو نقلها لغرض إخفاء أو تمويه مصدرها الحقيقي غير المشروع أو المشاركة أو المحاولة، أو المساعدة أو التآمر والتحريض على إرتكاب هذه الجريمة أو حتى تسهيل أو إسداء المشورة على ارتكابها، حيث يُعاقب المُجرِم وفقا للمادة 389 مكرر1 من نفس القانون، بالحبس من خمس(05) سنوات إلى عشرة(10) سنوات وبغرامة تقدّر من مليون دينار(1.000.000) إلى ثلاث ملايين دينار(3.000.000)، ويُمكِن أن تُطبّق عليه أحكام المادة 60 مكرر من نفس القانون، كما أنّ مُرتكِب هذه الجريمة على سبيل الاعتياد أو في إطار نشاطه المهني أو جماعة إجرامية، يُعاقب وفقا للمادة 389 مكرر2 من نفس القانون، بالحبس من عشرة(10) سنوات إلى عشرين(20) سنة وبغرامة تتراوح من أربعة ملايين دينار(4.000.000) إلى ثماني ملايين دينار(8.000.000).

وفي حالة المُحاولة على ارتكاب الجريمة، يعاقب وفقا للمادة 389 مكرر3 من نفس القانون بالعقوبات المقرّرة للجريمة التّامة، حيث يمكن أن يحكم القاضي وفقا للمادة 389 مكرر4 من نفس القانون[1]، بمصادرة الأملاك والمعدّات والأموال المجهولة المُستعملة في الجريمة، وكذا الحُكْم إلى جانب العقوبات الواردة في المادتين 389 مكرر1 ومكرر2، بعقوبة أو أكثر من العقوبات التّكميليّة الواردة في المادة 09 من قانون العقوبات.

ب– الجزاءات المتعلّقة بالتّوقيع والتّصديق الإلكترونيين:

نص المشّرع الجزائري بموجب الفصل الثاني(الباب الرابع) من القانون رقم 15–04 المحدد للقواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونين، على مجموعة من الجزاءات المتعلّقة بعملية التّصديق الإلكتروني، والمتمثلة في:

---

[1] راجع نص المواد 389 مكرر5 و389 مكرر6 و389 مكرر 7 من الأمر رقم 66–156 المؤرخ في 08 جويلية 1966، الذي يتضمن قانون العقوبات، معدل ومتمم، سالف الذكر.

ب–1– التّحايل في الحصول على شهادة التّصديق: كلّ من أدلى بإقرارات كاذبة للحصول على شهادة التّصديق الإلكتروني، يعاقب وفقا للمادة 66 من نفس القانون، بالحبس من ثلاثة(03) أشهر إلى ثلاث(03) سنوات وبغرامة مالية تتراوح من عشرين ألف دينار(20.000) إلى مائتي ألف دينار(200.000) أو بإحدى هاتين العقوبتين فقط، وكلّ شخص يستعمل شهادة التّصديق لغير الأغراض التي مُنحت من أجلها، يُعاقب وفقا للمادة 74 من نفس القانون[1]، بغرامة من ألفي دينار(2.000) إلى مائتي ألف دينار(200.000)، وكلّ من يخّل عمدًا بالتزام تحديد هوية طالب شهادة التّصديق الموصوفة، يُعاقب وفقا للمادة 69 من نفس القانون، بالحبس من شهرين(02) إلى ثلاث سنوات، وبغرامة مالية تتراوح من عشرين ألف دينار(20.000) إلى مائتي ألف دينار(200.000) أو بإحدى هاتين العقوبتين فقط.

ب–2– عدم إلتزام(م.خ.ت.إ) بسريّة البيانات: كلّ (م.خ.ت.إ) لا يقوم بالحفاظ على سريّة بيانات شهادة التّصديق، يُعاقب وفقا للمادة 70 من نفس القانون، بالحبس من ثلاث(03) أشهر إلى سنتين(02) وبغرامة من مائتي ألف دينار(200.000) إلى مليون دينار (1.000.000) أو بإحدى هاتين العقوبتين فقط، وكلّ من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خَاصَّة بالغيرِ، يُعاقب وفقا للمادة 68 من نفس القانون، بالحبس من ثلاث(03) أشهر إلى ثلاث(03) سنوات وبغرامة من مليون دينار (1.000.000) إلى خمسة ملايين دينار(5.000.000) أو بإحدى هاتين العقوبتين فقط.

ب–3– المساس بالمعطيات الشّخصيّة: كل (م.خ.ت.إ) يقوم بجمع البيانات الشّخصيّة للمعني من دون الحصول على موافقته الصريحة، مع عدم استعمالها لغرض منح وحفظ شهادة التصديق، يُعاقب وفقا للمادة 71 من نفس القانون، بالحبس من ستة(06) أشهر إلى

---

[1] قانون رقم 15–04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، سالف الذكر.

راجع كذلك نص المادتين **17** و**18** من القانون رقم 15–03 المؤرخ في 01 فيفري 2015، الذي يتعلق بعصرنة العدالة، ج ر عدد 06 الصادر في 10 فيفري 2015.

ثلاث(03) سنوات، وبغرامة مائتي ألف دينار(200.000) إلى مليون دينار(1.000.000) أو بإحدى هاتين العقوبتين فقط؛

ب–4– الإخلال بالنّظام القانوني لمزاولة خدمات التّصديق الإلكتروني: كلّ (م.خ.ت.إ) يباشر خدمات التّصديق من دون حصوله على ترخيص، أو يستأنف أو يُواصِل نشاطه بالرّغم من سحب ترخيصه، يُعاقب وفقا للمادة 72 من نفس القانون، بالحبس من سنة واحدة(01) إلى ثلاث(03) سنوات وبغرامة تتراوح من مائتي ألف دينار(200.000) إلى مليوني دينار(2.000.000) أو بإحدى هاتين العقوبتين فقط، وتُصادَر التّجهيزات التي أُستعملت لارتكاب الجريمة طبقا للتّشريع المعمول به، وكذا يُعاقب وفقا للمادة 67 من نفس القانون، كلّ(م.خ.ت.إ) يُخالف التزام إعلام(س.ض.ب.م.إ) بالتوقّف عن نشاطه، بالحبس من شهرين(02) إلى سنة(01)، وبغرامة تُقدّر من مائتي ألف دينار(200.000) إلى مليون دينار(1.000.000)، أو بإحدى هاتين العقوبتين فقط.

ب–5– الإخلال بالسّر المهني لمهام التّدقيق: كلّ شخص يقوم أثناء مباشرة مهام التّدقيق بكشف معلومات سريّة، يعاقب وفقا للمادة 73 من نفس القانون[1]، بالحبس من ثلاث(03) أشهر إلى سنتين(02) وبغرامة من عشرين ألف دينار(20.000) إلى مائتي ألف دينار(200.000) أو بإحدى هاتين العقوبتين فقط، كما أنّ الشخص المعنوي الذي ارتكب إحدى الجرائم الواردة في الفصل الثاني من نفس القانون، يُعاقب بغرامة مالية تعادل خمس مرّات الحدّ الأقصى للغرامة المُطبّقة على الشّخص الطبيعي.

ج– الجزاءات المتعلّقة بالمعطيات الشّخصيّة:

فرض المشرع الجزائري في القانون رقم 18–07 المؤرخ في 10 جويلية 2018 المتعلق بحماية المعطيات الشخصية للأشخاص الطبيعيين، مجموعة من الجزاءات والمتمثلة في:

---

[1] قانون رقم 15–04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، سالف الذكر.

ج–1– المساس بالحياة الخاصّة والحرّيات العامّة: كل من يَمُسَّ بحقوق وشرف وسُمعة الأفراد أثناء مُعالجة معطياتهم الشّخصيّة، يُعاقب وفقا للمادة 54 من نفس القانون، بالحبس من سنتين(02) إلى خمس سنوات(05) وبغرامة تُقدّر من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000).

ج–2– عدم الحصول على الموافقة الصريحة للشّخص المعني: كل من يقوم بمعالجة المعطيات الشّخصيّة للأفراد من دون موافقتهم الصّريحة، يُعاقب بالحبس من سنة(01) إلى خمس(05) سنوات مع غرامة مالية تتراوح من مائتي ألف دينار(200.000) إلى ثلاثمائة ألف دينار(300.000)، ويُعاقب وفقا للمادة 55 من نفس القانون، بتلك العقوبة في حالة القيام بالمعالجة بالرّغم من اعتراض الشّخص المعني.

وكل من يعالج المعطيات الشّخصيّة الحسّاسة من دون الموافقة الصّريحة للمعني، يُعاقب وفقا للمادة 57 من نفس القانون[1]، بالحبس من سنتين(02) إلى خمس(05) سنوات وبغرامة تتراوح من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000)، وفي حال جمع المعطيات الشّخصيّة بطريقة غير مشروعة يُعاقب وفقا للمادة 59 من نفس القانون، بالحبس من سنة(01) إلى ثلاث سنوات(03) وبغرامة من مائة ألف دينار (100.000) إلى ثلاثمائة ألف دينار(300.000)، وفي حالة معالجة المعطيات الشّخصيّة لغير الأغراض المُصرَّحِ أو المرخَّصِ لَهَا، يُعاقب وفقا للمادة 58 من نفس القانون، بالحبس من ستة(06) أشهر إلى سنة(01) وبغرامة من ستين ألف دينار(60.000) إلى مائتي ألف دينار(200.000) أو بإحدى هاتين العقوبتين فقط.

ج–3– مخالفة الإجراءات المُسبقة عن المعالجة: كل شخص يقوم بمعالجة المعطيات الشّخصيّة من دون حصوله على تصريح مُسبق أو ترخيص من السّلطة الوطنيّة، يُعاقب وفقا للمادة 56 من نفس القانون، بالحبس من سنتين(02) إلى خمس(05) سنوات وبغرامة من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000)، ويُعاقب بتلك

---

[1] قانون رقم 18–07 مؤرخ في 10 جويلية 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

العقوبة كل من قام بتصريحات كاذبة أو واصل نشاطه بالرّغم من سحب وصل تصريحه أو ترخيصه، وفي حالة قيام المسؤول عن المعالجة من دون ترخيص السّلطة الوطنيّة، بنقل أو إرسال أو تحويل معطيات شخصيّة إلى دولة أجنبيّة من شأنه أن يمس بالأمن العمومي أو المصالح الحيويّة للدّولة، أو لا تضمن تلك الدّولة حماية الحياة الخاصّة وحرّيات وحقوق الأفراد، يُعاقب وفقا للمادة 67 من نفس القانون[1]، من سنة(01) إلى خمس(05) سنوات، وبغرامة من خمسمائة ألف دينار(500.000) إلى مليون دينار(1000.000).

ج–4– عرقلة عمل السّلطة الوطنيّة: كل من يعترض عمل السّلطة الوطنيّة لإجراء التّحقيق، أو يرفض تزويد أعوانها بالمعلومات أو يقوم بإخفائها أو إزالتها، يُعاقب وفقا للمادة 61 من نفس القانون، بالحبس من ستة(06) أشهر إلى سنتين(02) وبغرامة من ستين ألف دينار(60.000) إلى مائتي ألف دينار(200.000) أو بإحدى هاتين العقوبتين فقط.

ج–5– الإخلال بالسّر المهني: كل من يسمح للغير بالولوج إلى المعطيات الشّخصيّة يُعاقب وفقا للمادة 61 من نفس القانون، بالحبس من سنتين(02) إلى خمس(05) سنوات وبغرامة من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000)، وكل من يَلِجُ خارج القانون إلى السّجل الوطني لحماية المعطيات الشّخصيّة، يُعاقب وفقا للمادتين 62 و63 من نفس القانون، بالحبس من سنة(01) إلى ثلاث سنوات(03) وبغرامة من مائة ألف دينار(100.000) إلى ثلاثمائة ألف دينار(300.000) أو بإحدى هاتين العقوبتين فقط، وفي حال إفشاء أعضاء السّلطة الوطنيّة للمعلومات، تُطبق عليهم المادة 301 من قانون العقوبات.

ج–6– المساس بحقوق المعني بالمعالجة: كل مسؤول عن معالجة المعطيات الشّخصيّة يرفض دون أي سبب مشروع لحقوق الإعلام أو الولوج أو التّصحيح أو الاعتراض، المنصوص عليها بموجب أحكام نصوص المواد 32 و34 و35 و36 من نفس القانون،

---

[1] قانون رقم 18–07 مؤرخ في 10 جويلية 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

يُعاقب وفقا للمادة 64 من نفس القانون، بالحبس من شهرين(02) إلى سنتين(02) وبغرامة تتراوح من عشرين ألف دينار(20.000) إلى مائتي ألف دينار(200.000).

ج–7– الإخلال بسرية وأمن المعطيات الشّخصيّة: إذا لم يقم المسؤول عن المعالجة أو المعالج من الباطن، بوضع تدابير تقنيّة وتنظيميّة لضمان أمن المعطيات الشّخصيّة، يُعاقب وفقا للمادة 65 من نفس القانون، بغرامة من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000)، ويُعاقب بتلك العقوبة كل من احتفظ بالمعطيات الشّخصيّة خارج المدّة الواردة في القانون أو التّصريح أو التّرخيص، وكلّ إخلال بالتزام إعلام السّلطة الوطنيّة والشّخص المعني بانتهاك معطياته الشّخصيّة، يُعاقب وفقا للمادة 66 من نفس القانون، بالحبس من سنة(01) إلى ثلاث(03) سنوات وبغرامة من مائة ألف دينار(100.000) إلى ثلاثمائة ألف دينار(300.000) أو بإحدى هاتين العقوبتين فقط، فإذا تسبّب المسؤول عن المعالجة أو المعالج من الباطن، ولو بإهمال، الاستعمال التّعسّفي أو التدليسي للمعطيات المُعالَجة أو المُستلَمة أو إتاحتها للغير، يُعاقب وفقا للمادة 69 من نفس القانون[1]، بالحبس من سنة(01) إلى خمس(05) سنوات وبغرامة من مائتي ألف دينار(200.000) إلى خمسمائة ألف دينار(500.000).

[1] راجع كذلك المواد 70 و71 و 73 و74 من القانون رقم 18–07 المؤرخ في 10 جويلية 2018، الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، سالف الذكر.

خلاصة الفصل الثاني

من خلال الدّراسة السّابقة، نصل إلى أنّ الملكيّة الذّهنيّة الرّقميّة تنطوي على مُصنّفات رقميّة محميّة في إطار تشريعات حقوق الملكيّة الفكريّة، على غرار برمجيات الحاسوب وقواعد البيانات وطبوغرافيا الدّوائر المتكاملة، حيث ساهمت الثّورة الرّقميّة في ظهور مصّنفات رقميّة حديثة لا تختلف في مدلولها أو تكوِينُهَا عن المُصّنفات التّقليديّة، ولم تكن مألوفة ومحميّة في إطار قوانين حقوق الملكيّة الفكريّة، كأسماء مواقع الإنترنت وما تتضمّنه من عناصر التّصميم لصفحات الويب، وروابط الإحالة، والوسائط المتعدّدة، الخ... التي تّم اِبْتِكَارُهَا عبر الإنترنت حيث تتطلّب بدورها الحماية القانونيّة لها.

أثارت أسماء مواقع الإنترنت العديد من النّزاعات مع حقوق الملكيّة الفكريّة المملوكة للغير، الأمر الذي يتطلّب توافُر مرجعيّة قانونيّة لفّض النّزاعات بشأن أسماء المواقِع، حيث قامت هيئة الإنترنت لمنح الأسماء والأرقام المخصّصة(ICANN) بناءً على توصيات المنظّمة العالميّة لحماية الملكيّة الفكريّة(WIPO)، اعتماد مبادئ وقواعد السّياسة الموّحدة(UDRP)+Les règles)) لتسويّة نزاعات أسماء مواقع الإنترنت، التي تُطبّق على النّزاعات النّاشئة فيما بين مُسَّجِلِي أسماء المواقِع ومالِكي العلامات(التّجاريّة أو الخدمة)، وليس النّزاعات النّاشئة فيما بين أسماء المَواقِع بِحَدِّ ذَاتِهَا.

لذا يُمكِن لأطراف النّزاع بشأن اسم موقِع الإنترنت اللّجوء إلى الهيئات المسؤولة على تسجيل أسماء المواقع العليا الوطنيّة(Registres) لتسوية النّزاع وفقا للقوانين المحليّة، التي قد لا تتّبع إجراءات السّياسة المُوّحدة((Procédures(UDRP) المعتمدة من طرف هيئة آيكان، كما يمكن لهؤلاء الأطراف اللّجوء إلى إحدى مراكز التّسوية المعتمدة من طرف هيئة الآيكان للفصل فيه وفقا لإجراءات السّياسة الموّحدة، التي من خلالها تقوم الهيئة(Panel) المُعيّنة من طرف المركز، بالفصل في موضوع النّزاع بقرار، الذي يتّم تنفيذه مُباشرةً من طرف مكتب التّسجيل بعد مرور العشرة(10) أيام الموالية لتاريخ تبليغه من طرف المركز، فمن خلال هذه المدّة يمكن للطرف الذي صُدر ضِدَّهُ القرار أن يرفع دعوى قضائيّة ضّد الطرف الذي صَدَرَ

لمصلحته القرار، وذلك لإعادة الفصل من جديد في قضية النّزاع، وليس لغرض "إلغاء" قرار التّسوية((Décision(UDRP)، الذي يقتصر فقط حول رفض الطلب أو إلغاء اسم الموقِع أو تحويل تسجيله إلى مالك العلامة، حيث يَتوقَّف مكتب التّسجيل عن تنفيذه خلال تلك الفترة(10 أيام) ويَمتنِع عن اتخاذ أيّ إجراء آخر، حَتَّى يَسْتَلِمَ مَا يُثبِتُ سواء وجود حلّ بين الطرفين أو قد تّم التّنازل عن الدّعوى القضائيّة وسحبها، أو عدم الاستمرار في استخدام اسم الموقِع المتنازع عليه.

تُشّكل المُمارسات التّجاريّة عبر بعض تقنيات روابط الإحالة تعدّيًا أو تجاوزًا على حقوق صاحب المصّنف الرّقمي، حيث يُنْظَرُ على أنّها أفعالا غير مشروعة مُخالفة للقواعد المنظّمة للمُمارسات التّجاريّة، الأمر الذي يَدْفَعُ بالطرف المُتضّرِر إلى طلب التّعويض في إطار إجراءات رفع الدّعوى المدنيّة أمام الجهات القضائيّة المُختصّة، أو يتحمّل الفاعِل المسؤوليّة الجزائيّة على أساس جُنحة تقليد مُعاقب عليها وفقا للقوانين الخاصّة بحماية حقوق الملكيّة الفكريّة، كما يمكن للمُتضّرر الاستعانة بالأحكام الجزائيّة المزدوجة لأعمال المنافسة غير المشروعة، مادام أنّ أعمال المُنافسة غير المشروعة تُشّكل بطابعها الضّار الفِعْلُ الوَحيد الذي يُجَرِّمُهُ القانون.

إنّ الخدمات التي يتيحها(م.خ.إ) يتّم التّعامل معها في إطار الضّوابط العقديّة والقانونيّة، التي تُحدِّد حقوق والتزامات كل طرف في عقد تقديم الخدمة، الذي من خلاله يتحمّل مُزوّد الخدمة المسؤوليّة المدنيّة نتيجة إخلاله بالتزام عقدي أو قانوني، ممّا يدفع بالشّخص المُتضّرر(المستهلك) إلى طلب التّعويض، استنادا إلى قواعد المسؤوليّة المدنيّة بشّقيها العقدي أو التّقصيري، كما أنّ الفّعل غير المشروع الذي يرتكبه(م.خ.إ) يُمكِن أَنْ يُكَيَّفَ على أساس جريمة يُعاقب عليها بموجب أحكام قانون العقوبات، كالمساس بالحياة الخاصّة أو اختراق مواقِع التّجارة الإلكترونيّة الخ...، حيث يتحمّل المسؤوليّة الجزائيّة وفقا لمبدأ الشّرعية الجزائيّة(Principe de Légalité Pénale) القائم على مبدأ "لا جريمة ولا عقوبة بدون نص".

خـاتمــة:

تُحظى مواقع التّجارة الإلكترونيّة بأهمّية بالغة في إنعاش الاقتصاد الرّقمي، وتحريك مبادلات التّجارة الالكترونيّة التي تتّم عبر تقنيّة المعلومات(الإنترنت)، حيث تُتيح للمُورّد الإلكتروني إمكانات وتطبيقات تقنيّة حديثة، تُسّهل له مهمّة إتّباع إستراتيجيات تسويق جديدة لمنتجاته، بطريقة سريعة، مع الاقتصاد في التّكاليف، وتحديد الجمهور المُستهدف والشّرائح المقصودة في آن واحد، وذلك من خلال القيام بحملات الدّعاية الإعلانيّة، وإجراء عمليات البيع، مُتخّطيا في ذلك الحدود الإقليميّة للدّولة التي يُقيم أو يتواجد فيها المستهلك، في حين يصعب تحقيق كلّ ذلك في ظّل الممارسات التّجاريّة المُتّبعة في صورتها التّقليديّة.

تساهم مواقع التّجارة الالكترونيّة في تحسين مستوى وَجَوْدَةَ القرارات الشّرائيّة لدى المستهلكين أو العملاء، حيث تتيح لهم فرص التّجول والبحث عبر المواقع الإلكترونيّة التّجاريّة المنتشرة بكثرة عبر شبكة الويب، مع اختيار الأفضل منها بما يتناسب وقدرتها أو كفاءتها على إشباع حاجيات المستهلكين، وتلبية رغباتهم وفق السّعر والجودة والمواصفات المتطلّبة في أيّة سلعة أو خدمة، وكذا فتح منافذ التّوزيع وكيفية الحصول عليها الخ....

ونتيجة لذلك، أصبح من المُمكِن على المستهلك أو العميل اقتناء أيّة سلعة أو خدمة معيّنة، بمجرّد الدّخول الفّوري لأيّ موقع تجاري وقع الاختيار عليه، وتصّفح محتواه، والاطّلاع على كتالوجاته، مع الالتزام بدفع مستحقّاتها(المنتجات) بتقنيات دفع إلكترونيّة مؤمّنة، وذلك في وقت قصير من دون أيّ انتظار أو تنّقلٍ إلى عين المكان.

قامت الحكومة الجزائريّة مؤخّرا بإطلاق خدمة الدّفع الإلكتروني عبر شبكة الإنترنت، بُغية تدارك التأخّر الكبير الذي شهدته بلادنا في مجال الثّورة الرّقميّة، وعصرنة مختلف القطاعات الاقتصاديّة الحيويّة، بما فيها القطاع المصرفي، وذلك بالمقارنة مع الجارتان تونس والمغرب وبالمقارنة مع البلدان العربيّة والغربيّة السّباقة إلى ذلك.

كان من المُسْتَحْسَنِ على المشّرع الجزائري قبل إطلاق خدمة الدّفع الإلكتروني عبر الإنترنت، المبادرة على إصدار ترسانة من القوانين، من خلالها يقوم بتأطير هذه الخدمة بموجب قانون خاص بالتّجارة الإلكترونيّة، وقانون خاص بتنظيم التّعامل بالعملات الالكترونيّة، كوسيلة دفع حديثة، إلى جانب القوانين الخاصّة بحماية كلّ من المعطيات الشّخصيّة والمستهلك الإلكتروني، بالإضافة إلى إطلاق مخطّط التّصديق الإلكتروني المنتهج في الجزائر.

إنّ الجَزَائِرَ، على غرار غالبيّة دول العالم، ترفع حاليًا شعار التّحول إلى مجتمع المعلومات والمعرفة، من خلال إصدار القانون رقم 15-04 المتضمّن القواعد العامّة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، الذي يُمَهِّدُ الطّريق نحو تفعيل أنشطة التّجارة والمعاملات الإلكترونيّة على نطاق واسع، مع إعداد وتنظيم مخطّط التّصديق الإلكتروني الهرمي، الذي يستوجب تطوير شبكات الاتّصالات، ونشر وتعميم استخدام شبكة الإنترنت، بالإضافة إلى زيادة معدّل تدفّقها.

تُشكّل الإنترنت، باعتبارها شبكة الشّبكات، الوسط أو البيئة التي تتّم عبرها مختلف المعاملات الالكترونيّة، وبالخصوص التّجارة الإلكترونيّة والعمليات المصرفيّة، وذلك بعدما تّم تجريدها من طابعها المادّي التّقليدي، وتحويلها إلى وسائل أو دعامات إلكترونيّة حديثة، تتداول وتُخزّن فيها مختلف البيانات الإلكترونيّة، وبالتّالي فإنّ تشييد بُنية معلوماتيّة وطنيّة شاملة – متعدّدة الأوجه والمستويات مع تبّني التّوجه نحو مجتمع المعلومات أو الرّقمنة – يتطلّب حتمًا نقل أو تحوّل المجتمع والدّولة والمؤسّسات، إلى بيئة المخاطر المتعلّقة بانتحال الهويّة واختراق البيانات الالكترونيّة، وإنكار عمليات البيع والشّراء، وانتهاك الأسرار السّياسية والعسكريّة الخ...، ممّا يؤدّي إلى تهديد الأمن الوطني ككل.

لقد أجمع خبراء أمن المعلومات، على أنّ الأمن بصفة مطلقة ينعدم بتاتًا في البيئة الإلكترونيّة الافتراضيّة، في حين يُكيّف "كخطأ جسيم" قيام أيّة دولة بتشييد بِنْيَة معلوماتيّة وطنيّة واسعة على كلّ المستويات، دون القيام بتطوير سياسة أو "إستراتيجيّة وطنيّة شاملة"

لحماية هذه البنيّة وأمن البيانات والمعلومات الإلكترونيّة المتداولة عبرها، وذلك بالنّظر إلى حجم الأخطار، وتزايد التّهديدات الإلكترونيّة التي يصعب التّنبؤ بها في غالب الأحيان.

إنّ التّهديدات الالكترونيّة غالبا ما يكون وراء تنفيذها أفراد ذي كفاءات وقدرات عالية المستوى في مجال تكنولوجيا الإعلام والاتّصال، كما يُمكِن أن تكون أيّة دولة معيّنة تتحكّم في تقنيات الثّورة الرّقميّة من وراء تنفيذ هذه الهجمات الإلكترونيّة، بُغية الحصول على الأسرار الصّناعيّة أو الاقتصاديّة أو العسكريّة للدّول الأخرى، أو حتّى تغيير المسار الانتخابي لمرشّح حزب معيّن الخ...، وبالتّالي فإنّ البنيّة المعلوماتيّة الشّاملة تتطلّب إعداد سياسة أمن معلوماتيّة موثوقة، شاملة ومُنسّقة، وتحتاج إلى إعداد هيئات مؤسّساتيّة مؤهّلة تتكفّل بذلك، تقوم تحت إشراف الدّولة، حيث لا يصّح تركها لاجتهادات أفراد ومؤسّسات وخبراء، مهما علا شأنهم وتجاربهم وقدراتهم في مجال تكنولوجيا الإعلام والاتّصال.

إنّ ضمان أمن البيانات أو المعلومات المتداولة داخل البنيّة المعلوماتيّة الاقتصاديّة بصفة عامّة، يُدِّعم حتمًا الأمن الوطني لأيّ بلد، حيث يتطلّب الأمر تقديم رؤى جديدة لمناهج وأساليب وتقنيات تداول المعلومات، وتنفيذ مُخطّطات واستراتيجيات شاملة، موثوقا بها في مجال أمن المعلومات، باعتبار هذا الأخير قضية تقنيّة بحتة، وركيزة أساسيّة من ركائز الأمن الوطني الشّامل، التي تتطلّب رفعها إلى مستوى التّعامل السّياسي والإستراتيجي.

