جامعة مولود معمري – تيزي وزو
كلية الحقوق والعلوم السياسية
قسم الحقوق

آليات مكافحة الجريمة المرتكبة عبر الإنترنت

رسالة لنيل درجة دكتوراه في العلوم
تخصص قانون

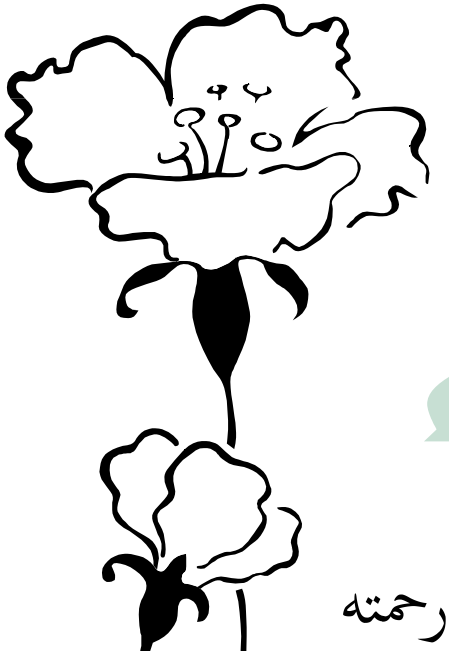
إعداد الطالب:
صغير يوسف

إشراف الأستاذ:
أ د. إقلولي محمد

لجنة المناقشة:

أ.د واضح رشيد، أستاذ التعليم العالي جامعة مولود معمري، تيزي وزو..... رئيسا
أ. د إقلولي محمد، أستاذ التعليم العالي جامعة مولود معمري، تيزي وزو..... مشرفا ومقررا
أ . د حمودي ناصر، أستاذ التعليم العالي جامعة آكلي محند أولحاج، البويرة..... ممتحنا
د. خليفي سمير أستاذ محاضر قسم "أ" جامعة آكلي محند أولحاج، البويرة..... ممتحنا
د. موكه عبد الكريم أستاذ محاضر قسم "أ" جامعة الصديق بن يحي، جيجل..... ممتحنا
د. براهيمي جمال أستاذ محاضر قسم "أ" جامعة مولود معمري، تيزي وزو..... ممتحنا

تاريخ المناقشة: 01 جويلية 2024



إهداء

إلى الوالدة تغمدها الله بواسع رحمته

إلى والدي أمده الله بموفور الصحة والعافية

إلى زوجة أبي التي كانت بمثابة أم ثانية

إلى زوجتي وابنتي أدامهم الله قرّة لعيني.

إلى أخي وأخواتي

إلى كل أساتذتي وأصدقائي

إلى كل من مدّ لي يد العون في إنجاز هذا العمل

أهدي ثمرة جهدي

يوسف

كلمة شكر

إلى أستاذي المشرف
الدكتور إقلولي محمد
أتقدّم بخالص الشكر وعظيم الامتنان لتفضّله بقبول
الإشراف على هذا العمل وتعهّده بالتصويب في جميع
مراحل إنجازه.

يوسف

قائمة أهم المختصرات

1-باللغة العربية

1-**ص:** صفحة
2-**ص ص:** من الصفحة إلى الصفحة
3-**ج ر:** جريدة رسمية
4-**د د ن:** دون دار نشر
5-**د س ن:** دون سنة نشر

2-باللغة الفرنسية

1-**P** : Page
2-**P p** : de page a page
3-**N** : Numéro
4-**Vol** : Volume
5-**Op-cit** : Ouvrage déjà cité
6-**Crisp** :Centre de recherche et d'information sociopolitiques
7-**I N H E S** : Institut national des hautes études de la sécurité et de la justice
8-**C N R S** : Centre national de la recherche scientifique
9-**I R S E M** : Institut de recherche stratégique de l'école militaire

3-باللغة الإنكليزية

1-**UN** : United nations
2-**U N O D C** : United Nations Office on Drugs and Crime
3-**OFCOM**: Office of communications
4-**A U** : African Union
5-**N T I S** : National technical information service
6-**I P** : Internet Protocol
7-**T C P** : Transmission control protocol
8-**I P S E C** : Internet protocol security
9-S S L: Secure sockets layer

مقدمة

يتطور الإنسان حسب الرغبات التي يريد أن يحققها حيث يستعمل نعمة العقل التي حباه الله بها من أجل التكيف مع ظروف الطبيعة المحيطة به من جهة ومحاولة إشباع الرغبات التي تختلج بين ثنايا نفسه من جهة أخرى، فهو يعد اجتماعيا بطبعه، وأنّ تميّزه بهذه الخاصية جعله ينتقل من الحياة الانفرادية التي كان يعيشها إلى حياة اجتماعية مع أفراد آخرين تربط بينهم أهداف مشتركة أساسها ضمان البقاء الذي يعتبر الغاية الأسمى لكل مخلوق على وجه الأرض.

لقد أدّى هذا التعايش والترابط في العلاقات إلى تغيير أسلوب الإنسان في الحياة حيث بعد أن سعى إلى تحقيق غايات شخصية بحتة أصبح يرمي إلى تحقيق غايات مجتمعية وبعد أن اعتمد على الصيد ليأكل ويلبس أوراق الاشجار ليتدفأ أصبح يفكر من خلال العلاقات الاجتماعية التي أسسها إلى إيجاد الحلول اللازمة لكي يحسّن نمط معيشته.

انجرّ عن التطور الذي عرفه الإنسان داخل المجتمعات التي كوّنها عن طريق العلاقات مع أفراد آخرين بروز العديد من الرغبات التي لم يكن يعرفها من قبل، حيث أصبح يسعى إلى إحداث تنظيم أكثر في أسلوب حياته من أجل وضع أسس تحكم هذه التطورات التي عرفها في مختلف نواحي حياته، ولم يتوقف تطور الإنسان وحاجياته عند هذا الحد بل تعداه إلى تطور المجتمعات التي يعيش فيها حيث اصبحت تنتظم وتتكتّل إلى أن بدأت تتكوّن القرى والمدن.

يعتبر ظهور المجتمع بهذه الصيغة الحديثة اللبنة الأولى التي تشكّل الدولة حيث أن التطوّرات التي عرفتها هذه المجتمعات شكلت تجمعات إنسانية كبيرة أطلق عليها فيما بعد اسم الدولة والتي تربط بين أفرادها علاقات اجتماعية متنوعة ومتعددة سواء كانت اجتماعية بحتة أو سياسية أو اقتصادية.

أدّى بروز هذا النوع من الكيان البشري بالفرد الذي يعيش داخله إلى التغيير في دوافعه ونشاطاته وحتى رغباته حيث اصبحت كثيرة ومتشعبة وطغى عليها الطابع المادي الأمر الذي انجر عنه التنافس بين الأفراد من أجل تحقيقها وإشباعها، حيث صاحب هذا الطابع التنافسي

لجوء بعض الأفراد إلى اتباع أساليب منافية للحياة الاجتماعية السليمة، فتزايد حاجيات ورغبات هؤلاء الأفراد أدى بهم إلى ارتكاب العديد من الأفعال الجرمية من أجل تحقيقها وإشباعها.

تعد هذه الجرائم نتيجة حتمية للحياة الجماعية للإنسان فكما عرف الكثير من السبل الجيدة والسليمة التي من خلالها طوّر أسلوب حياته عرف كذلك العديد من الأفعال المنافية لتقاليد الحياة الاجتماعية وذلك راجع إلى التباين والتصادم بين مصالح الأفراد داخل الجماعة أو المجتمع الواحد.

تطورت الجريمة عبر مختلف مراحل حياة الإنسان، فالجرائم التي كان يرتكبها في السابق، لم يعد يرتكبها في الوقت الحالي، والجرائم التي ترتكب في مجتمع لا نجد لها مثيل في مجتمع آخر وذلك راجع إلى تغير دوافعه وظروفه الاجتماعية من جهة والاختلاف في المستوى العلمي والثقافي والمادي من جهة أخرى.

غير أنه وبالرغم من السلبيات التي عرفها الإنسان داخل الحياة الجماعية إلا أنه لم يتوقف عن تطوير نفسه من أجل ضمان حياة أفضل فكما أن الجريمة تعتبر انتاجا اجتماعيا سلبيا هناك انتاج اجتماعي إيجابي يتمثل في التطور الفكري والثقافي والعلمي.

كرّس الإنسان بكل ما حباه الله من عقل وحب للتطور كل قدراته من أجل تنمية ذاته وحياته على أسس وطرق فكرية وعلمية حيث توّجت هذه القدرات والاجتهادات بظهور ما يعرف بالثورة الصناعية التي كانت عبارة عن الانطلاقة في تكوين مفهوم جديد للحياة الاجتماعية وذلك عن طريق إدخال وسائل مصنّعة تساعد الإنسان على تسهيل نمط حياته وتلبية حاجياته.

أدرك الإنسان بفضل الثورة الصناعية التي عرفتها المجتمعات في القرون الماضية مدى استطاعته في تغيير مفهوم حياته والتي فتحت له آفاق جديدة لم يكن يعرفها من قبل وأصبح في مقدوره فهم معنى الحياة المتطورة على أساس علمي وتكنولوجي ومنه لم يعد طموحه يتوقف عند اكتشاف الطاقة والقيام بتأسيس صناعة قوية بل تعداه إلى آفاق أخرى وهي عالم التكنولوجيا التي أدت إلى ظهور عدة اختراعات وابتكارات سهلت حياة الإنسان ولعل أهمها اختراع الحاسب

الآلي[1]، الذي يعتبر من بين أهم الاختراعات التي عرفها العالم في القرن الماضي حيث استطاع من خلاله الأفراد والدول تسهيل معاملاتهم اليومية فما كان القيام به صعبا في الماضي ويتطلب وقتا طويلا أصبح سهلا بفضل ما يحمله الحاسب الآلي من تقنية عالية قدمت خدمات كثيرة لهم.

تطوّرت الحاسب الآلي بشكل متسارع جراء الاعتماد عليها من طرف الأفراد والدول في مختلف مناحي الحياة حتى وصلت إلى إمكانية الربط بينها عن طريق شبكات تسمح باتصال هذه الحواسيب بعضها البعض، ويعتبر ظهور الشبكات الاتصالية التي تربط بين الحاسبات الآلية قفزة نوعية في مجال الاتصال والتواصل فمن خلالها أصبح من السهل القيام بمختلف التعاملات مهما كان نوعها دون عناء التنقل من مكان إلى آخر من جهة، ومن جهة أخرى تسمح بإتيان هذه المعاملات في وقت قصير وذلك لتميّزها بالسرعة واختصارها للوقت.

تطورت الشبكات الاتصالية بشكل كبير في وقتنا الراهن لتصبح واسعة النطاق حيث أنها انتقلت من طابعها المحلي إلى طابع دولي يربط بين دول عديدة بل وصلت إلى أبعد من ذلك لتصبح لها طابع عالمي يربط بين كل دول العالم لتجعل هذا الأخير يشبه قرية صغيرة.

تعد الإنترنت من بين أهم الشبكات الاتصالية التي عرفها العالم فهي تعتبر كمثال صريح عن التطورات التي عرفتها وخير دليل على ذلك كثرة الاعتماد عليها من طرف الأفراد والدول على حد سواء في مختلف تصرفاتهم القانونية أو الاجتماعية أو السياسية أو حتى الترفيهية إلى ما في ذلك من تسهيلات تقوم بتقديمها حتى أصبح يطلق عليها أم الشبكات[2]، حيث أنها تتميز

---

[1]- لتفاصيل أكثر أنظر: **بن يطو أسامة**، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الإختراع، مذكرة مقدمة لاستكمال نيل شهادة الماجستير في الحقوق، تخصص قانون الملكية الفكرية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة 1، 2018، ص 4

[2]- نشأت البدايات الأولى للإنترنت في وزارة الدفاع الأمريكية عام (1969)، منطلقين من حاجة هذه المؤسسة العسكرية إلى وسائل أمنية محكمة لتحريك معلوماتها عبر مناطق العالم المختلفة دون الاعتماد على طريقة تقليدية واحدة في استعلاماتها أو استخباراتها المعلوماتية.

تكون النموذج الأول للإنترنت من أربعة أجهزة حاسبات موزعة على جامعة يوتاه وجامعة كاليفورنيا ومعهد ستانفورد الدولي للأبحاث، وقد كان هذا النظام تحت تسمية شبكة أربانيت arpanet نسبة إلى وكالة المشاريع البحثية المتقدمة الأمريكية

بعدة خصائص أهمها طبيعتها المتعدية لحدود الدول فلقد ألغت كل المفاهيم المتعلقة بالحدود الجغرافية والسياسية بين الدول ووضعت مبدأ سيادة الدولة على إقليمها على المحك لتعارضه مع المنطق الذي تسير عليه الشبكة.

تعمل الإنترنت على ربط العديد من الشبكات في مؤسسات مختلفة كالمؤسسات التعليمية والبحثية والتجارية وحتى منظمات حكومية عبر مختلف أنحاء العالم، لتسمح هذه الخاصية الترابطية التي تميز الشبكة للمتعاملين عبرها بالقيام بمختلف التعاملات مثل التسوق وزيارة المتاحف والمعارض بالإضافة إلى التواصل مع أفراد آخرين في أماكن بعيدة دون عناء التنقل.

ترتبط الإنترنت في وقتنا الحالي ارتباطا وثيقا بالمكونات الاجتماعية لأي مجتمع بتفاعلها مع القيم والموروثات الثقافية في إطار تأثيرها على فئات المجتمع[3]، فطبيعة الشبكة بصفتها انتاجا اجتماعيا مرتبط بتطور الانسان عبر مختلف الحقب التي عاشها مما انجر عنه العديد من الممارسات سواء إيجابية كانت أو سلبية.

أثّر الترابط الاجتماعي للإنترنت على طريقة تسيير المجتمع حيث شهد هذا الأخير العديد من الممارسات السلبية عبرها رغم إيجابياتها. فالجريمة ومن ورائها المجرمين استغلوا الاستعمال

Advanced research projects agency حتى وصل عدد الحاسبات العاملة في هذا النظام الجديد في نهاية سبعينيات القرن الماضي إلى 254 حاسبا.

شهدت هذه الشبكة محاولات عدة حتى وصلت في النهاية إلى تكوين شبكة اتصالات دولية تحت اسم international network، وقد بقي الاستخدام والتأثير الأكبر لهذا النظام ضمن حدود الولايات المتحدة الأمريكية، إلا أنه سرعان ما تطور استخدامه إلى نطاق عالمي، حيث بدأ التعامل معه ومن قبل الشركات الكبرى في العالم، وفي ثمانينيات القرن الماضي، وليتسع الاستخدام في التسعينيات منه، ولتبدأ الشركات التجارية والصناعية والخدمية ومن كل الأنواع والأحجام باستخدام الإنترنت في عملها وعبر الشبكة العنكبوتية العالمية world wide web (www) والتي تلفظ اختصارا الوب web. نقلا عن: **أميمة معراوي**، التسوق الإلكتروني، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2020، ص 4.

[3]- **إسماعيل بن وصفي غانم الآغا**، سوء استخدام تقنية الإنترنت والجوال ودورها في انحراف الأحداث بدول مجلس التعاون الخليجي، أطروحة مقدمة استكمالا للحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العلوم الاجتماعية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 06.

الواسع لها، بالإضافة إلى عدم خضوعها لأي سلطة من أجل نقل أعمالهم الإجرامية إليها لتصبح مسرحا لعدة جرائم لم تشهدها الساحة القانونية من قبل.

برزت مع شيوع استخدام الكمبيوتر أواخر سبعينات القرن الماضي ظاهرة القرصنة الإلكترونية وسرعان ما تحوّل السلوك الذي بدا في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا إلى حربا تشنّ بين الدول وهي تهدد منشئات حيوية كالمفاعلات النووية ومحطات الكهرباء، كما تدمر المخزونات النقدية لبنوك ودول وتهتك أسرارا لا يراد لها الخروج إلى العلن[4].

ظهرت الجريمة المرتكبة عبر الإنترنت ولم يتصور أحد من مخترعيها أنها سوف تستعمل في الأعمال الإجرامية[5] لأن الغرض من اختراعها كان لاستعمالها في تسهيل الحياة اليومية للأفراد والدول على حد سواء غير أن تنامي استعمالها والاعتماد عليها في مختلف مناحي الحياة بالإضافة إلى تضاعف وكثرة المشتركين عبرها أدى إلى ظهور هذا النوع من الإجرام.

---

[4]– كشفت أرقام وبيانات عالمية، تزايد جرائم تكنولوجيا الإعلام والاتصال في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الإنترنت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجتال" أن عدد ضحايا الهجمات والجرائم الإلكترونية يبلغ 555 مليون مستخدم سنويا، وأكثر من (1,5) مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم شويعا هي سرقة الهويات وعددها (224) مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذا بينت أن أكثر من (600) ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت ب (100) مليار دولار، بعدما كانت في حدود (63,1) مليار دولار سنة (2011)، تجاوزت (120) مليار دولار سنة (2017)، نقلا عن: **حفوظة الأمير عبد القادر، غرداين حسام، « واقع جرائم تكنولوجيا الإعلام والاتصال وسبل التصدي لها محليا، عربيا ودوليا »**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي بتندوف، العدد الأول، جوان 2017، ص 166.

[5]– سجلت أول حالة اعتداء أمني على شبكة الإنترنت في عام (1988)، أي بعد مضي ما يقارب من عشرين عاما على إنشائها، حيث قام "روبرت موريس" الطالب في جامعة "كورنل" بتطوير فيروس (عرف لاحقا باسم فيروس موريس) استغل هذا الفيروس ثغرة في نظام البريد الإلكتروني المستخدم آنذاك مكنته من استنساخ نفسه ونقل نسخة إلى عدد كبير من أجهزة الحاسب الآلي المرتبطة بالشبكة، أحدث هذا الفيروس شللا مؤقتا في جميع الأجهزة التي أصابها، وكانت ما يقرب من (10%) من مجموع الأجهزة المرتبطة بالشبكة آنذاك، نقلا عن: **إياس بن سمير الهاجري، « أمن المعلومات على شبكة الإنترنت »**، ندوة حقوق الملكية الفكرية، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص ص 137–138.

تطوّرت الجريمة المرتكبة عبر الإنترنت بشكل رهيب وذلك راجع إلى التطوّر الكبير للإنترنت من جهة وكثرة الاعتماد عليها في الحياة اليومية للأفراد والدول من جهة أخرى، الأمر الذي جعل منها مناخا لارتكاب الكثير من الجرائم نظرا للتسهيلات التي تقدمها.

تكمن خطورة الجرائم المرتكبة عبر الإنترنت في طريقة ارتكابها وذلك عن طريق استغلال المجرمين والجماعات الإجرامية إمكانياتها اللامحدودة وخفاء مرتكبها الذي يتمتع بمهارة ومعرفة عالية في مجال التقنية بل أكثر من ذلك فهي تتم بعيدا عن أعين سلطات إنفاذ القانون بالإضافة إلى أنها تتم في عالم افتراضي لا يترك أي أثر مادي.

امتدّت آثار الجريمة المرتكبة عبر الإنترنت إلى خارج الأقاليم الوطنية ليصبح لها بعد دولي وذلك تبعا للطابع العالمي لشبكة الإنترنت الأمر الذي كانت نتائجه وخيمة على الأفراد والدول والمجتمع الدولي ككل نظرا للخسائر التي تتكبدها يوميا مختلف المؤسسات والمنظمات سواء كانت وطنية أو دولية.

دقّت الدول ناقوس الخطر نظرا لجسامة الآثار المترتبة عن الجريمة المرتكبة عبر الإنترنت ونادت بضرورة الوقوف في صف واحد لمكافحة هذا النوع الجديد من الإجرام عن طريق تضافر الجهود الوطنية والدولية لوضع آليات قانونية فعالة لمكافحتها.

استجاب المجتمع الدولي للنداءات الرامية إلى ضرورة مكافحة الجريمة المرتكبة عبر الإنترنت وبدأت الدول وباقي أعضاء المجتمع الدولي في محاولة وضع هذه الجريمة في إطارها القانوني، غير أن ما لوحظ في بداية مكافحتها هو إدراجها في نطاق النصوص القانونية التقليدية القائمة وذلك راجع إلى عدم فهم هذا النوع المستحدث من الجرائم. غير أن الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت بيّنت أن النصوص التقليدية لا تفي بالغرض فيما يخص مكافحتها بل خلقت العديد من الإشكالات القانونية، حيث اختلفت وتباينت الأحكام القضائية في البلد الواحد فمنها من أدان الفاعلين على أساس السلوك الإجرامي المكوّن للجريمة ومنها من أباح هذه الأفعال على أساس أن النصوص القانونية التقليدية لم تنص صراحة عليها مطبقين في ذلك المبدأ السائد في الشق الجزائي من القانون المتمثل في "لا جريمة ولا عقوبة ولا

تدابير أمن إلا بنص قانوني" وهو مبدأ يؤدي إلى استحالة مواجهة هذه الظاهرة الإجرامية المستحدثة بنصوص تقليدية وضعت في زمن سابق لظهورها.

هذا الوضع فرض على الدول بأن تقوم بتطوير ترسانتها القانونية سعيا منها مواكبة تطور المجتمع ومسايرة التطورات التكنولوجية في مجال الاتصال من خلال تنظيم هذا المجال بأحكام تتماشى مع هذه التطورات تكريسا لمفهوم تطور النصوص القانونية كنتيجة اجتماعية والتي تعتبر الوسيلة الفعالة لحماية الأفراد والمجتمعات.

استدعى قصور النصوص التقليدية في مكافحة الجريمة المرتكبة عبر الإنترنت وتفاقم وتطور الاعتداءات المرتكبة عبر هذه الشبكة الافتراضية تدخلا تشريعيا عاجلا سواء على المستوى الدولي أو الوطني، فعلى المستوى الدولي ظهرت جهود جادة في إطار منظمة الأمم المتحدة ومختلف المنظمات التابعة لها والتي توجت بعقد العديد من المؤتمرات وتقديم الكثير من الإرشادات للدول الأعضاء فيها بالإضافة إلى عقد معاهدات واتفاقيات دولية توجت بوضع الإطار القانوني لمكافحة هذه الجريمة.

عاصر الوضع التشريعي الخاص بمكافحة الجريمة المرتكبة عبر الإنترنت جهود إقليمية قامت بها دول في شكل تكتلات دولية لعل أهمها الاتحاد الأوروبي والتي كانت جهودها كبيرة في هذا المجال خاصة وأنها تضمنت مختلف أشكال الإجرام المرتكب في العالم الافتراضي.

واكب التطور التشريعي الحاصل على المستوى الدولي والإقليمي تطورات كبيرة في تشريعات الدول، فمن منطلق أن الجريمة تكون بدايتها دائما وطنية قبل أن تكون دولية فإنه من الواجب أن تكون هناك نصوص قانونية تكفل مكافحتها، حيث أن النصوص الدولية لا تكفي وحدها لمكافحة الجريمة المرتكبة عبر الإنترنت بل يجب أن يكون هناك إسقاطات لهذه الأخيرة على مستوى القوانين الداخلية سواء كانت موضوعية أو إجرائية.

توجّه المشرع الجزائري أمام هذا التطور في الجريمة المرتكبة عبر الإنترنت والتسارع في تطوير التشريعات على المستوى الدولي والتي لم تدع له الخيار –حتى وإن كان متأخرا– إلى

حصر هذا النوع المستحدث من الجرائم في نطاقها القانوني من أجل أن يتسنى له وضع استراتيجية من خلالها يقوم بوضع الآليات القانونية الصحيحة لمكافحتها وذلك عن طريق تعديل النصوص القانونية القائمة ووضع نصوص قانونية خاصة بهذه الجرائم.

انطلاقا مما سبق، وفي خضم الحركية التشريعية الموضوعية والإجرائية التي عرفتها الجريمة المرتكبة عبر الإنترنت والتي أضفت إطارا قانونيا متكاملا يكفل مكافحتها، غير أننا وبالنظر إلى خصوصيتها نتساءل عن **مدى فعالية الآليات المكرسة لمكافحتها؟**

تقتضي الإجابة عن هذه الإشكالية اتّباع منهج قانوني يجمع بين الاستقراء الوصف والتحليل، وصفي واستقرائي لأن دراستنا تعتمد على وصف المفاهيم الخاصة بالآليات المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت واستقراء مختلف النصوص القانونية التي تكفل ذلك سواء على المستوى الدولي أو الوطني، وتحليلي لأننا سنستعرض أهم العراقيل والإشكالات التي واجهت هذه الآليات.

وعليه، عالجنا موضوع الإطار التشريعي والقانوني لمكافحة الجريمة المرتكبة عبر الإنترنت على المستويين الدولي والوطني من خلال التطرق إلى التكريس القانوني لآليات مكافحتها **(باب أول)**، ثم إبراز الإشكالات القانونية العملية التي واجهت آليات مكافحتها وذلك من خلال تطرقنا إلى تبيين قصور الآليات المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت **(باب ثان)**

الباب الأول

عن التكريس القانوني لآليات مكافحة الجريمة المرتكبة عبر الإنترنت

أدّى الانتشار الواسع لاستعمال الشبكة العالمية للإنترنت إلى تسهيل معاملات الأفراد والدول، فسرعة هذه الشبكة جعلت من المعاملات التي كانت تتطلب وقتا طويلا تتم في بضع لحظات، حيث فتحت المجال للأفراد قصد الاتصال والتواصل بكل سهولة، بل تعدى الأمر إلى أكثر من ذلك، فأصبحت الدول تعتمد عليها بشكل كبير، الأمر الذي جعل العالم يبدو قرية صغيرة نظرا للبعد العالمي لهذه الشبكة.

غير أن الاستعمال اللامتناهي لشبكة الإنترنت صاحبته العديد من السلوكيات السلبية، ففي خضم هذا التواصل استفاق الأفراد والمجتمع الدولي على عيوب عديدة تضرب قيم وأعراف المجتمعات ولعل أكثر السلوكيات السلبية عبر الإنترنت ارتكاب العديد من الجرائم، فهي تعتبر سلاحا ذو حدين، فكما قدمت تسهيلات في مجال معالجة المعاملات من طرف الأفراد والدول، استغل بعض الأشخاص أصحاب النيّة السيّئة هذا الوضع لينقلوا أعمالهم الإجرامية عبر هذا الفضاء الافتراضي، والذي انجر عنه خسائر جسيمة لم يشهد لها العالم مثيل من قبل.

دفع هذا النوع المستحدث من الإجرام برجال القانون سواء مشرعين أو جهات تطبيق القانون أو حتى الفقهاء إلى التحسيس بخطورة الوضع، محاولة منهم وضع آليات قانونية من أجل حماية مصالح الأفراد والدول التي مستها أيادي الإجرام عبر الشبكة العالمية للإنترنت، حيث يعمل رجال القانون والفقهاء على وضع هذه الظاهرة الإجرامية في صورتها القانونية، وذلك سعيا منهم إلى تكريس مبدأ الحماية من الجريمة عبر الإنترنت والتحكم فيها من الناحية القانونية والتقنية.