إضافة إلى ما سبق، ينبغي على أيّ كيان أو مؤسسة اقتصاديّة، العمل على تقليل مختلف الأخطار أو التّهديدات الإلكترونيّة، من خلال سّد الثّغرات أو الهفوات السّائدة في نظم الحماية الأمنيّة للشّبكات، ذلك لأنّ جميع مكوّنات الشّبكة الواحدة تحوي مَواطن ضُعف قابلة للاستغلال من طرف أهل الاختصاص، الذين يتمتّعون بدراية كافية، ومؤهّلات عالية في مجال اختراق نظم أمن حماية المعلومات، الأمر الذي يستوجب بذل الجهود الكافية في تدريب مُستخدمي الحاسبات الآليّة، وبالخصوص المستهلك الالكتروني، وتوعيّته بأهمّية وضرورة تثبيت تحديثات في أنظمة التّشغيل والبرامج المضّادة للفيروسات والبرامج الخبيثة

الضّارة، مع الالتزام بالتّسوق الآمن، من خلال حُسن اختيار المواقع التّجاريّة الآمنة، وتجنّب زيارة مواقع الإنترنت غير الآمنة، واستخدام التّوقيعات الإلكترونيّة الموصوفة.

تعتبر التّوقيعات الالكترونيّة الموصوفة وسيلة أمان حديثة لتوثيق المعاملات الإلكترونيّة، تتطلّب الإعداد والتّنظيم المُحكم والدّقيق، لجميع المسائل التّقنيّة المتعلّقة بمرفق المفاتيح العموميّة، حسب ما هو متلائم ومتوافق مع السّياسة العامّة المنتهجة لكلّ دولة، كتحديد شكل مرفق المفاتيح العموميّة وعدد مُستويات السّلطة التي يشملها، وما إذا كان لا يُسمح إلاّ لسلطات تصديق معيّنة تنتمي لمرفق المفاتيح العموميّة، بإصدار أزواج مفاتيح التّشفير، أو من المُمكِن أن يُصْدِرَ أطراف التّعامل الإلكتروني بأنفسهم تلك الأزواج من المفاتيح، وتحديد ما إذا كانت سلطات التّصديق الإلكتروني. التي تشهد بصّحة أزواج مفاتيح التّشفير. ينبغي أن تكون عموميّة أو خاصّة، ومدى خضوعها للتّرخيص أو الاعتماد من طرف الدّولة.

كما أنّ العلاقات المُنْشَئَة فيما بين سلطات التّصديق الإلكتروني المنتميّة لأكثر من مرفق مفاتيح عموميّة، تشّكل مصدر قلق مُهدّد للمعاملات الإلكترونيّة، الشّيء الذي يستدعي النّظر في مدى إمكانية إبرام اتفاقيات التّصديق المتبادل، للاعتراف بالقيمة القانونيّة للتّوقيعات الإلكترونيّة، وشهادات التّصديق الإلكتروني المعتمدة التي يُصدرها(م.خ.ت.إ) التّابع لكلّ مرفق مفاتيح عموميّة، فمهما كان نموذج التّصديق الإلكتروني المنتهج في أيّ دولة، فإنّ المواءمة فيما بين سياسات التّصديق، تستدعي تواجد سلطة تصديق رئيسيّة لإبرام اتفاقيات الاعتراف المتبادل فيما بين مرافق المفاتيح العموميّة.

علاوة على ما سبق ذكره، نجد أنّ الآليات التّقنيّة التي تتيحها تكنولوجيا الإعلام والاتّصال لا تكفي لوحدها لضمان أمن مواقع التّجارة الإلكترونيّة، حيث تتضمّن هذه الأخيرة على محتويات أو مصّنفات رقميّة من خلق وإبداع الفكر البشري، والتي تستوجب الحماية القانونيّة بموجب القوانين الخاصّة بحماية حقوق الملكيّة الفكريّة، حيث نصّت معظم هذه القوانين في أحكامها– إلى حدّ الآن– على حماية ثلاثة أنواع من حقوق الملكيّة الفكريّة الرّقميّة، وهي برمجيات الحاسوب وقواعد البيانات وطبوغرافيا الدّوائر المتكاملة، في حين

تُثار التّساؤلات حول مدى القدرة على حماية حقوق الملكيّة الفكريّة الرّقميّة التي تتضمّنها محتويات مواقع التّجارة الإلكترونيّة، أو تلك المصّنفات الرّقميّة التي جعلت بيئة الإنترنت الوسط الوحيد الذي تّم إحداثها أو خلقها فيها، كأسماء مواقع الإنترنت والرّسوم والعلامات وإعلانات روابط الإحالة، أو عناصر وشكل إعداد الموقِع التّجاري وكذا الوسائط المتعدّدة، التي لا تجد وسيلة للنّشر إلاّ عبر شبكة الإنترنت.

وعليه، فإنّ الإشكاليّة لا تُثار في حالة ما إذا كان محتوى الموقع التّجاري يتضمّن على عنصرا أو مصّنفا من مصّنفات الملكيّة الفكريّة، التي تُحظى بالحماية بموجب القوانين الخاصّة بحماية حقوق الملكيّة الفكريّة، كالعلامات التّجاريّة أو الخدماتيّة أو الأسماء التّجاريّة ....الخ، التي تّم تجريدها من مادياتها وتحوّلت إلى دعامات إلكترونيّة، إذْ يتّم توزيعها ونشرها وتنزيلها مباشرة فيما بعد عبر الموقع التّجاري لصاحبه، حيث تتمتّع أساسا بواحد أو أكثر من التّشريعات أو التّنظيمات المتعلّقة بحماية حقوق الملكيّة الفكريّة، في حين ينبغي، في هذه الحالة، تكييف أحكام هذه القوانين مع المستجدّات والتّطوّرات التي تشهدها الثّورة الرّقميّة، مع إعطائها الوصف القانوني الملائم لتأمين حمايتها، إذ يمكن حمايتها بموجب الأحكام الواردة في القوانين المتعلّقة بحقوق المؤلف أو قوانين حماية حقوق الملكيّة الصّناعيّة والتّجاريّة، بشرط أن تستوفي الشّروط القانونيّة المطلوبة للحماية.

أمّا المصّنفات الرّقميّة الأخرى، التي تّم خلقها أو إبداعها عبر الإنترنت، ولم يتّم تصنيفها ضمن المصّنفات التي تشتملها الحماية، بموجب أحكام القوانين الخاصّة بحماية الملكيّة الفكريّة، كأسماء المواقع ومُحتواها التي لا تجد طريقة لإبداعها ونشرها أو توزيعها إلاّ عبر الإنترنت، فيستوجب الأمر حمايتها بموجب القوانين الخاصّة بها، أو منحها الوصف القانوني المُمْكِن إعطاؤه لها، بعد استيفائها للشّروط القانونيّة المتطلّبة لحمايتها.

إنّ معظم هذه المصّنفات أو الأعمال الرّقمية تتوافر فيها العناصر المتطلّبة للحماية كالأصالة والحداثة(الجدّة) والابتكار– إلى جانب الشّروط الأخرى المتطلّبة في كلّ مصنّف–

التي تظهر من خلال طرق وكيفيات إعداد صفحات ويب مواقع التّجارة الإلكترونيّة، وما تتضمّنه من رسومات وصور وفيديوهات، وما يُصاحبها من صوت وموسيقى أو عناصر حركيّة وحتّى التّطبيقات البرمجيّة الخ...، فمن المُستحسن إذاً تبسيط وتوسيع إجراءات طلب حماية هذه المصّنفات، من خلال منح أصحابها إمكانية إيداعها وتسجيلها لدى الهيئات الإداريّة الحكوميّة المختصّة لكلّ بلد، كالمعهد الوطني الجزائري للملكيّة الصّناعيّة(I.N.A.P.I) في حالة ما إذا تعلق الأمر بالمصّنفات الملكيّة الصّناعيّة والتّجاريّة، وكذا الدّيوان الوطني لحقوق المؤلف والحقوق المجاورة(O.N.D.A) إذا استوفت هذه المصّنفات للشّروط المتطلّبة لحماية حقوق الملكيّة الأدبيّة والفنيّة.

تعتبر روابط الإحالة(Liens hypertextes) بمثابة الوقود أو الطّاقة المُحرّكة لمواقع التّجارة الإلكترونيّة، حيث تسمح للمورّد الالكتروني بعرض مختلف السّلع والخدمات عبر الإنترنت في أيّ مكان من العالم، وتُمكّنُ المُستهلك الالكتروني من الوصول إلى المنتجات بمجرّد الضّغط على رابط الإحالة المُروِّج لتلك السّلعة أو الخدمة، حيث أثارت هذه الرّوابط في الآونة الأخيرة نقاشات قانونيّة عديدة بشأن التّقنية المُستخدمة في عرض أو الوصول إلى المصّنفات الرّقميّة المحميّة عبر الإنترنت، التي تمّس بحقوق الملكية الفكرية الأدبية أو الصّناعيّة والتّجاريّة، أو حتّى خرق قواعد المنافسة المشروعة، الخ...

ونظرا لغياب النّصوص التّشريعيّة والتّنظيميّة المُنظّمة لروابط الإحالة، تُركَت مُهمّة الفصل في النّزاعات التي تُثيرها بعض تقنيات هذه الرّوابط بشأن المصّنفات الرّقميّة، إلى الاجتهاد القضائي الذي أقّر في أكثر من مُناسبة بأنّ طريقة الإحالة السّطحيّة (Lien en surface) ليس فيها ما يضّر بالمصّنفات الرّقميّة، لكونها تأتي في إطار نظام عمل شبكة الإنترنت والاستعمال المألوف والمشروع لها، بينما أقرّ بعدم شرعية استخدام بقيّة تقنيات روابط الإحالة(Lien en profondeur, Le cadrage, Lien Automatique.)، لكونها لا تضمن حفظ المُصنّف الرّقمي من كل تقليد أو تشويه أو تزوير.

إنّ الفصل في النّزاعات التي تثور بشأن نشاطات(م.خ.إ) لا يمكن أن يتّم خارج الإطار القانوني المناسب لها، حيث يمكن لقاضي الموضوع الاعتماد على الضوابط التّشريعيّة والتّنظيميّة التي فرضها المشّرع على مُستوى الإتّحاد الأوروبي والقانون المقارن والوطني للدّول، التي تُساعدُه على تحديد المسؤوليّة المدنيّة أو الجزائيّة، لكلّ من مُزوّد النّقل والاتّصال والإيواء، سواءً في إطار حدود نشاطاته أو خارجها في حالة ما إذا تجاوزها.

لكن الحلول التّشريعيّة والتّنظيميّة المتعلّقة بنشاطات(م.خ.إ) لم تَحْسُمْ الأمر في أشَّدِ النّقاطِ حرجاً، المتعلّقة بالخصوص في كيفية الإثبات في البيئة الافتراضيّة بأنّ المزوّد على علم أو جهل بالمحتوى غير المشروع، ولعلّ أنّ خدمات الإيواء والبحث والمحتوى من أكثر الخدمات عرضة للمساءلة من هذا الجانب، وكانت سبباً في عدّة نقاشات أدّت إلى تناقض الحلول المقترحة من جانب الفقهاء والاجتهاد القضائي، حيث قرّر هذا الأخير في أكثر من مناسبة على أساس افتراض الخطأ للمزوّد بحكم الإمكانيات التّقنيّة المتوّفرة لديه، وفي جميع الظروف، يجب على القضاة تكييف الوقائع على الأساس القانوني الصّحيح لإسناد المسئولية لكل(م.خ.إ).

إنّ القواعد العامّة ساهمت بدرجة كبيرة الاجتهاد القضائي في إيجاد بعض الحلول للقضايا المعقّدة في مجال المعاملات الإلكترونية، وإن كان الأمر ليس بالهيّن في تحديد مسؤولية كل فاعل في حالة تعدّد روابط الإحالة نحوى المحتوى غير المشروع، أين تتعقّد الأمور أكثر فأكثر في تحديد مسؤولية من قام بعملية الرّبط أولا، أو الحُكم بمسؤولية جميع من توّلى تنظيم روابط الإحالة، أو الاعتماد على معيار العِلم بالمحتوى غير المشروع كأساس لتحديد المسؤول، فإذا بقي الفقه بين مؤيّد ومُنكر حول هذه المسائل، فإنّ الاجتهاد القضائي أقّر في أكثر من مناسبة بمسئولية صاحب الموقع الأصلي عن المحتوى غير المشروع الذي يُنظّمه بالموقع التّابع له، حيث لا يوجد ما يَمنعُ القاضي من مساءلة من قامُوا بالرّبط نحوى ذلك المحتوى، على أساس "المشاركة" إذا تحقّقت شروط المسئوليّة الجزائيّة، والقول على أساس "التّضامن" إذا تحققت شروط المسؤوليّة المدنيّة.

نتيجة لكل ما سبق ذكره، تّم اقتراح **المقترحات** التّالية:

1. يجب سّن نصوص تشريعيّة وتنظيميّة تتعلّق بتنظيم المركز القانوني لـ(م.خ.إ)، تتضّمن أخلاقيات وقواعد السّلوك الواجب التّحلي بها، وتُحدد شروط مزاولة نشاطاتهم، وإبرار حقوق والتزامات كل طرف (مقدمي الخدمات والمشتركين).
2. يجب وضع نصوص قانونيّة ردعيّة، تُبيّن الجزاءات التي تُسلّط على (م.خ.إ) في حالة إخلالهم بالنّصوص القانونيّة والأنظمة السّارية المفعول، وذلك من أجل خلق روح المسؤوليّة، ومن أجل جعلهم يحترمون الآخرين، ويطبّقون القانون.
3. يجب تحديث المنظومة المصرفيّة، من خلال إصدار قانون خاص ينظّم نشاطات المؤسّسات المصرفية المكلّفة بإصدار العملات الالكترونيّة ورقابتها.
4. يجب وضع برامج تحسيسيّة، لتوعيّة المستهلك الالكتروني من المخاطر المتعلّقة بالتّسوق عبر الانترنت، وتوعيّته من عواقب التّعامل بسلاسل التّسويق غير القانونيّة، التي تتجسّد من خلال اعتماد الشّركات تقنيات البيع الهرمي كوسيلة لتحقيق الأرباح فقط.
5. يجب تفعيل القوانين المتعلّقة بحماية المستهلك الالكتروني والقوانين المتعلّقة بالممارسات التّجاريّة والقانون المتعلّق بحماية المعطيات الشّخصيّة للأشخاص الطبيعيين.
6. باعتبار الأمن المعلوماتي يمّس الأمن الوطني للدّول، ويمّس اقتصادها ومجالاتها الحيويّة، فإن ذلك يستوجب وضع سياسة أو إستراتيجية أمنية موثوقة، شاملة لجميع مرافق ومؤسّسات الدّولة بُغية حماية البنيّة المعلوماتيّة الوطنيّة.
7. للتغلّب على صعوبات الحماية الأمنيّة الوطنيّة، يجب السّعي على إعداد برامج تدريبيّة مُستمرة، في إطار إستراتيجيّة متكاملة لأمن الأنظمة المعلوماتية، تُنّفذها الدّولة، لحماية أمنها الوطني، السّياسي والعسكري والاقتصادي، الخ...

الـملاحق

الملحق رقم: (01)	-Exemple sur la structure d'un document HTML	الصّفحة رقم: (18)

```
<html>
<head>
<tilte> <h1 align="center"><font face="Arial">Université MOULOUD MAMMERI de Tizi -
Ouzou</font></h1><p><font face="Arial"></title>
<meta name="Description" content="Faculté de Droit et des Sciences Politiques">
<meta name="Keywords" content="bibliothèque, archive documentation ">
<meta name="Author" content="M.DAHMANI Samir">
<meta name="Generator" content="Bloc-notes">
<meta name="Date" content="2016">
                    (Balises d'en−tête)
</head>
<body bgcolor="#99CCFF"><div align="center"><h1
align="center"><fontface="Arial">Faculté de Droit et des Sciences Politiques</font></h1>
<p><font face="Arial"><br>
<hr>
<br> <b>Azul -<b>السـلام عليـكـم </br>
<h1 align="center"><font face="Arial">ضمانات أمن مواقع التجارة الالكترونية </font></h1>
                    (Corps de la page)
</body>
</html>
```

Source : Benjamin CANOU, « Programmation Web Typée », thèse de doctorat en Sciences, mention : Informatique, Université Pierre et Marie Curie- École Doctorale Informatique, Télécommunications et Électronique, 2011, pp. 15 -18.

الملحق رقم: (02)	مثال على مَا وُرِدَ في المُلحق رقم(07)	الصّفحة رقم: (18)

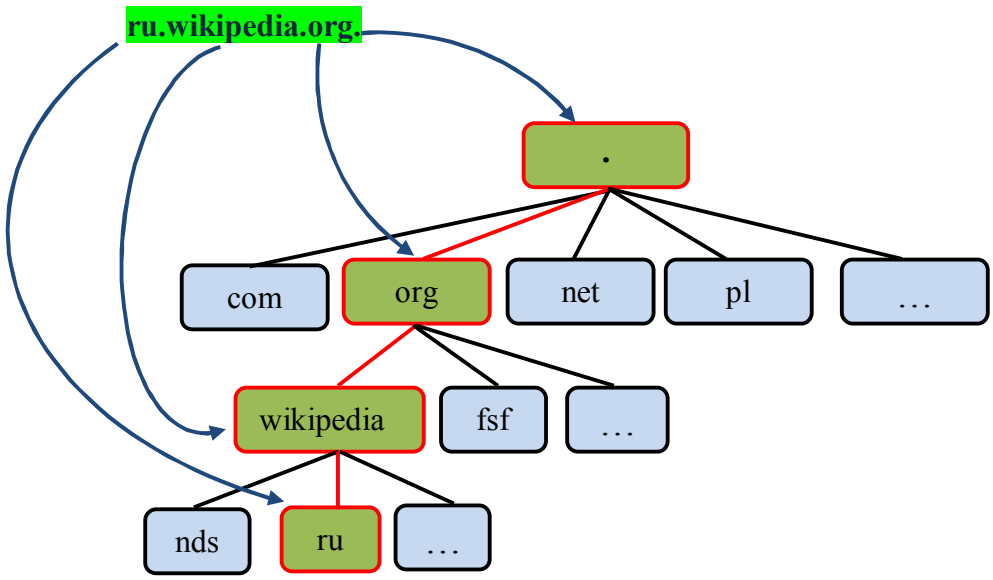
– **المصدر**: من إعداد الباحث.

الملحق رقم: (03)	- Exemple sur la structure d'un document (PHP)	الصفحة رقم: (20)

```
< ?=
echo 'Bonjour !' <br/>;
echo 'Comment allez-vous ?' ;
echo 'Il fait beau non ?' ;
$nomsAutorises= ['Alber', 'Bertrand'] ;
$nomsEncours= 'Eve'; ?>
< ?php if (in_array($nomEnCours, $nomsAutorises)) : ?><p>
{Bonjour}
< ?php echo $nomEnCours ; ?> !</p>
< ?php else : ?> <p>
{Vous n'êtes pas un utilisateur autorisé !}</p>
< ?php endif ;
?>
```

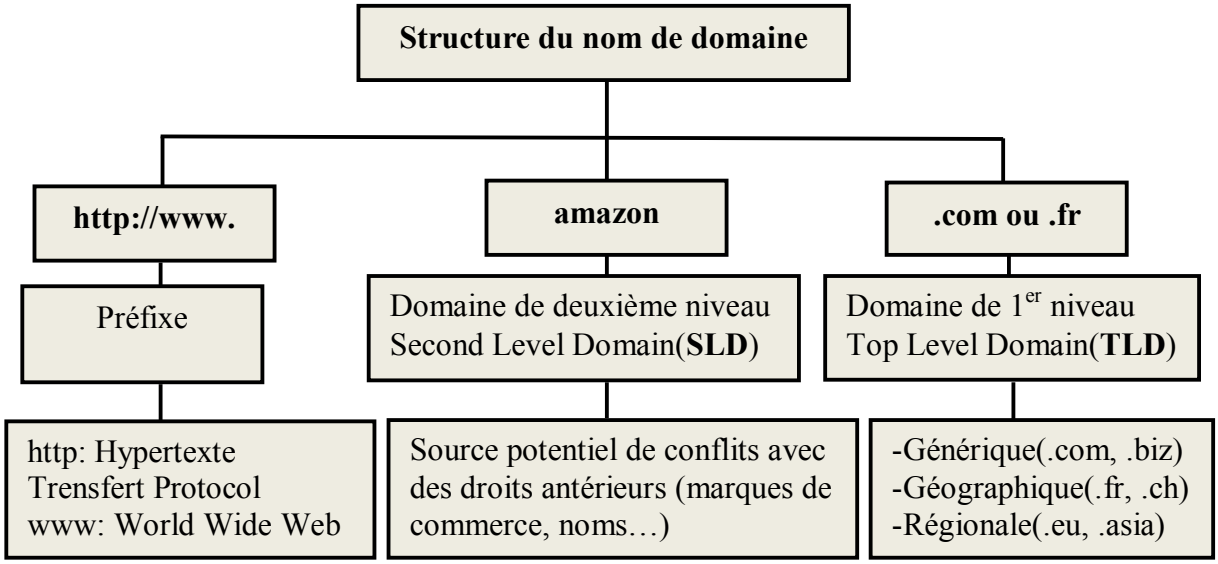
Source: **Lary ULLMAN**, op.cit., pp. 2-4.

الملحق رقم: (04)	البنية الهرمية لنظام أسماء النطاقات	الصّفحة رقم: (20)



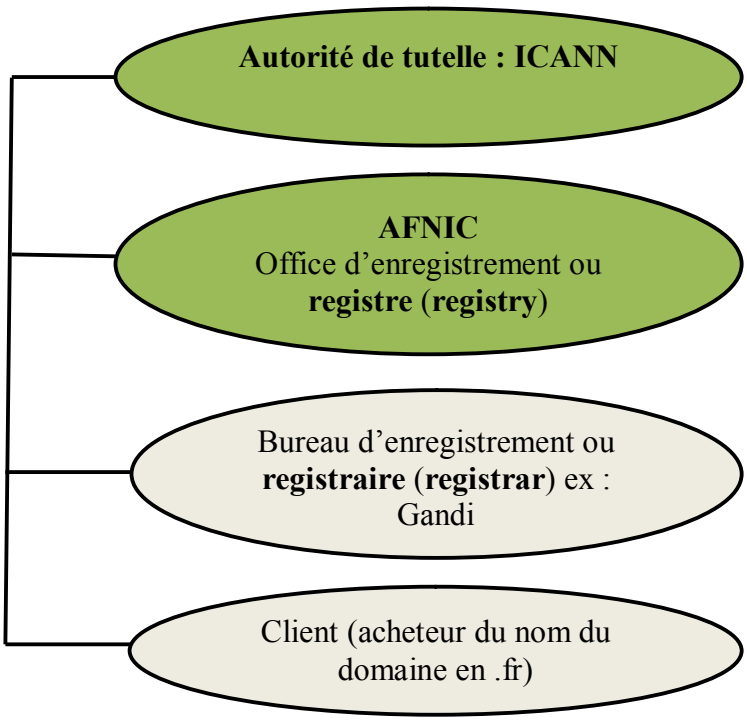
Source : Nathalie DRYFUS, op.cit., pp. 22, 23. **Hélie - SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., p. 193.

الملحق رقم: (05)	- Structure du nom de domaine	الصّفحة رقم: (22)



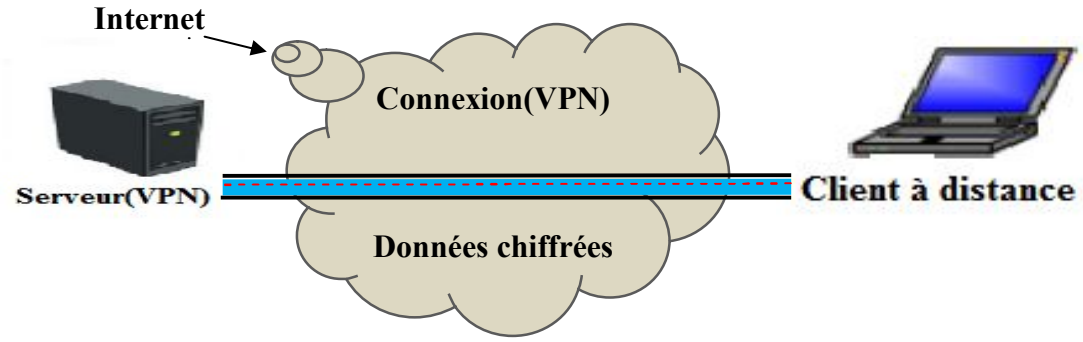
Source : **Romain V. GOLA**, op.cit., p. 39.

الملحق رقم: (06)	- Exemple sur l'autorité de tutelle de l'extension (.fr)	الصّفحة رقم: (26)



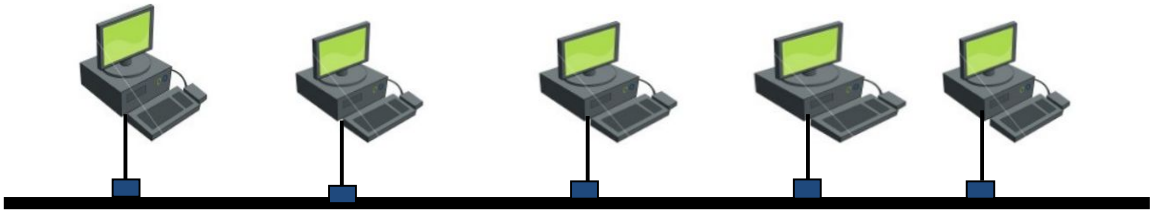
Source : Ibid., p. 48.

الصّفحة رقم: (54)	Réseau (VPN)	الملحق رقم: (07)



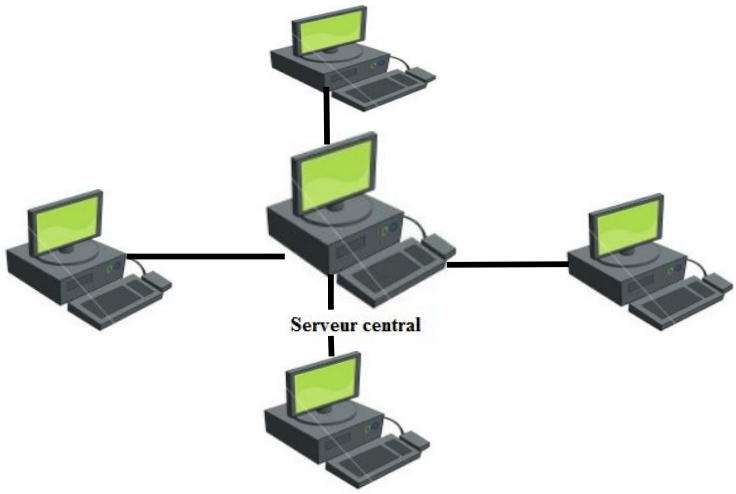
Source : - Hicham EL KHOURY, « Une modélisation formelle orientée flux de données pour l'analyse de configuration de sécurité réseau », thèse de doctorat de l'université de Toulouse III - Paul Sabatier, spécialité : Informatique et Télécommunications, 2014, p. 50.
- **Jean-François PILLOU, Fabrice LEMAINQUE**, op.cit., pp.230.

الصّفحة رقم: (56)	Réseau en bus	الملحق رقم: (08)



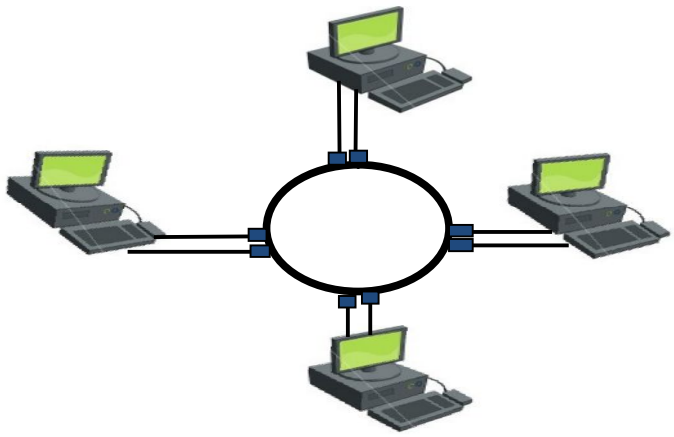
Source : - Jean-Yves DIDIER, Introduction aux réseaux, pp.04-07. http://www.lsc.univ-evry.fr~didierwebpagepedagogieii25_final.pdf (consulté le 28/01/2016.)

الصّفحة رقم: (57)	Réseau en étoile (Star)	الملحق رقم:(09)



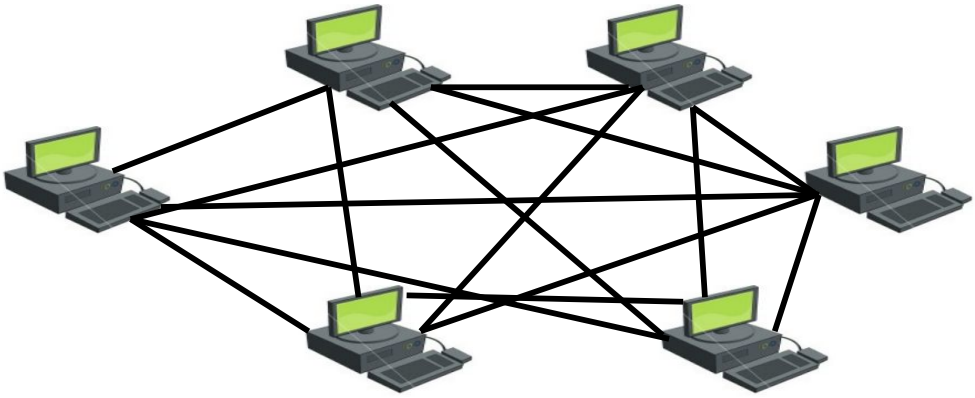
Source : - Olivier THARAN, Architecture réseaux, p. 06. http://www.pasteur.fr/formation/infobio/arch/archi-reseaux.pdf (consulté le 20/01/2016.)

الملحق رقم: (10)	Réseau en Anneau(Ring)	الصّفحة رقم: (58)



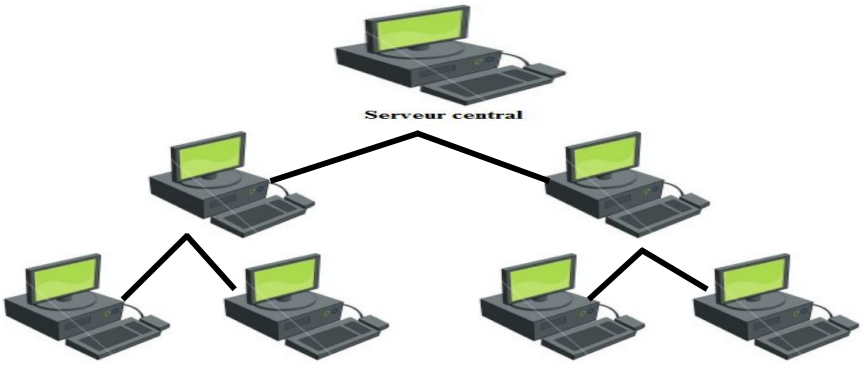
Source : - Olivier THARAN, op.cit., p. 06.

الملحق رقم: (11)	Réseaux maillé (Mesh)	الصّفحة رقم: (59)



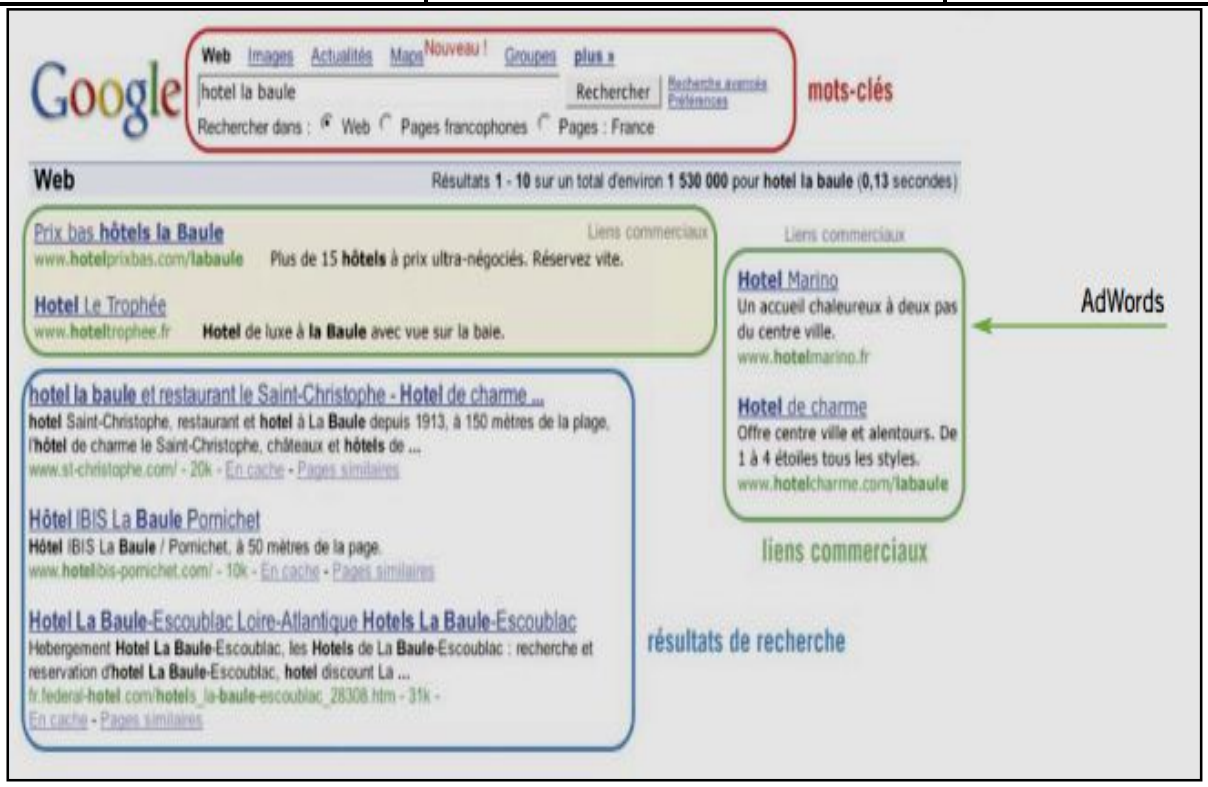
Source: Ibid., p. 09.

الملحق رقم: (12)	Réseau Hybride-Hiérarchique	الصّفحة رقم: (59)



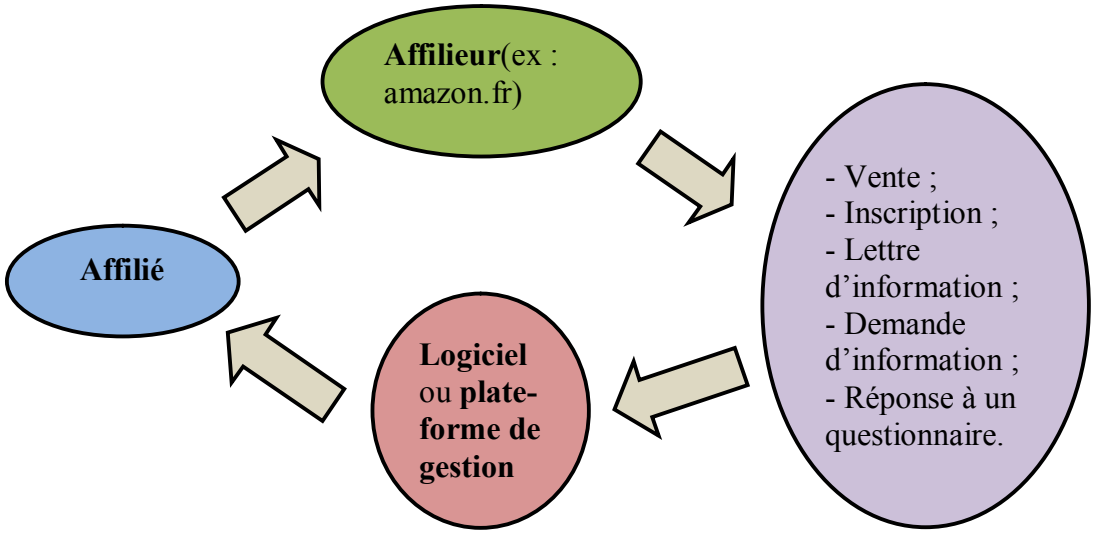
Source : Ibidem.

الملحق رقم: (13)	Exemple sur Google AdWords.	الصّفحة رقم: (80)



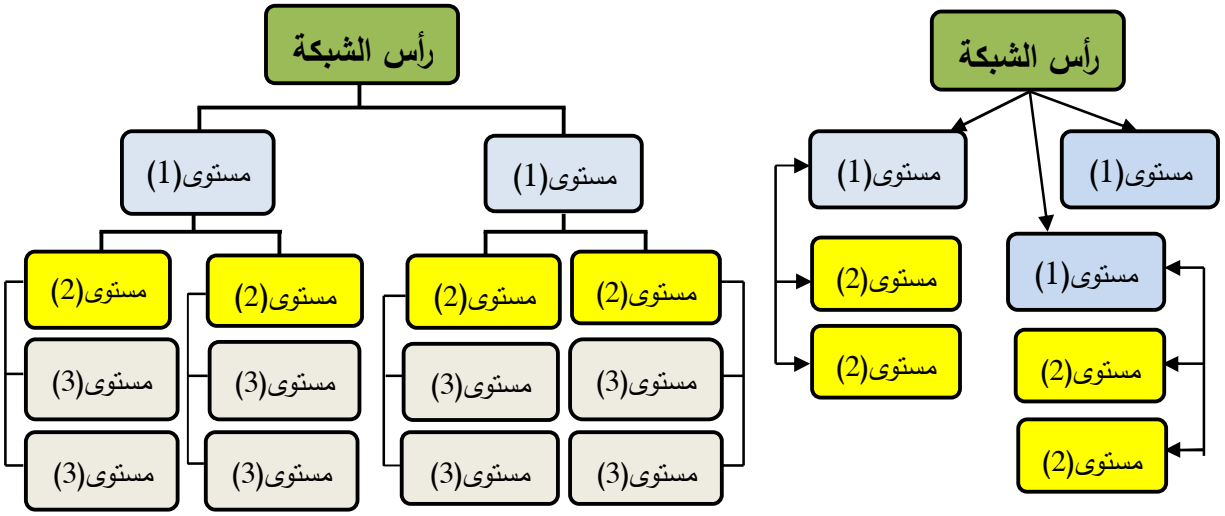
Source: - http://www.google.fr/adwords/miniguide(consulté le 03/08/2016.)

الملحق رقم: (14)	- Fonctionnement d'un réseau d'affiliés.	الصّفحة رقم: (82)



Source : Romain V.GOLA, Op.cit., p. 450.

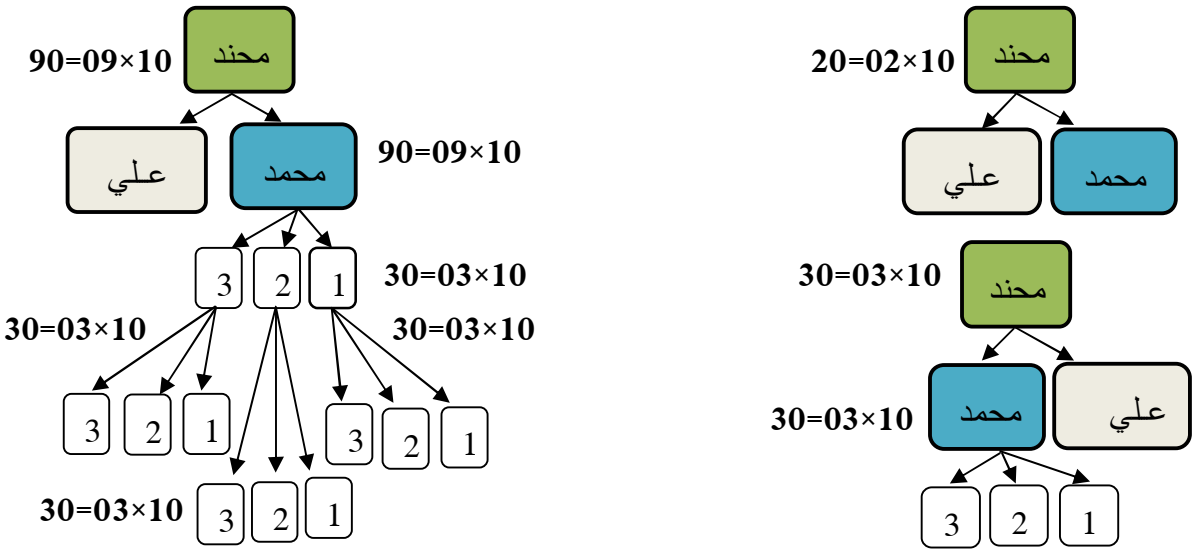
الملحق رقم: (15)	خطط التّسويق الشّبكي الهرمي.	الصّفحة رقم: (102)



خطة المستويات المتعددة الأعضاء خطة المستويات الثنائية

Source : https://fr.wikipedia.org/wiki/Vente_multiniveau/(consulté le 07/07/2016.)

الملحق رقم: (16)	نَموذج يُوضّح الشّبكة التّسويقية	الصّفحة رقم: (103)



المصدر: من إعداد الباحث.

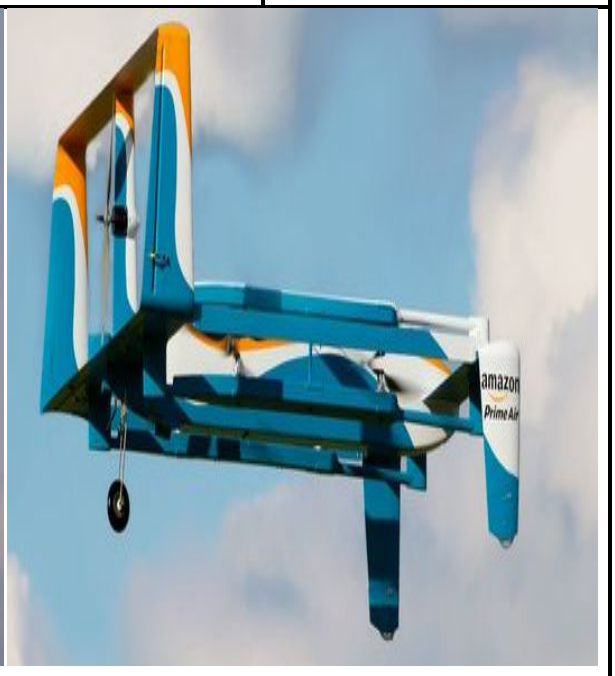
الصّفحة رقم: (105)	Exemple sur la structure pyramidale illégale.	الملحق رقم: (17)

Ce système s'appelle système "**pyramidal**" parce que ses membres forment une **pyramide**, chaque niveau est plus volumineux que le précédent avec, à la tête, au sommet de la pyramide, le créateur du système.

l'**argent** gagné par les membres **provient** d'autres membres de **niveaux inférieurs**, le système ne fait que transférer de l'argent vers le **sommet.**

Source : http://www.julienrio.commarketingfrenchsysteme-pyramidal-marketing-reseau-eviter-pieges(consulté le 14/07/2016.)

الصّفحة رقم: (118)	Les drones d'Amazon	الملحق رقم: (18)

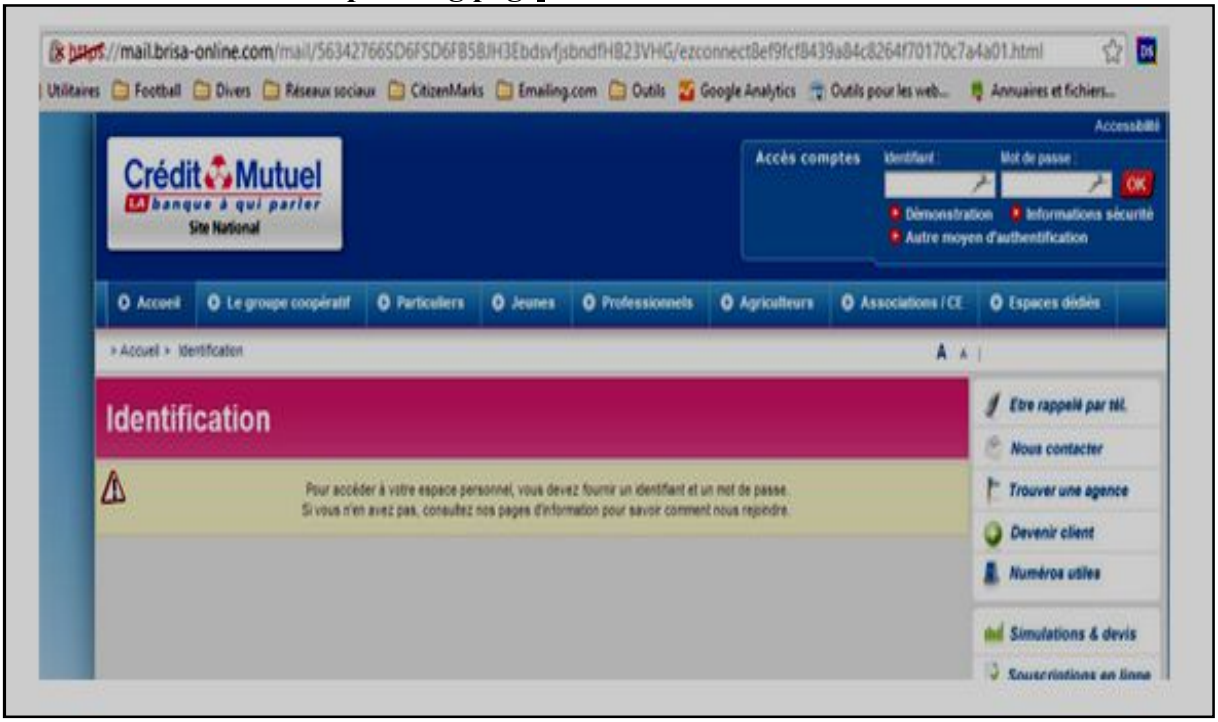


- Source: https://www.amazon.com

الصّفحة رقم: (136)	Exemples de phishing par e-mail.	الملحق رقم: (20)

- l'envoi d'e-mails frauduleux :

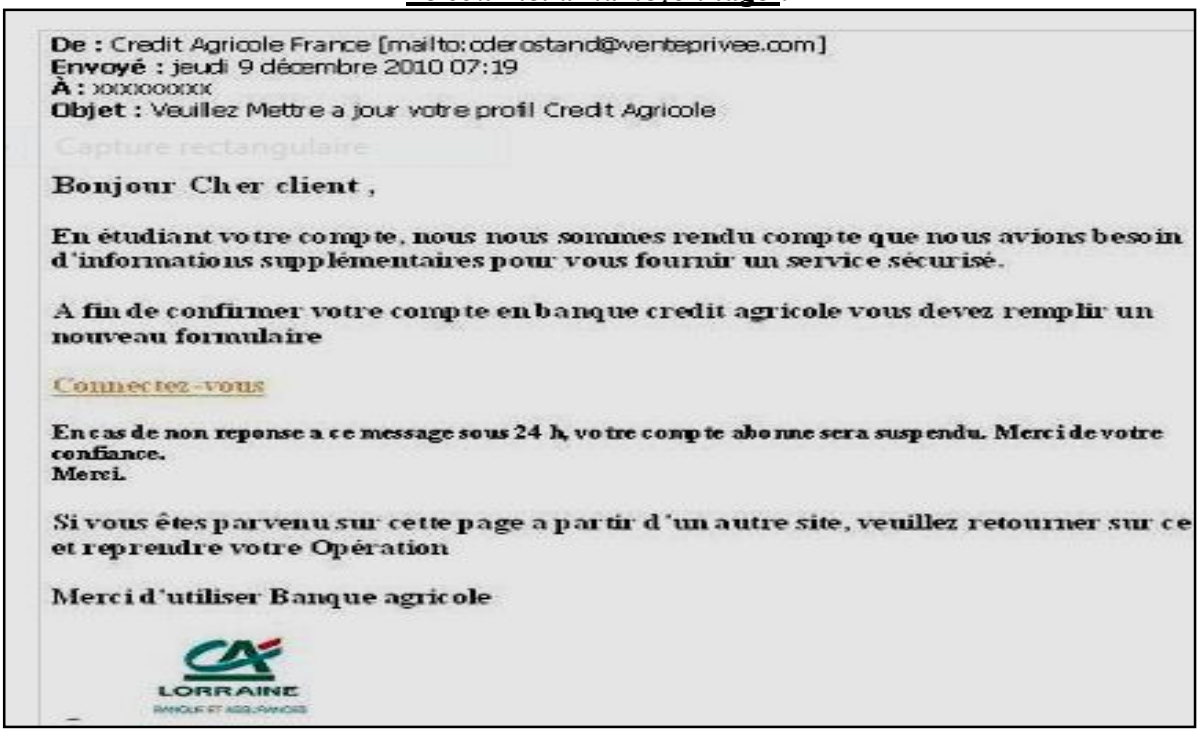
- La redirection vers une phishing page *:*



- **Source** : http://www.emailing.com/blog/email< -phishing/(consulté le 25/01/2016.)

الصّفحة رقم: (139)	Des exemples Phishing Crédit Agricole.	الملحق رقم: (21)

- ***Le courriel d'hameçonnage*** :



De : Credit Agricole France [mailto:cderostand@venteprivee.com]
Envoyé : jeudi 9 décembre 2010 07:19
À : xxxxxxxx
Objet : Veuillez Mettre a jour votre profil Credit Agricole

Capture rectangulaire

Bonjour Cher client ,

En étudiant votre compte, nous nous sommes rendu compte que nous avions besoin d'informations supplémentaires pour vous fournir un service sécurisé.

A fin de confirmer votre compte en banque credit agricole vous devez remplir un nouveau formulaire

Connectez-vous

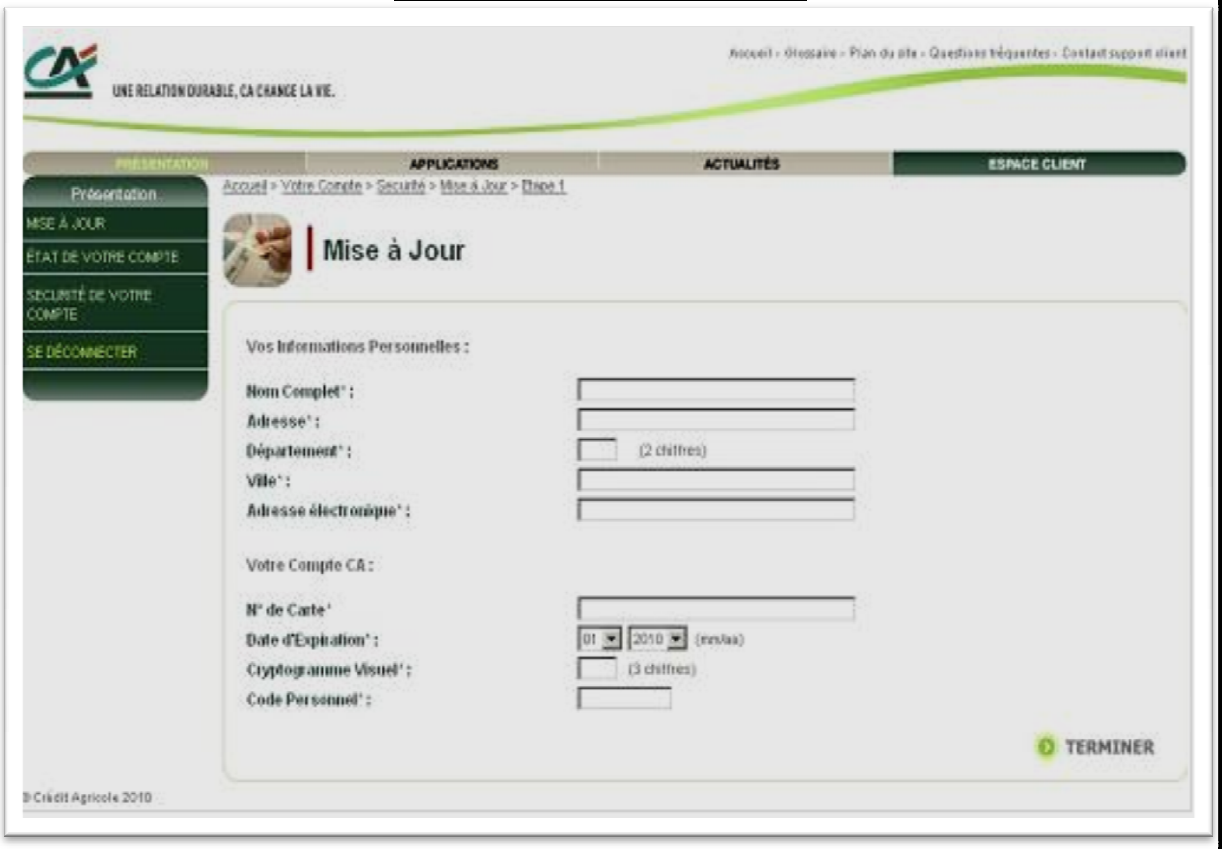
En cas de non reponse a ce message sous 24 h, votre compte abonne sera suspendu. Merci de votre confiance.
Merci.

Si vous êtes parvenu sur cette page a partir d'un autre site, veuillez retourner sur ce et reprendre votre Opération

Merci d'utiliser Banque agricole

LORRAINE

- ***Une copie d'écran du faux site*** :



- ***Le courriel d'hameçonnage*** :

Verified by VISA MasterCard SecureCode

Bonjour client de Visa Card ,

Votre Carte Bancaire est suspendue , Car Nous avons remarquer un probleme sur votre Carte.

Nous avons determiner que quelqu'un a peut-etre utiliser Votre Carte sans votre autorisation. Pour votre protection, nous avons suspendue votre Carte de credit. Pour lever cette suspention, Cliquez ici et suivez la procedure indiquer pour Mettre a jour de votre Carte Credit.

Note: Si ce n'est pas achever le 10 Septembre 2009, nous serons contraints de suspendre votre carte indfiniment, car il peut tre utiliser pour frauduleuses

Nous vous remercions de votre cooperation dans le cadre de ce dossier.

Merci,
Support Clients Service.

***- Une copie d'écran du faux site* :**

VERIFIED by VISA MasterCard SecureCode

Mettre a jour de votre Carte Crédit en ligne

Veuillez Remplire l'au dessous de la form Pour vous protéger contre l'utilisation frauduleuse de votre carte bancaire, Verifed By Visa a adopté la solution SecureCode™.

Une Fois Votre Carte de crédite est confirmé seraprotégé Contre les menaces est les Fraudes en ligne.