أصبحت الجريمة المرتكبة عبر الإنترنت تتمتع بالطابع العابر للحدود، رغم أن منطلقها كان وطنيا، فنظرا لعدم احترام شبكة الإنترنت للحدود السياسية والجغرافية للدول اكتسبت الجرائم التي ترتكب عبرها هذه الصفة، الأمر الذي أدى بالدول والمنظمات الدولية إلى تكريس فكرة الأمن المعلوماتي من الناحية القانونية.

يتمثل واقع الجهود المبذولة على المستوى الدولي سواء في إطار المنظمات الدولية كمنظمة الأمم المتحدة، أو في إطار إقليمي كالاتحاد الأوروبي، في وضع تشريع موضوعي يحصر الجريمة، أو إجرائي يضمن متابعة قانونية لها **(فصل أول)**.

واكبت التشريعات الوطنية الحركية التشريعية التي ظهرت على المستوى الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت، ومنها المشرع الجزائري الذي كانت له محاولات جادة حتى وإن كانت متأخرة، وذلك من أجل تطوير المنظومة التشريعية الخاصة بتكنولوجيا الإعلام والاتصال فسنّ نصوص قانونية موضوعية من خلالها وضع الجريمة في إطارها القانوني، ثم أتبعها بنصوص قانونية إجرائية تضمن له متابعة سليمة لهذه الجرائم، وذلك بهدف الالتحاق بركب الدول التي تتمتع بتجربة طويلة في هذا المجال **(فصل ثان)**.

الفصل الأول

الآليات الدولية المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت

فرضت الجريمة المرتكبة عبر الإنترنت نفسها كظاهرة إجرامية مستجدة على المجتمع الدولي، فالمجرمين المعلوماتيين يستغلون ما تمنحه شبكة الإنترنت من تسهيلات ليتخذوا منها مناخا سهلا يرتكبون عبره مختلف الجرائم التي تكون خسائرها جسيمة، حيث يستغل المجرمون والعصابات الإجرامية الطابع الدولي لشبكة الإنترنت لتوسيع أعمالهم الإجرامية عبر الحدود الوطنية، وذلك إما عن طريق مد نشاطاتهم الدولية من جهة، أو عن طريق التعاون فيما بينهم من جهة أخرى، الأمر الذي أدى بالمجتمع الدولي عن طريق المنظمات الدولية إلى محاولة وضع الأطر القانونية الموضوعية والإجرائية لمكافحة هذه الظاهرة الإجرامية المستحدثة.

تستوجب مكافحة الجريمة المرتكبة عبر الإنترنت تضافر الجهود فيما بين الدول، حيث أنها تعتبر من بين أهم الظواهر الإجرامية المطروحة للنقاش، سواء على المستوى الدولي أو الإقليمي مما انبثق عنه إصدار العديد من التشريعات الدولية وذلك رغبة من المجتمع الدولي حصر الجريمة في إطار قانوني فعال **(مبحث أول)**.

لا يفي حصر جرائم الإنترنت وفق إطار قانوني موضوعي بالغرض إذا لم يتبعه الإطار الإجرائي الذي من خلاله تتم متابعة ومكافحة الجريمة، وذلك عن طريق توفير إجراءات قانونية دولية مواكبة للتطورات التي تعرفها الجريمة المرتكبة عبر الإنترنت، وهذا ما سعى إليه المجتمع الدولي عن طريق تفعيل كل الآليات الإجرائية التي تعنى بالجرائم ذات البعد الدولي وبالأخص جرائم الإنترنت **(مبحث ثان)**.

المبحث الأول

الآليات الموضوعية الدولية لمكافحة الجريمة المرتكبة عبر الإنترنت

اكتسبت الجريمة المرتكبة عبر الإنترنت طابع العالمية الذي استمدته من الطبيعة العالمية ذاتها التي تتمتع بها شبكة الإنترنت، فالجريمة المرتكبة في هذا النطاق تعدت كل الحدود الجغرافية والسياسية للدول. تعتبر هذه الخاصية من بين أهم الأسباب التي أدّت بالمنظمات الدولية إلى المطالبة باستحداث أساليب جديدة من شأنها حماية البيئة الإلكترونية، وذلك عن طريق سن نصوص قانونية دولية ملزمة من أجل تنظيم العالم الافتراضي ووضع نظام وقائي للحد من جميع أشكال الجرائم المرتكبة في هذا النطاق **(مطلب أول)**.

لم تتوقف الجهود الدولية عند دور المنظمات الدولية في مكافحة الجريمة المرتكبة عبر الإنترنت، بل تعداه إلى المستوى الإقليمي، حيث أن تكتّل الدول في نطاق حيز جغرافي يربط بينها العديد من المسائل المشتركة أهمها مكافحة الجريمة ومتابعة المجرمين، وكان لذلك دور جد فعال في وضع أهم الآليات القانونية اللازمة لمكافحة الجريمة المرتكبة عبر الإنترنت **(مطلب ثان)**.

المطلب الأول

جهود المنظمات الدولية في مكافحة الجريمة المرتكبة عبر الإنترنت

سعى المجتمع الدولي إلى حصر الجريمة المرتكبة عبر الإنترنت في إطارها القانوني، حيث قام تحت قيادة المنظمات الدولية المختلفة بسن التشريعات والإرشادات التي من خلالها تقوم الدول بمواكبة التطور التشريعي الدولي.

ولعل من بين أهم المنظمات الدولية التي يمكن أن نذكرها في هذا الصدد على سبيل المثال لا الحصر نظرا للجهود المبذولة من طرفها منظمة الأمم المتحدة **(فرع أول)**، وكذلك المنظمة العالمية للملكية الفكرية **(فرع ثان)**، بالإضافة لمنظمة التعاون والتنمية الإقتصادية **(فرع ثالث)**.

الفرع الأول

جهود منظمة الأمم المتحدة لمكافحة الجريمة المرتكبة عبر الإنترنت

بذلت الأمم المتحدة جهودا معتبرة في مكافحة الجرائم المرتكبة عبر الإنترنت، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة للإنسانية جمعاء، إيمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[6]، وفي ذلك نتطرق إلى المؤتمرات الدولية والإقليمية اليت عقدتها منظمة الأمم المتحدة **(أولا)** ثم إلى القرارات التي أصدرتها **(ثانيا)** في مجال مكافحة الجريمة المرتكبة عبر الإنترنت والتي نذكر منها ما يلي على سبيل المثال لا الحصر:

أولا: على مستوى المؤتمرات

عقدت منظمة الأمم المتحدة سلسلة من المؤتمرات في هذا الخصوص منها:

1-مؤتمر هافانا سنة 1990:

حثت الأمم المتحدة في هذا المؤتمر الدول الأعضاء في موضوع الجرائم ذات الصلة بالكمبيوتر على تكثيف جهودها لمكافحة إساءة استعمال الحاسب، كما طالبت بإنشاء لجنة حكومية من أجل الحماية من الجريمة والتي تكون العضو الرئيسي لمنظمة الأمم المتحدة في هذا المجال[7]، بالإضافة إلى اتخاذ -متى دعت الضرورة- الاجراءات التالية:

أ- ضمان أن تطبق القوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم، وإدخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك.

---

[6]- **مراد مشوش، «الجهود الدولية لمكافحة الإجرام السيبراني»**، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 12، العدد 02، 2019، ص 706.

[7]- **OUDER Hadjira**, Les dispositifs légaux de lutte contre la cybercriminalité, ceristnews, bulltin d'information trimestriel, treizième numéro, juin 2013, Alger, p 13. p p 12-26.

ب- النص على إجراءات تتعلق بالتحقيق والأدلة عندما تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم[8].

ت- تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة احترام الخصوصية وحقوق الإنسان.

ث- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية بمخاطر هذه الجرائم وإبراز أهمية مكافحتها.

ج-اعتماد تدابير خاصة ومناسبة لتدريب القضاة والضبطية القضائية بما يتناسب مع متطلبات الجريمة المرتكبة عبر الإنترنت.

ح-مضاعفة الأنشطة التي تبذلها الدول على الصعيد الدولي من أجل مكافحة هذه الجرائم بما في ذلك دخولها -حسب الحاجة- كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة.

خ-يجب أن تعمل الدول على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على الأشكال الجديدة للإجرام، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف.

د- اعتماد سياسات بشأن ضحايا الجرائم المعلوماتية تنسجم مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة، وتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير

---

[8]- أنظر في ذلك: مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، البند الخامس من جدول الأعمال المؤقت، النهج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدة للجريمة العابرة للحدود الوطنية والتصدي لها على نحو ملائم، المنعقد بالدوحة من 12 إلى 19 أفريل 2015، A/CONF.222/8 وثيقة متوفرة على موقع منظمة الأمم المتحدة www.un.org

مشروعة، وتدابير لتشجيع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم[9].

2- المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين المنعقد بالقاهرة سنة 1995:

خصص هذا المؤتمر للقيام بحلقة عمل لمناقشة حوسبة نظم العدالة الجنائية، حيث أكدت الحلقة على الحاجة للحوسبة لمواجهة أشكال الجريمة الجديدة وخاصة جرائم الإنترنت والجرائم ذات الصلة بالحواسيب[10]، وركزت الحلقة على ما يلي:

أ- ضرورة قيام الدول الغنية بالمال والخبرات والمنظمات الدولية والإقليمية بتقديم العون إلى الدول النامية في شكل موارد مالية وفي شكل خبرة تقنية.

ب- إحترام حقوق الإنسان وحرياته خاصة أثناء ممارسة أجهزة العدالة الجنائية للتحري عبر الحاسوب أو الإنترنت أو أثناء تنفيذ عمليات القبض والتفتيش وضبط الأدلة الإلكترونية[11].

3- المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين المنعقد بفيينا سنة 2000:

نظّم المؤتمر كل من معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين أثناء عقد المؤتمر حلقة عمل لمدة يوم واحد هو الخامس عشر من أفريل سنة 2000 لمناقشة موضوع الجرائم المتصلة بشبكات الحاسوب[12].

---

[9]- **بن خليفة إلهام**، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه علوم في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2015-2016، ص ص 330-331.

[10]- **محمد فتحي عيد**، الإنترنت ودوره في انتشار المخدرات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 195.

[11]- مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين المنعقد بالقاهرة، مصر بتاريخ 28 أبريل-05 مايو 1995، مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC وثيقة متوفرة على موقع منظمة الأمم المتحدة www.un.org

شكلت حلقة العمل أربعة فرق، حيث ناقش الفريق الأول الجرائم الحاسوبية من منظور علم الإجرام، وناقش الفريق الثاني المشكلات التقنية والقانونية التي تنشأ عن التفتيش القانوني عن البيانات في الشبكات الحاسوبية وضبط تلك البيانات، وناقش الفريق الثالث تعقب الاتصالات في الشبكات الحاسوبية المتعددة الجنسية والمشاكل المقترنة بها، وناقش الفريق الرابع والأخير التعاون بين أجهزة إنفاذ القوانين وصناعتي الحاسوب والإنترنت، وقد توصلت حلقة العمل إلى التوصية بما يلي:

1-أن تقوم الدول -إذا لم تكن قد فعلت- بتجريم الأفعال ذات الصلة بالحاسوب.

2-أن تقوم الدول -إذا لم تكن قد فعلت- بإصدار قوانين إجرائية ملائمة للتحقيق في الجرائم السيبرانية وملاحقة المجرمين السيبرانيين.

3-أن تعمل الحكومات مع المسؤولين في صناعة الحاسوب والأنترنت في تعاون وثيق شفاف لمنع الجرائم الحاسوبية ومكافحتها حتى يصبح الإنترنت مجالا آمنا مع مراعاة الدوافع التجارية للقطاع الخاص واهتمامه بالناحية التقنية لا القانونية.

4-تحسين التعاون الدولي من أجل تسهيل تتبع أثر المجرمين على الإنترنت من من طرف سلطات التحري والتحقيق.

5-أن تعمل الأمم المتحدة على توفير العون والمساعدة التقنية للدول التي تطلبها بشأن الجرائم ذات الصلة بالشبكات الحاسوبية، كما يجب بذل المزيد من الجهد لتقدير الاحتياجات إلى المساعدة التقنية لدى الدول النامية والوفاء بتلك الاحتياجات في أقرب وقت ممكن وخاصة في ظل الاستخدام العالمي المتزايد لتكنولوجيات نظم الحواسيب والاتصالات ومنع الجريمة[13].

---

[12]- Dixième congrès des nations unies pour la prévention du crime et le traitement des délinquants, document de base pour l'atelier consacré au thème « Délits liés à l'utilisation du réseau informatique », Vienne, 10-17 avril 2000, A/CONF.187/10, disponible sur le site www.un.org

[13] - **محمد فتحي عيد**، مرجع سابق، ص ص 196-197.

4-المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية المنعقد بالبرازيل أيام 12-19 أفريل 2010:

ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، حيث احتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[14].

ثانيا: على مستوى القرارات

أصدرت منظمة الأمم المتحدة في هذا الموضوع العديد من القرارات نذكر منها ما يأتي:

1-قرار الجمعية العامة للأمم المتحدة رقم 55/63 لمكافحة استغلال تكنولوجيا المعلومات لأهداف إجرامية المؤرخ في 4 ديسمبر 2000:

يحث هذا القرار الدول الأعضاء على تنسيق أعمال أجهزة الردع لديها وتبادل المعلومات بشأن المشكلات التي تواجههم في مكافحة استغلال تكنولوجيا المعلومات لتحقيق أهداف إجرامية ويؤكد القرار على أن أنظمة المساعدة القانونية المتبادلة تمكن من إجراء تحقيقات بشكل سريع في قضايا استغلال تكنولوجيا المعلومات لأهداف غير مشروعة، وتحث على الجمع والتبادل السريع لعناصر الأدلة المتعلقة بهذه القضايا[15].

---

[14] – مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12-19 أفريل 2010، رقم A/conf.213/9 وثيقة متوفرة على موقع منظمة الأمم المتحدة www.un.org

[15] – **جان فرنسوا هنروت**، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص 103.

2-قرار رقم 19/56 المؤرخ في 29 نوفمبر 2001:

تم اصدار هذا القرار بشأن التطورات في ميدان المعلومات والاتصالات، حيث توجهت الأمم المتحدة إلى جميع الدول الأعضاء بضرورة مواصلة إبلاغ الأمين العام بأدائها وتقويماتها بشأن ما يأتي:

أ- التقويم العام لمسائل أمن المعلومات.

ب- تحديد المفاهيم الأساسية المتعلقة بأمن المعلومات.

ت- مضمون المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات[16].

3-قرار رقم 121/56 يتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية المؤرخ في 23 جانفي 2002:

تشير الجمعية العامة للأمم المتحدة في هذا القرار إلى إعلان الأمم المتحدة بشأن الألفية[17]، الذي عقدت فيه الدول الأعضاء العزم على أن تكفل إتاحة منافع التكنولوجيا الجديدة، وخاصة تكنولوجيا المعلومات والاتصالات للجميع، مما يتفق والتوصيات الواردة في الإعلان الوزاري الصادر عن الجزء الرفيع المستوى من الدورة الموضوعية للمجلس الاقتصادي والاجتماعي لعام 2000، وقرارها رقم 63/55 المؤرخ في 4 ديسمبر

---

[16]- **تركي بن عبد الرحمن المويشر**، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 167.

[17]- الأمم المتحدة، المكتب المعني بالمخدرات والجريمة، خلاصة وافية لمعايير الأمم المتحدة وقواعدها في مجال منع الجريمة والعدالة الجنائية، نيو يورك، 2007، ص 265، www.un.org

2000[18]، الذي دعت فيه الدول الأعضاء إلى أن تضع في اعتبارها اتخاذ تدابير لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[19].

الفرع الثاني

جهود المنظمة العالمية للملكية الفكرية في مكافحة الجريمة المرتكبة عبر الإنترنت

في العصر الرقمي المذهل بتطوراته لم يعد هناك حدود ولا قيود تمنعك من فعل ما تريد وما تحتاج من نسخ لأي مخطوط أو نسخة إلكترونية لكتاب وغير ذلك دون حسيب ورقيب في عالم افتراضي يعج بالناس والأفكار والآراء، الأمر الذي سهل حدوث الجرائم الإلكترونية بالاعتداء على حقوق الملكية الفكرية بصفة عامة[20].

وضعت هذه الحالة المنظمة العالمية للملكية الفكرية وغيرها من المنظمات والجهات المعنية بحماية حقوق الملكية الفكرية أمام تحد كبير بحثا عن أفضل السبل لكيفية حماية حقوق الملكية الفكرية عبر سن نصوص قانونية وتشريعية تكفل حمايتها[21]، ومنها نجد

---

[18]– قرار الجمعية العامة لمنظمة الأمم المتحدة رقم 63/55، الدورة الخامسة والخمسون، البند 105 من جدول الأعمال، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بتاريخ 22 جانفي 2001، A/RES/55/63، www.un.org

[19]– قرار الجمعية العامة لمنظمة الأمم المتحدة رقم 121/56، الدورة السادسة والخمسون، البند 110 من جدول الأعمال، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بتاريخ 23 جانفي 2002، A/RES/56/121، www.un.org

[20]- « Il est bien possible, par exemple, qu'un programme d'ordinateur ayant couté des milions de dollars à mettre au point soit lancé le lundi, obtenu illégalement le mardi, téléchargé sur internet le mercredi et transformé en partagiciel le jeudi; le vendredi il n'est plus qu'un gratuiciel inutile » voir: **RACICOT Michel, S.HAYES Mark, R.SZIBBO Alec, TREUDEL Pierre**, Etude des questions relatives à la responsabiilité à l'égard du contenu circulant sur internet, industrie Canada, 1997, p 216.

[21]– أجرت شركة حماية العلامات التجارية على الإنترنت دراسة حول (50) كتاب الأكثر شعبية بين الطلاب في بريطانيا، وتبين من خلالها أن النسبة المقرصنة فيها (76%) مقارنة بنسبة (24%) تم تحميلها بصفة قانونية، وحسب الدراسة فإن مجالات الكتب الأكثر قرصنة كانت في العلوم والهندسة، وفي مسح أجرته مجموعة صناعة الكتب في أمريكا أنه خلال فصل الربيع (2013) قام ما يزيد من (34%) من طلاب الجامعات الأمريكية بتحميل مواد دراسية من مواقع غير مصرح بها، وفي روسيا يقوم (92%) من مستخدمي القارئ الإلكتروني (eBook) بتحميل الكتب من الإنترنت بطرق غير قانونية، في مقابل (12%) من المستخدمين في أمريكا، وفي عام (2013) تم قرصنة حوالي (400) مليون ملف رقمي من قبل مستخدمي الإنترنت في بريطانيا، ووفقا لدراسة (Ofcom) كان (16%) من مستخدمي الإنترنت قد وصلوا إلى نسخ رقمية مقرصنة، والتي شملت الأفلام والموسيقى والبرامج التلفزيونية والكتب والبرمجيات وألعاب الفيديو، وفي إسبانيا تتسبب النسخ المقرصنة على الإنترنت لصناعة الكتاب خسائر في الإيرادات تص إلى (467) مليون دولار سنويا، وفي عام (2009)

معاهدة برن لحماية المصنفات الأدبية والفنية **(أولا)**، ثم اتفاقية المنظمة العالمية للملكية الفكرية بشأن حق المؤلف لسنة 1996 **(ثانيا)**

أولا: معاهدة برن لحماية المصنفات الأدبية والفنية

تعتبر معاهدة برن التي تم التوقيع عليها في عام 1971 في سويسرا حجر الاساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الإتفاقية 120 دولة وتعد المادة التاسعة الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان، وفضلا عن ذلك، تمنح صاحب المؤلف الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذا تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أو أجنبيا[22].

1-مبادئ حماية حقوق المؤلف بمقتضى اتفاقية برن:

تتمثل مبادئ الحماية التي أقرتها اتفاقية برن لحماية حقوق المؤلف في مبدأ المعاملة الوطنية ومبدأ الحماية التلقائية ومبدأ المعاملة بالمثل ومبدأ الحماية في بلد المنشأ ومبدأ مراقبة تداول المصنفات والتي سنتطرق لها على النحو التالي:

كانت الخسائر في السوق الرقمية للموسيقى تقدر بحوالي (2,83) مليار دولار، أما في روسيا فإن الاعتداء على حقوق المؤلفين مرتفعة بشكل كبير، إذ واعتبارا من (2012) =كان هناك أكثر من (100,000) من الكتب الروسية متاحة في مواقع قرصنة الكتب، مقارنة مع (60,000) من العناوين المتوفرة في المواقع المشروعة وفقا لوكالة الصحافة والاتصالات في روسيا، ويتكون سوق الكتاب الإلكتروني في روسيا من ما يقارب (90%) من الكتب المقرصنة، أما في ألمانيا فذكرت رابطة صناعة الكتاب أن نحو (60%)= =من الكتب الإلكترونية التي يتم تحميلها في البلاد تكون مقرصنة. إحصائيات مشار لها لدى: **غسان فطوم**، حقوق المؤلف والملكية الفكرية والحقوق المجاورة في العالم العربي والشرق الأوسط، منشورات الاتحاد الدولي للصحفيين، بروكسل، 2020، ص ص 15-16.

[22] – **فيصل كامل نجم الدين، « واقع الجريمة الإلكترونية في مواقع التواصل الإجتماعي الحماية النظامية في دول مجلس التعاون الخليجي »**، المجلة الدولية للاتصال الإجتماعي، جامعة عبد الحميد ابن باديس، مستغانم، المجلد 05، العدد 04، سنة 2018، ص 25.

أ- مبدأ المعاملة الوطنية

يعني ضرورة إعطاء نفس الامتيازات الناجمة عن الحماية المكفولة لمواطني الدولة الواحدة التي تكون عضوا في اتحاد "برن" إلى كافة مصنفات مواطني الدول الاعضاء داخل الاتحاد.

ب- مبدأ الحماية التلقائية واستقلالها

يعني عدم اشتراط أي إجراءات لحماية المصنفات بما في ذلك برامج الحاسب الآلي، بالإضافة إلى شمول حماية المصنفات كامل النطاق الجغرافي لدول الاتحاد، بمجرد نشر المصنف في دولتين على الأقل[23].

ت- مبدأ المعاملة بالمثل

يعني هذا المبدأ أن حماية حقوق المؤلف الأجنبي في الدول متوقفة على مدى الحماية التي يتمتع بها المؤلف من رعاياها في الدولة الأخرى[24]، وتم تكريس هذا المبدأ بموجب الفقرة الأولى من المادة السادسة من اتفاقية برن[25].

ث- مبدأ الحماية في بلد المنشأ

يؤكد هذا المبدأ على ما ورد في المادة الخامسة الفقرة الثانية من اتفاقية برن[26]، والتي أعطت للدولة العضو في الاتحاد الحق في أن تضع ما تشاء من الإجراءات والشروط لحماية حقوق المؤلف وتحديد كيفية استعمال ونطاق هذه الحقوق[27].

---

[23] – **بن يطو أسامة، عبدلي حمزة، « حماية برامج الحاسب الآلي في ضوء التشريع الجزائري والمواثيق الدولية »**، مجلة معارف، قسم العلوم القانونية، جامعة البويرة، العدد 19، ديسمبر 2015، ص 147.

[24]– **فتحي نسييمة**، الحماية الدولية لحقوق الملكية الفكرية، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012، ص ص 34-35.

[25]- تنصّ على أنه: "**عندما لا تقرر دولة خارج الاتحاد الحماية الكافية لمصنفات مؤلفين من رعايا دولة من دول الاتحاد فلهذه الأخيرة أن تقيد من حماية مصنفات المؤلفين الذين كانوا في تاريخ أول نشر من رعايا تلك الدولة دون أن يقيموا عادة في في إحدى دول الاتحاد الأخرى منح مثل هذه المصنفات التي تخضع لمعاملة خاصة، حماية أوسع من تلك التي تمنح لها في دولة أول نشر**".

ج- مبدأ مراقبة تداول المصنفات

استنادا لمبدأ الحماية التلقائية، فإن حقوق المؤلف تستحق بمجرد إبداع العمل وليس بناءً على استيفاء بعض الإجراءات الشكلية كالتسجيل وأنه بظهور العمل الإبداعي تولد معه أيضا الحقوق الاستئثارية للمؤلف على مصنفه.

غير أن هذه الحقوق لا تستعمل إلا عند وجود الحماية القانونية اللازمة للمصنفات الأدبية والفنية التي تقررها دولة منشأ المصنف والتي لها أن تخضع هذه الحماية أو استعمالها لما تشاء من الشروط أو القيود أو الضوابط، لذا فقد جاء هذا المبدأ لمراقبة تداول المصنفات الذي نصت عليه المادة السابعة عشر من الاتفاقية، ليعطي للدول الحق في أن تتخذ ما تراه مناسبا من الأحكام والقيود والضوابط حفاظا على مصالحها العليا والنظام العام فيها، والتي قد تتعرض أحيانا للانتهاك جراء استعمال واستغلال المؤلفون لحقوقهم المقررة لهم على مصنفاتهم، إلا أن الدولة لا يمكنها بأي حال من الأحوال تجريد المؤلف من أي حق أو سلطة استئثارية تقرر له على مصنفه[28].

2-المصنفات المحمية والحقوق الواردة عليها

أفردت اتفاقية برن تعداداً لإبداعات فكرية باعتبارها مصنفات محمية طبقا للأحكام المقررة ضمنها، غير أنها لم تكن على سبيل الحصر وهو ما يستنبط من لفظ المادة الثانية التي تنصّ على: "**تشمل عبارة المصنفات الأدبية والفنية كل انتاج في المجال الأدبي والعلمي والفني أي كانت طريقة أو شكل التعبير عنه مثل الكتب والكتيبات وغيرها...**"، وذلك بهدف احتواء كل أنماط التعبير الفني الداخل في مفهوم الملكية الأدبية والفنية، كما

---

[26]- تنصّ على أنه: "**...لا يخضع التمتع أو ممارسة هذه الحقوق لأي إجراء شكلي، فهذا التمتع وهذه الممارسة مستقلان عن وجود الحماية في دولة منشأ المصنف. تبعا لذلك، فإن نطاق الحماية وكذلك وسائل الطعن المقررة للمؤلف لحماية حقوقه يحكمها تشريع الدولة المطلوب توفير الحماية فيها دون سواه، وذلك بصرف النظر عن أحكام هذه الاتفاقية...**".

[27]- **بن ديدي جميلة**، الحماية الوطنية والدولية للمصنفات الأدبية، مذكرة مكملة لنيل شهادة الماجستير في الحقوق، تخصص الملكية الفكرية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015-2016، ص 125.