Nom Prénom * :

Date de Naissance * : Jour Mois Anée

Nome De jeune fille de votre mére? * :

Type De Carte * : VISA

Numéro de carte * :

Date d'expiration * : 01 09

Cryptogramme * :

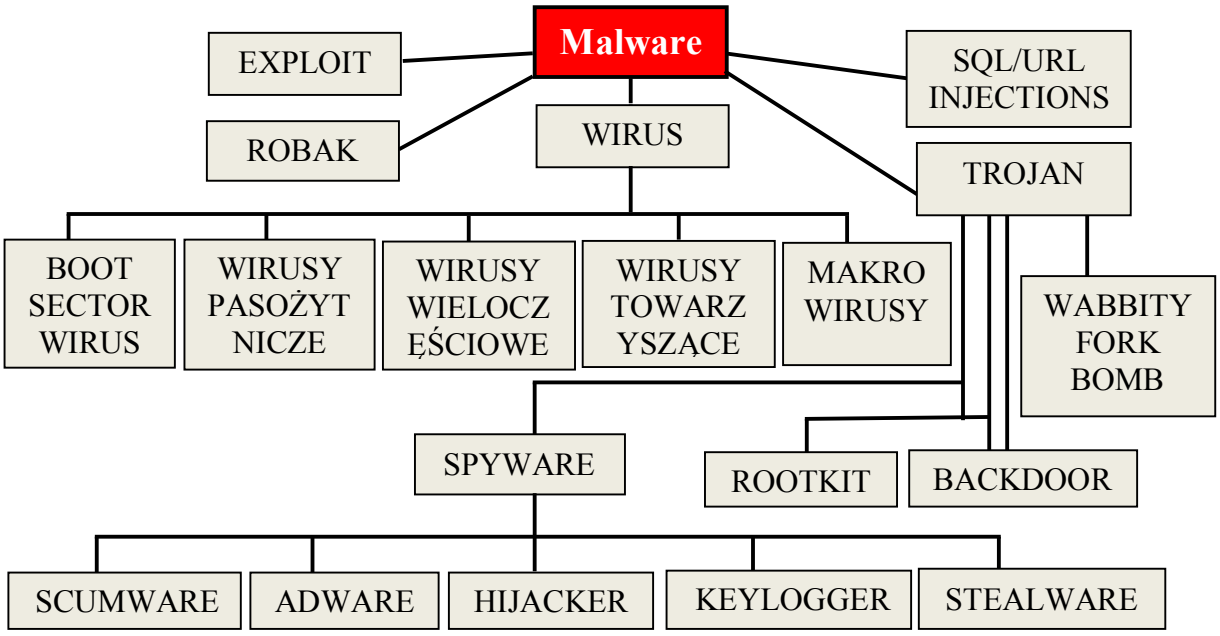
Valider

Verifed by visa vous garanti un paiement sécurisé par la technologie de cryptage SSL. En savoir plus

- Source : https://www.credit-agricole.fr/guidesecurite/Des-exemples.html(consulté le 26/01/2016.)

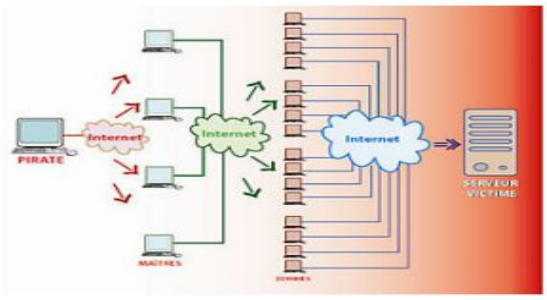
الملحق رقم: (22)	نماذج للبرمجيات الخبيثة وتهديداتها الأمنية	الصّفحة رقم: (146)

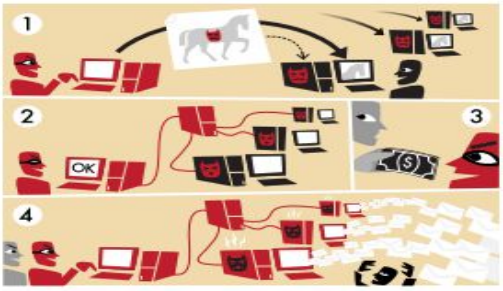
-Déférents types de logiciels.



Source : https://fr.wikipedia.org/wiki/Logiciel_malveillant/(consulté le 16/01/2016.)

- Principe de fonctionnement d'un botnet servant à envoyer du courriel.





Source: https://fr.wikipedia.org/wiki/Botnet/ et http://www.robert-schuman.eu/question_europe.php?num=qe-7(consultés le 18/01/2016.)

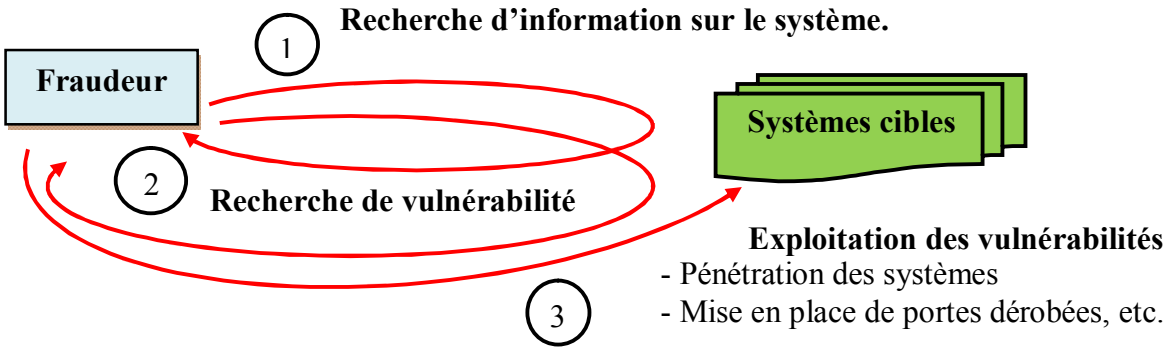
- Fonctionnement d'une attaque en déni de service répartie.

Source : http://www.clusif.asso.fr(consulté le 20/01/2016.)

الصّفحة رقم: (165)	Capture d'écran d'un ordinateur d'un hôpital britannique infecté par le logiciel WannCry, Vendredi 12 mai 2017.	الملحق رقم: (23)

Source : **Nathalie GUIBERT, Damien LELOUP et Philippe BERNARD**, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », article de journal Le Monde, publié le 13/05/2017 sur: http://www.lemonde.fr/international/article/2017/05/13/, consulté le 08/06/2017.

الصّفحة رقم: (165)	Déroulement d'une attaque.	الملحق رقم: (24)



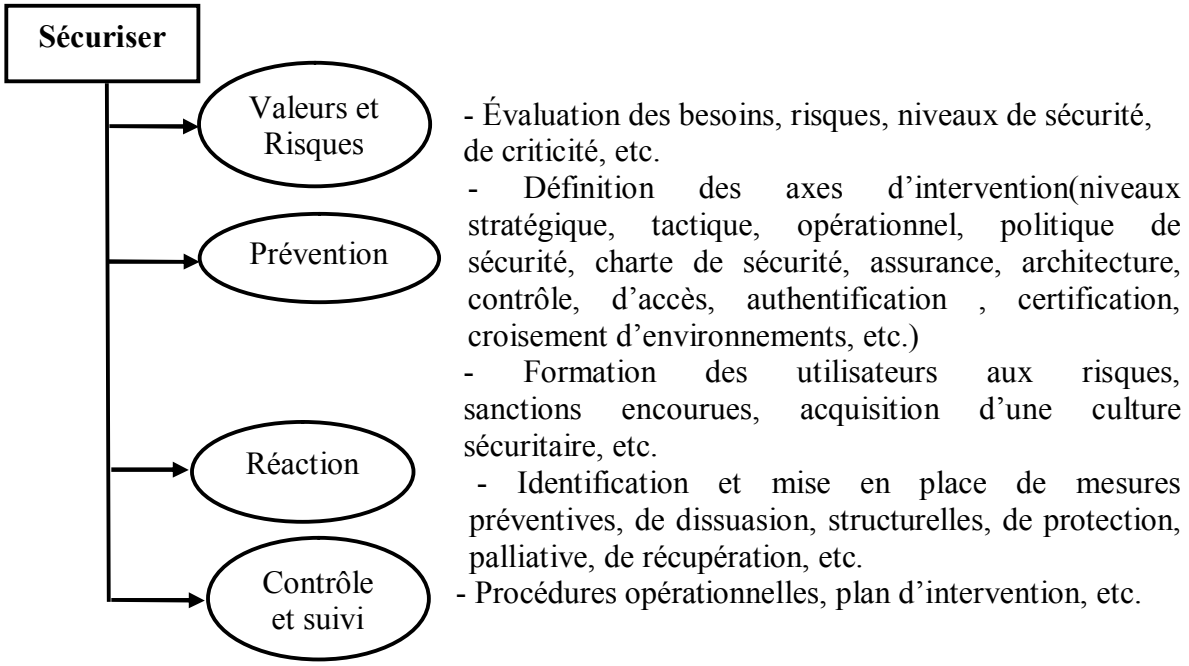
Source : Hélie- SOLANGE GHERNAOUTI, Sécurité Internet : Stratégies et technologies, op.cit., p. 75.

الصّفحة رقم: (210)	Distributeurs automatiques de bitcoins.	الملحق رقم: (25)

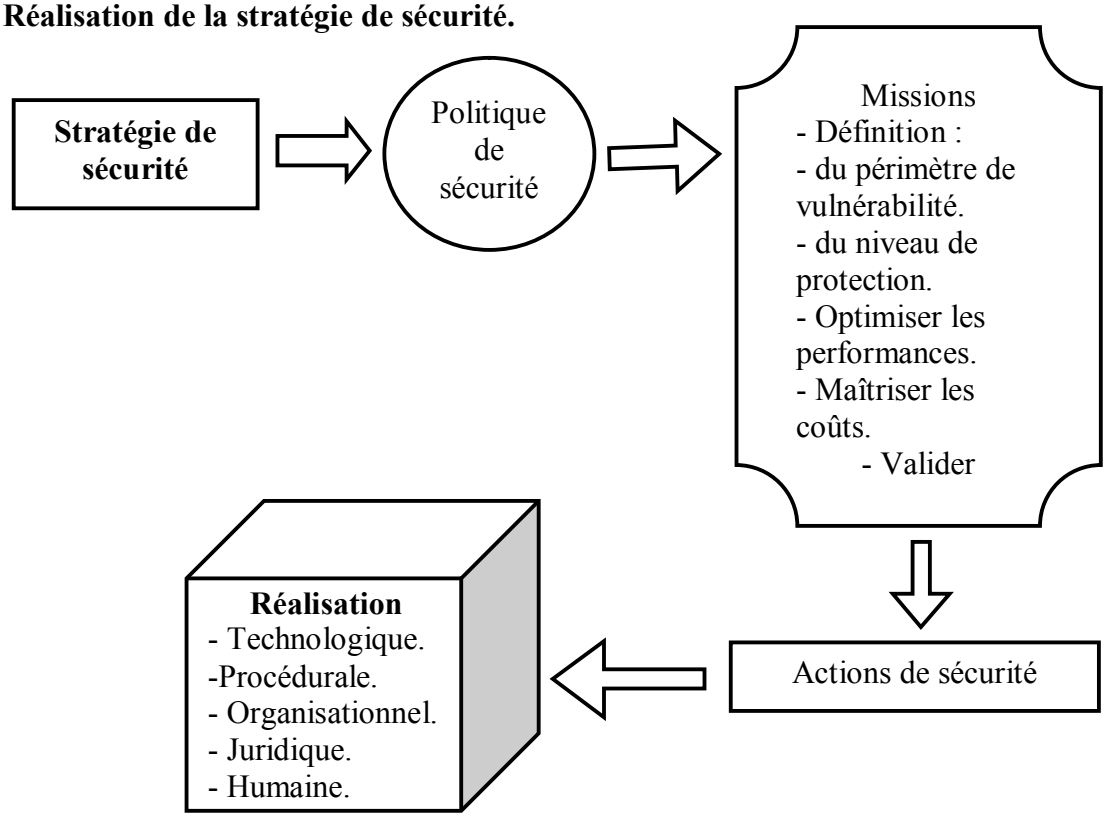
Sources : http://www.cbc.ca/news/business/world-s-first-bitcoin-atm-goes-live-in-vancouver-tuesday-1.2251820 et http://www.24heures.ch/vaud-regions/lausanne-region/bitcoin-s-ancre-realite-lausannoise/story/31473670(consultés le 23/01/2016.)

الصّفحة رقم: (236)	Démarche sécuritaire et réalisation de la stratégie de sécurité.	الملحق رقم: (26)

- Démarche sécuritaire et champ d'application de la sécurité.

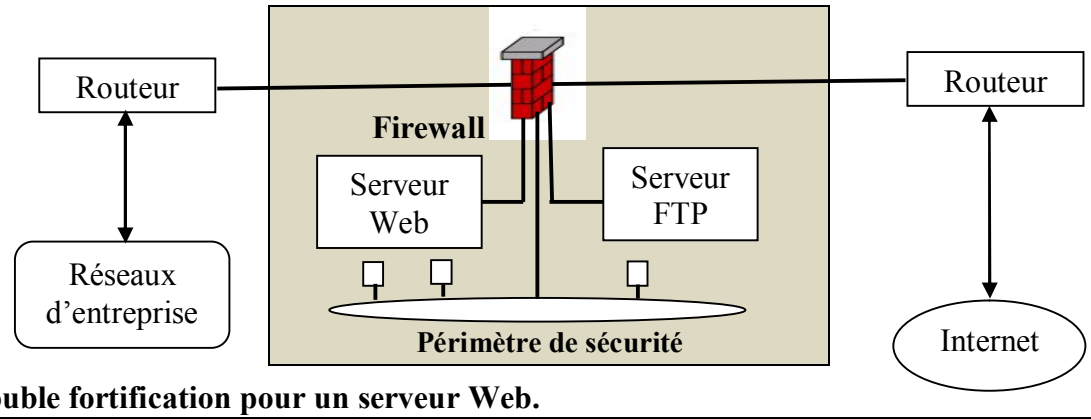


- Réalisation de la stratégie de sécurité.

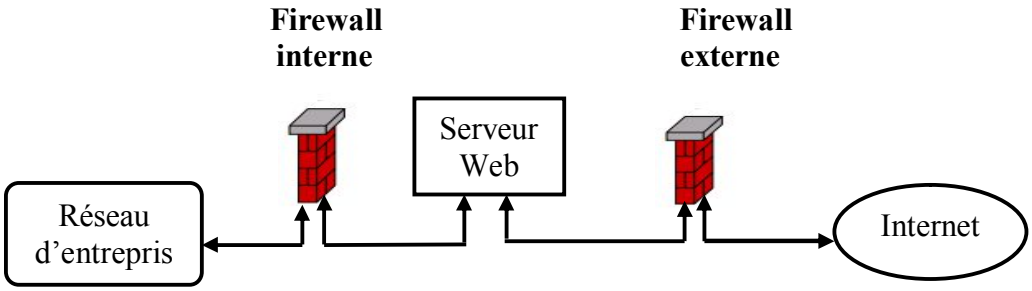


Source : - **Hélie- SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 64, 69.

الصّفحة رقم: (239)	Exemples de périmètre de sécurité.	الملحق رقم: (27)



- Double fortification pour un serveur Web.



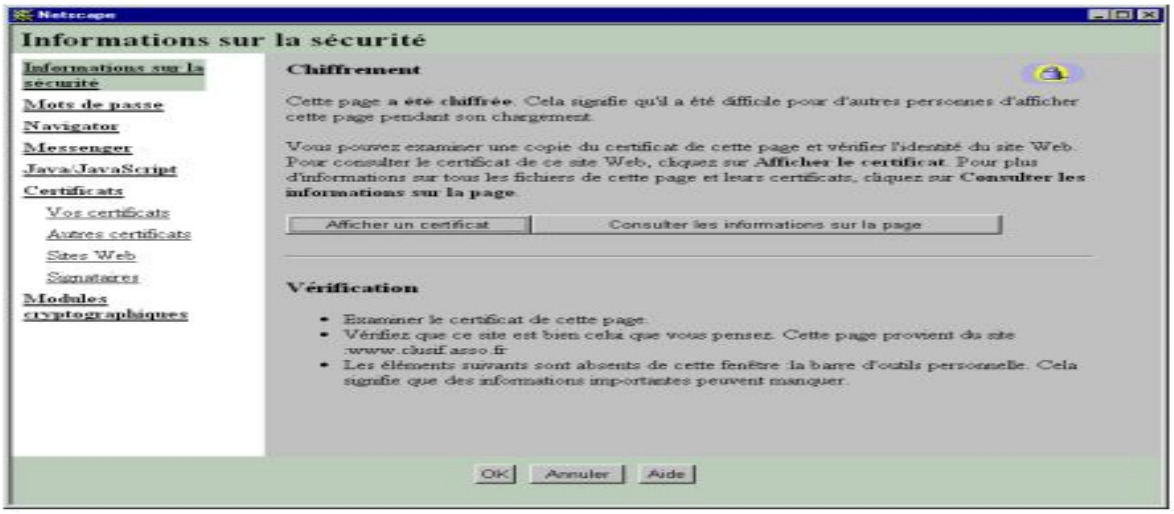
Source : - **Hélie- SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, op.cit., pp. 217, 220.

- Des informations sur la sécurité du site internet.


En bas à gauche sous Netscape Navigatore.

En bas à droite sous Microsoft Internet Explorer.

- En double-cliquant sur ce cadenas, des informations sur l'identité du site sont vérifiées **:**



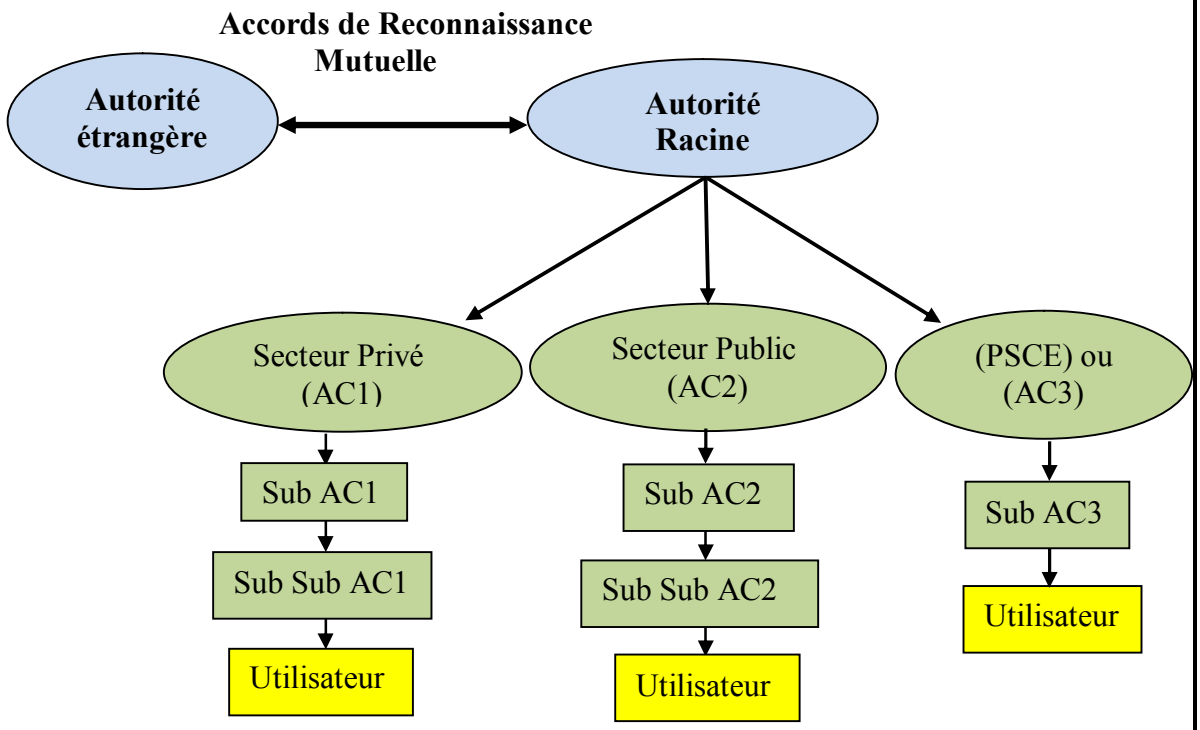
- Source : http://www.clusif.asso.fr

الملحق رقم: (28)	Assurances et usages par classe de certificat.	الصّفحة رقم: (300)

Source : **Arnaud- F.FAUSSE**, op.cit., pp 175, 176.

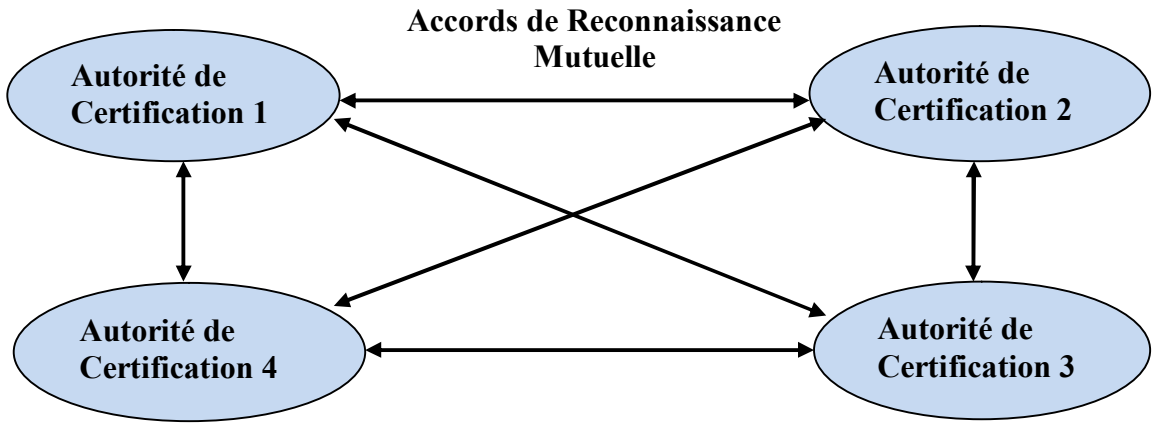
Classe	Méthode d'identification du titulaire	Protection de la clef privée de l'émetteur	Protection de la clef privée du titulaire du certificat	Types d'applications visées
Classe 1	Enregistrement automatique, garantit l'unicité du nom.	Clefs racine en module matériel Clef secondaire émetteur : en module ou logiciel.	Chiffrement par un code confidentiel. Recommandé mais non obligatoire.	Navigation Internet, application de courrier électronique.
Classe 2	Idem Classe 1, plus vérification des informations et de l'adresse du courrier électronique.	Clef racine et secondaires en module matériel.	Chiffrement par un code confidentiel obligatoire.	Courrier électronique individuel, communications inter entreprise à faible risque, authentification forte, enregistrement à des services à distance, signature de logiciel.
Classe 3	Idem Classe 1 et 2, et enregistrement en présence personnelle du requérant, papier d'identité ou documents officiels de société pour une personne physique représentant une personne morale.	Clefs racine et secondaires en module matériel	Chiffrement par un code confidentiel obligatoire. Usage d'un stockage matériel (jeton, carte à puce), recommandé mais non obligatoire.	Banque à domicile, service « sensible », serveurs commerce électronique, authentification des opérateurs des PSC, support au chiffrement fort.

الملحق رقم: (29)	النموذج الهرمي(Modèle Hiérarchique)	الصّفحة رقم: (330)



Source : Manel ABDELKADER, (SICE' 2009 ARPCE, Alger du 08 et 09/12/2009), op.cit, p.7. **Ahmed BERBAR,** (SICE' 2009 ARPCE, Alger du 08 et 09/12/2009), op.cit., p.7. http://www.arpce.dz

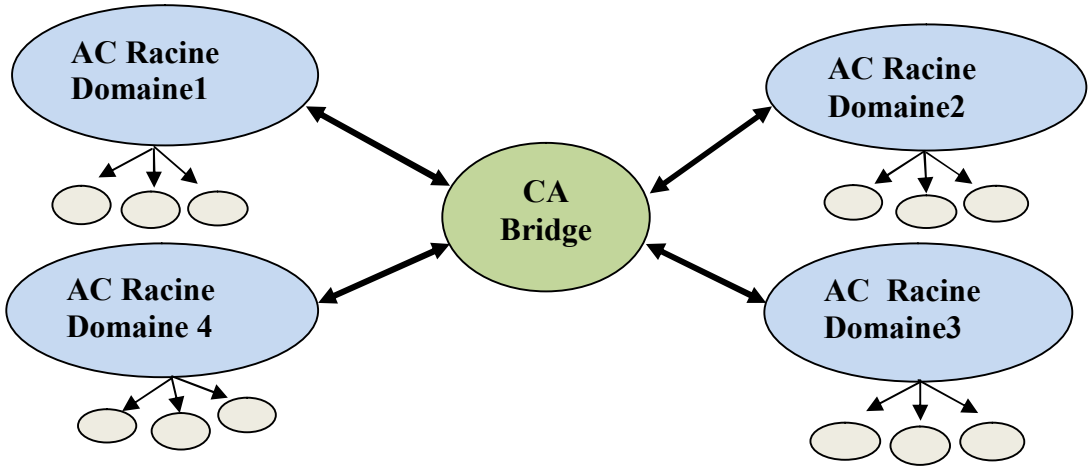
الملحق رقم: (30)	النّموذج المتشابك (Modèle Maillé)	الصّفحة رقم: (331)



- Absence de hiérarchisation et de contrôle.
- Reconnaissance mutuelle entre toutes les AC.

Source : Ahmed BERBAR, (SICE' 2009 ARPCE, Alger du 08 et 09 décembre 2009), p. 09. http://www.arpce.dz

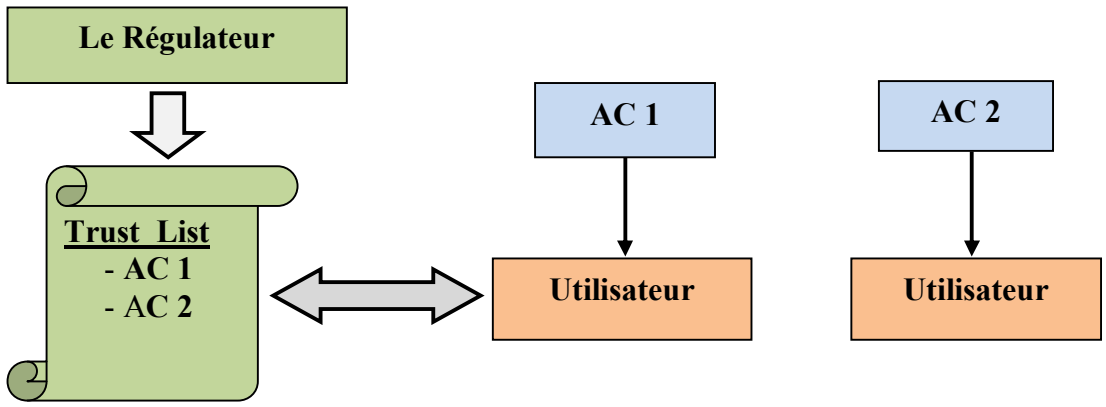
الملحق رقم: (31)	نموذج الجسر(Modèle Bridge)	الصّفحة رقم: (331)



- Diminue le nombre de reconnaissances mutuelles (CA Bridge).
- AC Bridge n'est pas émetteur du Certificats mais prestataire de liaison effectuant un pont de certification entre les domaines de certification.
- Dédié généralement à un modèle d'organisation Fédéral.