[28]- **فتحي نسيمة**، مرجع سابق، ص 38.

عبرت نفس المادة في الفقرة الخامسة منها على أن المصنفات الأدبية لدوائر المعارف والمختبرات الأدبية التي تعتبر ابتكارا فكريا، بسبب اختيار وترتيب محتوياتها جديرة بالحماية دون المساس بحقوق مؤلفي المصنفات المتضمنة فيها[29].

ثانيا: اتفاقية المنظمة العالمية للملكية الفكرية بشأن حق المؤلف لسنة 1996

تم في إطار المنظمة العالمية للملكية الفكرية انعقاد هذه الاتفاقية[30] التي أتت مواكبةً للتطورات التكنولوجية التي يعرفها مجال الملكية الفكرية خاصة مع ظهور العديد من المصنفات المتداولة عبر الإنترنت الأمر الذي استوجب استحداث آليات جديدة تكفل حماية هذه المصنفات التي لم تتم معالجتها طبقا لمعاهدة "برن" والتي سوف نفصلها على النحو التالي:

1-الحماية المقررة وفق اتفاقية المنظمة العالمية للملكية الفكرية بشأن حق المؤلف لسنة 1996.

قصد بلوغ حماية أكفل –طبقا للمادة عشرون من اتفاقية برن– تعتبر اتفاقية الويبو بشأن حق المؤلف لسنة 1996 اتفاق خاص، فهي لا تخل بأي التزام أو حق من الحقوق المتضمنة في اتفاقية برن لارتباطها بها.

اعتمدت معاهدة الويبو من أجل مواجهة المشكلات الناجمة عن التكنولوجيا الرقمية والإنترنت خاصة، ما يعرف باسم جدول الأعمال الرقمي، المنصوص عليه في المادة الأولى منها، وذلك عبر قواعد مقررة لحق المؤلف بشأن تخزين المصنفات ونقلها عبر الأنظمة الرقمية، كما تطرقت الاتفاقية للمشكلات التي أثيرت حول اعتبار التثبيت على الدعامة

---

[29]– **بوزيدي أحمد التيجاني**، حماية حق المؤلف في إطار النشر الإلكتروني –دراسة مقارنة–، أطروحة لنيل شهادة دكتوراه علوم تخصص ملكية فكرية، كلية الحقوق، جامعة الجزائر 1، 2019/2018، ص 228.

[30]– تسمى كذلك معاهدة الإنترنت الأولى حيث اعتمدها المؤتمر الدبلوماسي للمنظمة العالمية للملكية الفكرية في 20 ديسمبر 1996، كما هناك معاهدة الإنترنت الثانية والتي تسمى كذلك معاهدة الويبو بشأن الأداء والتسجيل الصوتي والتي اعتمدت في نفس المؤتمر وبنفس التاريخ، لتفصيل أكثر أنظر: **عبد الله عبد الكريم عبد الله**، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دار الجامعة الجديدة، مصر، د س ن، ص 260 وما يليها.

الإلكترونية يعد من قبيل النسخ، وما إذا كان التحميل ولو للحظات محدودة لأحد المصنفات محل الحماية يعد انتهاكا لحقوق المؤلف أم لا، وكذا التساؤل حول وجوب استصدار الترخيص من صاحب الحق قبل القيام بذلك خاصة ما يتعلق بالنسخ الألكتروني للمصنفات[31].

2-الأمور المستحدثة في مجال حماية حقوق الملكية الفكرية طبقا لاتفاقية المنظمة العالمية للملكية الفكرية لسنة 1996:

اعتمدت اتفاقية المنظمة العالمية للملكية الفكرية لسنة 1996 على مبادئ وحقوق لم تكن موجودة من قبل خاصة في ظل اتفاقية "برن" وذلك سعياً منها إلى مواكبة التطور التكنلوجي الذي تعرفه شبكات الاتصال خاصة الإنترنت التي يتم تداول المصنفات الأدبية عبرها من جهة، ومن جهة أخرى فرض حماية ذات فعالية أكثر لها من مختلف الجرائم المرتكبة في هذا النطاق، ومن بين هذه الحقوق نذكر ما يلي:

أ- حق التأجير:

يتمتع مؤلفو المصنفات بالحق الإستئثاري في التصريح بتأجير النسخة الأصلية أو غيرها من نسخ مصنفاتهم للجمهور لأغراض تجارية، وهذه المصنفات هي:

- برامج الحاسوب.
- المصنفات السنمائية.
- المصنفات المجسّدة في تسجيلات صوتية.

يستثنى من ذلك حالتان تتلخصان فيما إذا تعلق الموضوع ببرنامج حاسوب ولم يكن البرنامج في حد ذاته هو موضوع التأجير الأساسي، أو إذا تعلق الموضوع بمصنف سينمائي، ما لم يكن ذلك التأجير قد أدى إلى انتشار نسخ ذلك المصنف بما يلحق ضررا ماديا بالحق الاستئثاري في الاستنساخ[32]

---

[31]- **بوزيدي أحمد التيجاني**، مرجع سابق، ص 232-234.

[32]- **عبد الله عبد الكريم عبد الله**، مرجع سابق، ص 265.

ب- حق نقل المصنف إلى الجمهور

نصّت اتفاقية المنظمة العالمية للملكية الفكرية لسنة 1996 لحماية حق المؤلف على حق نقل المصنف إلى الجمهور بالنسبة للمصنفات الموضوعة في موقع إلكتروني، بحيث يتمتع مؤلفوا المصنفات الأدبية والفنية بالحق الإستئثاري في التصريح بنقل مصنفاتهم إلى الجمهور بأي طريقة سلكية أو لا سلكية، بما في ذلك إتاحة مصنفاتهم للجمهور بما يمكن أفراد من الجمهور من الاطلاع على تلك المصنفات من مكان وفي وقت يختارهما، وذلك دون الإخلال بأحكام المواد ذات الصلة في اتفاقية برن[33].

ت- حدود الحقوق في بيئة الإنترنت

منحت المادة 2/10 من الاتفاقية للدول الأعضاء إمكانية اعتماد استثناءات وحدود على الحقوق بمناسبة النشر الإلكتروني للمصنفات الرقمية، فلدول الأخذ بالإستثناءات التي جاءت في اتفاقية برن وتكييفها وفق طبيعة الإنترنت بشرط عدم إضرارها وتعارضها مع الاستغلال العادي للمصنف وحقوق المؤلف[34].

ث- التدابير التكنولوجية للحماية والمعلومات الضرورية لإدارة الحقوق

من بين التدابير التكنولوجية التي أقرتها اتفاقية المنظمة العالمية للملكية الفكرية لسنة 1996 نذكر ما يلي:

- **الالتزامات المتعلقة بالتدابير التكنولوجية**

بدأت قواعد الملكية الفكرية منذ ظهور الإنترنت بالتغيّر الأمر الذي أثّر على قواعد هذه الاتفاقية، وتحديدا فيما يتعلق بالالتزامات الخاصة بالتدابير التكنولوجية[35]، وأوجبت هذه الاتفاقية على الأطراف المتعاقدة النص في قوانينها على حماية مناسبة وعلى جزاءات فعّالة ضد التحايل على التدابير التكنولوجية التي يستعملها المؤلفون عند ممارسة حقوقهم بناء

---

[33]- **فتحي نسييمة**، مرجع سابق، ص 111.

[34]- **بوزيدي أحمد التيجاني**، مرجع سابق، ص 237

[35]- **GAUTRAIS Vincent**, Neutralité technoloqique rédaction et interpritation des lois face aux changements technologique, les éditions Thémis, Canada, 2001, p 15.

على هذه المعاهدة والتي تمنع من مباشرة أعمال لم يصرح بها المؤلفون المعنيون أو لم يسمح بها القانون، فيما يتعلق بمصنفاتهم[36].

- **الإلتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق**

نصت المادة 12 من معاهدة الويبو بشأن حق المؤلف بأنه:

1-على الأطراف المتعاقدة أن تنص في قوانينها على جزاءات مناسبة وفعّالة توقع على أي شخص يعتدي على أي حق من الحقوق التي تشملها هذه المعاهدة أو اتفاقية برن أو يسهّل ذلك وهو يعلم:

- أن يحذف أو يغير دون إذن أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.
- وأن يوزع أو يستورد لأغراض التوزيع أو يذيع أو ينقل إلى الجمهور، دون إذن، مصنفات أو نسخا عن مصنفات مع علمه بأنه قد حذفت منها أو غيرت فيها، دون إذن؛ معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.

2-يقصد بعبارة "المعلومات الضرورية لإدارة الحقوق"، كما وردت في المادة 12، المعلومات التي تسمح بتعريف المصنف ومؤلف المصنف ومالك أي حق في المصنف، أو المعلومات المتعلقة بشروط الانتفاع بالمصنف، وأي أرقام أو شفرات ترمز إلى تلك المعلومات، متى كان أي عنصر من تلك المعلومات مقترنا بنسخة عن المصنف أو ظاهرا لدى نقل المصنف إلى الجمهور"[37].

---

[36]- **عبد الله عبد الكريم عبد الله**، مرجع سابق، ص 266.

[37]- يتبين من هذا النص ما استقرت عليه المعاهدة من بعد جدل طويل ونقاش مستعر أثناء العمل التحضيري، بالنظر إلى عدم جدوى النصوص الحمائية التقليدية التي أوردتها الاتفاقيات الدولية ومن بعدها النصوص التشريعية الوطنية في شأن حماية حقوق المؤلفين على مصنفاتهم، وذلك لما تتميز به المصنفات الرقمية والتي يتم نقلها وبثها عبر الشبكات وعلى وسائط رقمية من طبيعة خاصة تسهل نقلها والاعتداء عليها بغير إذن صاحب الحق فيها. أنظر في ذلك: **حسن الجميعي**، قضايا عالمية جديدة في مجال الملكية الفكرية، مداخلة مقدمة لندوة الويبو الوطنية حول الملكية الفكرية للمسؤولين الحكوميين وأعضاء غرف التجارة، المنظمة من طرف المنظمة العالمية للملكية الفكرية، بالتعاون مع وزارة الصناعة والتجارة، بتاريخ 10 و11 جوان 2004، صنعاء، ص 13.

- **أحكام تتعلق بإنفاذ القانون**

تتعهد الأطراف المتعاقدة بأن تتخذ، وفقا لأنظمتها القانونية، التدابير اللازمة لضمان تطبيق هذه المعاهدة كما تكفل الأطراف المتعاقدة أن تتضمن قوانينها إجراءات إنفاذ تسمح باتخاذ تدابير فعالة ضد أي تعد على الحقوق التي تغطيها هذه المعاهدة، بما في ذلك توقيع الجزاءات العاجلة لمنع التعديات والجزاءات التي تعد رادعا لاعتداءات أخرى[38].

الفرع الثالث

جهود منظمة التعاون والتنمية الإقتصادية لمكافحة الجريمة المرتكبة عبر الإنترنت

لعبت منظمة التعاون والتنمية الإقتصادية، منذ منتصف السبعينات من القرن الماضي دورا أساسيا في تعزيز احترام الحق في الخصوصية، كقيمة أساسية، وشرط لضمان التدفق الحر للبيانات الشخصية عبر الحدود، فأقرت قواعد إرشادية لحماية هذا الحق، والحركة الحرة لتدفق البيانات[39]، حيث سنبين أهم تطورات هذه القواعد وفق تدرج زمني.

تهدف هذه المنظمة إلى تحقيق النمو الإقتصادي لأعضائها، حيث وضعت هذه المنظمة سنة 1978 قواعد إرشادية من أجل حماية الخصوصية ونقل المعطيات وأوصت الأعضاء بالالتزام بها، تغطي الأشخاص الطبيعيين فقط وتطبق على القطاعين العام والخاص، وتتعلق بالمعطيات المتعلقة بالمعالجة الآلية أو غير الآلية[40].

سعت منظمة التعاون والتنمية الإقتصادية إلى حل الإشكال الخاص بحماية الحياة الخاصة وذلك عن طريق محاولة إيجاد توازن عادل بين الحق في حماية الحياة الخاصة من جهة، وحرية نقل المعلومة من جهة أخرى، الأمر الذي أدى بها إلى إصدار توجيهات تم

---

[38]– **عبد الله عبد الكريم عبد الله**، مرجع سابق، ص 267.

[39]- **منى الأشقر جبور**، **محمد جبور**، البيانات الشخصية والقوانين العربية الهمّ الأمني وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، 2018، ص 51.

[40]- **BELABED Amine**, La protection de la vie privée sur internet, Thèse pour l'obtention du diplôme de doctorat en sciences, spécialité: informatique, departement d'informatique, faculté des sciences, université de Tlemcen, 2018, p 15.

اعتمادها من طرف مجلس المنظمة في سبتمبر 1980، ومن خلاله كل الأعضاء فيها إلا إرلندا فقد امتنعت عن اعتماد هذه التوجيهات.

تمثلت التوجيهات التي وضعتها المنظمة في هذا المجال في خمسة محاور هي:

- التعريف بموضوع التوجيهات[41].
- أهم المبادئ الأساسية الواجب تطبيقها على المستوى الوطني[42].
- أهم المبادئ الأساسية الواجب تطبيقها على المستوى الدولي.
- تفعيل المبادئ على المستوى الوطني من خلال تفعيل المؤسسات الإدارية والقضائية من أجل حماية الحريات.
- تطوير التعاون الدولي بين الدول الأعضاء فيما يخص تبادل المعلومات والمساعدة المتبادلة[43].

بدأت المنظمة بمطلع سنة 1983 بالاهتمام بظاهرة الجريمة المعلوماتية، حيث تم عقد عدة اجتماعات لمناقشة هذه الظاهرة، وفي سبتمبر من عام 1985 شكلت لجنة لدراسة الجريمة المعلوماتية قامت بإجراء مسح لهذه الجريمة في الدول الأعضاء من خلال إعداد

---

[41]- **HANS-PETER Gassmann**, « **Ver un cadre juridique international pour l'informatique et autres technique nouvelles de l'information** », annuaire de droit international, volume 31, 1985, p 749.

[42]- تتضمن التوجيهات المبادئ الثمانية الرئيسية للحق في حماية المعطيات الخاصة، وهذه المبادئ هي تحديد عمليات جمع المعطيات الاقتصار على طبيعة المعطيات الشخصية وتحديدها وتحديد الغرض وحصر الاستخدام بالغرض المحدد وتوفير وسائل حماية وأمن المعلومات والعلانية والحق في المشاركة، أنظر في ذلك: **بوكر رشيدة**، الحماية= =الجزائية للتعاملات الإلكترونية، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2017، ص ص 88-89.

[43]- **HANS-PETER Gassmann,** op-cit, p 750.

مقارنة لقوانين هذه الدول، وقد أسفر عمل تلك اللجنة عن صدور تقرير نشر عام(1986 تحت عنوان **(جرائم الحاسب الآلي تحليل للأنظمة القانونية المختلفة)**[44].

أوصت اللجنة في تقريرها الدول الأعضاء بضرورة مواجهة المشكلات الناجمة عن الجريمة المعلوماتية من خلال قوانينها الداخلية، وكان يهدف إلى تحقيق ثلاثة أهداف رئيسية، هي:

1-تسهيل تبادل المعلومات فيما بين الدول بالنسبة لمفهوم الجريمة المعلوماتية وحجمها في كل منها.

2-التعرف على سياسة كل دولة على حدة في التعامل مع الجريمة المعلوماتية.

3-محاولة الوصول إلى فهم مشترك لمفهوم الجريمة المعلوماتية من ناحية، وكيفية مواجهة القانون لها من ناحية أخرى[45].

أنشأت في عام 1990 لجنة سياسة الإعلام والمعلومات والاتصالات فريقا من الخبراء لإعداد وصياغة مجموعة من المبادئ التوجيهية التي تحكم أمن المعلومات، والتي اعتمدت من طرف مجلس منظمة التعاون والتنمية الإقتصادية في عام 1992، من أجل محاربة هذه التهديدات، قررت الدول وصف هذه الأعمال الخبيثة والرد عليها بطرق متنوعة، فعلى الصعيد الدولي، تم تحديد الحد الادنى الأساسي من الجرائم السيبرانية التي تدخل في نطاق القانون الجنائي الوطني، وعلى مستوى الدول الاعضاء في منظمة التعاون والتنمية الإقتصادية، وعلى مدى السنوات العشرين الماضية، حدث تطور في التشريعات المتعلقة بالجريمة الحاسوبية وحماية البيانات[46].

---

[44]- **خالد بن عبيد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 117-118.

[45]- **خالد بن عبيد الله بن معيض العبيدي**، مرجع سابق، ص ص 117-118.

[46]- **بن قارة مصطفى عائشة، « الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية »**، المجلة العربية للعلوم ونشر الأبحاث، المركز القومي للبحوث، فلسطين، المجلد الثاني، عدد 5، يونيو 2016، ص 43.

تمت مراجعة عدد من المبادئ التوجيهية المتعلقة بمكافحة الجريمة الإلكترونية، وذلك في عام 1997[47]، وتم تحديثها في عام 2001 من طرف مجموعة ثانية من الخبراء شكلتها لجنة سياسة الإعلام والمعلومات والاتصالات، وفي 2002 تم إصدار صيغة جديدة بعنوان "**المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية من أجل أمن نظم وشبكات المعلومات**"، وتم اعتمادها كتوصية من مجلس المنظمة، وتحتوي هذه المبادئ التوجيهية على تسعة مبادئ تكميلية **(التوعية، المسؤولية، رد الفعل، الأخلاقيات، الديمقراطية، تقييم المخاطر، تصور وتنفيذ الأمن، إدارة الأمن، وإعادة التقييم)**[48].

أما في عام 2005 نشرت المنظمة تقريرا يحلل آثار الرسائل الاقتحامية على البلدان النامية، ويظهر هذا التقرير أن مشكل البريد المزعج أشد خطرا في البلدان النامية منه على البلدان الغربية، إذ أن موارد تلك البلدان محدودة وأعلى تكلفة مما هي عليه في غيرها من البلدان.

استجابة لطلب فريق التخطيط الاستراتيجي للمكتب التنفيذي للأمن العام للأمم المتحدة بشأن إعداد عرض مقارن للحلول التشريعية الداخلية في مجال استخدام الإنترنت لأغراض إرهابية، قامت منظمة التعاون التنمية الإقتصادية عام 2007، بنشر تقرير عن تعامل المشرع مع مسألة الإرهاب السيبراني في التشريعات الداخلية للدول[49].

نشرت المنظمة في 17 يناير 2011[50]، تحليلا لمخاطر وأثر الهجمات الإلكترونية، ويعرض التقرير المنشور نبذة تاريخية عن هذه الظاهرة، وبيان مخاطرها، ثم يقدم سلسلة من التوصيات الموجهة للدول، ويوصي هذه الدول بتحسين نظم الأمن الخاصة بها والتي تندرج ضمن مجال يلتقي فيه الأمن المدني بالدفاع العسكري، ويقترح التقرير كذلك إقامة شراكات

---

[47]- Recommandation du conseil relative aux lignes directrices régissant la politique de cryptographie adoptée par le conseil lors de la 895 éme session, le 27 mars 1997, C/M (97) 6/prov.

[48]- La recommandation du conseil concernant les lignes directrices régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité C(2002) 131/final.

[49]- **ليلى القجيري**، الدليل العلمي للمخاطر المرتبطة بجرائم الإنترنت المحدقة بالطفل، منشورات المنظمة الإسلامية للتربية والعلوم والثقافة، الرباط، 2012، ص ص 91-92

[50]- La recommandation du conseil sur les principes pour l'élaboration des politiques de l'internet C(2011) 154.

بين القطاعين العام والخاص، وتطوير التعاون الدولي في هذا المجال، وكانت التوصية الرئيسية تتعلق بأن ينظر إلى مكافحة الجريمة الإلكترونية بكونه أمرا لا يقتصر على إعمال الإمكانيات التقنية فقط، بل أن يقتضي كذلك إعمال البحث والتربية على هذه المخاطر[51].

اعتمد مجلس وزراء منظمة التعاون والتنمية الإقتصادية بتاريخ 11 جويلية 2013 المبادئ التي أعيد النظر فيها من طرف المنظمة سنة 2011، حيث جاءت أهم التعديلات متمثلة في تقوية المسؤولية الخاصة بالمؤسسات التي تعنى بحماية الأنظمة المعلوماتية، وضرورة تسهيل التعاون العابر للحدود الوطنية[52].

المطلب الثاني

جهود التكتّلات الإقليمية في مكافحة الجريمة المرتكبة عبر الإنترنت

كان للجهود المبذولة من طرف المنظمات الدولية في مجال مكافحة الجريمة المرتكبة عبر الإنترنت عدة اسقاطات على المستوى الإقليمي، فالاستعمال المتزايد لتكنولوجيا الإعلام والاتصال من طرف المجرمين جعل منها جريمة أكثر تعقيدا وفداحة من حيث الخسائر بالمقارنة مع الجرائم التقليدية، الأمر الذي استوجب وضع حلولا قانونية على المستوى الإقليمي وذلك تماشيا مع الجهود المبذولة على المستوى الدولي، لأن الجهود الدولية تبقى غير فعالة إذا اعتبرت أنها الآلية الوحيدة لمكافحة هذه الجريمة، لهذا كان لابد من تمرير هذه المجهودات الدولية إلى إقليمية من أجل وضع إطار قانوني أعم وأشمل لمكافحة هذه الظاهرة الإجرامية المستحدثة، ومنه سوف نتطرق إلى الجهود المبذولة على مستوى الاتحاد الأوروبي **(فرع أول)**، ثم إلى الجهود المبذولة على المستوى العربي **(فرع ثان)**، وكذلك جهود الاتحاد الإفريقي **(فرع ثالث)**.

---

[51]– **ليلى القجيري**، مرجع سابق، ص93.

[52]- **BERSET-BIRCHER Valerie**, Les systèmes d'information et la vie privée du salarié: analyse en droit européen, en droit suisse et en droit français, thèse en vue de l'obtention du grade de docteur en droit privé, faculté de droit, de sciences politiques et gestion, Université de Strasbourg, 2013, p p 192-193.

الفرع الأول

جهود الاتحاد الأوربي في مكافحة الجريمة المرتكبة عبر الإنترنت

تعتبر دول الاتحاد الأوروبي من الدول السباقة في مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك في إطار ما يسمى بمجلس أوروبا حيث حرص هذا الأخير على مكافحة الاستخدام غير المشروع للحاسب الآلي وشبكاته بداية سبعينيات القرن الماضي، وذلك من خلال اتخاذ عدة جهود منها عقد اتفاقيات يمكن اعتبارها كنموذج يحتذى به في إطار مكافحة هذه الجريمة المستحدثة، وسوف نتطرق في هذا السياق إلى اتفاقية مجلس أوروبا (اتفاقية سترسبورغ) **(أولا)**، ثم إلى اتفاقية بودابست لسنة 2001 **(ثانيا)**

أولا: اتفاقية مجلس أوربا (اتفاقية ستراسبورغ)

أطلق على اتفاقية مجلس أوروبا اسم الاتفاقية رقم 108 لعام 1981 بشأن حماية الأفراد فيما يتصل بالمعالجة الآلية للبيانات الشخصية[53]، وقد ركزت هذه الاتفاقية على مسألة قواعد نقل البيانات خارج الحدود وضمان حمايتها خصوصا أمام التطور العلمي الحاصل في تكنولوجيا المعلومات وازدياد استخدامها في أعمال الإدارة المختلفة سواء في القطاع العام أو القطاع الخاص، مما سهل توسيع دائرة معالجة البيانات على نطاق عالمي، لذلك كرست الاتفاقية ضرورة حماية هذه البيانات وحصول صاحبها على نفس الحماية المقررة في بلده قصد توسيع الحماية إلى كل رقعة جغرافية تنتقل إليها هذه البيانات، تجنبا لهدر مستخدميها لقواعد الحماية عند نقل عمليات المعالجة لدول تفتقر لقواعد الحماية أو تضعف عندها[54].

---

[53]- La convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été conclue à Strasbourg le 28 janvier 1981 dans le cadre du conseil de l'europe, voir **Métille**: **Sylvain**, mesures techniques de surveillance et respect des droits fondamantaux en particulier dans le cadre de l'istruction pénale et de reseignement, thèse de doctorat, faculté de droit, université de neuchatel, Bale, 2010, p 96.

[54] – **بشان عبد النور**، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2018/2017، ص 264.

تغطي قواعد الاتفاقية مسائل نقل وتبادل المعطيات بين الدول المتعاقدة، كما تمنع نقل المعطيات إلى خارج الحدود ما عدا الدولة التي توفر لها حماية موازية، مع استثناءات من هذه القاعدة، ثم أن مجلس أوربا من خلال لجنة الخبراء العاملة في حقل حماية المعطيات، قد أصدر سلسلة من الدلائل التوجيهية المعتمدة على الاتفاقية وتتعلق بـ: حماية المعطيات الطبية المؤتمنة، الاحصائيات، قاعدة المعلومات الخاصة للأغراض التسويق، قاعدة المعلومات الخاصة لأغراض الضمان الاجتماعي أو لآغراض البوليس والمعطيات الجنائية وقواعد المعلومات الخاصة بأغراض التوظيف وكذلك خدمات الاتصال[55].

ثانيا: اتفاقية بودابست

وضعت هذه الاتفاقية سنة 2001 ودخلت حيز التنفيذ سنة 2004، ويطلق عليها تسمية اتفاقية بودابست نسبة لمكان انعقادها في العاصمة المجرية[56]، وقد جاءت تتويجا للجهود التي بذلها المجلس الأوروبي في سبيل التوصل إلى وضع إطار اتفاقي فعال لمكافحة الجرائم المعلوماتية[57]، ومن أهم الدول التي وقعت عليها خارج دول الإتحاد الأوروبي نذكر جنوب إفريقيا، اليابان والولايات المتحدة الأمريكية، والملاحظ حول هذه الاتفاقية أنها اتفاقية إقليمية المنشأ عالمية التطبيق، حيث أن لأول مرة في تاريخ أوروبا يفتح باب التوقيع لدول تقع خارج الاتحاد الأوروبي.

تنبع أهمية هذه الإتفاقية كونها اتفاقية تهدف إلى توفير إطار دولي مشترك للتعامل مع الجرائم الإلكترونية[58]، حيث تلتزم الدول الموقعة عليها بتعديل تشريعاتها لمواجهة التحديات

---

[55] – نقلا عن: **بوكر رشيدة**، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص 89.

[56]- **BERTHELET Pierre,**« **La lutte contre la cybercriminalité à l'échelle de l'union: Analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels**», revue québécoise de droit international, hors-série, novembre 2018, p 29.

[57]- **HARIVEL Jean**, Libertés publiques, libertés individuelles risques et enjeux de la société numérique, Thèse de droit public, Ecole doctorale de droit de la sorbonne, Université Paris 01 panthéon sorbonne, 2018, p 306.