Source: - Ahmed BERBAR, (SICE' 2009 ARPCE), op.cit., p. 09. - **Arnaud-F. FAUSSE**, op.cit., p. 127.

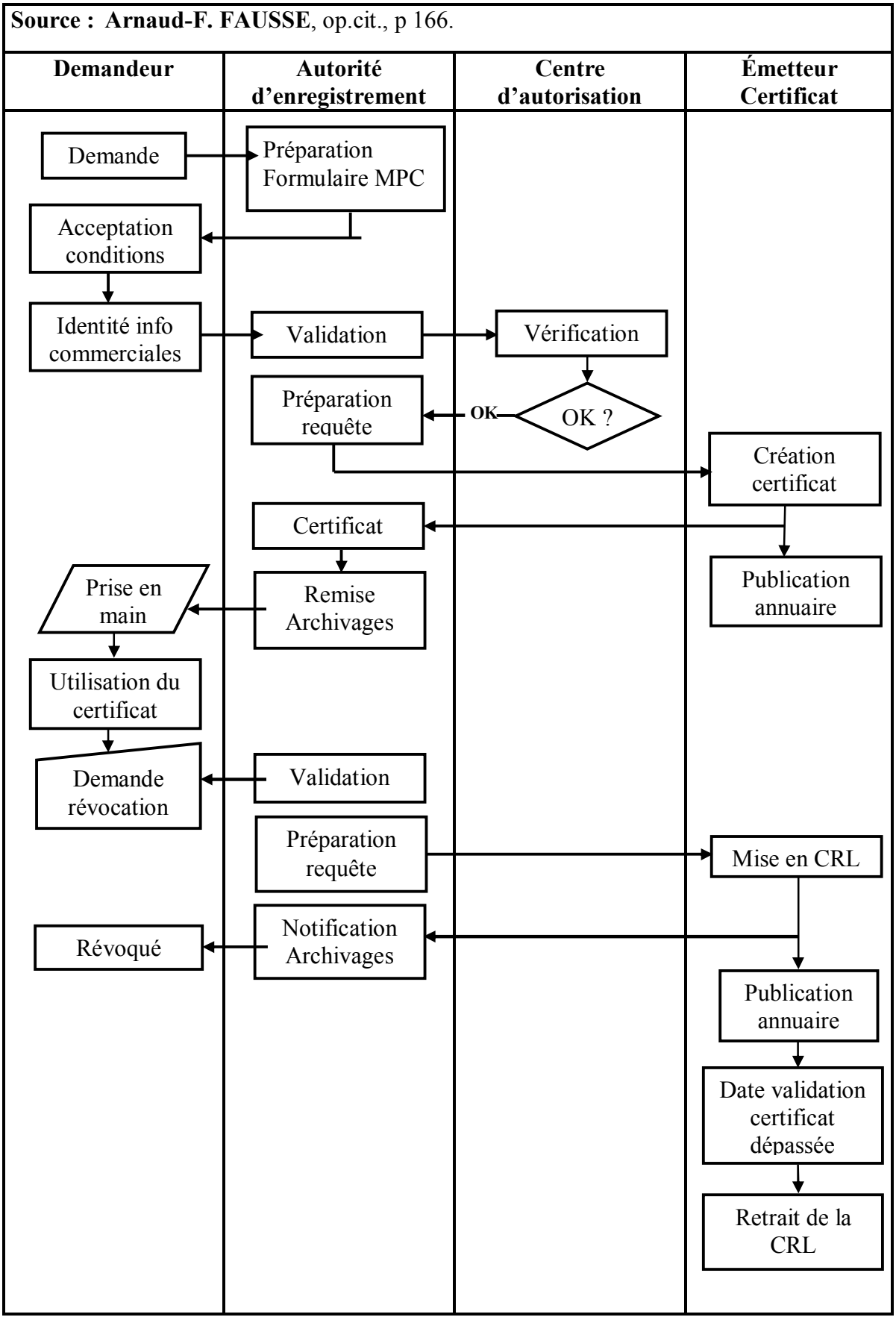
الملحق رقم: (32)	نموذج قائمة الثقة(Modèle Trust List)	الصّفحة رقم: (333)



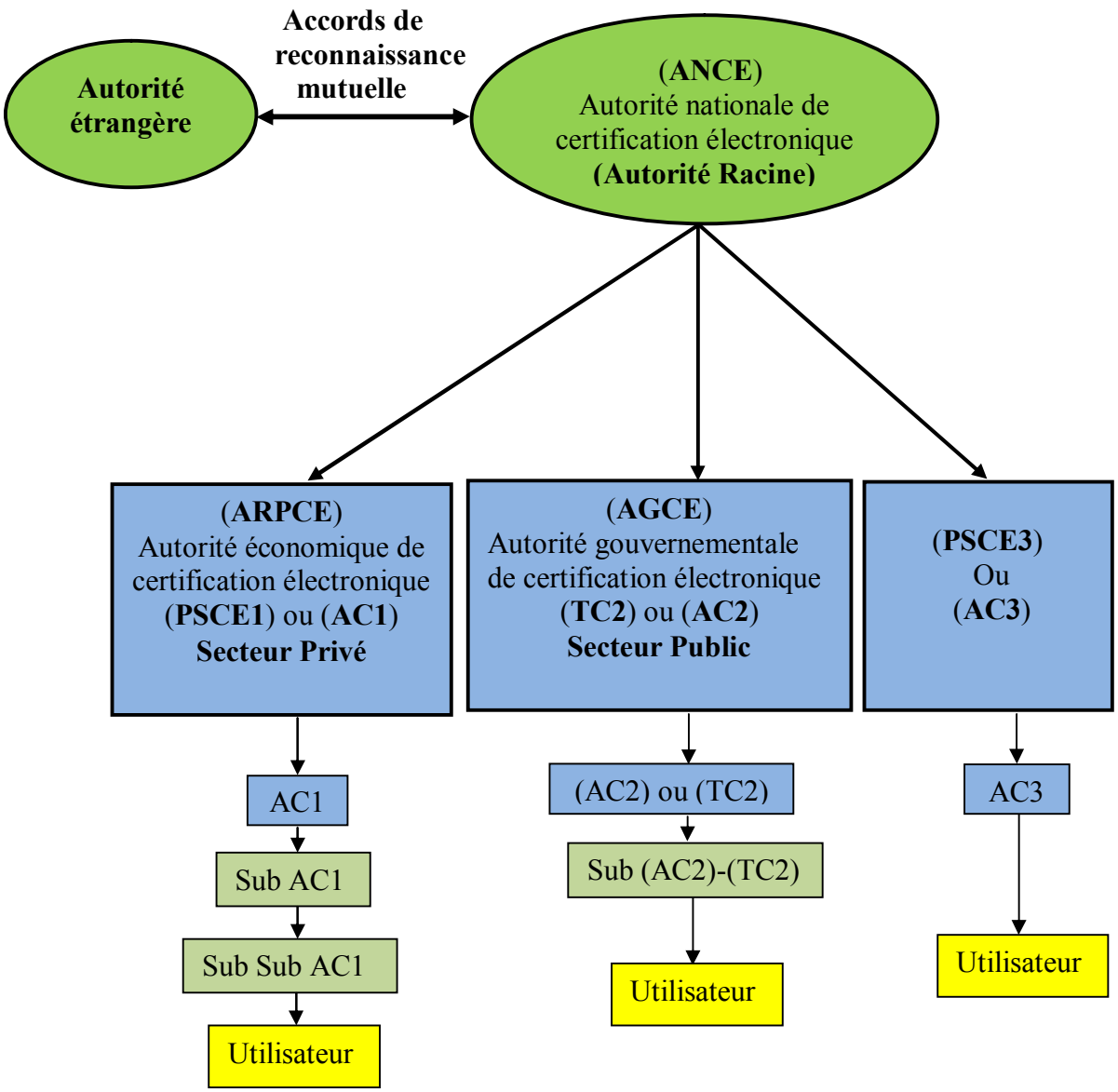
- Modèle plus ouvert, plus flexible que le modèle hiérarchique.
- Absence de : Contrôle et un Processus de normalisation et de validation (interopérabilité), et d'une entité nationale qui signe les conventions de reconnaissance mutuelles avec les instances internationales.

Source: - Ahmed BERBAR, (SICE' 2009 ARPCE), op.cit., p.08.

الملحق رقم: (33)	**Model représente le rôle d'interface de l'AE dans le cycle de certification.**	الصّفحة رقم:(334)


Source : Arnaud-F. FAUSSE, op.cit., p 166.
Demandeur
Autorité d'enregistrement
Centre d'autorisation
Émetteur Certificat
Demande
Préparation Formulaire MPC
Acceptation conditions
Identité info commerciales
Validation
Vérification
Préparation requête
OK
OK ?
Création certificat
Certificat
Publication annuaire
Prise en main
Remise Archivages
Utilisation du certificat
Demande révocation
Validation
Préparation requête
Mise en CRL
Révoqué
Notification Archivages
Publication annuaire
Date validation certificat dépassée
Retrait de la CRL

الملحق رقم: (34)	نموذج التصديق الهرمي المنتهج في الجزائر	الصّفحة رقم: (349)



- **المصدر**: من إعداد الباحث.

قائمة المراجع

أوّلا- باللغة العربية:

I- الكتب:

1- **أحمد سفر**، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2008.

2- **أحسن بوسقيعة**، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر، الطبعة 10، الجزائر، 2011.

3- **أمير فرج يوسف**، الجرائم التجارية الإلكترونية وأساليب مكافحتها، وكيفية حماية المستهلك الإلكتروني وأطراف العقد الإلكتروني التجاري، مكتبة الوفاء القانونية، الإسكندرية، 2013.

4- .....، عالمية التجارة الإلكترونية وعقودها وأساليب مكافحة الغش التجاري الإلكتروني، المكتب الجامعي الحديث، الإسكندرية، 2009.

5- **أوليغ عوكي**، فايسبوك(Facebook) للجميع(دليل إلى التسلية مع الأصدقاء وإلى الترويج للمشاريع على فايسبوك)، الدار العربية للعلوم ناشرون، (د.ب.ن)، 2009.

6- **إيمان فاضل السامرائي**، تسويق المعلومات وخدمات الانترنت، الطبعة الثانية، دار صفاء للنشر والتوزيع، عمان، الأردن، 2015.

7- **إيمان مأمون أحمد سليمان**، إبرام العقد الإلكتروني وإثباته(الجوانب القانونية لعقد التجارة الإلكتروني)، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2008.

8- **بشار محمود دودين، محمد يحيى المحاسنة**، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006.

9- **بشير عباس العلاق**، التسويق الإلكتروني، دار اليازوري العلمية للشر والتوزيع، عمان، الأردن، 2010.

10- .....، التسويق عبر الإنترنت، مؤسسة الوراق للنشر والتوزيع، عمّان، الأردن، 2002.

11- **تيسير العجارمة**، التسويق المصرفي، دار حامد للنشر والتوزيع، عمان، الأردن، 2005.

12- **جعفر حسن جاسم الطائي**، جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة الحديثة)، دار البداية، عمان، الأردن، 2007.

13- **حميد الطائي، أحمد شاكر العسكري**، الاتصالات التسويقية المتكاملة(مدخل استراتيجي)، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009.

14- **خالد جمال أحمد**، الالتزام بالإعلام قبل التعاقد، دار النهضة العربية، القاهرة، مصر، 1996.

15- **خالد عبده الصرايره**، النشر الإلكتروني وأثره على المكتبات ومراكز المعلومات، دار كنوز المعرفة العلمية للنشر والتوزيع، عمان، الأردن، 2008.

16- **خالد ممدوح إبراهيم**، أمن المعلومات الالكترونية، الدار الجامعية، الإسكندرية، مصر، 2010.

17- **دلال صادق الجواد، حميد ناصر الفتال**، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2008.

18- **ديالا عيسى ونسه**، حماية حقوق التأليف على شبكة الإنترنت، منشورات صادر الحقوقية، لبنان، 2002.

19- **ديفيد ميرمان سكوت(ترجمة ديب القيس)**، القواعد الجديدة للتسويق والعلاقات العامة، دار الكتاب العربي، بيروت، لبنان، 2007.

20- **رامي إبراهيم حسن الزواهرة**، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف: دراسة مقارنة في القوانين الأردني والمصري والإنجليزي، دار وائل للنشر، عمان، 2013.

21- **ربحي مصطفى عليان**، البيئة الإلكترونية(E- Environment)، الطبعة الثانية، دار صفاء للنشر والتوزيع، عمّان، الأردن، 2015.

22- **ربحي مصطفى عليان، إيمان السامرائي**، النشر الالكتروني، الطبعة الثانية، دار صفاء للنشر والتوزيع، عمان، الأردن، 2014.

23- **رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية(دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي)، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2008.

24- **زياد محمد الشرمان، عبد الغفور عبد السلام**، مبادئ التسويق، الطبعة الثانية، دار صفاء للنشر والتوزيع، عمان، الأردن، 2001.

25- **زيبحة زيدان**، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار هدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011.

26- **سعد غالب ياسين**، تحليل وتصميم نظم المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2010.

27- **سلطان عبد الله محمود الجواري**، عقود التجارة الإلكترونية والقانون الواجب التطبيق(دراسة مقارنة)، منشورات الحلبي، بيروت، لبنان، 2010.

28- **سمير جميل حسين الفتلاوي**، الملكية الصناعية وفقا للقوانين الجزائرية، ديوان المطبوعات الجامعية، الجزائر، 1988.

29- **سمير دنون**، العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية، شركة المؤسسة الحديثة للكتاب، لبنان، 2012.

30- **سوسن زهير المهتدى**، تكنولوجيا الحكومة الإلكترونية، دار أسامة للنشر والتوزيع، الأردن، عمان، 2011.

31- **شريف محمد غنام**، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني(Domain Name)، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

32- **صالح بن علي بن حمد الحراصي**، الإثبات في عقود التجارة الالكترونية في القانون العماني والقانون المقارن، مكتبة الضامري للنشر والتوزيع، السيب، سلطنة عمان، 2009.

33- **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي(النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

34- **طارق عفيفي صادق أحمد**، الجرائم الإلكترونية، جرائم الهاتف المحمول(دراسة مقارنة بين القانون المصري والإماراتي والنظام السوري)، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2015.

35- **عامر إبراهيم قنديلجي، إيمان فاضل السامرائي**، شبكات المعلومات والاتصالات، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، 2012.

36- **عامر محمود الكسواني**، التجارة عبر الحاسوب، ماهيتها- إثباتها- وسائل حمايتها- القانون الواجب التطبيق عليها في كلّ من الأردن ومصر وإمارة دبي(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

37- **عايد رجا الخلايلة**، المسئولية التقصيرية الإلكترونية: المسئولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

38- **عبد الرحمن بن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترونية(الحاسب الآلي وشبكة المعلومات(الإنترنت))، دار الوراق للطباعة والنشر والتوزيع، بيروت، لبنان، 2004.

39- **عبد الرزاق السنهوري**، الوسيط في شرح القانون المدني (نظرية الالتزام- الإثبات)، الطبعة الثالثة، الجزء الثاني، دار النهضة العربية، القاهرة، 1981.

40- **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

41- .....، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2007.

42- .....، التجارة الالكترونية وحمايتها القانونية: نظام التجارة الإلكترونية وحمايتها المدنية، الكتاب الأول، دار الكتب القانونية، مصر، 2007.

43- .....، التجارة الإلكترونية(شرح قانون المبادلات والتجارة الإلكترونية)، الكتاب الأول، دار الكتب القانونية، مصر، 2007.

44- .....، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2003.

45- **عبد الله أحمد غرايبة**، حجية التوقيع الإلكتروني في التشريع المعاصر، دار الراية للنشر والتوزيع، عمان، الأردن، 2008.

46- **عبد الله عبد الكريم عبد الله**، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2008.

47- **عبد الله فرغلي علي موسى**، تكنولوجيا المعلومات ودورها في التسويق التقليدي والإلكتروني، دار ايتراك للنشر والتوزيع، القاهرة، مصر، 2007.

48- **عصام عبد الفتاح مطر**، التجارة الإلكترونية في التشريعات العربية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

49- **علاء حسين الحمامي، سعد عبد العزيز العاني**، تكنولوجيا أمنية المعلومات وأنظمة الحماية، دار وائل للنشر والتوزيع، الأردن، عمان، 2007.

50- **علاء حسين الحمامي، علاء الدين جواد الراضي**، الإصدار السادس لبروتوكول الإنترنتIPv6(العمود الفقري لإنترنت الأجيال القادمة)، دار الراية للنشر والتوزيع، عمان، الأردن، 2015.

51- **علاء عبد الرزاق السالمي**، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2017.

52- **علي كحلون**، المسؤولية المعلوماتية(محاولة لضبط مميّزات مسؤوليّة المتدخلين في إطار التطبيقات المعلوماتية وخدماتها)، مركز النشر الجامعي، تونس، 2005.

53- **عمر حسن المومني**، التوقيع الإلكتروني وقانون التجارة الإلكترونية(دراسة قانونية وتحليلية مقارنة)، دار وائل للنشر والتوزيع، عمان، الأردن، 2003.

54- **عمر خالد زريقات**، عقود التجارة الإلكترونية: عقد البيع عبر الإنترنت(دراسة تحليلية)، دار الحامد للنشر والتوزيع، عمان، الأردن،2007.

55- **عمرو عيسى الفقى**، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، مصر، 2006.

56- **عيسى غسان ربضي**، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

57- **غسان قاسم داود اللامي، أميرة شكرولي البياتي**، تكنولوجيا المعلومات في منظمات الأعمال(الاستخدامات والتطبيقات)، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2010.

58- **فاتن حسين حوى**، المواقع الإلكترونية وحقوق الملكية الفكرية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

59- **فداء حسين أبودبسة، خلود بدر غيث**، تصميم الإعلان والترويج الإلكتروني، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن، 2009.

60- **لزهر بن سعيد**، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2014.

61- **لورنس محمد عبيدات**، إثبات المحرر الالكتروني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

62- **محمد إبراهيم عبيدات**، مبادئ التسويق، دار المستقبل للنشر والتوزيع، عمان، الأردن، 1989.

63- **محمد الصيرفي**، التسويق الإلكتروني، دار الفكر الجماعي، الإسكندرية، مصر، 2008.

64- **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

65- **محمد حسين منصور**، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.

66- **محمد سعيد أحمد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت لبنان، 2009.

67- **محمد طاهر نصير**، التسويق الإلكتروني، دار الحامد للنشر والتوزيع، عمان، الأردن، (د، ت، ن).

68- **محمد عبد حسين الطائي**، التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

69- **محمد عبد حسين الطائي، ينال محمود الكيلاني**، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015.

70- **محمد فريد الصحن**، الإعلان، الدار الجامعية للنشر والطبع والتوزيع، الإسكندرية، مصر، 2005.

71- .....، التسويق(المفاهيم والإستراتيجيات)، الدار الجامعية، الإسكندرية، 1998.

72- **محمد فريد الصحن، نبيلة عباس**، مبادئ التسويق، الدار الجامعية، الإسكندرية، مصر، 2004.

73- **محمد فواز المطالقة**، النظام القانوني لعقود إعداد برامج الحاسوب الآلي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

74- .....، الوجيز في عقود التجارة الإلكترونية: أركانها، إثباتها، حمايتها(التشفير)، التوقيع الإلكتروني، القانون الواجب التطبيق(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

75- **محمد محمد سادات**، حجية المحرّرات الموقعة إلكترونيًّا في الإثبات (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2011.

76- **محمد مدحت عزمي**، المعاملات التجارية الإلكترونية(الأسس القانونية والتطبيقات)، مركز الإسكندرية للكتاب، مصر، 2008.

77- **محمود أحمد عبابنة، محمد معمر الرازقي**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

78- **محمود جاسم الصميدعي**، إستراتيجية التسويق(مدخل كمي وتحليلي)، دار ومكتبة الحامد للنشر والتوزيع، عمان، الأردن، 2000.

79- **محمود محمد أبو فروة**، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

80- **مروة زين العابدين صالح**، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، بين القانون الدولي الإتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، 2017.

81- **مصطفى كمال طه، وائل أنور بندق،** الأوراق التجارية(الكمبيالة- السند الإذني- الشيك- النقود الإلكترونية- الأوراق التجارية الإلكترونية- بطاقات الوفاء والإئتمان)، دار الفكر الجامعي، الإسكندرية، 2005.

82- **منير محمد الجنبيهي، ممدوح محمد الجنبيهي،** البنوك الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2004.

83- **ناصر خليل،** التجارة والتسويق الإلكتروني، دار أسامة للنشر والتوزيع، عمان، الأردن، 2009.

84- **نزيه محمد الصادق المهدي،** الالتزام قبل التعاقدي بالإدلاء بالبيانات المتعلقة بالعقد وتطبيقاته على بعض أنواع العقود(دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 1999.

85- **نظام موسى سويدان، شفيق ابراهيم حداد،** التسويق: مفاهيم معاصرة، دار الحامد للنشر والتوزيع، عمان، الأردن، 2003.

86- **نواف كنعان،** حق المؤلف: النماذج المعاصرة لحق المؤلف ووسائل حمايته، الطبعة الثالثة، دار الثقافة للتوزيع والنشر، عمان، 2000.

87- **هدى حامد قشقوش،** الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، مصر، 2000.

88- **الياس ناصيف،** العقود الدولية: العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.

89- **يوسف أحمد أبو فارة،** التسويق الإلكتروني: عناصر المزيج التسويقي عبر الإنترنت، دار وائل للنشر والتوزيع، عمان، الأردن، 2004.

90- **يوسف حسن يوسف،** الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011.

91- .....، التسويق الالكتروني، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012.

92- .....، البنوك الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012.

II - الرّسائل والمذكرات الجامعيّة:

أ)- رسائل الدكتوراه:

1- **إبراهيم بختي**، "دور الإنترنت وتطبيقاته في مجال التسويق(دراسة حال الجزائر)"، دكتوراه دولة في العلوم الإقتصادية، كلية العلوم الإقتصادية وعلوم التسيير، جامعة الجزائر، 2002.

2- **حابت آمال**، "التجارة الإلكترونية في الجزائر"، دكتوراه في العلوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، 2015.

3- **حسين نوارة**، "الحماية القانونية للمستثمر الأجنبي في الجزائر"، رسالة دكتوراه في العلوم، تخصص: القانون، كلية الحقوق، جامعة مولود معمري- تيزي وزو، 2013.

4- **حوالف عبد الصمد**، "النظام القانوني لوسائل الدفع الإلكتروني"، رسالة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، 2014.

5- **زواوي الكاهنة**، "المنافسة غير المشروعة في الملكية الصناعية"، شهادة دكتوراه في العلوم، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر- بسكرة، 2015.

ب)- مذكرات أو رسائل الماجستير:

1- **بن خليفة مريم،** "التسويق الإلكتروني وآليات حماية المستهلك"، مذكرة الماجستير في الحقوق، تخصص: قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 02، 2015.

2- **بوباح عالية،** "دور الإنترنت في مجال تسويق الخدمات(دراسة حالة قطاع الاتصالات)"، مذكرة الماجستير في العلوم التجارية، تخصص: التسويق، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، 2010.

3- **بوعافية رشيد،** "الصيرفة الإلكترونية والنظام المصرفي الجزائري- الآفاق والتحديات"، مذكرة الماجستير في العلوم الاقتصادية، تخصص: نقود، مالية وبنوك، جامعة سعد دحلب- البليدة، 2006.

4- **دحماني سمير،** "التوثيق في المعاملات الإلكترونية(دراسة مقارنة)"، مذكرة الماجستير في القانون، فرع: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، 2015.

5- **شيروف فضيلة،** "أثر التسويق الإلكتروني عل جودة الخدمات المصرفية(دراسة حالة بعض البنوك في الجزائر)"، مذكرة الماجستير، تخصص: تسويق، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري- قسنطينة، 2009.

6- **عبد الله ذيب عبد الله محمود،** "حماية المستهلك في التعاقد الالكتروني(دراسة مقارنة)"، رسالة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009.

7- **عمر طارق عمر سالم،** "علاقة التسويق الإلكتروني بتعزيز الميزة التنافسية"، رسالة الماجستير في إدارة الأعمال"، كلية الاقتصاد والعلوم الإدارية، جامعة الأزهر، غزة، 2017.

8- **ليث محمود أحمد الحاج**، "نظام الخدمات المصرفية الإلكترونية عبر (SMS) ودوره في تحقيق ولاء العملاء في البنوك التجارية الأردنية"، رسالة الماجستير، قسم إدارة الأعمال، كلية الأعمال، جامعة الشرق الأوسط، 2012.

9- **مروة نبيل حلمي الحايك**، "التسويق عبر شبكات التواصل الاجتماعي وعلاقته في تعزيز إدارة العلاقة مع الزبون في شركات تكنولوجيا المعلومات- قطاع غزة"، رسالة الماجستير في إدارة الأعمال، كلية الاقتصاد والعلوم الإدارية، جامعة الأزهر، غزة، 2017.

III- المقالات العلمية:

1- **أحمد عبد الله مصطفى**، "حقوق الملكية الفكرية والتأليف في بيئة الإنترنت"، مجلة الكترونية محكمة في المكتبات والمعلومات(Cybrarians journal)، عدد 21، ديسمبر 2009، ص ص 01-30.
https://www.cybrarians.info/journal/no21/searchengines.htm

2- **أحمد قاسم فرح**، "النظام القانوني لمقدمي خدمات الإنترنت- دراسة تحليليّة مقارنة-" مجلة المنارة، المجلد 13، عدد 09، 2007، (ص ص 319-390).

3- **أسماء بنت لشهب، باسم محمد ملحم**،"التنظيم القانوني للمقاصة الإلكترونية للشيكات وللعلاقات القانونية الناشئة عنها في القانون الأردني"، مجلة دراسات، علوم الشريعة والقانون، عدد 2013/02، كلية الحقوق، الجامعة الأردنية، ص ص 456- 473.

4- **باسم السيد**، "النظام القانوني لمزودي خدمة الإنترنت في سورية"، مجلة جامعة البعث، المجلد 39، العدد 50، 2017، ص ص 67- 89.

5- **رامي علوان**، "المنازعات حول العلامات التجارية وأسماء مواقع الإنترنت"، مجلة الشريعة والقانون، عدد 2005/22، كلية الشريعة والقانون، جامعة الإمارات.

6- **رشا محمد تيسير الحطاب، مها يوسف خصاونة**، "تطبيق النظام القانوني للمحل التجاري على الموقع التجاري الإلكتروني"، مجلة الشريعة والقانون، عدد 2011/02، كلية القانون، جامعة اليرموك، ص ص 343- 382.

7- **فاطمة الزهراء محمد عبده**، "محركات البحث على شبكة الإنترنت"، مجلة الكترونية محكمة في المكتبات والمعلومات(Cybrarians journal)، عدد 02، سبتمبر 2004، 01-25. https://www.cybrarians.info/journal/no2/searchengines.htm

8- **يونس عرب**، "التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية"، مجلة العربية 3000، عدد2003/1، النادي العربي للمعلومات، سوريا، ص ص 155-219.

9- .....، "العقود الإلكترونية- أنظمة الدفع والسداد الإلكتروني"، ص ص 105-129، مقال منشور عبر الموقِع التّالي: http://www.arablaw.org/

10-.....، "أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها"، ص ص 01-62، مقال منشور عبر الموقع الإلكتروني التّالي: http://www.arablaw.org/Download/Information_Security.doc

11-.....، "نظام الملكية الفكرية لمصنفات المعلوماتية"، ص ص 01-40، مقال منشور عبر الموقع الإلكتروني التّالي: https://www.arablawinfo.com/

IV- المداخلات:

1- **إبراهيم الدسوقي أبو الليل**، "النشر الإلكتروني وحقوق الملكية الفكرية"، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية- الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، المجلد الثاني، ص ص 148- 174.