[58]– ترمي الاتفاقية بشكل أساسي إلى: 1– مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية، 2– والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائيا علاوة على الجرائم الأخرى التي ترتكب عن طريق الكمبيوتر أو التي تكون الأدلة المتصلة بها في

التي تفرضها تكنلوجيا المعلومات إذ تولت تحديد الجرائم المعلوماتية، واعتماد أدوات إجرائية لمكافحة الجريمة المعلوماتية وضبط مرتكبيها[59].

وقد تضمنت الاتفاقية الأقسام التالية:

1-**الفصل الأول:** تحديد المصطلحات، حيث جاء فيه تعريفات بنظام الكمبيوتر، ومقدم الخدمة، وبيانات الحركة عبر شبكات الاتصال.

2-**الفصل الثاني:** الخطوات الواجب اتخاذها في إطار التشريع الوطني[60].

أ- القسم الأول: حيث تطرق إلى القانون الجنائي الموضوعي، وكذلك إلى السلوكيات التي يجب اعتبارها جريمة جنائية، لهذا نجد أن الاتفاقية جاءت تغطي مجموعة كبيرة من الجرائم الجنائية حيث تشمل بالتحديد:

أ/1- الجرائم ضد سرية وسلامة وتوافر بيانات الكمبيوتر وانظمته والذي يطالب بتجريم الدخول غير المشروع والاعتراض غير المشروع والتدخل في البيانات والأنظمة، وإساءة استخدام الاجهزة.

أ/2- الجرائم المرتبطة بالكمبيوتر، وهي التزوير والاحتيال المرتبط بالكمبيوتر.

أ/3- الجرائم المرتبطة بالمحتوى، وهي الجرائم المرتبطة باستغلال الأطفال في انتاج مواد إباحية.

أ/4- الجرائم المرتبطة بانتهاك حق الطبع والحقوق ذات الصلة[61].

الشكل الإلكتروني، 3- وإلى إرساء نظام سريع وفعال للتعاون الدولي، أنظر في ذلك: التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، المؤرخ في 23 نوفمبر 2001، بودابست، ص 04.

[59] - **شوقي يعيش تمام، عزيزة شبري، « تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية »**، مجلة الإجتهاد القضائي، مخبر أثر الإجتهاد القضائي على حركة التشريع، العدد 15، جامعة محمد خيضر بسكرة، سبتمبر 2017، ص 98.

[60]-**Département fédérale de justice et police,** Approbation et mise en œuvre de la convention du conseil de l'europe sur la cybercriminalité, avant-projet et rapport explicatif, office fédéral de la justice, Berne, 2009, p 7.

ت- **القسم الثاني:** قانون الإجراءات: ويتناول التدابير التي تتخذ لإجراء تحقيقات أكثر فعالية فيما يتعلق بجرائم الإنترنت[62]، ويجب التأكيد على هذه التدابير الإجرائية يمكن استخدامها مع أية جرائم جنائية يشترك فيها نظام الكمبيوتر[63].

3-**الفصل الثالث: التعاون الدولي.**

يعتبر التعاون الدولي أمر هام جدا في مجال مكافحة جرائم الإنترنت وبدونه لن يكون هناك أثر لأي مجهود تقوم به أي من الدول بمفردها لأنه سوف يكون عديم الفائدة، ولن يؤدي إلى الحد من ارتكاب تلك الجرائم التي تكون في الاغلب الأعم عابرة للحدود[64].

جاءت الإتفاقية بأحكام أكثر تفصيلا فيما يتعلق بالتعاون الدولي[65]، حيث نصت عليها المواد من 23 إلى 35[66]، وتتعلق هذه الأحكام بالمبادئ العامة والخاصة التي تحكم المساعدة القضائية[67] وتسليم المجرمين[68]، حيث تحث الاتفاقية كل الدول الأطراف على

---

[61] – **خالد محي الدين أحمد**، الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص 41.

[62]- **PAYE Jean-Claude**, Lutte antiterroriste et contrôle de la vie privée, revue-multitudes, n° 11, vol 1, 2003, p 93, disponible en ligne à l'adresse, https://www.cairn.info/revue-multitudes-2003-1-page-91.htm

[63] – **كريستينا سكولمان**، المعايير الدولية المتعلقة بجرائم الإنترنت (مجلس أوربا)، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص 63.

[64] – **فيصل كامل نجم الدين**، مرجع سابق، ص 24.

[65]- **TYRODE Jean-françois**, Elements de procedure penale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen, mémoire master droit de l'internet public-administration-entreprises, Université Paris 01 Panthéon-sorbonne, 2006/2007, p 58.

[66]- أنظر الاتفاقية المتعلقة بالجريمة الإلكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية –رقم 185، المنعقة ببودابست بتاريخ 2001/11/23.

[67]– تنصّ المادة 25 فقر 1 من اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية على: "**يقوم الأطراف بتقديم المساعدات المتبادلة لبعضهم البعض إلى أقصى حد ممكن وذلك لأغراض التحقيق أو الإجراءات المتعلقة بالجرائم ذات العلاقة بنظم وبيانات الكمبيوتر، أو جمع أدلة الجريمة في شكل إلكتروني**".

[68]– تنصّ المادة 24 فقرة 1 من اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية على: "**تطبق هذه المادة على تسليم المجرمين فيما بين الأطراف بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من هذه الاتفاقية، بشرط أن تكون هذه الجرائم يعاقب عليها بموجب قوانين كلا الطرفين المعنيين، بعقوبة مقيدة الحرية لمدة سنة على الأقل، أو بعقوبة أشد**".

إعطاء إجراء المساعدة القضائية أوسع الإمكانيات لغاية الحصول على الدليل الإلكتروني المثبت للجريمة الإلكترونية كما توصي الاتفاقية بإبرام اتفاقيات ثنائية بين الدول الأعضاء حول تسليم المجرمين، على أنه يمكن اعتبار هذه الاتفاقية كقاعدة قانونية لتسليم مجرمي المعلوماتية في الحالة التي لا يوجد فيها معالجة لنظام التسليم بين الدول الموقعة، ومن جهة أخرى إذا كانت الدولة الطرف لا تشترط وجود معاهدة لتسليم المجرمين فيمكنها أن تعتبر الجرائم المنصوص عليها في هذه الاتفاقية كجرائم قابلة لتسليم المجرمين[69].

4-**الفصل الرابع:** الشروط النهائية حول الانضمام إلى الاتفاقية، حيث يهتم هذا الفصل على وجه الخصوص بالدول غير الأوروبية، كما ينص على سبل انضمام الدول غير الأعضاء إلى الاتفاقية[70].

الفرع الثاني

جهود جامعة الدول العربية في مكافحة الجريمة المرتكبة عبر الإنترنت

تمّ توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من طرف الدول العربية[71]، وذلك بعد اقتناعهم بضرورة تعزيز التعاون فيما بينها لمكافحة هذا النوع الحديث من الجرائم التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وأيضا بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد الجرائم التقنية بصفة عامة وجرائم الإنترنت بصفة خاصة، حيث تهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[72].

---

[69] – **بن خليفة إلهام**، مرجع سابق، ص 334.

[70]- **MATIGNON Emmanuelle**, La cybercriminalité un focus dans le monde des télécoms, Mémoire master droit du numérique administrations-entreprises de l'école de droit de la Sorbonne, Université Paris 1 Panthéon-Sorbonne, 2011/2012, p 34.

[71] – صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بمقتضى مرسوم رئاسي رقم 14-252 مؤرخ في 08 سبتمبر سنة 2014، ج.ر عدد 57، صادر في 28 سبتمبر سنة 2014.

[72] – **حاج مخناش نوال**، « **التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الإتمان** »، مجلة العلوم القانونية والسياسية، المجلد 10، العدد01، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، ص1127.

تتجلى أولى الجهود التي بذلتها جامعة الدول العربية بمقتضى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في أنها حاولت حصر هذه الجرائم ضمن نطاق قانوني، يتضمن أهم صور التجريم التي انتهجتها هذه الاتفاقية **(أولا)**، ثم النص على الجرائم المتصلة بالحاسوب **(ثانيا)**، وكذلك الجرائم المتصلة بالاستخدام غير المشروع لأدوات الدفع الإلكتروني **(ثالثا)**، بالإضافة إلى تبيان أشكال الشروع والاشتراك مع تحديد المسؤولية التي تقع على عاتق مرتكب هذا النوع من الجرائم **(رابعا)**، وتحديد قواعد الاختصاص **(خامسا)**.

أولا: تجريم المساس بسرية وسلامة البيانات وإتاحة البيانات والنظم المعلوماتية

تتمثل الجرائم الماسة بسرية وسلامة البيانات بمقتضى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في:

1-جريمة الدخول غير المشروع

يعرف الدخول أو الاتصال غير المشروع[73] بأنه: "**الولوج والاتصال بكل أو جزء من نظام أو شبكة تقنية المعلومات دون رضا المسؤول عن النظام، أو هو الولوج والوصول إلى المعلومات والمعطيات المخزنة داخل تقنية المعلومات للاطلاع عليها أو لمجرد التسلية أو إشباع الشعور بالنجاح في اختراق الحاسب الآلي**"[74].

---

[73]- تنصّ المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على النحو التالي: "**1- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.**

2-تشديد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

-الحصول على معلومات حكومية سرية".

[74]- **أحمد حمي، كيسي زهيرة، « صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014 »**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 10، العدد01، ص 781.

2-جريمة الاعتراض غير المشروع

وضّحت المادة السابعة من الاتفاقية الاعتراض على أنه: "**الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات**"

3-جريمة الاعتداء على سلامة البيانات

حصرت المادة الثامنة من الاتفاقية جرائم الاعتداء على سلامة البيانات في تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق[75].

4-جريمة إساءة استخدام وسائل تقنية المعلومات

حددت المادة التاسعة من الاتفاقية جريمة إساءة استخدام وسائل تقنية المعلومات في حالتين هما:

1-إنتاج أو بيع أو شراء او استيراد او توزيع أو توفير:

أ-أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المواد من السادسة إلى الثامنة.

ب-كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأي من الجرائم المبينة في المواد من السادسة إلى الثامنة.

2-حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغاية ارتكاب أي من الجرائم المذكورة في المواد من السادسة إلى الثامنة.

---

[75]- استلزمت هذه المادة بمقتضى الفقرة الثانية منها لكي تقوم الدول الأطراف فيها بتجريم الأفعال المذكورة في الفقرة الأولى أن تسبب هذه الأخيرة أضرارا جسيمة، وفي نظرنا أنه ما يعاب على هذا الشرط أن الاتفاقية لم تحدد معنى الضرر الجسيم أي ماهية المعايير التي بمقتضاها يتم تحديد الضرر الجسيم من جهة، ومن جهة أخرى أغفلت معيار الخطورة التي تتميز بها هذه الأفعال خاصة إذا وقعت على مصالح أساسية للدول.

ثانيا: الجرائم المتصلة بالحاسوب

تنصّ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على تجريم الأفعال التي لها صلة بالحاسوب كجرائم التزوير وجريمة الاحتيال، والتي نبينها على النحو التالي:

1-جريمة التزوير

عرفت المعاهدة جريمة التزوير من خلال المادة الحادية عشر على أنه: استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

2-جريمة الاحتيال

لايوجد تعريف محدد لجريمة الاحتيال المعلوماتي، وقد حاولت منظمة التعاون والتنمية الاقتصادية تعريف الاحتيال بأنه كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها[76].

عرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في نص المادة الحادية عشر جريمة الاحتيال بأنها: التسبب بإلحاق ضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير عن طريق:

- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات
- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغيرها.
- تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

[76] – **أحمد حمي، كيسي زهيرة**، مرجع سابق، ص784. أنظر كذلك: **موفق علي عبيد، ساهر ماضي ناصر، «ماهية جريمة الاحتيال المعلوماتي»**، مجلة جامعة تكريت للعلوم القانونية، السنة 07، العدد 25، سنة 2015.

ثالثا: الجرائم المتصلة بالاستخدام غير المشروع لأدوات الدفع الإلكتروني

حددت المادة الثامنة عشر من الاتفاقية الحالات التي تعتبر استخدام غير مشروع لأدوات الدفع الإلكتروني على النحو التالي:

- كل من زوّر أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.
- كل من استولى على بيانات أي أداة من أدواة الدفع واستعملها أو قدمها للغير أو سهل للغير الحصول عليها.
- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك[77].

رابعا: تحديد أحكام الشروع والاشتراك والمسؤولية الجزائية

بيّنت نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أحكام الشروع والاشتراك في هذا النوع من الجرائم، كما حددت نطاق المسؤولية الجزائية فيها سواء للشخص الطبيعي أو المعنوي بالإضافة إلى إقرار حالات تشديد العقوبة على مرتكب هذه الجرائم، وسوف نوضح ذلك على النحو التالي:

1-الشروع والاشتراك في ارتكاب الجرائم

بينت الاتفاقية ماهية الشروع والاشتراك في جرائم تقنية المعلومات بمقتضى المادة التاسعة عشر وذلك على النحو التالي: الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف، الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية[78].

---

[77]- أنظر المادة (18) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة عن الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، بتاريخ (2010/12/21)، متوفر عبر الشبكة القانونية العربية: www.arablegalnet.org

[78]- الملاحظ في هذه المادة أنها قد أجازت للدول الأطراف بمقتضى الفقرة الثالثة منها لأي دولة الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا، وفي نظرنا أن هذا الاستثناء هو عبارة عن ترك مجال من الحرية من

2-المسؤولية الجنائية للاشخاص الطبيعية والمعنوية

تلتزم كل دولة طرف طبقا لنص المادة عشرون، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الاخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا.

3-تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات

نصت الاتفاقية على هذا الإجراء في المادة واحد والعشرون، حيث تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات[79]

خامسا: تحديد الإختصاص

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على قواعد الاختصاص في الفصل الرابع منها والمتعلق بالتعاون القانوني والتقني بمقتضى المادة ثلاثون، حيث نلاحظ باستقرائنا هذه المادة أنها لم تخرج عن قواعد الاختصاص المعروفة، وذلك باتخاذها لمبدأ الإقليمية كمبدأ أصيل في تحديد الاختصاص، ثم تلتها بالمبادئ الاحتياطية والمتمثلة في مبدأ الشخصية ومبدأ العينية دون الإشارة إلى مبدأ العالمية، بالإضافة إلى ذلك فإن الحلول التي قدمتها المادة سالفة الذكر فيما يخص تنازع الاختصاص، لم تأت بجديد يذكر بل اكتفت بتقديم وإعادة صياغة الحلول المتعلقة بتنازع الاختصاص الإيجابي والسلبي المتعارف عليها في القواعد القانونية التقليدية[80].

طرف المشرع العربي للدول الأطراف في تحديد ماهية الشروع في الجرائم طبقا لقوانينها الداخلية من جهة، ومن جهة أخرى حصر كل دولة للجرائم التي يعاقب عليها في الشروع بارتكابها.

[79] – **شرف الدين وردة، بشير سليم، « حل مشكلة تنازع الاختصاص الدولي في مجال مكافحة جرائم التجارة الإلكترونية »**، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، بسكرة، المجلد 05، العدد 01، 2019، ص 126.

[80]– تنصّ المادة (30) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على: "**1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت:**

- في إقليم الدولة الطرف.

يمكننا على ضوء قراءة التجربة العربية في التعامل مع العصر الرقمي واحتياجاته التشريعية، أن نلاحظ تخبطا في التعامل مع المتطلبات التشريعية لتقنية المعلومات، وهو أشبه بحالة التخبط التي شهدتها النظم المقارنة في مطلع السبعينات وخلال الثمانينات، ولا تزال تشهد بعضا من ملامحه في عدد من مسائل تقنية المعلومات في الوقت الحاضر.

يلمس المتابع في هذا السياق عدم وضوح الرؤية، ويلمس اتجاه المؤسسات التشريعية في الدول النامية بصفة عامة إلى حلول ناقصة وليست حلولا كافية تدرك التحديات التقنية ذاتها وتدرك حالة التغير والتطور في الاحتياجات القانونية لمواجهة العصر الرقمي، وتدرك أكثر أن الحلول المقتبسة دون إعادة تواؤم واعي ومدروس على الاقل حلول معطلة وليست فاعلة لاعتبارات اجتماعية وسياسية واقتصادية وقانونية، حتى أننا لا نكون مبالغين إن قلنا أن هذه الحلول الجزئية المقتبسة تزيد التحديات ولا توفر حلولا لها، كما أنها في بعض الأحيان تقيم مزيدا من العوائق نحو الأهداف النبيلة في خطط توظيف التقنية بدلا من أن تذلل هذه العوائق[81].

- على متن سفينة تحمل علم الدولة الطرف.

- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة 1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف و لا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم".

[81] – **سعيداني سلامي**، المرجع السابق، ص 203.

الفرع الثالث

جهود الإتحاد الإفريقي في مكافحة الجريمة المرتكبة عبر الإنترنت

سعت دول الاتحاد الإفريقي إلى مواكبة الحركية التشريعية المتسارعة على المستوى الدولي والإقليمي في مجال المعلوماتية، وذلك إدراكا منها

أن القارة الإفريقية لن تكون بمعزل عن مخاطر الجرائم المرتكبة عبر الإنترنت، فرغم أن هذه الجهود قليلة نسبيا مقارنة بالعالم المتقدم في هذا المجال، إلا أنها تبقى كمظهر لنية الاتحاد الإفريقي في مكافحة هذا النوع المستحدث من الجرائم، ولعل من بين أهم الجهود المبذولة من طرف دول الاتحاد الإفريقي موافقتهم على وضع الاتفاقية الإفريقية لمكافحة الاجرام المعلوماتي والتي نستهل دراستها من حيث نطاقها **(أولا)**، ثم أهم قواعدها **(ثانيا)**، بالإضافة إلى تبيان دور الشرطة الإفريقية كمظهر من مظاهر التعاون الأمني الإفريقي **(ثالثا)**.

أولا: نطاق اتفاقية الاتحاد الإفريقي لمكافحة جرائم الإنترنت

وافق رؤساء الاتحاد الإفريقي في جوان من عام 2014 على اتفاقية تاريخية تؤثر على كثير من مناحي الحياة الرقمية، والتي نتخذها كنموذج للسياسة التشريعية للاتحاد الافريقي في مكافحته لجرائم الإنترنت.

تغطي هذه الاتفاقية نطاقاً واسعاً جدا من الأنشطة على الإنترنت، متضمن التجارة الإلكترونية، حماية البيانات، الجرائم الإلكترونية، مع تركيز خاص على العنصرية وكراهية الأجانب، استغلال الأطفال في المواد الإباحية، الأمن السيبراني الوطني، إن نفذت هذه الاتفاقية فإن العديد من الدول الإفريقية ستسن قوانين لحماية البيانات الشخصية لأول مرة، مؤيدة من قبل سلطات عامة جديدة ومستقلة، وهي تحركات من شأنها أن تمثل هدية كبيرة لسيطرة المستخدم على البيانات الشخصية بالإضافة إلى أنه سيطلب من كل دولة وضع استراتيجية وطنية للأمن السيبراني، وتمرير قوانين الجرائم الإلكترونية، والتأكد من أن التجارة الإلكترونية تمارس بحرية.

تمثل هذه الاتفاقية قفزة إلى الأمام في تنظيم التعاملات في مجال تكنولوجيا الإعلام والاتصال خاصة وأن القارة الإفريقية تعرف انطلاقة من الاعتماد على التكنولوجيا السلكية نحو الاتصال عبر الإنترنت، هذا التغيير لن يحدث بين عشية وضحاها وذلك لأن الاتفاقية يجب أن يصادق عليها من قبل خمسة عشر دولة لتدخل حيز التنفيذ[82]، وحتى ذلك الحين فمن المرجح أن تكون هناك مدة زمنية قبل أن تمرر أربعة وخمسين حكومة إفريقية القوانين التي تسمح بدخول هذه الاتفاقية حيز التنفيذ[83].

ثانيا: أهم قواعد اتفاقية الاتحاد الإفريقي لمكافحة الجريمة المرتكبة عبر الإنترنت

يعكس جزء كبير من الاتفاقية إطار حماية البيانات التي طوّرت بواسطة الاتحاد الإفريقي وبما أنه راعى الاصلاح الشامل من خلال تنظيم حماية البيانات، فإنه ينبغي على المشرعين اعتبار الاتفاقية كواحدة من امثلة "وضع المعايير" التي تجسد أغلب عملهم، ومن أهم القواعد التي أتت بها هذه الاتفاقية نذكر ما يلي:

1-فيما يخص معالجة المعطيات ذات الطابع الشخصي

أقرّت هذه الاتفاقية العديد من الالتزامات الخاصة بمعالجة المعطيات ذات الطابع الشخصي عبر الإنترنت التي يجب احترامها من قبل الدول الأطراف فيها، كما وضعت مبادئ من خلالها تتم حماية هذه المعطيات، وسوف نبين ذلك على النحو التالي:

---

[82]- اعتمد المؤتمر الثالث والعشرين لرؤساء دول وحكومات الاتحاد الإفريقي اتفاقية الأمن الإلكتروني وحماية البيانات الشخصية للاتحاد الإفريقي، وتسعى هذه الاتفاقية المعروفة أيضا باسم اتفاقية مالابو إلى اتباع نهج مشترك على المستوى القاري بشأن أمن الفضاء الإلكتروني ووضع الحد الأدنى من المعايير والإجراءات لتحديد بيئة رقمية موثوقة لتطوير الاتصالات الإلكترونية وضمان احترام الخصوصية على الإنترنت، وهذه الاتفاقية الآن مفتوحة لجميع الدول الأعضاء في الاتحاد الإفريقي للتوقيع والتصديق بما يتفق مع الإجراءات الدستورية لكل منها، وبعد ذلك يبدأ نفاذ الاتفاقية بعد ثلاثين (30) يوم من تاريخ استلام رئيس مفوضية الاتحاد الإفريقي صك التصديق الخامس عشر (15)، أنظر في ذلك: مشروع استراتيجية التحول الرقمي لإفريقيا (2020-2030)، ص 53، متوفر على موقع الاتحاد الإفريقي، www.au.int.

[83] - **درار نسيمة**، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني -دراسة مقارنة-، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015-2016، ص ص 285-286.

أ- التزامات الدول الأطراف في الاتفاقية

- يطلب من كل دولة عضو بالاتحاد الإفريقي أن يكون لها سلطة حماية البيانات الوطنية وأن يتم معالجة البيانات فقط في غرض مشروع.
- يطلب أيضا من الدول الأعضاء أن تكون معالجة وحفظ البيانات محدد بالوقت اللازم للغرض الذي تم جمعها أو معالجتها من أجله مع وجود استثناء المصلحة العامة.
- تتعهد الدول الأطراف بحظر أي جمع للبيانات ومعالجتها تكشف الأصل العرقي والإثني والإقليمي، أو البنوة الأبوية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الانتماء النقابي، الحياة الجنسية والمعلومات الوراثية أو بشكل عام بيانات عن الحالة الصحية للشخص[84].

ب- مبادئ حماية البيانات ذات الطابع الشخصي

- مبدأ الموافقة والشرعية في معالجة البيانات ذات الطابع الشخصي
- مبدأ القانونية والنزاهة في معالجة البيانات ذات الطابع الشخصي
- مبدأ القصد، الصلة والتخزين للبيانات ذات الطابع الشخصي المعالجة
- مبدأ الدقة في البيانات ذات الطابع الشخصي
- مبدأ الشفافية في معالجة البيانات ذات الطابع الشخصي
- مبدأ السرية والتأمين في معالجة البيانات ذات الطابع الشخصي[85]

ج- حقوق الأفراد أثناء معالجة بياناتهم الشخصية

سعيا من الاتحاد الافريقي إلى فرض حماية فعالة للبيانات الشخصية فقد كرّس بمقتضى هذه الاتفاقية العديد من الحقوق التي يتمتع بها الأشخاص أثناء معالجة بياناتهم ذات الطابع الشخصي، والتي يمكن حصرها في:

---

[84]- أنظر المادة 14 من اتفاقية الاتحاد الإفريقي، مرجع سابق

[85]- أنظر المادة 13 من اتفاقية الاتحاد الإفريقي، مرجع سابق

- **الحق في المعلومات**

يلزم هذا الحق المسؤول عن معالجة البيانات تزويد الشخص الذي ستعالج بياناته، في موعد لا يتجاوز الوقت الذي يتم فيه جمع هذه البيانات، بغض النظر عن الوسائل والتسهيلات المستخدمة ، بالمعلومات المتعلقة بهذه المعالجة مثل الهوية والغرض من هذه المعالجة وحق الاطلاع وتصحيح هذه البيانات، مع الالتزام بمدة الاحتفاظ بها[86].

- **الحق في الوصول إلى المعلومات**

يحق لأي شخص طبيعي ستعالج بياناته الشخصية أن يطلب من الموظف القائم بهذه المعالجة تزويده في شكل أسئلة بمختلف المعلومات التي تمكنه من تقييم والاعتراض وتأكيد المعالجة أو عدمها للبيانات الخاصة به، بالإضافة إلى نقل البيانات المعالجة للشخص المعني، وتزويده بالمعلومات الخاصة بغرض المعالجة[87].

- **الحق في الاعتراض**

حددت المادة الثامنة عشر من الاتفاقية حق الفرد في الاعتراض على المعالجة التي تضاف للبيانات، وهو ما يمكن أن يمثل دعما للمستخدمين، كما نصت الفقرة الثانية من نفس المادة ولأول مرة على أن لأصحاب البيانات الحق في اخبارهم قبل أن يتم مشاركة البيانات الخاصة بهم مع أطراف أخرى.

- **حق التصحيح أو الحذف**

أجازت الاتفاقية بمقتضى المادة التاسعة عشر لأي شخص طبيعي أن يطلب من المسؤول معالجة تصحيح أو إكمال أو تحديث أو حجب أو حذف، حسب الإقتضاء، للبيانات ذات الطابع الشخصي الخاصة به في حال إن كانت هذه البيانات خاطئة أو ناقصة أو غير واضحة أو قديمة، أو تم حظر جمعها أو استعمالها أو كشفها أو الاحتفاظ بها.

---

[86]– أنظر المادة 16 من اتفاقية الاتحاد الإفريقي، مرجع نفسه

[87]– أنظر المادة 17 من اتفاقية الاتحاد الإفريقي، مرجع نفسه

2- فيما يخص تعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية:

حددت الفقرة الثالثة من المادة خمسة وعشرين من اتفاقية الاتحاد الإفريقي أقسام الأمن السيبراني، حيث أوجبت على الحكومات أن تكفل الميثاق الإفريقي لحقوق الإنسان والشعوب وغيرها من الحقوق الأساسية الأخرى مثل حرية التعبير والحق في الخصوصية والحق في محاكمة عادلة أثناء وضعها لقوانين جديدة خاصة التي تمس ببياناتهم الشخصية أثناء معالجتها عبر الإنترنت.

نصت الفقرة الأولى والثالثة من المادة ستة وعشرون على تضمين المجتمع المدني صراحة كجزء من اصحاب المصلحة والشركات من القطاعين العام والخاص وثقافة الأمن السيبراني.

كما نصت المادة الثامنة وعشرون على قواعد الأمن السيبراني وتدعيم سيادة القانون، حيث تصر الاتفاقية على أن تقوم الدول الإفريقية بالتوقيع على اتفاقيات المساعدة القانونية المتبادلة لوضع معايير التبادل الدولي للبيانات بطريقة فعالة[88].

ألزمت المادة التاسعة وعشرون الدول الأعضاء بتمرير القوانين التي تحمي أمن البيانات وإعلام المستخدمين عن المخاطر التي تتعرض لها بياناتهم، مع تشجيع الشراكات العامة والخاصة في مجال الأمن السيبراني.

تحضر الاتفاقية استخدام الحاسوب في إهانة شخص ما لأسباب العرق أو اللون أو الأصل القومي، أو الدين، أو الرأي السياسي، كما تمنح هذه الأخيرة صلاحيات واسعة للمحاكم للوصول إلى قواعد البيانات وإجراءات مراقبة الشبكات إذا كان ذلك مفيدا في كشف الحقيقة.

[88]- Nations unies, Commission économique pour l'afrique, note d'orientation, Relever les défis de la Cybersécurité en Afrique, NTIS/002/2014, p 5

ثالثا: استحداث الشرطة الإفريقية Afripol كمظهر من مظاهر التعاون الإفريقي في مجال مكافحة جرائم الإنترنت

هي منظمة الشرطة الجنائية للدول الإفريقية التي تم انشائها سنة 2015، يوجد مقرها بالجزائر العاصمة وتضم (41) دولة[89]، وقد جاءت لتسهيل التعاون وتبادل المعلومات بين إدارات الشرطة الوطنية للدول الاعضاء في مكافحة الجرائم الدولية والارهاب، المخدرات، وتهريب الأسلحة والمتاجرة فيها على المستوى الإفريقي ومن أهم ما تهدف إليه المنظمة نذكر مايلي[90]:

- وضع استراتيجية افريقية لمحاربة الإجرام.
- تعزيز القدرات التحليلية للشرطة الإفريقية في مجال تقدير المخاطر الإجرامية واقتراح الحلول المناسبة لها، وتحقيق التضامن والتعاون فيما بين إدارات الشرطة في إطار العمليات الأمنية.
- تطوير الشرطة الإفريقية ماديا وبشريا من خلال ضمان الاطار التكويني الملائم والذي يتماشى وطبيعة القارة الإفريقية.
- وضع مركز افريقي خاص بالشرطة العلمية والتقنية والتحليل الجنائي ومحاربة الجريمة العابرة للحدود والمخدرات.

---

[89]– تعود فكرة إنشاء هذه المنظمة إلى الملتقى الإقليمي الإفريقي (22) للأنتربول المنعقد من (10 إلى 2013/09/12) بوهران بمشاركة (41) مسئول للأمن الإفريقي، وقد تم وضع الخطوط العريضة لهذه المنظمة خلال الملتقى الإفريقي للمدراء والمفتشين العامون حول الأفريبول المنعقد في الجزائر من (10 إلى 2014/02/11) حيث تم تجسيد إرادة مسئولو الشرطة بشكل رسمي لإنشاء منظمة الشرطة الإفريقية وذلك من خلال تبني وثيقة الاعلان بالعاصمة الجزائر، وبمناسبة القمة (23) للاتحاد الإفريقي في مالابو بغينيا المنعقد من (20 إلى 2014/06/27) قام رؤساء الدول والحكومات الافريقية بالمصادقة على الفكرة التي اعتمدها مسئولو الشرطة في إعلان العاصمة الجزائر، أنظر: **خديجة خالدي**، « **آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول** »، مجلة العلوم الإجتماعية والإنسانية، العدد الخامس عشر، جامعة المسيلة، د.س.ن، ص 67.

[90]– **بوصلعة ثورية**، السياسة الجنائية والأمنية في مواجهة الجريمة العابرة للحدود، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة أبو بكر بلقايد، تلمسان، 2017–2018، ص ص 190–191.

- تبني الطرق الصحيحة والمناسبة والعملية في مجال حوكمة الشرطة واحترام حقوق الانسان والتسيير الديمقراطي لمناهج الشرطة في كيفية التعامل في حالة الشغب واسترجاع النظام العام.
- توفير الوسائل العلمية والتكنولوجية ووسائل التدخل للشرطة الإفريقية وذلك من خلال المساعدة التقنية للاتصال وتبادل الخبرات العملية الخاصة بمكافحة الاجرام والتحليل الجنائي واستعمال التكنولوجيا وتبني طرق أمنية متجددة.

نستخلص مما سبق أن الجهود الموضوعية المبذولة على المستوى الدولي والإقليمي تتسم بالتباين وذلك راجع إلى عدة عوامل نذكر منها الفارق الموجود بين العالم المتقدم في مجال شبكات الإعلام والاتصال وخاصة شبكة الإنترنت والعالم المتخلف عن هذا المجال.

حيث أنه باستقرائنا لأساليب التجريم المتبعة من طرف المنظمات الدولية وحتى الاتحاد الأوروبي بصفته الإطار الرائد في هذا المجال، نستنتج أنّه هناك هوّة تقنية وقانونية مقارنة مع الجهود المبذولة على مستوى جامعة الدول العربية والاتحاد الإفريقي، الأمر الذي جعل من مكافحة الجريمة المرتكبة عبر الإنترنت يتسم بالصعوبة، لأنّ هذا التباين أثّر بطريقة مباشرة على هذه النصوص القانونية خاصة في ظل عالمية الجريمة من حيث الارتكاب والآثار المترتبة عنها، الأمر الذي يستلزم مد يد المساعدة للدول المتخلفة تكنولوجياً وتقنياً من خلال وضع آليات إجرائية تضمن التصدي بفعالية لهذه الجريمة.

المبحث الثاني

الآليات الإجرائية الدولية لمكافحة الجريمة المرتكبة عبر الإنترنت

يسعى المجتمع الدولي دائما إلى وضع الأطر القانونية اللازمة لمكافحة الجريمة بصفة عامة، ومواكبة مختلف المستجدات التي لم يعرفها القانون الموضوعي من قبل، وهكذا كان تعامله مع ظهور الجريمة المرتكبة عبر الإنترنت خاصة وأن الدول بقت عاجزة عن مجابهتها منفردة، فقام بمعالجة هذه الظاهرة موضوعيا عن طريق إبرام الاتفاقيات والمعاهدات لكي تكون الإطار الأنجع للحد من هذه الجريمة.

غير أن الجهود التشريعية الموضوعية تبقى غير فعالة إن لم تصاحبها قواعد إجرائية، فالقاعدة الموضوعية تستمد قوتها من القاعدة الإجرائية التي تعطي الإحساس بإلزامية هذه القواعد عن طريق تنفيذها، أو بمعنى آخر تعتبر القاعدة الإجرائية الوسيلة الفعالة لضمان حسن تطبيق القاعدة القانونية الجنائية الموضوعية.

في هذا الإطار تم اعتماد قواعد إجرائية دولية تندرج ضمن سياسة التعاون الدولي بشأن مكافحة الجرائم العابرة للحدود سيما التعاون القضائي الدولي **(مطلب أول)**، والتعاون الأمني الدولي **(مطلب ثان)**.

المطلب الأوّل

التعاون القضائي الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

يستلزم تتبع النشاط الإجرامي في الجريمة المرتكبة عبر الإنترنت على المستوى الدولي تقصي آثارها من المصدر إلى مكان تحقق النتيجة الإجرامية، ولا يتأتى ذلك إلا عن طريق اتخاذ العديد من الإجراءات مثل تبادل المساعدة القضائية بين الدول **(فرع أول)**، كتبادل المعلومات والإنابات القضائية الدولية، بالإضافة إلى تسليم المجرمين في حالة القبض عليهم ومطالبة دولة من الدول متابعة المجرمين المعلوماتيين الذين ارتكبوا جرائمهم عبر الفضاء الافتراضي **(فرع ثان)**.

الفرع الأول

المساعدة القضائية الدولية في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

تلجأ الدول إلى أسلوب التعاون الدولي من أجل متابعة المجرمين الذين يرتكبون الجرائم العابرة للحدود الوطنية مخلفين ورائهم أدلة أو معلومات في أماكن عديدة عبر العالم تفيد جهات تنفيذ القانون من إدانتهم، و لا يتأتى لها ذلك إلا عن طريق توفير العديد من الإجراءات والتي تتمثل في تبادل المعلومات**(أولا)**، نقل الإجراءات **(ثانيا)**، الإنابة القضائية الدولية **(ثالثا)**، التنسيق القضائي والتقني **(رابعا)**، الاعتراف بالأحكام الأجنبية **(خامسا)**.

أولا: تبادل المعلومات

يعرف العصر الحالي ثورة في مجال المعلومات مما حتم على المجتمع الدولي أن يولي تبادل المعلومات أهمية قصوى لاعتباره وسيلة لمكافحة الإجرام عموما، والجريمة المرتكبة عبر الإنترنت خصوصا، لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في ذلك متابعة نشاط المنظمات الإجرامية.

لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات لأنه يعد عنصرا رئيسيا من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وأوصى بأن تنشئ منظمة الأمم المتحدة قاعدة معلوماتية لإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة[91].

في هذا الشأن يتم تبادل المعلومات بين الدول في إطار المساعدة القضائية الدولية بطريقتين، إما بمنح المعلومات حول جريمة ذات البعد الدولي بطريقة تلقائية والتي تفيد الدولة الأخرى في التوصل إلى أدلة من خلال التحقيقات إلى مرتكب الجريمة، أو عن طريق تقديم طلب وهي الطريقة الشائعة في تعاملات الدول في المجال الجنائي.

وإعمالا لبنود اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة فإنه على السلطات المختصة التي تتلقى المعلومات أن تمتثل لأي طلب بإبقاء المعلومات المتلقاة طي الكتمان وإن كان مؤقتا أو تلتزم بفرض قيود على استخدامها، غير أنه يمكن للدولة المتلقية للمعلومات إذا رأت أنه من شأنها تبرئة أشخاص معينين أن تفشي هذه المعلومات بعد

[91]– **نقموش محمد، ميلودية أحمد، « الجريمة المعلوماتية: المفهوم–حتمية تطوير آليات التعاون الدولي في مجال مكافحتها »**، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، العدد 02، المجلد 04، جوان 2018، ص 274.

إخطار الدولة المحيلة أو التشاور معها وفي حالات الاستعجال يمكن لها توجيه إخطار مسبق[92].

ثانيا: نقل الإجراءات

يقصد بهذا الإجراء قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة، من أهمها التجريم المزدوج، وأن تكون الإجراءات المطلوب اتخاذها ذات أهمية، بحيث تؤدي دورا مهما في الوصول إلى الحقيقة.

هذه الصورة أقرتها العديد من الاتفاقيات الدولية منها والإقليمية حيث تعد إحدى صور المساعدة القضائية[93]، شرط توافر شروط معينة هي[94]:

1-أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة، والدولة المطلوب منها.

2-أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

---

[92]- **ربيعة فرحي**، « **المساعدة القانونية المتبادلة كآلية للتعاون الدولي الأساس القانوني ومعوقات التفعيل** »، مجلة المفكر للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة بسكرة، المجلد 03، العدد 04، ديسمبر 2020، ص 101.

[93]- من بين هذه الإتفاقيات نجد: معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة (2000) في المادة (21) منها، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة (1999) في المادة (09) منها، وأيضا المادة (16) من النموذج الإسترشادي لاتفاقية التعاون القضائي الصادر عن مجلس التعاون الخليجي لسنة (2003). أنظر في ذلك: **محمد أحمد سليمان عيسى**، «**التعاون الدولي لمواجهة الجرائم الإلكترونية** »، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، المجلد 14، العدد 2، 2016، ص ص 55-56.

[94]- **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي دراسة مقارنة، دار الكتب القانونية، مصر، 2011، ص 130.

3-أن يؤدي الإجراء المطلوب اتخاذه إلى كشف الحقيقة.

ثالثا: الإنابة القضائية الدولية

تلجأ الدول للاتصالات المباشرة بين السلطات القضائية بغرض تحقيق العدالة والكشف عن أدلتها، فالاتفاق في التحقيق والعدالة في الحكم والسرعة في إحقاق الحق كلها مزايا قد لا تبلغها الدول في العصر الحاضر ما لم تتح الاتصال المباشر بين رجال القضاء والمسؤولين عن إقامة العدل في جميع الأقطار، وقد أدركت الدول هذه الضرورات فأصبحت تتيح الاتصال المباشر بين السلطات القضائية في الحالات الطارئة، إضافة إلى إرسال الإنابات القضائية ودعوات الشهود ومقابلات الموقوفين وتبليغ المذكرات والوثائق بالطريق الدبلوماسي[95].

تعد الإنابة القضائية الدولية من الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية[96] .

تستلزم الإنابة القضائية إرسال الملف الخاص بالدعوى الجنائية بمرفقاتها من محضر جمع الاستدلالات، والتحقيق، والوثائق التي أجريت بمعرفة السلطة القضائية في الدولة طالبة الإنابة إلى السلطة القضائية في الدولة المطلوب منها اتخاذ بعض إجراءات التحقيق، وقد عقدت عدة اتفاقيات في مجال الإنابة القضائية بين الدول المختلفة، سواء كانت ثنائية، أم متعددة، وغالبا ما تتضمن هذه الإتفاقيات شرط استبعاد تنفيذ الأحكام في المجال السياسي

---

[95]- **ذنايب آسية**، الأليات الدولية لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل شهادة ماجستير في القانون العام، فرع علاقات دولية وقانون المنظمات الدولية، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، 2009-2010، ص 200

[96]- **نقموش محمد، ميلودية أحمد**، مرجع سابق، ص 272.

والضريبي والعسكري، أو إذا رأت الدولة المطلوب منها الإجراء، أن هذا الإجراء المطلوب تنفيذه يمس بسيادة الدولة، أو مصالحها الأساسية، ويترك تقدير ذلك لسلطة الدولة[97].

رابعا: التنسيق القضائي والتقني

يعتبر الاستدلال والتحقيق من بين أهم الإجراءات الهادفة للوصول إلى الادلة الواضحة لإثبات الجريمة سواء على المستوى الوطني أو ذات البعد الدولي، غير أنه يطرح إشكال في هذا الصدد حول تصادم هذه الإجراءات مع مبدأ سيادة الدولة على إقليمها، الأمر الذي لا يدع مجالا للشك من ضرورة وجود آلية دولية تتم في إطار المساعدة القضائية الدولية، حيث تبلورت في اتباع طريقة التنسيق بين مختلف جهات انفاذ القانون سواء في شقه القضائي أو التقني.

يعتبر التنسيق القضائي والتقني بين الدول في مجال مكافحة الجريمة المرتكبة عبر الإنترنت من بين أهم صور المساعدة القضائية الدولية، خاصة فيما يتعلق بإجراءات استخلاص الدليل الإلكتروني.

أبرمت الدول في هذا الإطار معاهدات واتفاقيات سعيا منها تسهيل عمليات الاستدلال والتحقيق في الجرائم المرتكبة عبر الإنترنت، خاصة إذا اقتضى الأمر فحص بيانات متواجدة في مراكز دول أخرى، وذلك من أجل حل مشكلة الاختصاص وتبادل الأدلة الجنائية الرقمية[98].

---

[97]– **سامي جلال فقي حسين**، مرجع سابق، ص 131.

[98]– كمثال عن التنسيق القضائي والتقني ما حدث في شهر جويلية (2009)، حيث تلقت السلطات الجزائرية معلومات من سفارة ألمانيا بالجزائر مفادها أن مصالح الشرطة الألمانية اكتشفت بأن شخصا ما قام بتاريخ (30 جوان 2009) على الساعة الثامنة وخمسون دقيقة مساء باختراق قاعدة بيانات متواجدة بميونخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة بـ (15000) بطاقة ائتمان باستعمال عنوان إلكتروني، وبتاريخ (21 أكتوبر) من نفس السنة تلقى كذلك مكتب الإنتربول بالجزائر مراسلة من مكتب الإنتربول بكندا مفادها أن مصالح شرطة كيبك تمكنت خلال العام الماضي من القبض على شبكة إجرامية مختصة في القرصنة الإلكترونية بتحميل المعطيات الرقمية المتبادلة بين الزبائن والبنك وتحويل الأموال من حسابات بنكية، وعلى إثر هذه المعلومات تمكنت المديرية العامة للأمن الوطني من إلقاء القبض على المتهم وهو شاب جزائري وتقديمه بتهمة القرصنة الإلكترونية المرتكبة بحق مراكز معطيات إلكترونية أجنبية متواجدة بكل من ألمانيا، كندا وصدر بحقه حكم رقم (10/05637) من محكمة عنابة بتاريخ (28 جوان 2010)، أنظر في ذلك: **عصماني ليلى**،

خامسا: الإعتراف بالأحكام الأجنبية

حسب القاعدة الكلاسيكية، أن الدول لا تعترف إلا بأحكام قانونها الجنائي ولا تعتد إلا بالأحكام الجنائية الصادرة عن محاكمها الوطنية، ولهاته القاعدة ما يبررها فهي من ناحية تعبير عن سيادة الدولة، ومن ناحية أخرى فإن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهذا ما يحول دون إمكانية تطبيق القانون الأجنبي.

لكن مع استفحال ظاهرة الإجرام الدولي، وضرورة تعاون الدول فيما بينها لمكافحة الجرائم عبر الوطنية وحتى لا يفلت الجناة من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة صار ممكنا الاعتراف بحجية الأحكام الأجنبية استنادا إلى معاهدات تبرم بين الدول[99].

إذن من العراقيل التي يجب تجاوزها لدعم أواصر التعاون الدولي عدم قابلية الحكم الأجنبي للتنفيذ بحجة أنه مظهر لسيادة الدولة ولحقها في العقاب، حيث أنه لا ينبغي أن يقتصر الأمر على ما يرتبه الحكم الأجنبي من آثار سلبية تتعلق بعدم جواز محاكمة

صهيب سهيل غازي زامل، « المساعدة القضائية الدولية كآلية للحصول على الدليل الإلكتروني »، مجلة القانون المجتمع والسلطة، المجلد 09، العدد 02، جامعة وهران 2، سنة 2020، ص 30.

[99]– بالنسبة لتنفيذ الأحكام الجزائية الأجنبية في الجزائر فإنه يجد له تجسيدا واقعيا من خلال بعض الاتفاقيات التي أبرمتها الجزائر والمتعلقة بالتعاون القضائي في المجال الجزائي، كما هو الحال في اتفاقية الرياض العربية للتعاون القضائي، التي نصت على الشروط التي يتعين توافرها من أجل مد التعاون الدولي بين الدول الأطراف في مجال تنفيذ الأحكام الجزائية في دولة غير الدولة التي أصدرت هذه الأحكام، عندما يكون المحكوم عليهم من مواطني الدولة المطلوب منها التنفيذ، وذلك في حالة توافر شروط، أن تكون العقوبة المحكوم بها سالبة للحرية لا تقل مدتها أو المدة المتبقية منها أو القابلة للتنفيذ عن ستة أشهر، أو أن تكون العقوبة من أجل إحدى الجرائم التي لا يجوز فيها التسليم طبقا للمادة (41) من هذه الاتفاقية، أو أن تكون العقوبة من أجل فعل معاقب عليه لدى الطرف المتعاقد المطلوب منه التنفيذ لديه بعقوبة سالبة للحرية لا تقل مدتها عن ستة أشهر، أو أن يوافق على طلب التنفيذ كل من الطرف المتعاقد الصادر عنه الحكم والمحكوم علية، أنظر في ذلك: **زغودي عمر، « الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية »**، مجلة البحوث القانونية والاقتصادية، المركز الجامعي آفلو، الأغواط، المجلد 02، العدد 02، ماي 2020، ص 107.

الشخص مرتين، حيث يدعوا الفقه الجنائي إلى ضرورة الاعتداد بالسوابق القضائية للحيلولة دون إفلات الجناة من العقاب اتفاقا مع متطلبات العدالة[100].

يعد هذا الإجراء من الضرورات الملحّة في مجال مكافحة الجريمة المرتكبة عبر الإنترنت نظرا لبعدها الدولي وامتداد آثارها للعديد من الدول، وذلك لتفادي إفلات مرتكب هذه الجريمة من العقاب.

الفرع الثاني

تطبيق نظام تسليم المجرمين كآلية لمكافحة الجريمة المرتكبة عبر الإنترنت

يعتبر نظام تسليم المجرمين من الإجراءات التي استقر عليها المجتمع الدولي في إطار العلاقات الدولية في المجال الجنائي، حيث من منطلق أن متابعة المجرمين الذين يرتكبون الجرائم العابرة للحدود الوطنية مثل الجريمة المرتكبة عبر الإنترنت يكون صعبا للغاية، وذلك راجع إلى وجود المتهم خارج حدود الدولة، الأمر الذي أدى بالمجتمع الدولي إلى إقرار هذا النظام من أجل تكريس التعاون الدولي لتفادي استفحال الجريمة وإفلات المجرمين من العقاب، وفي هذا النطاق يمكن أن نبين ذلك من خلال إظهار أسس نظام تسليم المجرمين **(أولا)**، وشروطه **(ثانيا)**، ثم الاستثناءات الواردة عليه **(ثالثا)**، بالإضافة إلى إجراءاته **(رابعا)**.

أولا: أسس تسليم المجرمين

يعد تسليم المجرمين بصفة عامة إجراء تسلم بموجبه الدولة فرداً مطلوباً موجود لديها لسلطات دولة أخرى، بغرض محاكمته عن جريمة ارتكبها أو لتنفيذ حكم صادر ضده بعقوبة جنائية[101]، في إطار إتفاقية مبرمة بين الدولتين.

ومن بين أسس تسليم المجرمين أن الدول لا تلتزم بالتسليم إلا إذا كان بناء على معاهدات دولية أو على أساس المعاملة بالمثل، مع حظر تطبيق مبدأ التسليم في الجرائم

---

[100]– **رابحي عزيزة**، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017–2018، ص 314.

[101] – **بن خليفة إلهام**، مرجع سابق، ص 361

السياسية، ومن بين الاتفاقيات الدولية لتسليم المجرمين اتفاقية الدول الأمريكية لتسليم المجرمين لسنة 1933، والاتفاقية العربية لتسليم المجرمين لسنة 1952، والاتفاق الأوروبي لتسليم المجرمين لسنة 1957، واتفاقية الدول الشمالية الاسكندنافية لتسليم المجرمين لسنة 1962، وخطة الكومنولث للتسليم لسنة 1966[102].

ويمكن تعريف المعاملة بالمثل في مجال تسليم المجرمين بأنها تطابق الحقوق والالتزامات، وهو ما يعني التزام كل دولة في مواجهة دولة أخرى بمجموعة من الحقوق والالتزامات التي يفرضها عليها حسن تطبيق هذا المبدأ، ويلزم كل منها بتطبيقه في المستقبل، وتعتبر المعاملة بالمثل من الوسائل الهامة والمعاصرة في مجال العلاقات الدولية بصفة عامة وفي المسائل الجنائية بصفة خاصة[103].

ثانيا: شروط تسليم المجرمين

تعد شروط التسليم مسألة أولية لإتمام إجراءات التسليم، فمتى تحققت تباشر الدولة الطالبة هذه الإجراءات بتقديم الطلب والوثائق المرفقة به للدولة المطالبة التي تتولى فحص الطلب والبت فيه، إما بقبوله في حالة توافر شروطه وخلوه من أي مانع من موانع التسليم أو رفضه في حالة انعدام أحد شروطه أو تحقق مانع يحول دون تسليمه[104].

1-الشروط المتعلقة بالشخص المطلوب تسليمه

اختلفت الدول فيما بينها حول مدى جواز تسليم رعاياها ولا يخرج وضع الشخص المطلوب تسليمه عن أحوال ثلاثة[105]:

---

[102]- نقلا عن: **جيلالي حسين**، « **التعاون الجنائي الدولي في مكافحة الجريمة العالمية** »، مجلة القانون، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد زبانة غيليزان، المجلد 07، العدد 02، 2018، ص 23.

[103]- المرجع نفسه، ص 24

[104]- **بن زحاف فيصل**، تسليم مرتكبي الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، 2011-2012، ص189.

[105] - **علواش فريد**، « **نظام تسليم المجرمين في الاتفاقيات الدولية** »، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، العدد 05، المجلد 02، جانفي 2017، ص 401.

- رعية الدولة الطالبة
- رعية الدولة المطلوب منها التسليم
- رعية دولة ثالثة

2-الشروط المتعلقة بالجريمة سبب التسليم

تستلزم الجريمة التي يتعين فيها تسليم المجرمين للدولة التي تطالب بذلك من أجل محاكمتهم توفر شروط تتعلق بالاختصاص القضائي أي أن تكون الدولة المطالبة مختصة إقليميا، وكذلك أن يكون الفعل مجرّما بمقتضى قانون الدولتين، وهو ما سوف نوضّحه فيما يأتي:

أ- من حيث الاختصاص القضائي

تشترط الدولة المطالبة لقبول طلب التسليم أن تكون الدولة الطالبة مختصة بمحاكمة الشخص المعني بالطلب وفقا لقواعد الاختصاص القضائي المتمثلة في الاختصاص الإقليمي، بحيث تكون الجريمة قد ارتكبت في اقليم الدولة التي تقدمت بالطلب، أو الاختصاص الشخصي الإيجابي، أين يكون الجاني حاملا لجنسية الدولة المقدمة للطلب، أو الاختصاص الشخصي السلبي أين يكون المجني عليه من مواطني الدولة الطالبة[106].

ب- من حيث التجريم المزدوج للسلوك

يقصد بالتجريم المزدوج أن يكون السلوك المطلوب التسليم من أجله مجرما في تشريع كلا الدولتين الطالبة والمطلوب إليها التسليم حتى ولو اختلف وصف الجريمة في تلك الدولتين، كذلك بالنسبة للأفعال المكوّنة للشروع أو الاشتراك فيجب أن تكون معاقبا عليها طبقا لقانون كل من الدولة الطالبة والمطلوب منها التسليم[107].

---

[106]- **عصماني ليلى**، التعاون الدولي لقمع الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة وهران، 2012-2013، ص 227.

[107]- **خرشي عثمان**، « **تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية** »، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، العدد العاشر، جوان 2018، ص 935.