2- **إبراهيم الدسوقي أبو الليل**، "توثيق التعاملات الإلكترونية و مسؤولية جهة التوثيق تجاه الغير المضرور"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و 12 ماي 2003، المجلد الخامس، الصفحات 1745 إلى 1913.

3- **سعد محمد سعد،** "المسائل القانونية التي تثيرها العلاقة الناشئة عن استخدام بطاقة الإئتمان بين الجهة مصدرة البطاقة والتاجر"، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الثاني، ص ص 797-846.

4- **شريف محمد غنام،** "محفظة النقود الرقمية(رؤية مستقبلية)"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و 12 ماي 2003، المجلد الأول، ص ص 101- 128.

5- **عبد الحق حميش،** "حماية المستهلك الالكتروني"، بحث مُقدّم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و12 ماي 2003، المجلد الثالث، ص ص 1267- 1315.

6- **عصام حنفي محمود موسي،** "الطبيعة القانونية لبطاقة الائتمان"، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الثاني، ص ص 847-936.

7- **محمد إبراهيم محمود الشافعي،** "الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، المجلد الأول، ص ص 129- 177.

8- **محمد البنان،** "العقود الإلكترونية"، منشورات المنظمة العربية للتنمية الإدارية(أعمال المؤتمرات)، مصر، 2007، ص ص 01- 49.

9- **محمود أحمد إبراهيم الشرقاوي**، "مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، المجلد الأول، ص ص 17- 61.

10- **موسى رزيق**، "رضا حامل البطاقة الائتمانية بالعقد والحماية التي يقررها المشرع له"، دراسة في ضوء تشريع المعاملات المدنية الاتحادي، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة و القانون، الذي نظمته كلية الشريعة و القانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية و صناعة دبي، في 10 و12 ماي 2003، المجلد الأول، الصفحات من 1035 إلى 1087.

11- **نبيل صلاح محمود العربي**، "الشيك الإلكتروني والنقود الرقمية(دراسة مقارنة)"، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003، المجلّد الأول، الصفحات من 63 إلى 81.

V- النّصوص القانونيّة:

أ)- الاتفاقيات الدوليّة التي صادقت عليها الجزائر:

1- أمر رقم 75-02 مؤرخ في 9 جانفي 1975، يتضمن المصادقة على اتفاقية باريس لحماية الملكية الصناعية المبرمة في 20 مارس 1883، والمعدلة ببروكسل في 14 ديسمبر 1900 وواشنطن في 02 جوان 1911، ولاهاي في 06 نوفمبر 1925 ولندن في 02 جوان 1934 ولشبونة في 31 أكتوبر 1958، واستكهولم في 14 جويلية 1967، ج ر عدد 10 الصادر في 04 فيفري 1975.

2- مرسوم رئاسي رقم 97-341 مؤرخ في 13 سبتمبر 1997 يتضمن انضمام الجمهورية الديمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 09 سبتمبر 1886، والمتممة بباريس في 04 ماي 1896 والمعدلة ببرلين

في 13 نوفمبر 1908، والمتممة ببرن في 20 مارس 1914، والمعدلة بروما في 02 جوان 1928، وبروكسل في 26 جوان 1948 واستكهولم في 14 جويلية 1967 وباريس في 24 جويلية 1971، والمعدلة في 28 سبتمبر 1979. ج ر عدد 61 الصادر في 14 سبتمبر 1997.

3- مرسوم رئاسي رقم 99-92 مؤرخ في 15 أفريل 1999 يتضمن المصادقة بتحفظ على معاهدة التعاون بشأن البراءات، المبرمة في واشنطن بتاريخ 19 جوان 1970 والمعدلة في 28 سبتمبر 1979، وفي 03 فيفري 1984، وعلى لائحتها التنفيذية، ج ر عدد 28 الصادر في 19 أبريل 1999.

ب)- النّصوص التّشريعيّة:

1- أمر رقم 66- 156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، المعدل والمتمم، بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر2004، ج ر عدد 71 الصادر في 10 نوفمبر 2004.

2- أمر رقم 75-58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، المعدل والمتمم، بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005، ج ر عدد 44 الصادر في 26 جوان 2005.

3- أمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، المعدل والمتمم، بموجب القانون رقم 05-02 المؤرخ في 06 فيفري 2005، ج ر عدد 11 الصادر في 09 فيفري 2005.

4- مرسوم تشريعي رقم 93-17 مؤرخ في 07 ديسمير 1993، يتعلق بحماية الاختراعات، ج ر عدد 81 الصادر في 24 ديسمبر 1993.

5- أمر رقم 03-07 مؤرخ في 19 جويلية 2003، يتعلق ببراءات الاختراع، ج ر عدد 44 الصادر في 23 جويلية 2003.

6- أمر رقم 03-08 مؤرخ في 19 جويلية 2003، يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، ج ر عدد 44 الصادر في 23 جويلية 2003.

7- أمر رقم 03-11 مؤرخ في 26 أوت 2003، يتعلق بالنقد والقرض، ج ر عدد 52 الصادر في 27 أوت 2003، المعدل والمتمم، بموجب الأمر رقم 09-01 المؤرخ في 22 جويلية 2009، ج ر عدد 44 الصادر في 26 جويلية 2009، المعدل والمتمم، بموجب الأمر رقم 10-04 المؤرخ في 26 أوت 2010، ج ر عدد 50، الصادر في 01 سبتمبر 2010، والمعدل والمتمم، بموجب القانون رقم 17-10 المؤرخ في 11 أكتوبر 2017، ج ر عدد 57، الصادر في 12 أكتوبر 2017.

8- قانون رقم 04-02 مؤرخ في 23 جويلية 2004، يحدد القواعد المطبقة على الممارسات التجارية، ج ر عدد 41 الصادر في 27 جويلية 2004، المعدل والمتمم، بموجب القانون رقم 10-06 المؤرخ في 15 أوت 2010، ج ر عدد 46 الصادر في 18 أوت 2010، المعدل والمتمم بموجب القانون رقم 17-11 المؤرخ في 27 ديسمبر 2017، الذي يتضمن قانون المالية لسنة 2018، ج ر عدد 76، الصادر في 28 ديسمبر 2017، والمعدل والمتمم بموجب القانون رقم 18-13 المؤرخ في 11 جوان 2018، الذي يتضمن قانون المالية التكميلي لسنة 2018، ج ر عدد 42 الصادر في 15 جوان 2018.

9- قانون رقم 09-03 مؤرخ في 25 فيفري 2009، يتعلق بحماية المستهلك وقمع الغش، ج ر عدد 15 الصادر في 08 مارس 2009.

10-قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47 الصادر في 16 أوت 2009.

11-قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06 الصادر في 10 فيفري 2015.

12- قانون رقم 17-11 مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، ج ر عدد 76، الصادر في 28 ديسمبر 2017.

13- قانون رقم 17-02 مؤرخ في 10 جانفي 2017، يتضمن القانون التوجيهي لتطوير المؤسسات الصغيرة والمتوسطة، ج ر عدد 02، الصادر في 11 جانفي 2017.

14- قانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر عدد 27، الصادر في 13 ماي 2018.

15- قانون رقم 18-05 مؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، ج ر عدد 28، الصادر في 16 ماي 2018.

16- قانون رقم 18-09 مؤرخ في 10 جوان 2018، يعدل ويتمم القانون رقم 09-03 المؤرخ في 25 فيفري 2009، المتعلق بحماية المستهلك وقمع الغش، ج ر عدد 35 الصادر في 13 جوان 2018.

17- قانون رقم 18-07 المؤرخ في 10 جويلية 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34 الصادر في 10 جويلية 2018.

18-قانون رقم 20-05 مؤرخ في 28 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج ر عدد 25 الصادر في 29 أفريل 2020.

ج)- نصوص تنظيميّة:

1- مرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 53 الصادر في 08 أكتوبر 2015.

2- مرسوم رئاسي رقم 20-05 مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04 الصادر في 26 جانفي 2020.

VI- النّصوص القانونيّة الأجنبيّة.

1- أمر عدد 2768 لسنة 1999 مؤرخ في 06 ديسمبر 1999 يتعلق بإحداث وحدة تصرف حسب الأهداف لإنجاز مشروع تطوير السلامة الإعلامية وبضبط تنظيمها وطرق سيرها، ر.ر.ج.ت عدد 102 الصادر في 21 ديسمبر 1999.

2- قانون عدد 83 لسنة 2000 مُؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية، المنشور في ر.ر.ج.ت عدد 64، الصادر في 9 أوت 2000.

3- قانون أساسي عدد 63-2004 مؤرخ في 27 جويلية 2004 يتعلق بحماية المعطيات الشخصية، ر.ر.ج.ت عدد 61 الصادر في 30 جويلية 2004.

4- قانون عدد 05- 2004 مؤرخ في 03 فيفري 2004 يتعلق بالسلامة المعلوماتية، ر.ر.ج.ت عدد 10 الصادر في 03 فيفري 2004.

5- مرسوم سلطاني رقم 69-2008 مؤرخ في 17 ماي 2008، يتعلق بإصدار قانون المعاملات الإلكترونية، الجريدة الرسمية لسلطنة عمان عدد 864، الصادر في 17 ماي 2008.

6- قرار وزاري رقم(1) لسنة 2008(الإمارات) بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني. https://www.government.ae

VII- الوثائق الآخرى:

1- أضافه عباس، "شركة حوسب الفلسطينية تبدأ التعامل بالبتكوين"، مقال منشور في 2014/05/04؛ التوقيت18:16، على الموقع التالي:

http://arabicbitcoin.net/news/hawsib-starts-accepting-bitcoin (تم الاطّلاع عليه في 2016/02/27.)

2- **أمناي أفشكو**، "إعلانات فيس بوك: أفضل وسيلة لنشر الأخبار المزيفة والفيروسات"، مقال منشور بتاريخ 06 مارس 2017، عبر الموقع الإلكتروني التالي: https://www.google.com/amp/s/www.amnaymag.com/ (تم الاطّلاع عليه في 10 سبتمبر 2018.)

3- **جهاد بالكحلاء**، "كيف تنجح في التسويق عبر مواقع التواصل الاجتماعي؟"، مقال منشور بتاريخ 25 مارس 2019، عبر موقع عربي 21. https://arabi21.com/story/997093/ (تم الاطّلاع عليه في 11 ماي 2019.)

4- **دارين العمري**، "افتتاح أوّل صرّاف لعملة "بتكوين" الافتراضية في دبي"، مقال منشور في 29 ابريل 2014، التوقيت 12:42(آخر تحديث له تم في 01 ماي 2014، التوقيت 06:32)، على الموقع التالي:http://arabic.cnn.com/business/2014/04/29/bitcoin-sergey-yusopov-interview(تم الاطّلاع عليه في 2016/02/25.)

5- **عبلة عيساتي**، "وزارة الاقتصاد الرقمي ماذا ستضيف للجزائر؟"، مقال منشور في جريدة أخبار اليوم، في 26 جويلية 2016، على الموقع الإلكتروني التالي: http://www.akhbarelyoum.dz (تم الاطّلاع عليه في 2016/07/28.)

6- **علي وديع حسن**، "كيف تختار كلمة مرور قوية قدر الإمكان لتحمي نفسك من الاختراق ؟"، مقال منشور في 24 أغسطس 2018، عبر الموقع الإلكتروني التالي: https://www.tech247.me/how-to-choose-a-password/ (تم الاطّلاع عليه في 2019/02/20.)

ثانيا- باللغة الفرنسية:

I- **Ouvrages**:

1- **Arnaud-F. FAUSSE**, La signature électronique : transaction et confiance sur Internet, DUNOD, Paris, 2001.

2- **Ali EL AZZOUZI**, La cybercriminalité au Maroc, Bishops Solutions, Casablanca, 2010.
3- **Armel BENARAB**, Commerce & Internet : comprendre les règles juridiques, L'Harmattan, Paris, 2013.
4- **Christophe CAMBORDE**, Sécuriser vos applications Internet (Messageries, Intranet, sites web, e-commerce), Dunod, Paris, France, 2004.
5- **Cédric BERGÉ**, Je crée mon site Internet avec Dreamweaver 8 et Flash 8, éditions EYROLLES/DEMOS, Paris, France, 2006.
6- **Chiheb GHAZOUANI**, Le commerce électronique international, Latrach édition, Tunis, 2011.
7- **Daniel AMOR**, La révolution e-business, Pearson Éducation France, Paris, France, 2000.
8- **Daniel- Jean DAVID**, Développer son site web, édition ellipses, Paris, France, 2007.
9- **……**, HTMLE5 et CSS3, par la pratique (construire un site internet de qualité professionnelle), édition ellipses, Paris, France, 2014.
10- **Didier MAZIER**, PrestaShop : créer un site de e-commerce, édition ENI, France, 2011.
11- **Étienne WÉRY,** Facture, Monnaie et paiement électroniques, édition du Juris-Classeur, Litec, France, 2003.
12- **Eric CHARTON**, Sites Internet : conception et réalisation, édition Simon et Schuster Macmillan, Paris, France, 1997.
13- ----------, créer votre site web, Campus Press, Paris, France, 2004.
14- **François- XAVIER BOIS**, Sites web dynamiques (PHP, MySQL, JavaScript™, Ajax), MA édition, France, 2012.
15- **Fabrice MATTATIA**, Traitement des données personnelles- le guide juridique (La loi informatique et libertés et la CNIL Jurisprudence), éditions EYROLLES, France, 2013.
16- **Franck LEROY**, Réseaux sociaux et C^{ie} (Le commerce des données personnelles), ACTES SUD, France, 2013.
17- **Jeffrey F. RAYPORT, Bernard J. JAWORSKI**, Commerce électronique, édition de la chenelière McGraw-Hill, Québec, Canada, 2003.
18- **Jaime ANGELES**, Commerce électronique : de la perspective américaine à un cadre international, Collection Droit du cyberespace, Édition UNESCO/ Economica, 2005.

19- **Jakob NEILSEN, Hoa, LORANGER**, Sites web: priorité à la simplicité, Pearson, Paris, 2007.
20- **Jean-François PILLOU, Fabrice LEMAINQUE**, Tout sur les réseaux et Internet, 2e édition, Dunod, Paris, France, 2010.
21- **Jean-MARC HARDY, Gaetano PALERMO**, Réussir son site web en 60 fiches, 3e édition, Dunod, Paris, France, 2010.
22- **Jean-Marc DÉCAUDIN, Jacques DIGOUT**, e-Publicité (Les fondamentaux), Dunod, France, 2011.
23- **Hélie- SOLANGE GHERNAOUTI**, Sécurité Internet : Stratégies et technologies, Dunod, Paris, France, 2000.
24- **Lionel BOCHURBERG**, Internet et commerce électronique (Sites web- Contrats- Responsabilités- Contentieux), 2e édition, Delmas, France, 2001.
25- **Lary ULLMAN**, PHP 6 et MySQL 5(Créez des sites web dynamiques), Dunod, Paris, France, 2008.
26- **Loïc ANDRÉ**, Le droit des marques à l'heur d'internet, Gualino éditeur, Paris, 2012.
27- **Laure MARINO**, Droit de la propriété intellectuelle, Thémis droit, Paris, 2013.
28- **Michelle Jean- BAPTISTE**, Créer et exploiter un commerce électronique, Litec, France, 1998.
29- **Michel VIVANT**, Les contrats du commerce électronique, Litec, Paris, 1999.
30- **Martine HLADY RISPAL**, Marketing contextuels (Industries- Grande distribution- Web 2.0- Organisation sportives- Arts et culture- Produits biologique- Économie solidaire- Politique des petites communes.), Dunod, Paris, France, 2008.
31- **Marie- Pierre FENOLL- TROUSSEAU, Gérard HASS**, La cybersurveillance dans l'entreprise et le droit, édition Litec, Paris, 2012.
32- **Nicole TORTERELLO, Pascal LOINTIER**, Internet pour les juristes, édition DALLOZ, Paris, 1996.
33- **Nicolas CHU**, réussir un projet de site web, 3e édition, EYROLLES, Paris, France, 2005.
34- **Nathalie DRYFUS**, Marques et Internet (Protection, valorisation, défense.), éditions Lamy, France, 2011.
35- **Olivier ABOU**, Créer son site web(de la construction d'une équipe jusqu'à la mise en ligne d'un site d'entreprise), Microsoft Press, France, 2001.

36- Olivier ANDRRIEU, Réussir son référencement web, éditons Eyrolles, Paris, France, 2012.

37- Patrick THIEFFRY, Commerce électronique: droit international et européen, édition Litec, Paris, 2002.

38- Philippe IRRMANN, Jean BROUSSE, Maurice LEVY, Dominique SCAGLIA, L'informatique au service du marketing, Masson Éditeur, Paris, France, 1976.

39- Philippe RIGAUX, Pratique de MySQL et PHP(Conception, et réalisation de site web dynamique.), 4e édition, Dunod, Paris, France, 2009.

40- Philippe LE TOURNEAU, Contrats informatiques et électroniques, 8e édition, Dalloz, France, 2014.

41- Robert LEDUC, Initiation aux techniques commerciales, Entreprise moderne d'édition, Paris, France, 1976.

42- Romain V. GOLA, Droit du commerce électronique :(Guide pratique du e-commerce), Gualino, Lextenso éditions, France, 2013.

43- Stéphane LOHIER, Dominique PRÉSENT, Internet : Services et réseaux, Dunod, Paris, France, 2004.

44- Sandrine CARNEROLI, Les contrats commentés du monde informatique : Logiciels, Bases de données, Multimédia, Internet, 2e édition, Larcier, Belgique, 2013.

45- Thibault VERBIEST, La protection juridique du cyber-consommateur (Publicité- Contrat- Contentieux), Litec, Paris, 2002.

46- Thomas SCHULTZ, Réguler le commerce électronique par la résolution des litiges en ligne (Une approche critique), BRUYLANT (L.G.D.J), Bruxelles, Belgique, 2005.

47- Vincent FAUCHOUX, Pierre DEPPREZ, Le droit de l'internet : Lois, Contrats, Usages, Litec, France, 2009.

48- William STEINMETZ, Brian WARD, PHP clé en main (76 scripts efficaces pour enrichir vos sites web), Pearson éducation France, 2008.

49- Yan CLAEYSSEN, L'e-mail marketing, 3e édition, Dunod, Paris, France, 2008.

50- Zouheir TRABELSI, Henri LY, La sécurité sur Internet, Lavoisier, Paris, 2005.

Ⅱ - Thèses:

1- **Alexandre SERRES**, « Aux sources d'Internet : l'émergence d'ARPANET », thèse de Doctorat, en Sciences de l'Information et de la Communication, Université Rennes 2 - Haute Bretagne (U.F.R), Arts Lettres Communication, 2000.

2- **Aude PLATEAUX,** « Solutions opérationnelles d'une transaction électronique sécurisée et respectueuse de la vie privée », Thèse de Doctorat, spécialité : Informatique et Applications, Université de Caen Basse-Normandie (école doctorale SIMEM), 2013.

3- **Benjamin CANOU**, « Programmation Web Typée », thèse de doctorat en Sciences, mention : Informatique, Université Pierre et Marie Curie- École Doctorale Informatique, Télécommunications et Électronique, 2011.

4- **Fernand LONE SANG**, « Protection des systèmes informatiques contre les attaques par entrées- sorties », thèse du doctorat, spécialité : Réseaux, télécommunications, Systèmes et Architecture, École Doctorale Mathématique Informatique Télécommunication de Toulouse(EDMITT), Université de Toulouse, 2012.

5- **Géraldine VACHE MARCONATO**, « Évaluation quantitative de la sécurité informatique : approche par les vulnérabilités », Thèse de Doctorat, Spécialité : Système Informatiques, École Doctorale Systèmes, Université de Toulouse, 2009.

6- **Hicham EL KHOURY**, « Une modélisation formelle orientée flux de données pour l'analyse de configuration de sécurité réseau », thèse de doctorat de l'université de Toulouse III - Paul Sabatier, spécialité : Informatique et Télécommunications, 2014.

7- **Laetitia Chaix**, « Le paiement mobile : perspectives économiques, modèles d'affaire et enjeux concurrentiels », Thèse de Doctorat en Sciences Économiques, Université Nice Sophia Antipolis, 2013.

8- **Mickaël LE BORLOCH**, « L'application du droit d'auteur aux hyperliens analyse de droit Français et de droit américain », Thèse de doctorat en droit privé, Université Panthéon-Sorbonne - Paris I, France, 2016.

9- **Sylvie ROLLAND**, «Impact de l'utilisation d'Internet sur la qualité perçue et la satisfaction du consommateur », thèse de doctorat en sciences de gestion, Université Paris IX- Dauphine, U.F.R, Sciences des organisations, Centre de recherche DMCP (Dauphine- Marketing-Stratégie-Prospective), 2003.

10- **Wilson GOUDALO**, « Vers une ingénierie avancée de la sécurité des systèmes d'information d'entreprise : une approche conjointe de la sécurité, de l'utilisabilité et de la résilience dans les systèmes sociotechniques », thèse de doctorat, spécialité : Informatique, Génie Informatique, Université de Valenciennes et du Hainaut-Cambrésis, France, 2017.

Ⅲ- Articles:

1- **A. BRUGEL**, « La vente directe : La vente de personne à personne », Revue Gazette du palais, n°18, 19/1995, pp. 32, 33.
2- **Aglietta MICHEL et Scialom LAURENCE**, « Les risques de la monnaie électronique », Revue L'Économie politique, 2002/2 n° 14, pp. 82-95.
3- **Alain d'IRIBARNE, Robert TCHOBANIAN**, « PME et TIC : quels sites web pour quelles PME ? », Revue Réseaux, 2003/5 n° 121, pp. 145-169.
4- **Alain STROWEL, Nicolas IDE**, « La responsabilité des intermédiaires sur internet: actualités et question des hyperliens (2ème partie) », pp. 01-37. Article publié le 02/02/2001 sur le site: https://www:droit-tchnologie.org, consulté le 11/03/2018.
5- **……**, « Responsabilité des intermédiaires : actualités législatives et jurisprudentielles », pp. 01-44. Article publié le 10/10/2000 sur le site: https://www:droit-tchnologie.org, consulté le 03/03/2018.
6- **Alexandre DEFOSSEZ**, « Conflits entre noms de domaine et marques (renommées) : l'approche OMPI », Revue Internationale de droit économique 2006/2 (t. XX, 2), pp. 167-209.
7- **Ali ELIDRISSI**, « Les sites Web bancaires. Un outil de communication et de distribution au service du client », Revue des Sciences de Gestion, 2005/4 (n°214-215), pp. 165-176.
8- **Alix DESFORGES**, « Le cyberespace : un nouveau théâtre de conflits géopolitiques. », Questions internationales, n° 47- janvier- février 20011, pp. 46-54.
9- **Anat BEN-DAVID**, « La Palestine et ses frontières virtuelles 2.0, du « non-lieu » à l'espace généré par les utilisateurs », Revue Réseaux, 2010/1 n° 159, pp. 151-179.
10- **Anne SOUVIRA, Myriam QUÉMÉNER**« Cyber-sécurité et entreprises : se protéger juridiquement et se former », Revue Sécurité et stratégie, 2012/4 (n°11), pp. 86-94.
11- **Anthony PONCIER**, « La gestion de l'image de l'entreprise à l'ère du web 2.0 », Revue Internationale d'intelligence économique, 2009/1 Vol 1, pp. 81- 91.

12- **Antoinette ROUVROY, Thomas BERNS,** «Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Revue réseaux, 2013/1 n° 177, pp. 163-196.

13- **Antonio CASILLI**, « Être présent en ligne : culture et structure des réseaux sociaux d'Internet », Revue Idées économiques et sociales, 2012/3 (N° 169), p. 16-29.

14- **Bernard BRUN**, « Nature et impacts juridiques de la certification dans le commerce électronique sur Internet », pp. 01-81. Article disponible à partir de l'adresse: http://www.signelec.comcontentsearticlesarticle_bernard_brun_html, consultée le 25/02/2019.

15- **Bertrand QUÉLIN**, « Rapport sur les rapports - Développement du commerce électronique et économie d'internet. », Revue d'économie industrielle, vol 84, 2e trimestre 1998. pp. 105-115.

16- **Bertrand WARUSFEL**, « La protection des bases de données en question : un autre débat sur la propriété intellectuelle européenne », pp. 896- 906. Article disponible à partir de l'adresse: http://www2.droit.parisdescartes.frwarusfelarticlesbasesdonnees_warusfel04.pdf, consultée le 04/01/2019.

17- **Bounie DAVID**, « Quelques incidences bancaires et monétaires des systèmes de paiement électronique », Revue Économique, 2001/7 Vol. 52, pp. 313-330.

18- **Bojana SALOVIC, Etienne WERY, Thierry LÉONARD,** «Celui qui a une page Facebook est coresponsable du traitement des données visiteurs ». Article publié le 05/06/2018, sur le site: https://www.droit-technologie.org, consulté le 17/06/2018.

19- **……**,« Bouton "J'aime" de Facebook: voici le verdict final de la CJUE ». Article publié le 29/07/2019, sur le site: https://www.droit-technologie.org, consulté le 17/08/2019.

20- **Bruce SNELL**, « Piratage de drones : la menace plane », Rapport McAfee Labs- Prévisions 2017 en matière de menaces, Novembre 2016, pp. 40, 45. https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf, consulté le 13/12/2016.

21- **Bruno DURAND**, « L'épicerie en ligne. Les atouts des petits commerces indépendants », Revue des Sciences de gestion, 2005/4 (n°214-215), pp. 143-154.

22- **Benoît CRÉPIN**, « Vers un Internet quantique », article publié le 31/01/2019, sur le site : https://www.industrie-techno.com/, consulté le 02/02/2019.

23- **Christiaan BEEK**, « Déclin des logiciels de demande de rançon au 2e semestre 2017 », pp. 32-37, Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre 2016. Disponible sur le site : https://www.mcafee.com/fr, consulté le 27/01/2018.

24- **Christophe BOUDRY, Clémence AGOSTINI**, « Étude comparative des fonctionnalités des moteurs de recherche d'images sur Internet », Revue Documentaliste-sciences de l'information, 2004/2 (Vol. 41), pp. 96-105.

25- **Christophe COQUIS**, « NFC, QR Codes, iBeacon, RI : tout savoir sur les technologies sans contact », article publié le 29/09/2014 sur le site: https://www.fr.softonic.com/articles/nfc-qr-codes-ibeacon-ri-technologies-sans-contact, consulté le 25/02/2016.

26- **Christophe VERDURE**, « Les hébergeurs de sites web : victimes ou régulateurs de la société de l'information? », DCCR, n° 68/ 2005, pp. 31-52. Article disponible sur le site: https://www.droit-technologie.org, consulté le 08/01/2019.

27- **Claire FÉNÉRON PLISSON**, « La blockchain, un bouleversement économique, juridique voire sociétal », Revue I2D – Information, données & documents, 2017/3 (Volume 54), pp. 20-22.

28- **Clara WALTER**, « Le marketing sur Twitter : les bonnes pratiques », article publié le 6 avril 2017 sur le site: https://www.restoconnection.fr/le-marketing-sur-twitter-les-bonnes-pratiques/, consulté le 10/02/2017.

29- **Cyril FIÉVET**, « Bitcoin peut-il devenir la banque des pauvres? », article publié à partir de l'adresse: https://www.bitcoin.fr/bitcoin-peut-il-devenir-la-banque-des-pauvres.html, consultée le 03/09/2018.