تشترط معظم الدول ازدواج التجريم للسلوك الذي يطالب بالتسليم من أجله وأن يكون معاقبا عليه في قوانين الدولة طالبة التسليم والدولة المطلوب إليها، وهو شرط منطقي لأن التزام الدولة بالتسليم يبدو ضعيفا فيما لو كان الفعل غير مجرم في قانونها وكذلك فيما لو كان غير مجرم ابتداء في قانون الدولة الطالبة لذلك، فشرط ازدواج التجريم يعد أحد مبادئ النظام القانوني للتسليم ولا يتصور الخروج عنه[108].

ثالثا: إستثناءات تسليم المجرمين

وردت حول نظام تسليم المجرمين عدة استثناءات نذكر منها:

أ- ألا تكون الجريمة مما جرى العرف على عدم التسليم فيها

من الجرائم التي جرى العرف على عدم التسليم بشأنها نجد الجرائم العسكرية كالفرار من الخدمة العسكرية والتمرد والخيانة والجوسسة، أما الجرائم السياسية فقد حرمت المعاهدات بوجه عام تسليم الأشخاص الذين يرتكبون هذه الجرائم، كما تحرمه القوانين الداخلية في بلاد عديدة[109].

ب- عدم جواز تسليم الرعايا

يعتبر عدم جواز تسليم الرعايا من الشروط المتعلقة بالأشخاص المطلوب تسليمهم طبقا لنص المادة 698 الفقرة 1 من قانون الإجراءات الجزائية الجزائري[110]، وواحد من المبادئ السائدة التي استقر عليها المجتمع الدولي، أيا كان نوع الجريمة المرتكبة من قبل أحد الرعايا في أي إقليم خارج دولته، هذا الإجراء يقاس عليه حتى طالبي حق اللجوء السياسي بحيث لا يجوز تسليمهم.

---

[108]- **ذنايب آسيا**، مرجع سابق، ص 187.

[109]- **لعطب بختة، « أشكال التعاون الدولي في مكافحة الجرائم الدولية »**، مجلة المعيار، المركز الجامعي تيسمسيلت، العدد 04، ديسمبر 2011، ص 106.

[110]- التي تنص على أنه: "لا يقبل التسليم في الحالات الآتية:

1- إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها..."

ت- عدم جواز تسليم من تمت محاكمته عن ذات الجريمة المطلوب تسليمه لأجلها:

يعد أحد الضمانات الأساسية للمتهم لأنه يهدف إلى تحقيق أكبر قدر من الحماية القضائية للشخص المطلوب تسليمه، مع ذلك لا يحول دون إمكان إرسال الأجنبي مؤقتا للمثول أمام محاكم الدولة الطالبة بشرط أن يعاد بمجرد الفصل في موضوع الجريمة من طرف القضاء الأجنبي[111].

رابعا: إجراءات تسليم المجرمين

تتم إجراءات تسليم المجرمين وفق مجموعة من الشروط تتمثل في:

1-تقديم طلب التسليم

لايتم التسليم إلا بناء على طلب تقدمه الدولة طالبة التسليم، والذي يكون غالبا بواسطة الطرق الدبلوماسية، إلا أن بعض الاتفاقيات تنص على أن يقدم الطلب بواسطة البريد أو التلفون، ثم تتولى الدول المطلوب منها التسليم البحث عن الشخص وضبطه، وبعدها يتعين على الدولة تقديم جميع المستندات اللازمة خلال مدة زمنية لا تتعدى ثلاثين يوما[112].

2- الرد على طلب التسليم

بعد تقديم الدولة الطالبة طلب التسليم مرفقا بالمستندات اللازمة تقوم الدولة المطالبة بالنظر فيه وفقا للاجراءات التي ينص عليها قانونها وتبلغ الدولة الطالبة بقرارها على الفور، والذي يكون وفق ثلاثة حالات:

أ- الحالة الأولى: يكون الرد على الدولة الطالبة برفض الطلب كليا أو جزئيا مع تقديم أسباب ذلك الرفض.

---

[111]- **خرشي عثمان**، مرجع سابق، ص 936.

[112] – **قارة أمال، « تفعيل آليات تسليم المجرمين في إطار المنظمة الدولية للشرطة الجنائية »**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص 893.

ب- الحالة الثانية: يكون الرد بالموافقة على التسليم والذي يتبعه اتخاذ الطرفين دون تأخير لا مبرر له الترتيبات اللازمة لتسليم الشخص المطلوب، وتعلم الدولة المطالبة الدولة الطالبة بالمدة الزمنية التي كان الشخص المطلوب محتجزا أثناءها.

ت- الحالة الثالثة: تأجيل التسليم بعد الموافقة عليه بغرض محاكمة الشخص المطلوب أو بغرض تنفيذ حكم صادر ضده إذا كان مدانا بجرم غير الجرم المطالب بالتسليم لأجله[113].

يعد إجراء تسليم المجرمين من بين أهم مظاهر التعاون الدولي في مجال متابعة الجرائم العابرة للحدود الوطنية، أو الجرائم ذات البعد العالمي خاصة الجرائم المرتكبة عبر الشبكة العالمية للإنترنت، والتي لا يمكن متابعتها من طرف الدول منفردة، بشرط أن يتم هذا الإجراء وفق الاتفاقيات الدولية المبرمة في مجال التعاون الجنائي الدولي لمكافحة الجريمة الدولية.

المطلب الثاني

التعاون الأمني الدولي ودور منظمة الشرطة الجنائية الدولية في مكافحة الجريمة المرتكبة عبر الإنترنت

تضفي خاصية عبر الوطنية للجريمة المرتكبة عبر الإنترنت العديد من الإشكالات القانونية على المستوى الدولي في مرحلة الاستدلالات والتحري، حيث أنه تبعا لهذه الخاصية من المنطقي أن تقف الحدود الجغرافية كحاجز أمام أجهزة الشرطة القضائية في مكافحة الجريمة ومتابعة المجرمين لأنهم في هذه الحالة يكونون مقيدين بالسيادة الإقليمية للدول، فمن هذا المنظور لا تستطيع أي دولة ملاحقة المجرمين بمفردها، بل يجب أن يكون هناك تضافر للجهود بين الدول في المجال الأمني الذي يعتبر ضرورة ملحة **(فرع أول)**، بل أكثر من ذلك ونظرا للتوسع والانتشار الهائل للجرائم المختلفة عبر الفضاء الافتراضي أصبحت

[113] – **علواش فريد**، مرجع سابق، ص 409.

الحاجة ملحة إلى وجود جهاز دولي يأخذ على عاتقه تكريس التعاون بين الدول في مجال مكافحة هذه الظاهرة الإجرامية والذي تمثل في الدور الذي تلعبه المنظمة الدولية للشرطة الجنائية **(فرع ثان)**.

الفرع الأول

ضرورة اللجوء إلى التعاون الأمني الدولي في مكافحة الجريمة المرتكبة عبر الإنترنت

أثبت الواقع العملي أن الدولة –أي دولة– لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة[114]، لذلك أصبحت الحاجة ماسة إلى وجود تعاون أمني دولي، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من قبضة العدالة، لهذا سنبين في هذا النطاق أهمية التعاون الأمني الدولي **(أولا)**، وإظهار صوره **(ثانيا)**، ثم التدريب باعتباره مظهر من مظاهر التعاون الأمني الدولي **(ثالثا)**.

أولا: أهمية التعاون الأمني الدولي

أدى التطور في مجال الاتصالات وتكنولوجيات المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوع من الجرائم المعلوماتية، التي باتت تشكل خطر ليس على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الإستراتيجية[115]، خاصة وأنها تتميز بتعديها للحدود الوطنية للدول الأمر الذي جعل آلية التعون الدولي حتمية واقعية لأن هذه الجريمة لا يمكن مكافحتها من طرف الدول منفردة.

---

[114]– **محمد أحمد سليمان عيسى**، مرجع سابق، ص 52.

[115] – **حسين بن سعيد بن سيف الغافري**، « **الجهود الدولية في مواجهة جرائم الإنترنت** »، ص 05، مقال متوفر على الموقع التالي: www.minchawi.com. أنظر كذلك:

- **DUPONT Benoit**, La gouvernance polycentrique du cybercrime: les réseaux fragmentés de la coopération international, cultures et conflits, n° 102, centre d'études sur les conflits, été 2016, disponible sur le site, http://conflits.revues.org/19292

فمن المعلوم لكي يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل الجريمة بصفة عامة والجريمة المرتكبة عبر الإنترنت بصفة خاصة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، لهذا سعت دول عديدة إلى تكريس مبادئ التعاون الأمني ادراكا منها لأهميته من جهة، وعدم امكانية مكافحة الجريمة المرتكبة عبر الإنترنت لوحدها من جهة أخرى.

ثانيا: صور التعاون الأمني الدولي

يتخذ التعاون الدولي في مجال مكافحة الجريمة العابرة للحدود الوطنية عامة والجريمة المرتكبة عبر الإنترنت خاصة عدّة صور تتمثل في العمل التشاركي وتبادل الخبرات والقيام ببعض العمليات الأمنية المشتركة بالإضافة إلى التدريب الذي يكتسي أهمية كبيرة في اكتساب الخبرة للقائمين على مكافحة هذه الجريمة.

1-العمل التشاركي وتبادل الخبرات.

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث مفاجئة بشكل لا يمكن توقعه أو يستحيل التنبؤ بتوقيت حدوثه، أو يصعب معه مواجهته بالإمكانيات الخاصة للدولة التي تعرضت للكارثة بمفردها.

ومع وقوع مثل هذه الكوارث أو الأزمات غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتضافر الجهود الدولية[116].

وهذه الصور من صور التعاون الأمني تعد ذات أهمية بالغة في مجال مكافحة جرائم الإنترنت لا سيما وأن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول متقدمة تقنيا وتكنولوجيا ولها نصيب كبير

[116]- **رابحي عزيزة**، مرجع سابق، ص 306.

في مواجهة الجرائم المعلوماتية تشريعيا وفنيا، والبعض الآخر تفتقد ذلك[117] الأمر الذي يجعلها تحتاج إلى المساعدة والمعاونة لتدارك ذلك النقص لديها.

2-القيام ببعض العمليات الأمنية المشتركة.

يعد كل من تعقب مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة على ارتكاب الجريمة المعلوماتية، أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها تكوين مهارات وخبرات لدى القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها[118].

ثالثا: التدريب كمظهر للتعاون الأمني الدولي

تقتضي طبيعة الجرائم المرتكبة عبر الإنترنت معرفة متميزة بنظم الحاسبات وشبكاته وكيفية تشغيلها ووسائل استعمالها من قبل مستخدميها، ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري والمباشرين للتحقيق فيها.

يعد الاهتمام بعنصر التدريب للأجهزة الأمنية التي تضبط وتلاحق هذا النوع من الجرائم من المرتكزات الأساسية، والمقصود بالتدريب هنا ليس التدريب التقليدي فحسب، فلا يكفي أن تتوافر لدى رجال القضاء الخلفية القانونية، ولدى الضبطية القضائية خصائص عمل الشرطي، إنما لا بد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية، وهذه الأخيرة لا تتأتى دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر

---

[117] – **رابحي عزيزة**، مرجع سابق، ص ص 306-307.

[118]– **يوسف حسن يوسف**، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 149.

الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب[119]، بالإضافة لذلك ضرورة أن يكون لدى المتدرب خبرة في المجالات ذات العلاقة بتكنلوجيا المعلومات كإدارة الشبكات والبرمجة وتصميم النظم...الخ.

يجب أن يشتمل التدريب على كيفية تشغيل الحاسبات، بعد التعرف على أنواعها ونظمها المختلفة لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات والمعالجة الإلكترونية للبيانات والجرائم التي تقع على الحاسبات، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن الحاسبات، ووسائل اختراقها، مع دراسة حالات تطبيقية لجرائم وقعت سالفا وكيف تم مواجهتها[120].

بالنتيجة فإن التدريب أصبح يلعب دورا هاما في حياة الإنسان، حيث زاد الاهتمام بالتدريب بمختلف جوانبه الفنية والتكتيكية، وقد أضحى ضرورة للفرد المتدرب وللمنظمة التي ينتسب إليها في آن واحد، سواء أكانت منظمة مدنية أو عسكرية أو حكومية أو خاصة[121].

الفرع الثاني

دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المرتكبة عبر الإنترنت

الشرطة الجنائية الدولية هي منظمة دولية حكومية لها كيان دائم، وتتمتع بالشخصية القانونية الدولية، وهي من أقدم الأمثلة على التعاون الدولي[122]، وتعد من بين أهم المنظمات الدولية الناشطة في مجال مكافحة الجريمة، نظرا لما تقدمه من إمكانيات لضبط

---

[119] – **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2012-2013، ص93.

[120] – **محمد أبو العلا عقيدة**، « **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية** »، مقال منشور على الموقع: www.arablawinfo.com

[121]– **لورنس سعيد الحوامدة**، « **الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة** »، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، المجلد الرابع، العدد الأول، 2017، ص 211.

[122] – **مايا خاطر**، « **الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها** »، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الثالث، سنة 2011، ص 523.

مرتكبي الجرائم على اختلاف أنواعها أينما وجدوا ومن ثم تسليمهم إلى الهيئات المختصة لمحاكمتهم[123]، وفي هذا الصدد سنتطرق إلى أهداف المنظمة الدولية للشرطة الجنائية **(أولا)**، وتبيان وسائل التعاون الدولي فيها **(ثانيا)**، ثم نشير إلى نشراتها **(ثالثا)**، بالإضافة إلى التطرق لجهودها في مجال مكافحة الجريمة المرتكبة عبر الإنترنت **(رابعا)**.

أولا: أهداف المنظمة الدولية للشرطة الجنائية

تهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها، وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المنتشرة في عدة دول ومنها جرائم الإنترنت.

ويمكن إبراز أهداف الإنتربول فيما يلي:

- العمل على تأمين وتنمية التعاون الدولي بين كافة أجهزة الشرطة الجنائية في الدول الأعضاء.

---

[123] – تعود نشأة المنظمة الدولية للشرطة الجنائية إلى المؤتمر الدولي الثاني الذي عقده الدكتور "جوهانو سويرا" مدير شرطة فيينا، وذلك في الفترة (3–1923/09/7) الذي ضم مندوبي تسعة عشر دولة وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية، ومقرها فيينا للتعاون بين أجهزة الشرطة من أجل مكافحة الجريمة.

وفي بروكسل ببلجيكا عقد مؤتمر في الفترة من (6–1946/06/9) ولقد دعا إليه المفتش العام للشرطة البلجيكية "لوفاج" وبموجبه تم إحياء اللجنة الدولية للشرطة الجنائية، ونقل مقرها إلى باريس بفرنسا، وتم تشكيل لجنة تنفيذية من خمسة أعضاء برئاسة المفتش العام للشرطة البلجيكية "لوفاج" وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية، ثم انتقلت المنظمة لمقرها السابق في (سان كلود) ليصبح مقرها الجديد رسميا في مدينة (ليون) الفرنسية عام (1989)، أنظر في ذلك: **حاج مخناش نوال**، المرجع السابق، ص 1124. أنظر كذلك:

- **DEHOUSSE Franklin, ZGAJEWSKI Tania**, La convention europol: un tournant pour la coopération policiére européenne, courrier hebdomadaire du centre de recherche et d'information socio-politiques (crisp), n° 1577-1578, 1997, p 06. Dispnible sur le site: https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-1997-32-page-1.htm

- إنشاء وتفعيل كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.
- العمل على منع الجرائم الدولية، أو الحد منها عن طريق مكافحة الإجرام العابر للحدود، وعن طريق تعقب المجرمين والجرائم المرتكبة، وتسهيل عمليات إلقاء القبض عليهم وتسليمهم إلى الجهات المختصة[124].

ثانيا: وسائل التعاون الأمني الدولي في إطار المنظمة

تتمثل الوسائل المعتمد عليها من أجل تكريس التعاون الأمني الدولي من طرف المنظمة الدولية للشرطة الجنائية في:

1-الاتصالات اللاسلكية

وضعت الأمانة العامة للأنتربول في متناول الدول الأعضاء مجموعة من الأدوات الفنية والتقنيات التكنولوجية الحديثة لملاحقة المجرمين، حيث ترتبط معظم الدول الأعضاء بشبكة الاتصالات الشرطية الخاصة بالمنظمة، فالمكاتب المركزية الوطنية مرتبطة بالأمانة العامة ومع بعضها بالمحطات الإقليمية بشبكة لاسلكية مستقلة[125].

تعتبر منظومة الاتصالات أنتربول 24/7 من أحدث ما توصلت إليه التكنولوجيا الحديثة في مجال الاتصالات، إذ تسمح بتبادل الرسائل في ظرف قصير جدا بين المكاتب المركزية الوطنية والأمانة العامة للأنتربول، وقد تمكن المكتب المركزي الوطني-أنتربول الجزائر- من تحقيق الربط بهذه المنظومة بتاريخ 21 أوت 2003[126].

124- **عقون مصطفى، « دور منظمة الشرطة الجنائية الدولية الإنتربول في مكافحة الجريمة المنظمة »**، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، العدد الخامس، ديسمبر 2015، ص 222.

125- **معمر بن علي، عبد المالك الدح، « الوسائل المتاحة لمنظمة الأنتربول لمجابهة الجريمة المنظمة »**، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي آفلو، الأغواط، ماي 2020، ص 136.

126- **قسمية محمد، « الوسائل الفنية للمنظمة الدولية للشرطة الجنائية (الأنتربول) كآلية للتعاون الدولي الشرطي »**، حوليات جامعة الجزائر، المجلد 34، العدد 02، سنة 2020، ص 128.

2-التوثيق الجنائي

تتسلم المنظمة البيانات والمعلومات المتعلقة بالجريمة والمجرم وتتبادلها مع المكاتب المركزية للشرطة الجنائية في الدول الأعضاء، وتقوم المنظمة بتجميع هذه البيانات وتنظيمها لديها وهذه الوثائق تعتبر وثائق مهمة في مكافحة الجريمة على المستوى الدولي[127].

3-بث الإشعارات

وهي التي تبثها المنظمة لإطلاع البلدان الأعضاء على بعض المعلومات وتتمثل في:

أ- الإشعارات الإشارية الفردية، وتتمثل في أربعة أنواع:

- طلبات الاعتقال المؤقت بغرض التسليم الصادرة بناء على طلب سلطات قضائية قومية.
- البحث والتقصي عن هوية وتحديد مكان أشخاص مشتبه بارتكابهم جرائم على المستوى الدولي، أو الأشخاص الذين أبلغ عن فقدانهم أو الأشخاص العاجزين.
- لفت الانتباه بهدف الحذر من أشرار محترفين قد يقومون بأعمال على المستوى الدولي والبحث عن عناصر تحديد هوية جثث عثر عليها.

ب- الاشعارات بالأشياء المسروقة أو المطلوبة، وهي عادة ما ترفق بصور خاصة إذا كانت هذه الأشياء ثمينة كالتحف الفنية.

ت- إشعارات بطرق العمل الجديدة أو الخاصة التي قد يلجأ إليها الأشرار الدوليون التي قد تتعمم وتنتشر على المستوى الدولي.

ث- إشعارات عن طريق رسائل دورية أو كراسات تتعلق بأنماط معينة من الإجرام أو من المجرمين[128].

---

[127]- **بلعيور محمد نذير، بوعيشة بوغوفالة، « دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة »**، مجلة البحوث القانونية والاقتصادية، المركز الجامعي آفلو، المجلد 02، العدد 02، ماي 2020، ص 35.

4-عقد المؤتمرات والاجتماعات

عقدت الأنتربول عدة ندوات عالمية مثل تلك التي تعقد حول جرائم المخدرات، وهناك مؤتمرات إقليمية وجهوية تعقد لبحث الجريمة في هذا النطاق ووسائل المكافحة، مثل المؤتمر الآسيوي والمؤتمر الأوروبي والمؤتمر الإفريقي، وقد احتضنت الجزائر سنة 1997 الندوة الجهوية الإفريقية لمنظمة الإنتربول[129].

5-التعاون الأمني الدولي المتبادل.

يصعب على الدولة بمفردها القضاء على الجريمة العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين ومكافحة نشاط الإجرام الذي يتجاوز حدود الدولة.

تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف، على نحو فعال يحقق مكافحة الجريمة، وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة[130]، وتبادل المعلومات والبيانات فيما بينها، والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها، أي أن عضو الأنتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل أن هذا العمل منوط

---

[128] – **فنور حساين**، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مذكرة من أجل الحصول على شهادة الماجستير، تخصص القانون الدولي والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2012-2013، ص 90.

[129]– **بلعيور محمد نذير، بوعيشة بوغوفالة**، مرجع سابق، ص 37.

[130]– تنص المادة 32 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية على: "**لتأمين هذا التعاون، يعين كل بلد هيئة تعمل فيه كمكتب مركزي وطني، ويؤمن هذا المكتب الاتصال:**

أ- بمختلف أجهزة البلد.

ب- بالهيئات التي تعمل في البلدان الأخرى كمكاتب مركزية وطنية.

ج- بالأمانة العامة للمنظمة".

بجهاز الشرطة الوطنية في الدولة التي يتواجد المجرم على اقليمها، الأمر الذي يؤكد على احترام السيادة الوطنية[131].

ثالثا: نشرات المنظمة الدولية للشرطة الجنائية

تسعى المنظمة الدولية للشرطة الجنائية من أجل مساعدة أجهزة الشرطة في البلدان الأعضاء على تبادل المعلومات الجنائية بينها إلى إصدار العديد من النشرات، والتي تعتبر من بين أهم طرق عمل هذه المنظمة، ويتم إصدارها إما بطريقة مباشرة، أو عن طريق طلب من المكاتب المركزية الوطنية. نبين هذه النشرات على النحو التالي:

1- **النشرة الدولية الحمراء:** وتصدر في حالتين هما: حالات صدور حكم قضائي ضد الشخص الملاحق في هذه النشرة في جناية أو جنحة، وحالة اتهام الشخص الملاحق بارتكاب جريمة وصدور قرار بالقبض عليه من السلطات المختصة.

2- **النشرة الدولية الخضراء:** تصدر للتنبيه إلى أنشطة إجرامية التي يظطلع بها شخص يعتبر مصدر خطر محدق على السلامة العامة.

3- **النشرة الدولية الزرقاء:** تصدر لتحديد مكان شخص يتسم بأهمية خاصة بالنسبة لتحقيق جنائي، أو تحديد هوية أو الحصول على معلومات عنه.

4- **النشرة الدولية الصفراء:** تصدر في حالة قيام أحد المكاتب المركزية الوطنية بإخطار الإنتربول بتغيب أحد مواطنيها، أو في حالة العثور على شخص أجنبي فاقد التمييز.

5- **النشرة الدولية السوداء:** تصدر لتحديد هوية الأشخاص المتوفين.

6- **النشرة الدولية البرتقالية:** تستخدم من أجل تحذير الشرطة، والمؤسسات العامة من المنظمات الدولية من المخاطر التي يمكن أن تحدثها الأسلحة المموهة والقنابل والإرهاب.

---

[131]- **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، 2009، ص ص 593-594.

7-**النشرة الدولية البنفسجية:** تستخدم هذه النشرة للتزويد بالمعلومات عن طريق العمل والإجراءات والمواضيع والوسائل والمخابئ التي يستخدمها المجرمين.

8-**النشرات الخاصة بالإنتربول:** تستخدم لتوفير معلومات عن أشخاص خاضعين للجزاءات التي تفرضها منظمة الأمم المتحدة[132].

رابعا: جهود المنظمة الدولية للشرطة الجنائية في مكافحة جرائم الإنترنت

مرت جهود المنظمة في هذا المجال بمراحل عديدة، توجت بإنشاء عدة مراكز اتصالات في كل من طوكيو، نيوزيلاندا، نيروبي، أذربيجان، بيونس أيرس، لتسهيل مرور الرسائل، يضاف إلى ذلك مكتب إقليمي فرعي في بانكوك[133].

أكدت المنظمة في عدة مؤتمرات لها بشأن جرائم الإنترنت، على ضرورة إيجاد تعاون دولي لمكافحة هذا النوع المتميز من الإجرام، وعلى ضرورة تقرير ذلك، بحيث تعين كل دولة الإدارة المكلفة بالسهر على هذا النوع من القضايا لتلقي البلاغات واتخاذ الإجراءات المناسبة حسب قوانين بلادها[134].

---

[132]- **يوبي سعاد**، «**الإنتربول كآلية دولية شرطية لمكافحة جريمة الفساد**»، المجلة الإفريقية للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة أدرار، المجلد 03، العدد 01، جوان 2019، ص 119، أنظر كذلك:

- **عائشة عبد المجيد**، « **النظام القانوني للمنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مجال التعاون القضائي الشرطي** »، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار الحادي عشر، 2002، ص 09-10، متوفر على الموقع التالي: www.ajrsp.com

[133]- **محمد أحمد سليمان عيسى**، مرجع سابق، ص ص 53-54.

[134] - تطبيقا لذلك، أنشأت الولايات المتحدة الأمريكية نقطة مراقبة على شبكة الإنترنت تسمى شرطة الويب الدولية التي تضم فريق عمل من المتخصصين في تنفيذ القانون وضباط الشرطة ومتطوعين فنيين من (61) دولة حول العالم، وتتمثل مهمتها في تلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ونظرا لاتساع نشاط هذه المنظمة، وما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء، فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم، أنظر: **بن خليفة إلهام**، مرجع سابق، ص ص 339-340.

لا يقتصر عمل الانتربول في مجال مكافحة الجريمة المرتكبة عبر الإنترنت في صور عقد واحتضان المؤتمرات بل تعمل الإنتربول لأجل تجسيد ذلك ميدانيا، من خلال العمل على دعم إجراءات البحث والتحقيق بشأنها من خلال:

- جمع وتخزين وتحليل المعلومات المتعلقة بالجرائم المعلوماتية مع توفيرها لكافة الدول الأعضاء بواسطة منظومة 7/i24 للأنتربول، وهي عبارة عن شبكة اتصالات شرطية مؤمّنة تربط بين الدول الأعضاء[135].
- استحداث معيار منسق للاتصالات لتسهيل تبادل المعلومات الشرطية.
- إمكانية التحكم المباشر في البيانات والتدقيق فيها.
- إمكانية تسجيل أحدث المعلومات مباشرة في قاعدة البيانات الجنائية.
- تقديم الدعم لمصالح الشرطة على المستويين الدولي والداخلي.
- تكوين وتطوير أعوان الشرطة بحيث تنظم دورات تكوينية تسمح لأعوان الشرطة تحسين قدراتهم على التعامل مع منظومة الاتصال في إطار سياسة التعاون الدولي لمكافحة الجرائم المعلوماتية[136].

---

[135]– تسمى هذه الآلية بالأنتربول (24 ساعة في اليوم و7 أيام في الأسبوع)، وهي منظومة عالية الأمان ذات فاعلية قصوى تستخدم الإنترنت كنفق البيانات المرمزة، وهي تمكن مجموعة الأنتربول من تبادل المعلومات والوصول إلى قواعد البيانات الشرطية المتعددة، تشمل معلومات هامة، كأسماء الأفراد وبصمات الأصابع والصور ووثائق السفر. أنظر في ذلك: **بن عمر حاج عيسى**، « **الأنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود** »، مجلة الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد 03، جانفي 2016، ص 258، أنظر كذلك:
- **FRAYSSINET Jean**, Interpol et ses fichiers, p 03, article disponible en ligne à l'adresse: https://hal.archives-ouvertes.fr/hal-01427564

[136] – **ربيعي حسن**، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015–2016، ص 150–151.

الفصل الثاني

الآليات الوطنية المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت

لم يمر الاستعمال الواسع لشبكة الإنترنت على مستوى العالم المتقدم في مجال تقنية المعلومات بصفة خاصة والمجتمع الدولي بصفة عامة دون أن يترك أثره على الدول النامية ومنها الجزائر، فاستعمالها لشبكات الاتصال وخاصة الإنترنت حتى وإن كان متأخرا مقارنة بالدول المتقدمة، إلا أنه يبقى واقعا فرض نفسه في السنوات الأخيرة، وخير دليل على ذلك ما نلاحظه في اتجاها إلى تكريس نظام الإدارة الإلكترونية بمختلف فروعها سواء على المستوى المركزي أو اللامركزي.

هذا النهج المعلوماتي المتّبع كانت له آثاره السلبية التي استغلها المجرمون من أجل ارتكاب العديد من الجرائم سواء الماسة بالأفراد أو المؤسسات.

أدى هذا الوضع إلى محاولة التصدي للجريمة المرتكبة عبر الوسائط الإلكترونية وخاصة المرتكبة عبر الإنترنت، وذلك مواكبةً للتطور الحاصل في مجال تقنية الاتصال من جهة، والتطور الكبير للنظم التشريعية على المستوى الدولي في هذا المجال من جهة أخرى، وكان ذلك بداية بوضع آليات تشريعية ملائمة لمكافحة هذه الظاهرة الإجرامية المستحدثة خاصة وأن التشريع شهد فراغا رهيبا في هذا المجال **(مبحث أول)**.

لم يقف الأمر عند وضع تشريعات موضوعية لمكافحة جرائم الإنترنت فحسب، بل تعدّاه إلى تطوير الإجراءات الجزائية التي من خلالها يسمح لجهات المتابعة سواء الاستدلال أو التحقيق أو الحكم من أجل مكافحة إجرائية فعالة للجريمة المرتكبة عبر الإنترنت **(مبحث ثان)**.

المبحث الأول

الآليات الموضوعية الوطنية لمكافحة الجريمة المرتكبة عبر الإنترنت

أدى الاستعمال المتسارع للنظم المعلوماتية والتطور التكنولوجي الكبير الذي ميزها على المستوى الدولي والداخلي على حد سواء، بالمشرع الجزائري إلى التصدي للممارسات السلبية التي ترتبت عنه، فبالرغم من أن الجريمة المرتكبة عبر الإنترنت على المستوى الوطني لم يكن لها نفس الأثر مقارنة بالدول المتقدمة، إلا أن هذا لم يمنعه من مكافحتها خاصة وأن آثارها بدأت تتجلى بوضوح سواء على الأفراد أو المؤسسات.

اعتمد بداية مكافحته للجريمة المرتكبة عبر الإنترنت على النصوص القانونية القائمة، وذلك نظرا للفراغ التشريعي الكبير الذي كان يعرفه في هذا المجال، فسعى إلى تعديلها وتحيينها من أجل ضمان عدم استفحال الجريمة من جهة، ولتفادي إفلات المجرمين من العقاب من جهة أخرى **(مطلب أول)**.

بعد ذلك وأمام عدم إيفاء النصوص التقليدية بالغرض عدم سماحها بمكافحة فعالة للجريمة المرتكبة عبر الإنترنت خاصة مع التطور الهائل في تكنولوجيا الإعلام والاتصال، وتنويع أساليب ارتكابها، الأمر الذي أدى به إلى استحداث نصوص قانونية موضوعية خاصة بها **(مطلب ثان)**.

المطلب الأول

مكافحة الجريمة المرتكبة عبر الإنترنت في ظل النصوص التقليدية

واكب المشرع الجزائري التطورات التشريعية الموضوعية على المستوى الدولي من اجل مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك إدراكا منه أنه لن يكون بمعزل عن هذه التطورات من جهة، ولن يكون بمأمن من استفحال الجريمة المعلوماتية من جهة أخرى، فكانت محاولاته في الحد من هذه الجريمة المستحدثة منصبة على تحيين وتفعيل النصوص القانونية التقليدية القائمة لجعلها تتماشى مع التطورات التي تعرفها تلك الجريمة، فعدّل كأول

خطوة في هذا المجال قانون العقوبات **(فرع أول)**، ثم تلاه تعديل النصوص المتعلقة بالملكية الفكرية التي أصبحت مرتبطة ارتباطا وثيقا بتقنية الاتصال العالية **(فرع ثان)**.

الفرع الأول

تعديل قانون العقوبات لمكافحة الجريمة المرتكبة عبر الإنترنت

تم تدارك الفراغ التشريعي في مجال جرائم تقنية المعلومات بصفة عامة وجرائم الإنترنت بصفة خاصة عن طريق تعديل قانون العقوبات، وذلك بمقتضى القانون رقم 04-15[141]، والذي بموجبه جرّمت العديد من الأفعال التي يكون العالم الافتراضي مسرحا لها وذلك بتسميتها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والتي سنتطرق إليها من خلال تبيان تجريم الاعتداء على نظام المعالجة الآلية للمعطيات **(أولا)**، ثم إلى تجريم الاعتداء على معطيات نظام المعالجة الآلية للمعطيات **(ثانيا)**.

أولا: تجريم الاعتداء على نظام المعالجة الآلية للمعطيات

اعتبر المشرع جريمة المساس بأنظمة المعالجة الآلية للمعطيات كجريمة من الجرائم المستحدثة، لهذا وضعها ضمن إطار قانوني يكفل مكافحتها بطريقة فعالة وذلك بتجريمها وفق تعديل قانون العقوبات، حيث وضع لها قسم خاص تضمنته المواد من 394 مكرر إلى 394 مكرر 7، وذلك سعيا منه إلى مواكبة التطورات في المعاملات الإلكترونية بصفة عامة والجرائم التي ترتكب عبرها بصفة خاصة، وسوف نبين ذلك على النحو التالي:

1-الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنه: "**يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك**".

---

[141]- قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يتضمن تعديل قانون العقوبات، ج ر عدد 71، صادر في 10 نوفمبر 2004.

أ- الدخول غير المرخص به لنظام المعالجة الآلية للمعطيات

يفهم من نص المادة المذكورة أعلاه أن الجزاء عن مثل هذه الجرائم يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول عن طريق الغش، وطبعا هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط[142].

يستمد الدخول غير المصرح به عدم مشروعيته من كونه غير مصرح به وتم دون رضاء من صاحب هذا النظام أو رغما عنه، سواء كان الدخول لكل النظام أو لجزء منه فقط، وفي كلتا الحالتين نكون بصدد دخول معنوي لا يتم بالطرق التقليدية لذا نجد تعدد محاولات الفقه في تحديد معناه، وهي محاولات ركزت جميعها على أنه ولوج بالطرق المعلوماتية ذو مدلول معنوي يشبه الدخول في ذاكرة الإنسان ومدلول آخر مادي يتمثل في أن الشخص يكون قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي له دلالتان، دلالة المكان وهو التسلل لداخل النظام المعلوماتي، ودلالة زمنية وتتمثل في تجاوز وقت وحدود التصريح أو الترخيص إن وجد مثل هذا التصريح[143].

ب- البقاء غير المرخص به في نظام المعالجة الآلية للمعطيات

لم يتطرق المشرع الجزائري لمعنى البقاء، لذا نجد الفقه قد تصدى لبحث هذه المسألة، وتعددت تعريفاته، غير أنها في مجملها تركز على أن البقاء هو أن يكون الجاني قد دخل

---

[142] – **ناجية شيخ**، « **حول مكافحة الجريمة الإلكترونية في التشريع الجزائري** »، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص 690، أنظر كذلك:

- **CASILE Jean-François**, Le code pénal à l'épreuve de la délinquance informatique, presses universitaires d'Aix-marseille, France, 2002, p 65.

[143] – **حمودي ناصر**، « **الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري** »، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية الحقوق والعلوم السياسية، جامعة بجاية، سنة 2016، ص 74، أنظر كذلك:

- **CHILSTEIN David,** Législation sur la cybercriminalité en France, revue internationale de droit comparé, vol 62, n° 2, 2010, p 558, disponible en ligne à l'adresse: https://www.persee.fr/doc/ridc_0035-3337_2010_num_62_2_19954

النظام عن طريق الصدفة أو الخطأ، ومن بعدها يقرر البقاء داخله وعدم قطع الاتصال به، وبالتالي هي جريمة سلوك إيجابي يتحقق بالترك أو الامتناع كما أنها جريمة مستمرة[144].

يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام، وقد يجتمعان ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، فيجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي[145].

2-الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات

نصّت المادة 394 مكرر 3/2 على مضاعفة العقوبة إذا ترتب على هذا الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة، أما إذا انجر عن هذا الدخول أو البقاء تخريب لنظام اشتغال المنظومة فتكون العقوبة الحبس من ستة 6 أشهر إلى سنتين 2، والغرامة من 50,000 دج إلى 150,000 دج.

تضمنت الفقرة الثانية من المادة المذكورة أعلاه، الظرف المشدد في صورة ما إذا ترتب عن الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة، ويكفي لتوافر هذا الظرف المشدد أن يكون هنالك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات الموجودة به، وهي النتيجة التي اعتبرها المشرع ظرفا مشددا في هذه الجريمة[146].

144- **حمودي ناصر**، « **الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري** »، مرجع سابق، ص 75.

145- **قارة آمال**، الجريمة المعلوماتية، مذكرة مقدمة من أجل الحصول على درجة الماجستير، كلية الحقوق، جامعة الجزائر، سنة 2001-2002، ص 44.

146- **حمودي ناصر**، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة الماجستير، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2015، ص84.

ثانيا: تجريم الاعتداء على معطيات نظام المعالجة الألية للمعطيات

جرّم المشرع الاعتداء على معطيات نظام المعالجة الآلية للمعطيات من خلال نصّه على الأفعال التالية:

1- الاعتداء على المعطيات الداخلية للنظام

يتم الاعتداء على المعطيات الداخلية للنظام عن طريق فعل الإدخال والمحو والتعديل وهذا ما سنتطرق إليه كالتالي:

أ- فعل إدخال المعطيات في نظام المعالجة الألية

يقصد بذلك إدخال معطيات في نظام المعالجة لم تكن موجودة من قبل[147]، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولا سيما في المنشآت ذات الأموال، حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب[148].

ب- فعل محو معطيات من نظام المعالجة الآلية

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[149].

ت- فعل التعديل في معطيات نظام المعالجة الآلية

يقصد بهذا الفعل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق هذا الفعل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو

147- **MAALAOUI Ibtissem**, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit L L M, option droit des affaires, université de Montréal, 2011 p 71.

148- **خثير مسعود**، الحماية لبرامج الكمبيوتر أسايب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010، ص 124.

149- **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2007، ص 122.

جزئيا أو بتعديلها، وذلك كاستخدام القنابل المعلوماتية الخاصة بالمعطيات، برنامج الممحاة، أو برامج الفيروسات بصفة عامة[150].

مما سبق نجد أن هاته الأفعال (الإدخال، المحو، التعديل)، جاءت على سبيل الحصر، وبالتالي فلا يقع تحت طائلة التجريم أي فعل آخر غيرها كنسخ المعطيات أو نقلها، وإنما يمكن حمايتها ضمن نطاق حق المؤلف[151].

2- الاعتداء على المعطيات الخارجية للنظام

نصّت على ذلك المادة 394 مكرر 2 من قانون العقوبات، وكرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومة داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا.

تنص المادة 394 مكرر 2 الفقرة الأولى على أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو قرص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية مادامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

جرّمت الفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات أفعال الحيازة والإفشاء، النشر، والاستعمال أيا كان الغرض من هذه الجرائم الواردة في القسم السابع مكرر من قانون العقوبات، وقد يكون الهدف من ذلك المنافسة غير المشروعة، الجوسسة، الإرهاب أو التحريض على الفسق[152].

150- **MAALAOUI Ibtissem,** op-cit, p 72.

151 – **خثير مسعود**، مرجع سابق، ص ص 124-125.

152 – **مختارية بوزيدي**، ماهية الجريمة الإلكترونية، مقال موجه للملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص 18.

3- الاعتداء على سير نظام المعالجة الآلية للمعطيات

يقصد بعرقلة سير نظام المعالجة الآلية للمعطيات، ذلك الفعل الذي يسبب تباطؤ في عمل النظام أو ارتباكه[153]، مما يؤدي إلى تغيير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت[154].

يتحقق الركن المادي لهذا النوع من الجرائم من خلال وقوع اعتداء على نظام معلوماتي يسبب ارتباكا في عمله قد يكون دائما في حال استعمال الفيروسات، أو مؤقتا يهدف إلى شل أو تعطيل النظام كما هو الحال في حالة استعمال القنابل المنطقية أو من خلال إغراق الخادم بالرسائل الإلكترونية لأجل الحد من قدرته على التعامل مع المعلومة[155].

أ- تعطيل نظام المعالجة الآلية للمعطيات

تعتبر عملية عرقلة سير عمل نظام المعالجة الآلية للمعطيات بأنها "فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام، وهذا الارتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على السواء"[156].

يحصل فعل التعطيل أو التوقيف بأي وسيلة كانت، فالمشرع لم يشترط وسيلة معينة، وبالتالي فيستوي أن يكون بوسيلة مادية أو معنوية، ومن أمثلة وسائل التعطيل المادية استعمال العنف لمنع الوصول إلى الأجهزة ككسرها، أو تحطيمها أو تحطيم أسطوانة، أو

153- **MATIGNON Emmanuelle**, op-cit, p 16.

154- لم يورد المشرع الجزائري نصا خاصا بالاعتداء العمدي على سير النظام و اكتفى بالنص على الاعتداء ألعمدي على المعطيات الموجودة بداخل النظام و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية. فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء ألعمدي على النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الاعتداء ألعمدي على المعطيات، أنظر في ذلك: **فشار عطاء الله**، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا بليبيا، أكتوبر ، 2009ص 28.

155 - **خزار لمياء**، الحكومة الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون، تخصص قانون إداري وإدارة عامة، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة 1، 2017-2018، ص 134.

156- **خثير مسعود**، مرجع سابق، ص 121.

قطع شبكات الاتصال، أما الإعاقة أو التعطيل بوسيلة معنوية، فقد تتحقق بإدخال فيروس في البرنامج، أو تعديل كلمة السر، أو كيفية آداء النظام لوظيفته بوسيلة تؤدي إلى أن يتباطأ في آدائه لوظيفته المعلوماتية داخل النظام المعلوماتي[157].

ب- إفساد نظام المعالجة الآلية للمعطيات

يقصد بالإفساد كل فعل وإن كان لا يؤدي إلى التعطيل، فإنه يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

الإفساد من هذه الزاوية يقترب من التعييب الذي سبقت الإشارة إليه عند التعرض للظرف المشدد لجريمة الدخول والبقاء غير المشروعين، والفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة للجريمة التي نحن بصدد دراستها وهي جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات[158].

الفرع الثاني

مكافحة الجريمة المرتكبة عبر الإنترنت في قوانين الملكية الفكرية

واجهت حقوق الملكية الفكرية نتيجة لظهور الثورة التكنولوجية في مجال الاتصالات خاصة شبكة الإنترنت العديد من الاعتداءات وذلك راجع إلى التسهيلات التي تقدمها شبكة الإنترنت والتي أصبحت مناخا يلجأ إليه كل مبدع من أجل إظهار قدراته الفكرية والفنية، غير أن هذا التداول للإنتاج الفكري عبر الإنترنت طالته أيادي الإجرام وأصبح عرضة للاستيلاء والتقليد دون رقيب أو حسيب خاصة في ظل غياب قوانين تكفل هذا التحول الرقمي للإنتاج الفكري، الأمر الذي أدّى بالتشريعات المختلفة ومنها المشرع الجزائري إلى محاولة سد هذا الفراغ التشريعي عن طريق تعديل قوانين الملكية الفكرية لكي يحمي هذه

---

[157] – **خثير مسعود**، مرجع سابق، ص 121.

[158] – **آمال قارة**، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 119.

المصنفات من مختلف الجرائم التي تطالهم عبر الإنترنت، وسوف نحاول توضيح ذلك من خلال استقرائنا لقانون الملكية الأدبية والفنية **(أولا)**، ثم في قوانين الملكية الصناعية **(ثانيا)**.

أولا- في إطار قانون الملكية الأدبية والفنية

نظم المشرع الملكية الأدبية والفنية بمقتضى الأمر 73-14 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 97-10 المؤرخ في 1997/03/06 المعدل والمتمم بموجب الأمر 03-05 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، والذي حدد ما يلي:

1-المصنفات المحمية بموجب قانون حق المؤلف

أدّى الاعتماد المتزايد على جهاز الحاسوب وشبكاته خاصة شبكة الإنترنت في وقتنا الراهن من قبل المؤلفين نظرا للتسهيلات التي تقدمها من ناحية تقليل الجهد والوقت في إعداد أعمالهم من جهة، وظهور أعمال جديدة خاصة بمجال الإعلام الآلي لا نجدها في العالم الملموس، إلى سعي المشرع لحصرها من أجل حمايتها من كل الاعتداءات والتي حددها في برامج الحاسوب **(أ)** وقواعد البيانات **(ب)**:

أ- برامج الحاسوب

تعد برامج الحاسوب أول وأهم مصنّفات المعلوماتية التي حظيت باهتمام كبير من حيث وجوب الاعتراف بها وتوفير الحماية القانونية لها، ولم يضع المشرع تعريفا لها رغم أنه اعترف لها بالكيان الفكري المشمول بالحماية القانونية.

عرفت المنظمة العالمية للملكية الفكرية البرنامج على أنه تعليمات يمكنها إذا ما نقلت على ركيزة تستوعبها الآلة أن تساعد في الوصول إلى هدف أو نتيجة معينة، ويمكنها القيام بالتعامل مع المعلومة محل المعالجة، يلاحظ على هذا التعريف شموله أية آلة وليس فقط الحاسب الآلي، ثم أنه غائي يعتمد على الهدف من البرامج وهو الحصول على نتيجة[159].

[159]- **حابت آمال**، التجارة الإلكترونية في الجزائر، رسالة لنيل شهادة دكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2015، ص 318.

ب- قواعد البيانات

قواعد البيانات هي تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز ويكون مخزنا بواسطة الكمبيوتر ويمكن استرجاعه بواسطته أيضا[160]، فهي قواعد مرجعية تتوزع على العديد من المجالات منها: العلوم الإقتصادية، علوم الطب، العلوم التقنية.

هذا التجميع المهيكل في قاعدة البيانات يتم عرضه على جمهور المستعملين للاستفادة منه، ويمكن عرض عدة أمثلة على أنواع البيانات منها الموسوعات، المجموعات، الفهارس، المجلات، دليل الهاتف سواء كان عاديا أم إلكترونيا[161].

2-شروط المصنفات المحمية بموجب حق المؤلف

يشترط في المصنفات لكي تنال الحماية القانونية اللازمة بمقتضى حق المؤلف أن تتوفر فيها صفات معينة يمكن أن نوجزها على النحو التالي:

أ- شرط الإبتكار

تتمتع مجموعات البيانات وبرامج الحاسوب بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب محتواها أو ترتيبها[162]، والابتكار في ميدان الإنترنت ليس شرطا للحماية فقط، بل عنصرا رئيسيا في وجود الموقع وتحقيق النجاح والقدرة على المنافسة، ويظهر الابتكار في تصميم صفحة الويب (الموقع) وما يتضمنه من رسومات أو

---

[160]- **خالدة هناء سيدهم**، حماية حقوق الملكية الفكرية للمصنفات الرقمية في بيئة الإنترنت، مقال موجه للمؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، المنعقد بطرابلس، بتاريخ 24-25 مارس 2017، منشورات مركز جيل البحث العلمي، لبنان، ص 37.

[161]- **خثير مسعود**، مرجع سابق، ص 17-18. أنظر كذلك: **دعاس كمال**، حق المؤلف في ميدان المصنفات الرقمية، أطروحة دكتوراه علوم في القانون، كلية الحقوق، جامعة الجزائر، 2018، ص 163.

[162]- **أمير فرج يوسف**، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص 58.

ما يصاحبه من موسيقى أو عناصر حركية كما يتوفر الابتكار في المواد الصحفية والتقارير الإخبارية المنشورة عبر الإنترنت[163].

ب- الإيداع القانوني

يعتبر الإيداع القانوني شرط شكلي للاستفادة من الحماية القانونية للبرنامج، ذلك أن اتمام الإيداع يؤدي إلى استحداث مركز قانوني جديد يتمثل في انضمام برنامجه لنطاق المصنفات المحمية بموجب قانون المؤلف[164]، والايداع حسب المادة 02 من الأمر 96-16[165] هو إجراء ملزم لكل شخص طبيعي أو معنوي له انتاج فكري أو فني يوجه للجمهور.

يتم الايداع القانوني وفق إجراءات قانونية حددها الأمر رقم 96-16 بحيث يقوم المؤلف بالإيداع مباشرة أو عن طريق شخص آخر كالموزع أو المنتج، لمركز إيداع النسخ المطلوب إيداعها مرفقا بإقرار مؤرخ وموقع يتضمن هوية القائم بالايداع أو مسماه التجاري، عنوانه، صفته، هوية المؤلف، عنوان البرنامج، اسم المنتج، الطبعة أو إعادة الطبعة وتاريخ إنجازها، عدد النسخ، ثم يقوم مركز الإيداع بتسليم نسخة من المصنف عليها ختم المركز بعد تسجيل المصنف بتضمينه رقم الإيداع القانوني وتاريخه على المؤلف[166].

---

[163]- يرى جانب من الفقه أن المصنفات الرقمية محمية بموجب القواعد العامة للمصنفات الأدبية دون حاجة لإفراد قواعد جديدة، باعتبارها تتميز بتدخل برنامج كمبيوتر يسمح بالتفاعل بين وسائل التعبير المتعددة وبرنامج الكمبيوتر محل حماية أو لأنها بمفرداتها محل حماية باعتبار هذه المفردات من المصنفات الأدبية أصلا: -المواد المكتوبة، المواد السمعية، والمرئية، الأداء....الخ، وكلما توفر فيها عنصر الابتكار تحقق شرط الحماية المطلوب لحماية المصنفات الأدبية، أو باعتبارها من قبيل قواعد البيانات المحمية بموجب نصوص صريحة. أنظر في ذلك: **قلاتي دنيازاد، «الحماية الجزائية للحق المعنوي للمؤلف على المصنفات الرقمية»**، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 44، جوان 2016، ص 323.

[164]- نصت المادة 07 من الأمر رقم 03-05 على منح الحماية لكل مصنف مهما كان نوعه أو درجة استحقاقه بمجرد إيداعه.

[165]- أمر رقم 96-16 مؤرّخ في 02 يوليو سنة 1996، يتضمن الإيداع القانوني، ج ر، عدد 41، صادر في 03 يوليو 1996.

[166]- **حابت آمال**، مرجع سابق، ص 326.

3-الحقوق التي يخولها قانون حق المؤلف للمصنفات الرقمية

يترتب عن اعتراف القانون للمؤلف بالحق في المصنفات الرقمية عدة حقوق نذكر منها:

أ- الحقوق الأدبية

تتمثل الحقوق الأدبية في:

أ/1- الحق في نسبة المصنف الرقمي إلى المؤلف

يكون لمؤلف البرنامج وحده الحق في نسب البرنامج لشخصه، ويتم ذلك بوضع اسمه على الدعامة المادية لبرنامج الحاسب الآلي المحمي قانونا، ويستوي أن يكون صاحب البرنامج شخصا واحدا أو عدة اشخاص اشتركوا في تأليف البرنامج، فيكون من حقهم جميعا ذكر أسمائهم على دعامة البرنامج، كما يستوي أن يكون صاحب البرنامج شخصا طبيعيا أو معنويا، ويعتبر معتديا على هذا الحق كل من ينسب هذا البرنامج لشخصه دون أن تكون له مساهمة مباشرة ومعتبرة في إعداده[167].

أ/2- الحق في سحب المصنف الرقمي

قد يرى المؤلف بعد مدة من نشر مصنفه أنه أصبح غير معبر عن أفكاره وبعيد كل البعد عن معتقداته الجديدة أو أنه قد أصبح غير متطور مع فكرة أو ماسا بسمعته، وفي هذه الحالة يفكر في سحبه من التداول من أجل تعديله أو إتلافه نهائيا، ويستند في ذلك على حقه في سحب مصنفه من التداول والرجوع عنه. وحق السحب يعد في الواقع أحد مظاهر الحق الأدبي وفقا لما نصت عليه التشريعات المقارنة[168].

أ/3- الحق في الحفاظ على المصنفات الرقمية

يكفل نظام حقوق المؤلف لأصحاب المصنفات المحمية بهذا النظام، بمن فيهم أصحاب وملاك برامج الحاسب الآلي، الحق في دفع أي اعتداء من شأنه المساس بسلامة

---

[167] – **بن يطو أسامة، عبدلي حمزة**، مرجع سابق، ص ص 136-137.

[168] – **سليم عبد الله الجبوري**، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2011، ص 264.

هذا المصنف ومن ذلك، اي تعديل أو تحوير أو تحريف من شأنه أن يغيّر من الهدف أو الغرض الأساسي المبتغى من تصميم هذا البرنامج أول مرة، كما يحق لصاحب البرنامج أن يدفع أي اعتداء على برنامجه، الذي من شأنه أن يشكل مساسا بسمعته أو شرفه كمؤلف للبرنامج[169].