30- **Cyril ROJINSKY**, « Les techniques contractuelles du commerce électronique », Revue Legicom, 2000/1, n° 21-22, pp. 105, 121.

31- **…….**, « Sens interdit – La responsabilité du créateur de lien hypertexte du fait du contenu illicite du site cible », pp. 01-11, article publié le 17 décembre 2002, sur le site : https://www.juriscom.net

32- **Daniel HURSTEL**, « Principes juridiques : la vente multiniveaux serait-elle remise en cause ? », Gazette du palais, n° 18, 19/ 1995, pp. 41- 45.

33- **David BOUNIE, Marc BOURREAU**, « Sécurité des paiements et développement du commerce électronique », Revue Économique, 2004/4 (Vol. 55), pp. 689-714.

34- **David DESCÔTEAUX**, « Quel cadre réglementaire pour Bitcoin? », pp. 01-04. Article disponible à partir de l'adresse: http://www.iedm.orgfilesnote0514_fr.pdf, consultée le 09/05/2016.

35- **David LEFÈVRE**, « 60 informations pour tout savoir sur le MLM », pp. 01-12. Article publié à partir de l'adresse: http://www.kalipub.commediasfiles60-informations-pour-tout-savoir-sur-le-mlm.pdf, consultée le 20/06/2016.

36- **Denis C. ETTIGHOFFER**, « L'économique numérique sera-t-elle sous domination américaine ? », Revue Géoéconomie, 2010/2 (n° 53), pp. 89-99.

37- **Didier CARRÉ**, « L'entreprise : nouveaux défis cyber », Revue Sécurité et stratégie 2014/4 (n°19), pp. 90-93.

38- **Didier GOBERT, Francis DERYCKERE, Paul CAMBIE**, « Le « spamming » en 24 questions & réponses », pp. 01-28. Article publié en Janvier 2005 sur le site: https://www.droit-technologie.org, consulté le 02/09/2018.

39- **Didier GOBERT**, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie », pp. 01-51. Article publié en février 2015, sur le site : https:// www.droit-technologie.org, consulté le 09/09/2016.

40- **Dmitry KOROLEV, Yuri GUBANOV, Oleg AFONIN**, « Comprendre RootKits : Utilisation de l'analyse de vidage de mémoire pour la détection des RootKits », article publié le 22 novembre 2013 à partir de l'adresse: https://articles.forensicfocus.com/2013/11/22/understanding-rootkits/, consultée le 10/11/2016.

41- **Dominique BOULLIER**, « Avec Internet, un monde commun…mais pluriel. », Questions internationales, n° 47- Janvier- février 2011, pp. 22-34.

42- **Dan CALZ**, « Un Internet quantique plus rapide et plus sûr serait possible », article publié le 11/02/2019 à 11h 52, sur le site : https://www.devlopper.com/actu/24883/, consulté le 13/02/2019.

43- **Emmanuel KESSOUS**, « Le commerce électronique et la continuité de la chaine logistique. De l'approvisionnement des sites à la livraison aux consommateurs », Revue Réseaux, 2001/2 n° 106, pp. 103-133.

44- **Etienne WÉRY**, « Le référencement sur internet : que dit la loi ? », pp. 01-24. Article publié le 03/09/2014 sur le site : https://www.ulys.net, consulté le 04/02/2017.

45- **……..**, « Comment rédiger en pratique un contrat de commerce électronique ? », pp. 01-39. Article publié le 16/10/2000 sur le site : https://www.droit-technologie.org, consulté le 12/09/2017.

46- **……..**, « Celui qui a une page Facebook est-il un « responsable de traitement » ? », Article publié le 13/11/2017, sur le site: https://www.droit-technologie.org, consulté le 18/02/2018.

47- **Fabrice HARROUET**, « Écoute du réseau et usurpation d'identité ("Les aventures de SNIFF et SPOOF...") », pp. 01-22. Article disponible à partir de l'adresse: http://www.enib.fr/~harrouet/, consultée le 20/12/2018.

48- **François OLLÉON et al.**, « Monter son projet de gestion de contenu », Revue Documentaliste-Sciences de l'Information, 2008/3 (Vol. 45), pp. 56-66.

49- **François-BERNARD HUYGHE,** « Des armes à la stratégie », Revue Internationale et Stratégique, 2012/3 (n° 87), pp. 53-64.

50- **Gabriel DABI-SCHWEBEL**, « L'importance des réseaux sociaux dans le marketing digital », article publié le 05 mai 2017 sur le site: https://www.1min30.com/developpement-web/limportance-des-reseaux-sociaux-dans-le-marketing-digital-119459, consulté le 05/06/2017.

51- **Gerald STUBER**, « Le bitcoin : une monnaie virtuelle sans émetteur central », Revue de la Banque du canada- printemps 2014, p. 16. https://www.revue-bdc-printemps14-fung.pdf

52- **Gilles PACHÉ**, « La logistique de distribution du commerce électronique : des défis économiques, managériaux et écologiques à l'horizon », Revue Gestion, 2002/5 (Vol. 27), pp. 39- 45.

53- **Girard GAUTIER**, « Monter une stratégie marketing de réseau », pp. 01-03. Article publié le 14/01/2017, à partir de l'adresse: http://www.netalya.comfrArticle2.aspCLE=173#, consultée le 10/09/2017.

54- **Grégoire LOISEAU**, « Nom de domaine et Internet : turbulence autour d'un nouveau signe distinctif », Recueil DALLOZ, n° 23/ 1999, pp. 245-250.

55- **Guillaume HARRY**, « Failles de sécurité des applications Web ». Article disponible sur le site: http://www.cnrs.fr, consulté le 18/08/2018.

56- **Hans KLEIN,** « ICANN et la gouvernance d'internet. La coordination technique comme levier d'une politique publique mondiale », Revue Les Cahiers du numérique, 2002/2 (Vol. 3), pp. 91-128.

57- **Harry HALPIN**, « La souveraineté numérique. L'aristocratie immatérielle du World Wide Web », Revue Multitudes, 2008/4 (N° 35), pp. 201-213.

58- **Hélie- SOLANGE GHERNAOUTI**, « Menaces, conflits dans le cyberespace et cyberpouvoir », Revue Sécurité et stratégie, 2011/3 (n°7), pp. 61- 67.

59- **Hélie- SOLANGE GHERNAOUTI, Christian AGHROUM**, « Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité », Revue Sécurité et stratégie, 2012/4 (n°11), pp. 74-83.

60- **Hubert BITAN**, « Le site de commerce électronique : approche technique et juridique », Gazette du Palais - 18/04/2000 - n° 109, pp. 01-16.

61- **Hubert de VAUPLANE**, « l'analyse juridique du Bitcoin », pp. 351- 360. Article publié à partir de l'adresse suivante: http://www.kramerlevin.comfilesPublication26eb1df1-847a-40f0-bad1-d839880ddd3PresentationPublicationAttachmentc8021100-5, consultée le 15/04/2016.

62- **Ivan VASSILEFF, Gérard HAAS**, « Délinquance numérique : L'attaque des STAD par les données », revue Legicom, 1996/2, n° 12, pp. 43-50.

63- **Jacques BERLEUR, Yves POULLET**, « Réguler Internet », Revue Études, 2002/11 (Tome 397), pp. 463-475.

64- **Jean LUC**, « Un distributeur de bitcoins à Paris ». Article publié le jeudi 15 mai 2014 à 0:14, à partir de l'adresse: https://bitcoin.fr/un-distributeur-de-bitcoins-a-paris/, consultée le 22/02/2016.

65- **Julien FLOER**, « Ponzi, la plus célèbre des arnaques », article publié le 28/12/2015, sur le site : http://richesse-et-finance.com/ponzi-la-plus-celebre-des-arnaques/, consulté le 13/03/2016.

66- **Jean-Christophe GALLARD**, « Sécurité et Réseaux : Partie « Réseaux »- architecture et solution de sécurité », pp.01-31, article disponible à partir de l'adresse: http://www. jgallard.free.fr/RSX112.pdf, consultée le 21/01/2016.

67- **Jean-Claude PAILLÈS, «** Les systèmes de paiement électronique sur internet », Revue Les Cahiers du numérique, 2003/1 - Vol. 4, pp. 45-69.

68- **Jean-François PILLOU**, « Prendre un nom de domaine », article disponible à partir de l'adresse : http://www.commentcamarche.net/ Prendre-un-nom-de-domaine.pdf, consultée le 12/06/2018.

69- **……, «** VPN - Réseaux Privés Virtuels (RPV) », pp. 01-04, article publié le 15/09/2015, sur le site: http://www.commentcamarche.net/vpn-reseaux-prives-virtuels-rpv-514-mddyo0.pdf, consulté le 23/01/2016.

70- **Jean-GUY DE RUFFRAY** et al., « Droit de l'information », Revue Documentaliste-Sciences de l'information, 2013/4 (Vol. 50), pp. 16-21.

71- **Jean-MARC MANACH**, « En attendant la « Cryptocalypse » », Revue Vacarme, 2014/4 (N° 69), pp. 100- 109.

72- **Jeannette KOCSIS,** « Médias sociaux: 4 stratégies de marketing social essentielles (des tactiques personnalisées pour Facebook, Twitter, Google+ et LinkedIn) », article publié le 1er mai 2012 sur le site: https://www.targetmarketingmag.com/article/4-social-marketing-strategies-facebook-twitter-google-linkedin/all/, consulté le 07/O6/2016.

73- **Jean-Paul DELAHAYE**, « Le Bitcoin, première crypto-monnaie », Bulletin de la société informatique de France, n° 4, octobre 2014, pp. 67–104.

74- **Jean-Paul TRIAILLE**, « Le Contrat de création d'un site Web », pp. 01-16. Article publié le 08/03/2001 sur: https://www.droit-technologie.org, consulté le 15/04/2017.
75- **Jérôme DENIS**, « L'informatique et sa sécurité. Le souci de la fragilité technique », Revue Réseaux, 2012/1, n° 171, pp. 161-187.
76- **Joaquim ROBBE**, « Notre Guide complet sur le marketing des médias sociaux », article publié le 16 janvier 2019(Mis à jour le 24 janv. 2019 à 16:00) sur le site : https://www.e-marketing.fr/Thematique/social-media-1096/breve/notre-guide-complet-sur-le-marketing-des-medias-sociaux-329928.htm#, consulté le 20/02/2019.
77- **Jonathan BROSSARD**, « Sécurité : 15 ans d'échec », Revue Sécurité et stratégie, 2012/4 (11), pp. 6-14.
78- **Josef DREXL**, « Le commerce électronique et la protection des consommateurs », Revue Internationale de droit économique, 2002/2 (t. XVI), pp. 405-444.
79- **Julien PASTEUR**, « La faille et l'exploit : l'activisme informatique », Revue Cités, 2004/1 (n° 17), pp. 55-72.
80- **Karl WASS**, « Treillis et cravate - sécurité, le point de vue des managers », Revue Vacarme, 1999/1 (n° 7), pp. 20-22.
81- **Kevin MELLET**, « Marketing en ligne », Revue Communications, 2011/1 (n° 88), pp. 103-111.
82- **Kate KOCHETKOVA**, « Des drones armés de pistolets, de tronçonneuses et de vulnérabilités… », article publié le 28/04/2016, sur le site : https://www.kaspersky.fr/blog/haking-armed-drones/5590/, consulté le 03/05/2016.
83- **Laetitia CHAIX**, « Le paiement mobile : modèles économiques et régulation financière », Revue d'économie financière, 2013/4 (N° 112), pp. 277-298.
84- **Laurent BLOCH**, « La maîtrise d'internet : des enjeux politiques économiques et culturels », Questions internationales, n° 47- janvier- février, 2011, pp. 08- 21.
85- **……..**,« surveillance américaine sur l'Internet ». Article disponible à partir de l'adresse: http://www.diploweb.com/Surveillance-americaine-sur-l.html, consultée le 02/10/2017.
86- **Lionel THOUMYRE**, « L'échange des consentements dans le commerce électronique », pp. 01-48. Lex Electronica, vol. 05, n°1, Printemps 1999.
87- **……**, « De la responsabilité arachnéenne sur Internet : Quelle issue pour les tisseurs de liens en France », pp. 01-12. Lex Electronica, vol. 10, n°1, Hiver 2005.
88- **Louise MARTEL et René ST-GERMAIN**, « la Certification de Conformité des Sites Web », Revue Gestion, 2002/5 Vol. 27, pp. 91, 92.

89- ……., « Les sceaux de certification des sites web : un outil de confiance, outil de confusion », pp. 01- 15. Article disponible à partir de l'adresse: https://halshs.archives-ouvertes.fr/halshs-00584496, consultée le 20/02/2019.

90- Marc LACOURSIÈRE et Édith VÉZINA, « La sécurité des opérations bancaires par Internet », Revue juridique Thémis, R.J.T, vol 41 n°1/2007, pp 90-156.

91- Marc PUECH, « Jurisprudence du parrainage en matière de vente multiniveaux », Gazette du palais, n° 18, 19/ 1995, pp. 46- 49.

92- Marie-Christine MONNOYER-LONGÉ, Catherine LAPASSOUSE-MADRID, « Intégrer les sites web dans les stratégies. Concept et modèle », Revue Française de gestion, 2007/4 (n° 173), pp. 145-155.

93- Maurizio DE ARCANGELIS, « La responsabilité des (fournisseurs d'hébergement) - Étude de droit comparé entre la France et l'Italie », pp. 16, 17. Article publié le 07 novembre 2001 sur le site: http://www.droit-technologie.org, consulté le 06/01/2019.

94- Maxime WACK et AL, «certification et archivage légal de dossiers numériques», Revue Document numérique, vol 6, n°1/2002, pp. 152, 153.

95- Margaret ROUSE, « Sécurité de l'information (infosécurité, infosec) », article publié sur le site : https://www.lemagit.fr, consulté le 02/01/2016.

96- Michel AGLIETTA et Laurence SCIALOM, « Les défis de la monnaie électronique pour les banques centrales », pp. 01-29. Article publié à partir de l'adresse suivante: http://www.sceco.univ-poitiers.fr/franc-euro/articles/MAgliettaLScialom.PDF, consultée le 14/04/2018.

97- Moustapha MBENGUE, « Création et gestion de sites web et de portails documentaires », pp. 01-88. Article disponible à partir de l'adresse: http://docplayer.fr/7997805-Creation-et-gestion-de-sites-web-et-de-portails-documentaires.html, consultée le 13/02/2016.

98- Murielle Cahen, « Traitement civil et pénal du bitcoin », pp. 01-03, article juridique publié le 17/04/2015, à partir de l'adresse: http://www.legavox.frblogmurielle-cahentraitement-civil-penal-bitcoin-17601.pdf, consultée le 03/02/2016.

99- Mustapha BENJADA, « PKI (Public Key Infrastructure) », pp. 01-25. Article publié le 14 mars 2001, à partir de l'adresse: https://www.securiteinfo.com/cryptographie/pki.shtml, consultée le 07/09/2017.

100- Myriam QUÉMÉNER, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Revue Sécurité et stratégie, 2011/1 (5), pp. 56-67.

101- Myriam ROUSSILLE, « Le Bitcoin : objet juridique non identifié », Revue Banque & Droit, nº 159 janvier- février 2015, pp. 27- 31.

102- Nadia NOUALI-TABOUDJEMAT, « Les firewalls comme solution aux problèmes de sécurité », pp. 01-12. Article disponible sur le site: http://www.webreview.dz, consulté le 05/12/2018.

103- Nicolas LEFRANC, « Vente en réseaux : le markéting multiniveaux », Gazette du palais, n° 18, 19/ 1995, pp. 38- 40.

***104-* Nicolas MOYROUD**, « Introduction au langage PHP », pp.01-46. Article disponible sur le site: http://www.ird.fr/informatique-scientifique/.../php/cours_introduction_php.pdf, consulté le 10/02/2018.

105- Nicolas TILLI, « La protection des données à caractère personnel », Revue Documentaliste-Sciences de l'Information, 2013/3 (Vol. 50), pp. 62- 69.

106- Olivier GOFFARD, « Risques et responsabilités en cas de transfert électronique de fonds sur Internet », Revue de Droit commercial Belge(R.D.C)- Larcier, n°1, Janvier 2005, pp. 04-19.

107- Olivier GOURBESVILLE, « Faut-il avoir peur d'Internet ? », Revue Pour, 2007/3 (n° 195), pp. 21- 26.

108- Olivier HASSID, « Édito », Revue Sécurité et stratégie, 2012/4 (n°11), pp.01-02.

109- Olivier KEMPF, « Cyberstratégie à la française », Revue Internationale et Stratégique, 2012/3 (n° 87), pp. 121-129.

110- Patrice JOURDAIN, « La Distinction des Responsabilités Délictuelle et Contractuelle : État du Droit Français ». Article disponible sur le site: http://www.grerca.univ-rennes1.fr/, consulté le 14/02/2019.

111- Philippe BARBET, Isabelle LIOTARD, « Propriété intellectuelle et régulation des marchés des biens informationnels : le cas du nommage sur l'Internet », Revue d'Économie industrielle, 129-130 | 1er et 2e trimestres 2010, pp. 119-138.

112- Pierre MOUNIER, « L'ICANN : Internet à l'épreuve de la démocratie », Revue Mouvements, 2001/5 n°18, pp. 81- 86.

113- Pierre STORRER, « Droit des moyens et services de paiement : Les monnaies virtuelles dans tous leurs états », Revue Banque, n° 775- septembre 2014, pp. 86-89.

114- Pierre-HUGUES VALLÉE et Ejan MACKAAY, « La confiance, sa nature et son rôle dans le commerce électronique », Revue Lex Electronica, vol. 11 n° 2 (Automne / Fall 2006), pp. 1-45.

115- Riccardo SANSONETTI, « Les risques de la monnaie électronique », Revue L'Économie politique, 2002/2 (n° 14), p. 82-95

116- ....., « Commerce électronique par téléphonie mobile (m-commerce): un cadre juridique mal défini », Recueil Dalloz, n° 41, 2004, pp. 02-11.

117- ....., « Le bitcoin: opportunités et risques d'une monnaie virtuelle ». Article publié le 01/09/2014 à partir de l'adresse: http://dievolkswirtschaft.ch/fr/2014/09/sansonetti-4/, consultée le 12/02/2016.

118- Rodrigo NIETO GÓMEZ, « Cybergéopolitique : de l'utilité des cybermenaces », Revue Hérodote, 2014/1 (n° 152-153), pp. 98-122.

119- Romain MEGEMONT, « Paiement mobile sur smartphone : présentation, fonctionnement et sécurité », article publié le 28-04-2018, sur le site: https://www.frandroid.com/android/application/500871_Paiement-mobile-sur-smartphone-présentation-fonctionnement-sécurité, consulté le 01/05/2018.

120- Sylvain CROUZET, « Le BIOS - flashage et procédures de récupération », pp. 01-21. Article disponible à partir de l'adresse: http://crouzet.sylvain.free.fr/files/flashbios.pdf, consultée le 12/12/2017.

121- Sylvain MIGNOT, « Le Bitcoin : nature et fonctionnement », Revue Banque & Droit, nº 159 janvier- février 2015, pp. 10-13.

122- Sylvie HÉROUX, Jean-François HENRI, « Reporting sur le Web : optimisation de la gestion de contenu des sites web », Revue des Sciences de gestion, 2011/6 n° 252, pp.59-68.

123- Thibault VERBIEST, « Entre bonnes et mauvaises références. A propos des outils de recherche sur internet », pp. 2-23. Article publié le 31/05/2000 sur le site: https://www:droit-tchnologie.org, consulté le 12/03/2018.

124- Thibault VERBIEST et Etienne WÉRY, « La responsabilité des fournisseurs de services Internet : derniers développements jurisprudentiels », Journal des tribunaux, 17 février 2001, 120e année - N° 6000, pp. 165-172. Disponible sur le site: http://www.droittechnologie.org, consulté le 11/01/2019.

125- .....,« La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés », pp. 01-16. Article publié le 10/09/2002 sur le site: https://www.droit-technologie.org, consulté le 05/01/2019.

126- Thibault VERBIEST, Maxime LE BORNE, « Le fonds de commerce virtuel : une réalité juridique? », Journal des tribunaux, 23 février 2002, 121e année- n° 6044, pp. 145-150. Disponible sur le site: https://www.droit-technologie.org, consulté le 04/05/2016.

127- Thierry DISSAUX, « Paiements, monnaie, banque électroniques : quelle évolution pour la banque ? », Revue d'Économie financière, n°53/1999, pp.113-132.

128- Thomas BEAUVISAGE et al., « Notes et avis des consommateurs sur le web. Les marchés à l'épreuve de l'évaluation profane », Revue Réseaux, 2013/1 n° 177, pp. 131-161.

129- Vincent WEAFER, « Partage de cyberveille sur les menaces : le danger de l'inconnu », pp. 08-15, Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre 2016. Disponible sur le site : https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf. , consulté le 29/01/2018.

130- Yves RANDOUX, « La sécurisation du paiement sur les réseaux ouverts », Revue d'économie financière, n°53, 1999, pp. 39- 63.

131- Yashashree GUND, Ravikant TIWARI et Christiaan BEEK, « Mirai, le botnet de l'Internet des objets », pp. 16-34. Rapport McAfee Labs, sur le paysage des menaces, avril 2017, disponible sur le site : https://www.mcafee.com/fr, consulté le 29/01/2018.

132- Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », Journal des Tribunaux, 10 novembre 2018, 137e année - N° 6748, pp. 801- 819.

133- Zygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON et R. B. J. (ROB) WALKER, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », Revue Cultures & Conflits, 2015/02 n° 98, pp. 133- 166.

Ⅳ- Textes Juridiques:

A- Conventions et Traités :

1- Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, du 9 septembre 1886, complétée à PARIS le 4 mai 1896, révisée à BERLIN le 13 novembre 1908, complétée à BERNE le 20 mars 1914 et révisée à ROME le 2 juin 1928, à BRUXELLES le 26 juin 1948, à STOCKHOLM le 14 juillet 1967 et à PARIS le 24 juillet 1971 et modifiée le 28 septembre 1979. http://www.wipo.int

2- Traité sur la propriété intellectuelle en matière de circuits intégrés, adopté à Washington le 26 mai 1989. http://www.wipo.int

3- Traité de coopération en matière de brevets (PCT) fait à Washington le 19 juin 1970, modifié le 28 septembre 1979, le 3 février 1984 et le 3 octobre 2001. http://www.wipo.int

4- Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce(ADPIC)-Annexe 1C, signé à Marrakech(Maroc) le 15 avril 1994(l'Accord de Marrakech instituant l'Organisation mondiale de commerce(OMC)). https://www.wto.org
5- Traité de l'OMPI sur le droit d'auteur (WCT), (adopté à Genève le 20 décembre 1996). http://www.wipo.int

B - Droit de l'union européenne :

I- Règlements :

1- Règlement(CE) n° 733/2002 du parlement européen et du conseil du 22 avril 2002 concernant la mise en œuvre du domaine de premier niveau .eu. JOCE, n° L113/1 du 30/04/2002.
2- Règlement (CE) N° 874/2004 de la commission du 28 avril 2004, établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier niveau .eu et les principes applicables en matière d'enregistrement, JOUE, n° L 162/40 du 30/4/2004.
3- Règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) et abrogeant la directive 1999/93/CE. JOUE, n° L 257/73 du 28/08/2014.
4- Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). JOUE, n° L 119/1 du 4/5/2016.

II - Directives:

1- Directive 87/54/CEE du Conseil du 16 décembre 1986 concernant la protection juridique des topographies de produits semi-conducteurs, JOUE, n° L 024 du 27/01/1987.
2- Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données, JOUE n° L 077 du 27/03/1996.
3- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché

intérieur («directive sur le commerce électronique»), JOUE n° L 178 du 17/07/2000.

4- Directive 2005/29/CE du parlement européen et du conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («Directive sur les pratiques commerciales déloyales»), J.O.U.E, L 149/22 du 11/6/2005.

5- Directive 2006/114/CE du parlement européen et du conseil du 12 décembre 2006 en matière de publicité trompeuse et de publicité comparative (version codifiée), J.O.U.E, L 376/21 du 27/12/2006.

6- Directive 2007/64/CE du parlement européen et du conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, JOUE, n° L 319/1 du 5/12/2007.

7- Directive 2009/24/CE du parlement européen et du conseil du 23 avril 2009, concernant la protection juridique des programmes d'ordinateur, JOUE, n° L 111/16 du 05/05/2009.

8- Directive 2009/110/CE du parlement européen et du conseil du 16 septembre 2009, concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE, JOUE, n° L 267 du 10/10/2009.

9- Directive(UE) 2011/83/UE du parlement européen et du conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577, JOUE n° L 304/64 du 22/11/2011.

10- Directive(UE) 2015/2366 du parlement européen et du conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, JOUE, n° L 337/35 du 23/12/2015. - Règlement (CE) n° 460/2004 du parlement européen et du conseil du 10 mars 2004 instituant l'agence européenne chargée de la sécurité des réseaux et de l'information, JOUE, n° L 77/1 du 13/3/2004.

Ⅲ- **Proposition et Résolution** :

1- Proposition de directive du Parlement européen et du Conseil concernant la brevetabilité des inventions mises en œuvre par ordinateur, JOUE, n° C 151 E/129, du 25/6/2002. (Présentée par la Commission le 20 février 2002).
2- Résolution législative du Parlement européen relative à la position commune du Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil concernant la brevetabilité des inventions mises en œuvre par ordinateur (11979/1/2004 - C6-0058/2005 - 2002/0047(COD)), JOUE, n° C 157 E/265, du 6/7/2006.

C - **Droit des États Unis d'Amérique(USA)**:

1- Public law 95-511, Foreign Intelligence Surveillance Act(FISA) of Oct. 25, 1978. https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf
2- Public law 107–56, Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA patriot act) act of 2001. https://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf
3- Public law 110–55, Protect America Act of Aug 5, 2007. https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf
4- FISA Amendments Act of Jul 9, 2008(Passed Congress/Enrolled Bill). https://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf
5- Public law 114–23, Uniting and strengthening America by fulfilling rights and ensuring effective discipline over monitoring act of June 2, 2015, or the ''USA Freedom Act of 2015''. https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf

D - **Droit Suisse**:

1- Loi fédérale complétant le Code civil suisse (Livre cinquième: Droit des obligations) du 30 mars 1911, RS 220(État le 1er novembre 2019).
2- Loi fédérale contre la concurrence déloyale(LCD) du 19 décembre 1986, RS 241 (État le 1er juillet 2016).
3- Loi fédérale sur la protection des données (LPD) du 19 juin 1992, RS 235.1 (État le 1er mars 2019).
4- Loi sur la signature électronique, SCSE du 18 mars 2016, RS 943.03 (État le 1er janvier 2017).
5- Ordonnance sur la signature électronique, OSCSE du 23 novembre 2016, RS 943.032(État le 1er janvier 2017).
6- Ordonnance sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité,

d'enregistrement et d'homologation (Ordonnance sur l'accréditation et la désignation, OAccD) du 17 juin 1996, RS 946.512 (État le 20 avril 2016).
7- Code civil suisse du 10 décembre 1907, RS 210 (État le 1er janvier 2019).
8- Code pénal suisse du 21 décembre 1937, RS 311.0 (État le 1er novembre 2019).

E - <u>Droit Français</u> :

1- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O.R.F, n° 143 du 22 juin 2004.
2- Loi n° 2013-100 du 28 janvier 2013 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière économique et financière, JORF n°0024 du 29 janvier 2013.
3- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, J.O.R.F, n° 0141 du 21 juin 2018.
4- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, J.O.R.F, n°0288 du 13 décembre 2018.
5- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JORF, n° 0156 du 8 juillet 2009.
6- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, J.O.R.F n° 0229 du 30 septembre 2017.
7- Code de la consommation - Dernière modification le 02 février 2019 - Document généré le 13 février 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance/gouve.fr
8- Code civil - Dernière modification le 23 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance/gouve.fr
9- Code de la propriété intellectuelle - Dernière modification le 24 octobre 2019 - Document généré le 14 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance/gouve.fr
10- Code monétaire et financier - Dernière modification le 16 novembre 2019 - Document généré le 15 novembre 2019 Copyright (C) 2007-2019 Legifrance. https://www.legifrance/gouve.fr

F - Droit Belge :

1- Loi du 21 décembre 2009 relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement, MB n° 2199 du 19/01/2009.
2- Loi du 27 novembre 2012 modifiant la loi du 21 décembre 2009, relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement et d'autres législations dans la mesure où elles sont relatives au statut des établissements de paiement et des établissements de monnaie électronique et des associations de crédit du réseau du Crédit professionnel, MB n° 76567 du 30/11/2012.
3- Loi du 21 Juillet 2016, mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique, MB n° 67478, du 28/09/2016. (Loi « eIDAS » et Archivage électronique.)

Ⅳ- Rapports, Position, Fiches:

1- Avertissement de l'Autorité bancaire européenne(ABE) à l'attention des consommateurs concernant les monnaies virtuelles, du 12 décembre 2013, pp. 01-04. https://www.eba.europa.eu...EBA_2013_01030000_F....pdf ou http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014 08+Opinion+on+Virtual+Currencies.pdf
2- Fiche d'information(Suisse) de l'autorité fédérale de surveillance des marchés financiers (FINMA) sur : le «Bitcoins», du 25 juin 2014, pp. 01-02. https://www.finma.chfrdocumentationpublications-finmafiches-d-information/
3- Fiche d'information(Suisse) de l'autorité fédérale de surveillance des marchés financiers (FINMA) sur : « Lutte contre le blanchiment d'argent : les intermédiaires financiers doivent respecter les obligations de diligence », du 01 juillet 2016, pp. 01-02. https://www.finma.chfrdocumentationpublications-finmafiches-d-information/
4- Focus de la Banque de France, sur l'émergence du bitcoin et autres crypto-actifs: enjeux, risques et perspectives, n° 16 - 5 mars 2018, pp. 01-06. https://www.publications.banque-France.fr/liste-chronologique/focus/

5- Focus de la banque de France sur Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin, n° 10 du 05/12/2013, pp. 01-06. http://www.sibfi.banque-france.fruploadstx_bdfgrandesdatesFocus-10-stabilite-financiere.pdf

6- Position du 29 Janvier 2014 de l'Autorité de contrôle prudentiel et de régulation (ACPR), relative aux opérations sur Bitcoins en France, p.01. http://www.sacpr.banque-rance.fr/fileadminuser_uploadacppublicationsregistre-officiel201401-Position-2014-P-01-de-l-ACPR.pdf

7- Rapport d´information (Sénat Français) fait au nom de la commission des finances(1) sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles (Par MM. Philippe MARINI et François MARC, Sénateurs), du 23 juillet 2014, pp. 01-143. http://www.senat.frrapr13-767r13-7671.pdf

8- Rapport de groupe de travail(TracFin)- Juin 2014 sur l'encadrement des monnaies virtuelles (Recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment), pp. pp. 01-10. http://www.economie.gouv.fr/filesrapport_monnaiesvirtuelles_web.pdf

9- Rapport du Conseil fédéral(Suisse) sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, pp. 01-32. https://www.news.admin.chNSBSubscribermessageattachments35353.pdf

V-**Jurisprudence**:

A- **Union Européenne** :

1- Arrêt de la C.J.U.E(4ème ch.), du 13/02/2014, Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd c/ Retriever Sverige AB, (Affaire C-466/12). https://www.curia.europa.eu/juris/document

2- Arrêt de la C.J.U.E (5ème ch.), 22 octobre 2015, Skatteverket c/ David Hedqvist, (affaire C-264/14). https://www.curia.europa.eu/document/

3- Arrêt de la C.J.U.E (2ème ch.), du 08/09/2016, GS Media BV c/ Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker, (Affaire C-160/15). https://www.curia.europa.eu/juris/document/

4- Arrêt de la C.J.U.E (Grande ch.), 5 juin 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, (affaire C-210/16). http://curia.europa.eu/juris/document/

5- Arrêt de la C.J.U.E (2ème ch.), 29 juillet 2019, Fashion ID GmbH & Co. KG contre Verbraucherzentrale NRW, (affaire C-40/17). http://curia.europa.eu/juris/document/

B- **Belgique** :

1- Tribunal de Première Instance d'Anvers (référé), 21 déc. 1999, I.F.P.I. Belgium c/ Beckers Werner Guido, (R.G. 99/594/C). Disponible sur le site: http://www.droittechnologie.org, [rubrique jurisprudence].
2- Tribunal de Première Instance de Bruxelles, 05/09/2006, S.A.R.L COPIEPRESS c/ S Google Inc. Disponible sur le site : https://www.juriscom.net

C- France:

1- Cour de cassation, 1ère ch., civile, du 31 octobre 2012, Groupe M6 c/ Société SBDS, Arrêt n° 11-20480. https://www.legifrance.gouve.fr et https://www.doctrine.fr
2- CA de Paris, 4ème ch, 18 octobre 2000, Virgin interactive Entertainment Ltd et Virgin interactive Entertainment Sarl c/ France Télécom et BDDP-TBWA. https://www.legifrance.gouve.fr et https://www.doctrine.fr
3- CA de Paris, 4ème ch, 19 septembre 2001, NRJ et Jean-Paul B. c/ SA Europe 2 Communication. https://www.legalis.net et https://www.doctrine.fr
4- CA de Douai, 1ère ch, 09 septembre 2002, Michel P, Société Codina c/ Association le Commerce du bois. https://www.legifrance.gouve.fr et https://www.doctrine.fr
5- CA d'Aix-en-Provence, 5ème ch, 10 mars 2004, A. Emmanuel c/ S.E.V., SA INFOGRAMMES EUROPE, SA TAKE TWO, et autres, Arrêt n° 04/192. Disponible sur les sites : https://www.legalis.net et https://www.doctrine.fr
6- CA de Paris, 1er ch., sect. C, 17 juin 2004, Michel Le P., L'association Internationale des concours de beauté pour les Pays francophones (Miss francophonie) c/ La société Miss France, l'association Comite Miss France, Miss Europe, Miss Univers.https://www.legifrance.gouve.fr et https://www.doctrine.fr
7- CA de Paris, 25 mai 2005, S.A. OGF, son Président du Conseil d'Administration et Directeur Général c/ S.A. d'économie mixte des pompes funèbres de la ville de Paris-services funéraires de Paris. https://www.legifrance.gouve.fr et https://www.doctrine.fr
8- CA Paris, 14ème ch, 29/11/2009, Jean-Yves Lafesse c/ My Space. https://www.juriscom.net
9- TGI Le Mans, 29 juin 1999, SARL Microcaz c/ SARL Oceanet. https://www.legifrance.gouve.fr et https://www.juriscom.net/txt/jurisfr/
10- TGI de Saint-Étienne, 3ème ch, 6 décembre 1999, SACEM/SDRM et S.C.P.P. et Stuffed Monkey et S Sony Music et S Island et S Warner et X Recording Corporation, c/ M. V.V R et M. F. B, n° 99007491. https://www.doctrine.fr et https://www.legifrance.gouve.fr
11- TGI d'Épinal, 24 octobre 2000, S.C.P.P c/ M. C S, n° 00006350. https://www.doctrine.fr et https://www.legifrance.gouve.fr
12- TGI Paris, ord. réf., 31 juillet 2000, Bertrand Delanoé c/ Alta Vista Company, Kohiba Multimédia, Kohiba Productions, Objectif Net. https://www.juriscom.net

13- TGI Paris, 3ème ch, 3ème sect, 09 juillet 2002, SA Peugeot Motocycles c/ M. Guy c/ SA société Sherlocom. https://www.legifrance.gouve.fr et https://www.juriscom.net/txt/jurisfr/

14- TGI de Paris, 3ème ch, 1ère sect, 5 septembre 2001, SA Cadremploi c/ SA Keljob et Sté Colt Télécommunications France. https://www.juriscom.net/txt/jurisfr/

15- T.com de Nanterre, Ordonnance de référé, du 8 novembre 2000, Sarl Stepstone France c/ Sarl Ofir France. https://www.legalis.net et https://www.doctrine.fr

16- T. Com. Paris, réf., 26 décembre 2000, SNC Havas Numérique et Sté Cadres On Line c/ SA Keljob. https://www.juriscom.net/txt/jurisfr/

17- TGI Paris, 3ème ch, 2ème sect, 19/10/2007, Google c/ Zading Productions. https://www.juriscom.net

18- TGI Nanterre, réf, 28/02/2008, Olivier D. c/ Éric D. https://www.juriscom.net

19- TGI Paris, réf, 28/02/2008, Olivier D. c/ Sté Ad Soft Com. https://www.juriscom.net

20- TGI Paris, 4ème ch, 2ème sect. A, 06/05/2009, Dailmotion c/ Nord Ouest Production et A. https://www.juriscom.net

21- TGI Paris, 3ème ch, 3ème sect, 24/06/2009, Jean-Yves Lafesse et A. c/ Google et A. https://www.juriscom.net

22- TGI Paris, réf, 07/01/2009, Jean-Yeves Lafesse et A. c/ Youtube Inc. https://www.juriscom.net

23- TGI Paris, 3ème ch, 1ère sect, 22/09/2009, Adami, Omar, Fred et A. c/ Sté Youtube. https://www.juriscom.net

D- Grande-Bretagne :

- hetland Times Ltd v. Dr. Jonathan Wills, Court of Session: Outer House, (1996) Outer House Cases, 24 oct.1996. Disponible sur les sites: https://www.lectlaw.com/files/elw10.htm ou http://www.netlitigation.com/netligation/cases/shetland.htm

E- États Unis d'Amérique(USA) :

- United States of America v. Ross William ULBRICHT, United States District Court Southern District of the New York. Jul 09, 2014. Disponible à partir de l'adresse: https://fr.scribd.com/document/233234104/Forrest-Denial-of-Defense-Motion-in-Silk-Road-Case

VI- Séminaires:

1- **Ahmed BERBAR**, « Certification Électronique en Algérie Situation et Perspectives », pp. 01-30, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, Alger au niveau de l'hôtel Hilton. https://www.arpce.dz

2- **Manel ABDELKADER**, « La Certification Électronique en Tunisie : Expérience et Défis », pp.01-29, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, Alger au niveau de l'hôtel Hilton. https://www.arpce.dz
3- **Mahdi BOUZOUBA**, « Certification électronique et E-Services », pp. 01-19. (SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, au Cercle National de l'Armée, à Alger. https://www.arpce.dz
4- **Nejla BELOUIZDAD**, « La certification électronique appliquée au réseau monétique interbancaire (RMI) », pp. 01-33. (SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, Alger au Cercle National de l'Armée. https://www.arpce.dz
5- **Tarik CHALLALI**, « Solutions d'accès sécurisées pour opérer une Market Place Saas multitenante », pp. 01-30. (SICE' 2011 ARPCE), les 28, 29 et 30 juin 2011, au Cercle National de l'Armée, à Alger. https://www.arpce.dz
6- **Yassine CHALLAL**, « ICP/PKI: Infrastructures à Clés Publiques (Aspects Techniques et organisationnels) », pp. 01- 32, (SICE' 2009 ARPCE), les 08 et 09 décembre 2009, Alger au niveau de l'hôtel Hilton. https://www.arpce.dz

Ⅶ- Articles de presse:

1- **Adeline RAYNAL**, « Le premier distributeur automatique de bitcoins débarque au Canada », Article de journal La Tribune, publié le 29/10/2013 à 14:29 sur le site: http://www.latribune.frentreprises-financebanques-finance2013.10.29/, consulté le 14/02/2016.
2- **Adrien SCHWYTER**, « Le premier distributeur de Bitcoins arrive à Paris », article de journal Les Echos, publié le 15/05/14 à 17H40 sur le site: http://www.lesechos.fr/15/05/2014/, consulté le 17/02/2016.
3- **Arthur MILLERAND**, « Le Bitcoin peut servir à réaliser du blanchiment selon la justice américaine », article publié sur droitdupartage.com, le 20 Août 2014 à 20 H 07 Min. https://droitdupartage.com/2014/08/20/le-bitcoin-peut-servir-a-realiser-du-blanchiment/, consulté le 06/08/2016.
4- **Anne CONFOLANT**, « Yahoo France prépare un vaste plan de licenciements », article de journal ITespresso.fr, publié le 21 mars 2016 sur le site: http://www.itespresso.fr/yahoo-france-prepare-vaste -plan-licenciements-124456.html, consulté le 05/01/2017.
5- **Antoine CROCHET-DAMAIS**, « Facebook at Work se lance, et devient Workplace by Facebook », article de Journal Du Net, publié le 13 octobre 2016 sur le site: http://www.journaldunet.com/solutions/reseau-social-d-entreprise/1186206-facebook-at-work-lance-et-devientworkplace-by-facebook-6/, consulté le 18/11/2016.
6- **Benjamin GOURDET**, « Facebook vaut-il 104 milliards de dollars ? », article publié le 18 mai 2012 sur le site: http://www.01net.com/editorial/566339/facebook-vaut-il-104-milliards-de-dollars/),sur 01net.com, consulté le 14/11/2016.

7- **Benjamin FERRAN**, « Israël et les États-Unis accusés d'avoir créée le virus Flame », Article de journal Le Figaro, publié le 20/06/2012 à 16:07 sur le site: http://www.lefigaro.fr/secteur/high-tech/2012/06/20/, consulté le 03/01/2016.

8- **…..……**, « Yahoo ! confirme le piratage de 500 millions de comptes », article de journal Le Figaro, publié le 22/09/2016 à 10 h 35 sur le site : http://www.lefigaro.fr/secteur/high-tech/2016/09/22/, consulté le 09/10/2016.

9- **Benjamin POLLE**, « E-commerce : Jumia double son chiffre d'affaires en 2015 mais reste dans le rouge », article publié sur Jeune Afrique.com, le 19 avril 2016, sur le site: http://www.jeuneafrique.com/319093/economie/e-commerce-jumia-double-chiffre-daffaires-2015-reste-rouge/, consulté le 04/05/2017.

10- **Damien LELOUP** et **Martin UNTERSINGER**, « Piratage de TV5 Monde : l'enquête s'oriente vers la piste russe », article de journal Le Monde, publié le 09/06/2015 à 18h43 sur le site: http://www.lemonde.fr/pixels/article/2015/06/09/, consulté le 02/10/2016.

11- **Dave TAYLOR**, « Pour quoi Linux est meilleur que Windows ou macOS pour la sécurité », article publié le 19/02/2018 sur le site : https://www.global-informatique-securite.com/2018/02/19/, consulté le 02/03/2018.

12- **Florian REYNAUD**, « Plus d'un milliard de comptes d'utilisateurs Yahoo ! ont été piratés », article de journal Le Monde, publié le 14/12/2016 à 23h23 sur le site : http://www.lemonde.fr/pixels/article/2016/12/14/, consulté le 17/12/2016.

13- **Fabien SOYEZ**, « 83 millions de comptes Facebook sont faux », article de journal Le Figaro, publié le 03/08/2012 sur le site: http://www.lefigaro.fr/societes/2012/08/03/20005-20120803ARTFIG00397-83-millions-de-comptesfacebook-sont-faux.php, consulté le 21/11/2016.

14- **Gilles PARIS**, « Le parti démocrate voit la main de la russie derrière la publication d'e-mails par Wikileaks », article de journal Le Monde, publié le 25/07/2016 à 18h34 sur le site: http://www.lemonde.fr/elections-americaines/article/2016/07/25/, consulté le 28/08/2016.

15- **Guillaume BONVOISIN**, « Faille Krack Wi-Fi : 5 mesures à prendre pour se protéger du piratage », article de journal CNETFrance, publié le 17/10/2017 sur le site: http://www.cnetfrance.fr/news/wifi-mesures-securité-piratage-39858764.htm, consulté le 25/10/2017.

16- **Johann BRETON**, « Yahoo! se paie Vizify, les Numériques », article publié le 6 mars 2014 sur le site: http://www.lesnumeriques.com/yahoo-se-paie-vizify-n33502.html, consulté le 02/10/2016.

17- **Jean-Michel NORMAND**, « Premiers clients pour les drones d'Amazon et de La Poste », article de journal Le Monde, publié le 15.12.2016 à 15h22, sur le site : http://www.lemonde.frla-foire-du-dronearticle20161215premiers-clients-pour-les-drones-d-amazon-et-de-la-poste_5049503_5037916.html, consulté le 04/02/2017.

18- **Luc LENOIR**, « Cryptomonnaie : Le petro vénézuélien en vente », article de journal Le Figaro, publié le 20/02/2018, à 07 :19 sur le site: http://www.lefigaro.fr/flash-econ/2018/02/20/97002-20180220FILWWW00034-cryptomonnaie-le-petro-vénézuélien-en-vente.php, consulté le 13/02/2018.

19- **Louis ADAM**, « Le FBI lance l'offensive contre le malware Game over Zeus », article publié le 04 juin 2014 sur le site : http://www.zdnet.fr/actualités/ Le-FBI-lance-l-offensive-contre-le-malware-Gameover-Zeus -39801981.htm, consulté le 09/09/2017.

20- **Laure BELOT**, « Quatorze start-up qui font bouger l'Afrique », article de journal Le Monde, publié le 03/03/2015 sur le site: http://www.lemonde.fr/afrique/article/2015/04/02/quatorze-start-up-qui-font-bouger-l-afrique_4608623_ 3212.html, consulté le 03/03/2017.

21- **Marion-JEANNE LEFEBVRE**, « Yahoo étend son offre médiatique avec deux magazines en ligne, Stratégies/AFP », article publié le 9 janvier 2014, à partir de l'adresse : http://www.strategies.fr/actualites/medias/227458W/yahoo-etend-son-offre-mediatique-avec-deux-magazines-en-ligne.html, consultée le 20/12/2016.

22- **Martin UNTERSINGER, Damien LELOUP**, « Qu'est- ce que le USA Freedom Act ? », article de journal Le Monde, publié le 01/06/20015 à 11h08 sur le site : http://www.lemonde.fr/pixels/article/2015/06/01/, consulté le 03/10/2016.

23- **Martin UNTERSINGUR**, « Une grave vulnérabilité découverte dans les réseaux Wi-fi », article de journal Le Monde, publié le 16/10/2017 sur le site: http://www.mobile.lemonde.fr/pixels/2017/10/16/une-grave-vulnérabilité-découverte-dans-les-réseaux-Wi-fi_5201770_4408996.html, consulté le 20/10/2017.

24- **Marc ZAFFANI**, « OS X, IOS, Windows: quels sont les systèmes les plus vulnérables ? », article publié sur futura-sciences.com, le 26/02/2015. https://www.futura-sciences.com/tech/actualites/technologie-osx-io/, consulté le 23/01/2016.

25- **Nathalie GUIBERT, Damien LELOUP et Philippe BERNARD**, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », article de journal Le Monde, publié sur: http://www.lemonde.fr/international/article/2017/05/13/une-cyberattaque-massive-bloque-des-ordinateurs-dans-des-dizaines-de-pays_5127158_3210.html, consulté le 08/1/2017.

26- **Philippe GUERRIER**, « Yahoo acquiert Interclick pour 270 millions de dollars », article de journal Itespresso.fr, publié le 2 novembre 2011 sur le site: http://www.itespresso.fr/publicite-yahoo-acquiert-interclick-pour-270-millions-de-dollars-47710.html, consulté le 07/01/2017.

27- **Pierre MAGNAN**, « La NSA, le big brother américain, is watching you depuis 1952 », article publié le 14/06/2013 à 16H24 sur le site: http://geopolis.francetvinfo.fr/la-nsa-le-big-brother-americain-is-watching-you-depuis-1952-17641, consulté le 26/12/2018.

28- **Riccardo SANSONETTI**, « Le bitcoin: opportunités et risques d'une monnaie virtuelle », article publié le 01/09/2014 sur : http://dievolkswirtschaft.ch/fr/2014/09/sansonetti-4/

29- **Christophe COQUIS**, « NFC, QR Codes, iBeacon, RI : tout savoir sur les technologies sans contact », article publié sur le site de Softonic International S.A, le 29/09/2014. https://www.fr.softonic.com/articles/nfc-qr-codes-ibeacon-ri-technologies-sans-contact

30- **Rémy DARRAS**, « Africa Internet Group fait de Jumia la marque unique de ses principales sociétés », jeuneafrique.com, article de journal Jeune Afrique.com, publié sur le 23 juin 2016 sur le site : http://www.jeuneafrique.com/335955/economie/africa-internet-group-renomme-71-societes-jumia/, consulté le 06/05/2017.

31- **Romain MEGEMONT**, « Paiement mobile sur smartphone : présentation, fonctionnement et sécurité », article publié sur FrAndroid, le 28-04-2018. https://www.frandroid.com/android/application/500871_ Paiement-mobile-sur-smartphone-présentation-fonctionnement-sécurité

32- **Sarah BELOUEZZANE**, « Yahoo! officialise le rachat de Tumblr », article de journal Le Monde, publié le 20/05/2013 sur le site: http://www.lemonde.fr/technologies/article/2013/05/20/yahoo-veut-racheter-tumblr-pour-rajeunir-son-image_3380686_651865.html, consulté le 03/11/2016.

33- **Stéphane PLASSE**, « Drones : comment lutter contre le risque de piratage ? », article publié le 15/08/2013, à 8h21, sur le site : https://www.slate.fr/story/76418/drone-France-piratge, consulté le 04/03/2016.

34- **Sarah SERMONDADAZ**, « après WannaCry, voici le virus qui génère de la crypto-monnaie à votre insu », article de journal Sciences et avenir, publié le 18/05/2017 à 13h03, sur le site: https://www.sciencesetavenir.frhigh-techinformatiqueapres-wannacry-voici-le-virus-qui-genere-de-la-crypto-monnaie-a-votre-insu_113056.html, consulté le 03/06/2017.

35- **Tanguy ANDRILLON**, « Un hacker aurait réussi à prendre le contrôle d'un réacteur d'avion en plein vol », article de journal La Ruche, publié le 18 mai 2015 à 15 H 56 sur le site: http://www.laruche.it/, consulté le 15/03/2017.

36- **Thierry LOMBRY**, « Comment fonctionne un ordinateur quantique », article publié sur futura-sciences.com, le 26/10/2015. https://www.futura-sciences.com/sciences/dossiers/physique/, consulté le 08/01/2016.

37- **William AUDUREAU**, « Pour les djihadistes, la dynamique est plutôt d'abandonner Twitter », article de journal Le Monde, publié le 22 mars 2017 sur le site: http://www.lemonde.fr/pixels/article/2017/03/22/pour-les-djihadistes-la-dynamique-est-plutot-d-abandonner-twitter_5099068_4408996.html, consulté le 02/04/2017.

38- ……, « Le réseau social Mastodon, un «Twitter plus proche de l'esprit originel», article de journal Le Monde, publié le 4 avril 2017 sur : http://www.lemonde.fr/pixels/article/2017/04/04/le-reseau-social-mastodon-un-twitter-plus-proche-de-l-esprit-originel_5105900_4408996.html

Ⅷ-Documents:

1- Document du club de la sécurité des systèmes d'information Français(CLUSIF), « Gérer la sécurité d'un site de commerce électronique », Mai 2001, version 1.0, pp. 01-43. https://www.clusif.asso.fr/
2- Document du club de la sécurité des systèmes d'information Français(CLUSIF), « Sécurité des applications Web : comment maîtriser les risques liés à la sécurité des applications Web », septembre 2009, pp. 01-20. https://www.clusif.asso.fr/
3- Rapport McAfee Labs Prévisions 2017 en matière de menaces, Novembre 2016, pp. 01-53. https://www.mcafee.com/fr
4- Rapport McAfee Labs, sur le paysage des menaces, avril 2017, pp. 01-49. Disponible sur le site : https://www.mcafee.com/fr

Ⅸ- Sites Internet:

A- Sites Juridiques :

https://www.curia.europa.eu
https://www.legifrance.gouve.fr
https://www.doctrine.fr
https://www.legalis.net
https://www.juriscom.net
https://www.actu-juridique.fr
https://www.droit-technologie.org

B- sites de sécurité informatique :

https://www.kaspersky.com
https://www.mcafee.com/fr
https://www.symantec.com
http://www.exploit-db.com
http://www.secuobs.com
http://securityvulns.com
http://www.securityfocus.com
http://www.cert-ist.com

فهرس المحتويات

ملخص:

عرفت التجارة الإلكترونية خلال السنوات الأخيرة تطورات كبيرة نتيجة ازدياد تطبيقاتها، والانتشار المُذهل والكثيف للمتاجر الإفتراضية عبر شبكة الإنترنت، التي تعتبر كحافز مُشجّع للشركات والمستهلكين، وبالتالي فإنّ مواقع التجارة الإلكترونية تعتمد على الاختيار المُسبق لاسم النطاق، مع الأخذ بعين الإعتبار جميع مواصفاته التقنية الأساسية، من حيث التصميم المحكم والدقيق، واعتماد معايير الأمان المُتطلبة لغرض جذب العملاء.

انطلاقا من ذلك، فإنّ عوامل نجاح أو إخفاق مشاريع مواقع التجارة الإلكترونية تتوقف على ما تحتويه من مصنفات رقمية ذهنية محمية، كالبرمجيات وقواعد البيانات، إلى جانب المصنفات الأخرى التي تحتاج للحماية، كعناوين البريد الإلكتروني وأسماء النطاقات الخ...، حيث تعترضها مجموعة من المخاطر الإلكترونية التي تستوجب- إلى جانب الحماية القانونية والتقنية- تدخّل الدولة التي تعتبر كطرف فعّال، من خلال تشييد بِنية معلوماتية وطنية متعددة الأوجه، لحماية المواطنين والشركات والمصالح الحيوية لها، ما دام أنّ مسألة أمن الشبكات وأنظمة المعلومات أصبحت تمسّ السّيادة الوطنية.

Résumé :

Le E- commerce s'est fortement développé ces dernières années grâce au progrès rapide des programmes d'applications, ainsi que l'émergence accélérée de l'E-boutique sur Internet qui constitue une opportunité pour les entreprises et les consommateurs. Cependant, la création d'un site E-commerce implique la réservation en ligne d'un nom de domaine le plus en amont possible, en tenant compte des fonctionnalités fondamentales de E-commerce qui doit offrir un accueil de qualité(Communication, Graphisme, Ergonomie, etc.), et d'outils de fidélisation des clients et de développement de la clientèle (E-marketing, Référencement, Affiliation, etc.).

En effet, le service de commerce en ligne s'appuie sur des objets numériques, tels que des logiciels, des bases de données, des éléments visuels et multimédia, des signes distinctifs, adresses et des noms de domaine, qui constituent des facteurs décisifs de la réussite ou de l'échec commercial de l'activité d'un site marchand. Par ailleurs, les menaces logicielles sont en évolutions constantes et la sécurité des systèmes d'information, ne saurait reposer sur les seuls moyens juridiques et techniques de prévention et de protection (Solutions PKI, etc.), ni sur la vigilance des consommateurs.

Par conséquent l'État doit avoir un rôle primordial à jouer afin de protéger les citoyens, les entreprises et ses infrastructures vitales, étant donné que la sécurité des réseaux et des systèmes d'information est devenue un enjeu politique de souveraineté et de développement de l'économie nationale.