ب- الحقوق المالية

يتمتع مؤلفو المصنفات المبتكرة بعدد من الوسائل التي تمكنهم من استغلال مصنفاتهم من طرف الغير وذلك بقصد الحصول على عائد مالي ليتمتع المؤلف بحق استغلال مصنفه مستأثرا بهذا الحق وفقا للمادة 27 من الأمر رقم 03-05 وذلك عن طريق استنساخ المصنف بأية وسيلة، وضع أصل المصنف أو نسخ منه رهن التداول بين الجمهور بواسطة التأجير، إبلاغ المصنف إلى الجمهور بأية منظومة معلوماتية، الترجمة والاقتباس وإعادة التوزيع، وغير ذلك من التحولات المدخلة على المصنف المؤلف والتي تتولد عنها مصنفات مشتقة، وكل عمل مشروع من شأنه الحصول على عائد مالي منه، ونكتفي بهذه الصور لأنها ممكنة بالنسبة لبرامج الحاسوب وقواعد البيانات.

أما صور الاستغلال الاخرى كإبلاغ الجمهور عن طريق الآداء العلني، وكذا إذاعة المصنف بواسطة الوسائل السلكية واللاسلكية فلا تتوافق وطبيعة هذه المصنفات، وتتميز الحقوق المالية مقارنة بالحقوق الادبية بإمكانية أو جواز التصرف فيها، إذ للمؤلف التنازل جزئيا أو كليا عن حقوقه المالية بمقابل أو بدونه[170].

ثانيا: في إطار قانون الملكية الصناعية

تدعيما لقانون حق المؤلف والحقوق المجاورة في مجال حماية الملكية الفكرية في العصر الرقمي، قام المشرع الجزائري بتفعيل القوانين المتعلقة بالملكية الصناعية في شتى أنواعها وهي:

---

169 – **بن يطو أسامة، عبدلي حمزة**، مرجع سابق، ص 138.

170 – **مشري راضية، «الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف»**، مجلة التواصل في العلوم الإنسانية والإجتماعية، جامعة عنابة، عدد 34، جوان 2013، ص ص 140-141.

1-من خلال أحكام العلامات التجارية

تمت معالجة الملكية الفكرية في نطاق المعلوماتية من خلال أحكام العلامات التجارية على النحو التالي:

أ- مفهوم العلامة التجارية

نظم المشرع العلامات التجارية من خلال الأمر رقم 03-06[171] المؤرخ في: 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر رقم 66-57[172] المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 67-223 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية.

عرّفت المادة الثانية 02 من الأمر رقم 03-06 العلامة التجارية على أنها: "**العلامات: كل الرموز القابلة للتمثيل الخطي، لا سيما الكلمات بما فيها أسماء الأشخاص والأحرف والأرقام، والرسومات أو الصور والأشكال المميزة للسلع أو توضيبها، والألوان بمفردها أو مركبة، التي تستعمل كلها لتمييز سلع أو خدمات شخص طبيعي أو معنوي عن سلع وخدمات غيره**".

يفهم من نص المادة أن العلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات، ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام العام والآداب العامة.

ب- شروط حماية العلامة التجارية

1-يجب أن تكون العلامة ذات صفة فارقة مميزة لها عن غيرها من السلع أو مميزة لها عن نوع المنتج الذي توضع عليه.

---

[171]- أمر رقم 03-06 مؤرخ في 19 يوليو 2003، يتضمن العلامات، ج . ر عدد 44، صادر في 23 يوليو 2003.

[172]- أمر رقم 66-57 المؤرخ في 19 مارس 1966، يتضمن علامات المصنع والعلامات التجارية، ج. ر عدد 23، صادر في 22 مارس 1966.

2-يجب أن تكون العلامة التجارية جديدة لم يسبق تسجيلها أو استعمالها على منتجات أخرى.
3-لا يجوز أن تكون العلامة التجارية شائعة الاستعمال حتى لا يحتكرها أحد.
4-لا يجوز أن تكون العلامة التجارية مخالفة للنظام العام والآداب العامة[173].

غير أن السؤال المطروح هل يمكن تطبيق المبادئ المقررة لحماية العلامات التجارية على برامج الحاسب الآلي؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به.

وقد تكون الحماية بأحكام العلامة التجارية فعّالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد[174].

2-من خلال أحكام براءة الاختراع :

تم تنظيم براءة الإختراع بقوانين خاصة كغيرها من القوانين الأخرى وذلك بقانون شهادة المخترعين وبراءة الاختراع رقم 66-54 المؤرخ في 06 مارس 1966 والملغى بالمرسوم التشريعي رقم 93-17 المؤرخ في 07 ديسمبر 1993 والذي ألغي بمقتضى الأمر رقم 03-07[175]، حيث عرفت المادة الثانية 02 منه، "**الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية**"، بالإضافة إلى تبيان الشروط المطلوبة فيه كشرط الابتكار، شرط الجدة، القابلية للتطبيق الصناعي، المشروعية)[176].

---

[173]- **مؤيد زيدان**، حقوق الملكية الفكرية، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2020، ص 74.

[174]- **فشار عطاء الله**، مرجع سابق، ص 11. أنظر كذلك: **طارق بوبترة، «الحماية القانونية الداخلية للعلامة التجارية»**، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد 31، عدد 1، جوان 2020.

[175] - أمر رقم 03-07 المؤرخ في 2003/07/19، يتضمن براءات الإختراع، ج.ر عدد 44، صادر في سنة 2003.

[176]- شرط الابتكار: يعتبر شرط مهم لحماية البرمجيات لأنه يرد على طبيعة هذه البرمجة الفكرية وقيمتها الفنية ومدى استحقاقها للحماية، ويستند هذا الاستحقاق على درجة التقدير الذي تتلقاه هذه البرمجية أو ذاك المصنف بناءا على أصالته

أ- مدى تحقق شرط الاختراع على برامج الحاسب الآلي

يتحصل المخترع في حال توافر هذه الشروط على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

وإبراز شخصية صاحبها سواء في مضمون وجوهر الفكرة أو في الطريقة التي اتبعها لعرض هذه الفكرة. أنظر في ذلك: **بوذراع عبد العزيز**، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2011-2012، ص ص 52-53

- شرط الجدة: بحيث يجب أن يكون الاختراع جديدا ولم يسبق للجمهور أن تعرف عليه من قبل، ولقد أخذ المشرع الفرنسي بمبدأ الجدة المطلقة إلى أبعد حدود الاطلاق بشأن براءات الإختراع، فيكفي لإسقاط حماية أن يثبت أنه قد سبق اختراعه في أي مكان في العالم، وفي أي وقت وبأي وسيلة، ونفس المنهج انتهجه المشرع الجزائري بصدد الجدة. أنظر في ذلك: **بدرة عمارة، «الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية»**، مجلة الفقه والقانون، مجلة إلكترونية شهرية تعنى بنشر الدراسات الشرعية والقانونية، العدد السادس والثلاثون، أكتوبر 2015، ص 57.

- القابلية للتطبيق الصناعي: يشترط أن يتوفر في الاختراع الخاصية الصناعية، أي أن يكون قابلا للتطبيق والاستثمار في الصناعة، إذ أن البراءة تعطي لصاحبها حقا احتكاريا مانعا، لذلك يجب أن يكون هذا الاختراع قابلا للاستثمار، ذا صلة بشيئ مادي ملموس، ويترتب على ذلك أنه لا يعتبر من قبل الاختراعات الأفكار والنظريات العلمية البحتة والأساليب المالية التي لا تطبق في الصناعة كالنظرية النسبية، أو وضع طريقة جديدة لمسك الدفاتر الحسابية مثلا، وما يقال هنا عن الأفكار والنظريات، يصدق ايضا على الاكتشافات العلمية التي يصل إليها الإنسان عن طريق ملاحظة الظواهر الطبيعية، ككشف قانون الجاذبية أو غير ذلك، إلا إذا اقترنت بتطبيقات صناعية جديدة، ومرد ذلك هو قانون حماية الاختراعات يهتم فقط بالابتكارات الفنية المطبقة في مجال الصناعة دون غيرها عموما. أنظر في ذلك: **سليم عبد الله الجبوري**، مرجع سابق، ص ص 188-189

- المشروعية: نص المشرع الجزائري على هذا الشرط في المادة (08) من الأمر رقم (03-07) المتعلق ببراءة الاختراع بأنه: "لا يمكن الحصول على براءة اختراع بموجب هذا الأمر بالنسبة لما يأتي:...الاختراعات التي يكون تطبيقها مخلا بالنظام أو الآداب العامة...". نستشف من هذه المادة أنه لايمكن أن تمنح الهيئة المختصة براءة اختراع بخصوص الاختراعات التي يخالف تطبيقها النظام العام والآداب العامة، مثل اختراع آلة لإخفاء البصمات، أو آلة لتزييف العملة. أنظر في ذلك: **بن زواوي سفيان**، عقد الترخيص باستغلال براء الاختراع في التشريع الجزائري، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في القانون الخاص، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2020/2019، ص 24.

لكن في هذا الإطار يمكن أن نتساءل عن إمكانية استفادة برامج الحاسب من الحماية بواسطة براءات الاختراع ؟

لم تتعرض قوانين براءات الاختراع في التشريعات المقارنة لإمكانية منح براءة اختراع للمعلومات المدخلة في شبكة الإنترنت، ولعل السبب في ذلك يعود إلى أن المعلومات المدخلة في الشبكة المذكورة، وما تثيره من إشكالات سواء ما تعلق منها بتكييفها وتحديد طبيعتها وقابليتها لأن تكون منتجا من عدمه أو صلاحيتها للحماية وفق قواعد براءات الاختراع[177]. ولعل السبب في ذلك يعود إلى:

- إمّا لعدم تمتع البرنامج من أي طابع صناعي.
- أو إمّا صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة، فليس من الهيّن توافر شرط الجدّة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال التي تتولى بحثه[178].

تجدر الإشارة كذلك إلى أن المشرع قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للفقرة السادسة من المادة السابعة من الأمر رقم 03-07 المتضمن براءة الاختراع التي تنص على:

" **لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب** ".

نلاحظ أن المشرع قد اعترف فقط بالحماية القانونية لبرامج الحاسوب وقواعد البيانات بمقتضى قانون الملكية الأدبية والفنية وذلك حماية لها من كل أشكال الاعتداء التي كان ينص عليها قانون العقوبات فيما سبق طبقا للمواد 390 إلى 394، ليقوم فيما بعد بتجريمها

---

[177]– **سليم عبد الله الجبوري**، مرجع سابق، ص 195.

[178]– **قارة أمال**، الجريمة المعلوماتية، مرجع سابق، ص 112.

بموجب قانون خاص وهو الأمر 97-10 حيث أن قانون العقوبات كان يقرر بموجب المادة 393 الغرامة المالية كعقوبة للاعتداء على حق المؤلف بينما الأمر 97-10 وكذا الأمر 03-05 يقران عقوبتي الحبس والغرامة.

غير أنه لاحظنا في نفس الصدد أن المشرع لم يعط الشق الثاني من حقوق الملكية الفكرية والمتمثلة في الملكية الصناعية حقها من المعالجة القانونية، حيث نرى أن مكافحة الجرائم التي ترتكب في هذا المجال لم تنل قسطها من المكافحة الفعالة، وذلك راجع إلى أن النصوص القانونية التي تعالج هذا المجال جاءت مقتضبة وقليلة من جهة، وكذلك تبقى مسألة حماية حقوقها مرهونة بشروط معينة من جهة أخرى، لتبقى مكافحة الجريمة المرتكبة عبر الإنترنت الماسة بحقوق الملكية الفكرية عامة والملكية الصناعية خاصة دون معالجة فعّالة خاصة بالمقارنة مع الاعتماد المتزايد على شبكة الإنترنت في تداول هذه المصنفات وكثرة الجرائم التي تطالها في هذا النطاق.

المطلب الثاني

مكافحة الجريمة المرتكبة عبر الإنترنت من خلال قوانين مستحدثة

على الرغم من مواكبة المشرع للتطور التشريعي الحاصل على المستوى الدولي في مجال المعلوماتية من خلال تعديله للنصوص القانونية القائمة، إلا أن هذه المواكبة بقيت نسبية ولم تف بالغرض، نظرا للتطورات التي تعرفها الجريمة المرتكبة عبر الإنترنت على المستوى الدولي والوطني على حد سواء، حيث أنه لم يوفق في الإحاطة الشاملة بكل الجرائم المرتكبة من خلال نظم المعلوماتية، الأمر الذي أدى به إلى استحداث نصوص قانونية خاصة بداية من سنة 2009 لمّا أصدر القانون المتضمّن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيا الإعلام والاتصال ومكافحتها **(فرع أول)**، لتليها تشريعات أخرى تتضمن قواعد التجارة الإلكترونية نذكر منها خاصة قانون رقم 18-05 **(فرع ثان)**، وقانون رقم 18-04 الذي يتضمن قواعد البريد والاتصالات الإلكترونية **(فرع ثالث)**.

الفرع الأول

مكافحة الجريمة المرتكبة عبر الإنترنت في ظل القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تدارك المشرع النقص والمحدودية التي عرفتها النصوص التقليدية وكان ذلك سنة 2009 أين أصدر قانون خاص يتعلق "بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها" تحت رقم 09-04[179] والذي من خلاله وضع الإطار القانوني الشامل لمكافحة هذا النوع المستحدث من الجرائم وسوف نبين ذلك من خلال المحاور التي جاء بها هذا القانون:

1- **المحور الاول:** تم التطرق فيه إلى الأحكام العامة التي من خلالها تتبيّن الأهداف المتوخاة من القانون وتحديد مفاهيم المصطلحات التي جاء بها.

عرّف هذا القانون الجرائم المرتكبة بواسطة تكنولوجيا الاعلام والاتصال، على أنّها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية[180].

---

[179]- قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47، صادر بتاريخ 16 أوت 2009.

[180]- عرّفها المشرع الجزائري بمقتضى الفقرة الثالثة من المادة 211 مكرر 22 من الأمر رقم 21-11 المؤرخ في 25 غشت 2021، يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج ر عدد 65، صادر بتاريخ 26 غشت 2021 على النحو التالي: "...يقصد بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الألكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

كما عرّف هذا النوع من الجرائم التي تتسم بالتعقيد بمقتضى الفقرة الثانية من المادة 211 مكرر 25 من نفس الأمر على أنها: "...يقصد بالجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا، بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة أضرارها

كما عرّف المنظومة المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[181].

أمّا المعطيات المعلوماتية فعرفها على أنّها أي عملية عرض وطرح للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها، وعرّف الاتصالات الإلكترونية والتي تكون في غالب الأحيان معرضة أكثر للقرصنة على أنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[182].

2-**المحور الثاني:** تضمن حالات اللجوء إلى المراقبة الإلكترونية كتدبير وقائي

وردت هذه التدابير الوقائية في مضمون المادة 04 من القانون رقم 09-04 التي حددت الحالات التي يجوز فيها لأجهزة الأمن القيام بمراقبة المراسلات الإلكترونية، وهي أربع حالات:

1- الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة.

2- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

3- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي".

[181]- أنظر الفقرة الأولى والثانية من المادة الثانية من قانون رقم 09-04، مرجع سابق.

[182] - لمزيد من الشرح أنظر **بن عقون حمزة**، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012، ص ص 188-189.

4- في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة[183].

3-**المحور الثالث:** تضمن القواعد الإجرائية الخاصة بهذا النوع من الجرائم أهمها تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية، بالإضافة إلى حفظ المعطيات المتعلقة بحركة السير.

4-**المحور الرابع:** تطرق إلى التزامات المتعاملين في مجال الاتصالات الإلكترونية، وذلك من خلال تحديد تلك التي تقع على عاتق المتعاملين في مجال الاتصالات الالكترونية لا سيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، ويهدف هذا القانون إلى إعطاء مقدمي الخدمات دورا إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبيها[184]

5- **المحور الخامس:** تضمن إنشاء الهيئة الوطنية للوقاية من الاجرام المتصل بتكنولوجيات الاعلام والاتصال ومكافحته **و**هي هيئة نصّ عليها بالقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث أنها سلطة إدارية مستقلة لدى وزير العدل[185]، تعمل تحت اشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء[186].

---

183 – لمزيد من التفاصيل أنظر، **ناجية شيخ**، مرجع سابق، ص697-698.

184 – **الأزرق بن عبد الله، أحمد عمراني**، نظام المعلوماتية في القانون الجزائري واقع وآفاق، مداخلة ضمن المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة، المفاهيم والتشريعات والتطبيقات، المنعقد بالرياض خلال الفترة 06-07 أفريل 2010، ، ص 16.

185- **بوعون زكرياء**، «**دور الهيئة الوطنية للوقاية من الجرائم الإلكترونية في حماية المستهلك**»، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد 1، عدد 49، جوان 2018.

186 – أنظر: مرسوم رئاسي رقم 15-261، مؤرخ في 08 أكتوبر 2015، يتضمن التشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،، ج.ر عدد 53، صادر بتاريخ 08 أكتوبر 2015.

حددت المادة 14 من القانون رقم 09-04 مهام الهيئة كالآتي[187]:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

6-المحور السادس: التعاون الدولي والمساعدة القضائية الدولية

تضمن هذا المحور قواعد الاختصاص القضائي والتعاون الدولي، فبالنسبة للاختصاص القضائي، ففضلا عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الاستراتيجية للجزائر مستهدفة[188].

---

[187]- بالرجوع إلى المادة 04 من المرسوم الرئاسي رقم 15-261 نجد أن للهيئة مهام أخرى وهي:
-إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
-مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.
-ضمان المراقبة للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

[188]- نصّ المشرع الجزائري على قواعد جديدة في الاختصاص بعد تعديل قانون الإجراءات الجزائية بمقتضى الأمر 21-11 الذي نص في مادته 211 مكرر 22 فقرة أولى وثانية على أنه: "ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها. كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت جنحا..."

أمّا فيما يتعلق بالتعاون الدولي[189]، فهو يقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث يتم اعتماد مبدأ التعاون على أساس المعاملة بالمثل[190].

الفرع الثاني

مكافحة الجريمة المرتكبة عبر الإنترنت في ظل قوانين التجارة الإلكترونية

تعتبر التجارة الإلكترونية واحدة من الاساليب الحديثة التي أخذت بالدخول إلى حياتنا اليومية حتى أنها أصبحت تستخدم في العديد من الأنشطة الحياتية والتي هي ذات ارتباط بثورة تكنولوجيا المعلومات والاتصالات[191].

اهتمت الكثير من دول العالم بإصدار تشريعات منظمة للتجارة الإلكترونية، وبيان أحكام المعاملات التي تتم من خلالها، وذلك راجع إلى أهمية موضوع التجارة الإلكترونية على المستوى الدولي والمحلي[192] من جهة، وضرورة تكريس حماية خاصة لبياناتها من جهة أخرى، وسنتطرق في هذا الصدد إلى الحماية الجنائية الخاصة لبيانات التجارة الإلكترونية **(أولا)**، ثم إلى الحماية الجنائية الخاصة لمضمون التجارة الإلكترونية **(ثانيا)**.

كما نصّت المادة 211 مكرر 23 على الاختصاص الإقليمي وذلك على النحو التالي: "يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني".

[189]- **Radia TITOYCHE**, Territorialité du droit pénale et la cybercriminalité, cahiers de politique et de droit, faculté de droit et des sciences politique, Université de Ouargla, onzième année, volume 11, n° 01, janvier 2019, p 34.

[190]– **الأزرق بن عبد الله، أحمد عمراني**، مرجع سابق، ص 17. وفي تعريف التجارة الإلكترونية أنظر كذلك:
- **ADJAYI KODJO Ndukuma**, Cyberdroit telecoms,Iinternet, Contrats de E-commerce, presses universitaires du Congo, Kinshasa, 2009, p p 47-48.

[191] – **أحمد بن خليفة، حفوظة الأمير عبد القادر، «الجريمة الإلكترونية وآليات التصدي لها»**، مجلة الامتياز لبحوث الاقتصاد والإدارة، المجلد 01، العدد 01، جامعة الأغواط، جوان 2017، ص151.

[192] – **لشهب حورية، «النظام القانوني للتجارة الإلكترونية دراسة مقارنة»**، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 23، نوفمبر 2011، ص 31.

أولا: الحماية الجنائية الخاصة لبيانات التجارة الالكترونية

يكتسي موضوع حماية بيانات التجارة الإلكترونية أهمية كبيرة، فهو موضوع ينصب مفهومه على ضمان حماية حركة التجارة الإلكترونية وذلك بحماية بياناتها من مختلف الجرائم مثل التحايل الإلكتروني للبيانات أو سرقتها، وسنبين ذلك من خلال النقاط التالية:

1-تجريم التعامل في بيانات التجارة الالكترونية بدون ترخيص

من متطلبات التعامل التجاري الإلكتروني تبادل البيانات الشخصية لطرفي العقد أو أحدهما، هذه البيانات منها ما يتعلق بالعملاء وخصوصا عندما يتعلق الأمر بطلبات السلع والخدمات كأسمائهم وعناوينهم وأرقام حساباتهم وأرقام بطاقاتهم المالية، ومنها ما يتعلق بالعاملين بالمشروع، كالبيانات المتعلقة بالموظفين والقائمين على الإدارة، مما يترتب عليه ضرورة توفير الحماية القانونية اللازمة لهذه البيانات وتجريم الاعتداء عليها بالاطلاع أو الإفشاء أو الإستغلال[193]

يتحقق الركن المادي في هذه الجريمة، بمجرد التعامل في بيانات التجارة الإلكترونية دون ترخيص من الجهة المختصة، وذلك أن معظم الدول التي تهتم بالنظم المعلوماتية، توضع في اعتبارها وجود جهة تصدر التراخيص أو الإذن بالتعامل في البيانات المعلوماتية لدى هذه النظم، كما هو الحال بالنسبة للمشرع الجزائري[194].

تعتبر هذه الجريمة من الجرائم العمدية وصورة العمد فيها، هو القصد في انصراف إرادة الجاني إلى تداول بيانات التجارة الإلكترونية بدون ترخيص، مع علمه بأن ذلك محظور

---

[193] – **خالد بن عبيد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية دراسة تحليلية مقارنة، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 107.

[194]– أنظر المادة 25 من قانون رقم 18-07 المؤرّخ في 01 يونيو 2018، يتضمّن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، صادر في 10 يونيو 2018.

ويعاقب عليه قانوناً، ومع ذلك تنصرف إرادته إلى هذه الافعال، ويكتفي في هذه الجريمة بالقصد الجنائي[195].

2-تجريم انتهاك سريّة وخصوصية البيانات في نطاق التجارة الالكترونية

تزايدت على مدى السنوات الماضية ومنذ ظهور الإنترنت عمليات نقل البيانات، وهو ما أثيرت معه مسألة كيفية توفير السرية لهذه البيانات وحمايتها، وهذه الصعوبة تتعلق بالنواحي الفنيّة الخاصة بتكنولوجيا المعلومات والاتصالات والبرمجيات وأنظمة التشغيل، وهناك نقص واضح في الأمان والبروتوكولات الإلكترونية عبر الإنترنت، وأيضا أدوات تطوير البرمجيات التي تتغير باستمرار[196].

لذلك اهتمت غالبية التشريعات -ومنها التشريع الجزائري- بموضوع سرية البيانات، احتراما للحق في الخصوصية[197]، وتجريم أي فعل من شأنه انتهاك السريّة والخصوصية، سواء صدر عن الشخص بنفسه أو بواسطة غيره، وذلك بكشف مفاتيح التشفير المودعة بمكتب كشف الشفرات أو إساءة استخدامه بأية صورة من الصور، وكما يعاقب كل من يقوم بفض معلومات مشفرة في غير الأحوال المصرح بها قانونا.

ويتحقق الركن المادي لهذه الجريمة بمجرد انتهاك سرية بيانات التجارة الإلكترونية وخصوصيتها، حتى ولو لم يترتب على الفعل أي نتيجة إجرامية، لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات وليس تحقيق نتيجة إجرامية.

أمّا بالنسبة للركن المعنوي، فجريمة انتهاك سرية البيانات وخصوصيتها هي من الجرائم العمدية، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة[198]

---

[195] - **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004، ص 273-277.

[196] - **مخلوفي عبد الوهاب**، التجارة الإلكترونية عبر الإنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012، ص 37.

[197]- **Rami HALIM**, La protection pénale du consomateur dans le cadre du commerce électronique, reuvu de recherches et études juridique et poulitique, faculté de droit et des sciences politique, université de Blida, numéru 2, janvier 2012, p 392.

[198] - **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 283-287.

3- تجريم التصريح عمدا بمعطيات خاطئة فيما يتعلق ببيانات التجارة الالكترونية

تعتبر هذه الجريمة من الجرائم التي تقع على بيانات التجارة الإلكترونية والغاية من تجريمها هي حماية المتعاملين في نطاق هذه التجارة، الذين يتعاملون في بياناتها، لأن التجارة الالكترونية تعتمد بالأساس على نظام معلوماتي حيث تعد المعلومات والبيانات فيه عنصرا جوهريا لهذه البيانات قيمة كبيرة مما يستدعي حمايتها جنائيا بتجريم جميع أفعال المساس بها، الأمر الذي يؤدي إلى الزيادة في ثقة المتعاملين في نطاق التجارة الالكترونية وبالتالي ضمان تقدمها[199].

تعد هذه الجريمة من قبيل جرائم السلوك المجرد أو جرائم الخطر، وليست من جرائم الضرر، بمعنى أن المشرع لا يشترط لقيام الركن المادي فيها، حلول ضرر معين، وإنما يكفي تحقق النشاط الإجرامي، وهو إعطاء أي بيانات أومعلومات غير صحيحة، سواء كان ذلك من قبل أي شخص، وسواء أعطيت هذه المعلومات إلى مورد خدمات التوثيق الإلكتروني أو أحد أطراف التعاقد.

تعد جريمة الإفضاء بمعطيات غير صحيحة من الجرائم العمدية بنص القانون، حيث وردت عبارة كل من "**صرح عمدا**" ولذلك فصورة القصد الجنائي في هذه الجريمة هو القصد الجنائي العام بعنصريه العلم والإرادة، والعلم في هذه الجريمة يعني أن يعلم الجاني بكافة وقائع هذه الجريمة فيعلم أنه يدلي بمعطيات خاطئة، سواء كان هذا الإدلاء لمورد خدمات التوثيق الإلكتروني أو لأحد أطراف العلاقة التعاقدية في التجارة الإلكترونية وكذلك يجب أن يعلم أن ذلك الفعل محظور قانونا، ومع ذلك تنصرف إرادته إلى فعل الإدلاء بالمعطيات غير الصحيحة وكذلك إلى قبول النتيجة المترتبة على فعله بوصفها مخالفة للقانون[200].

---

[199] – **خليفي مريم**، الرهانات القانونية للتجارة الالكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011-2012، ص 356.

[200] – **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص ص 291-293.

ثانيا: الحماية الجنائية الخاصة لمضمون التجارة الالكترونية

ظهرت مع زيادة التعامل في التجارة الإلكترونية العديد من الطرق والمفاهيم الحديثة في التعامل حيث تعتبر جوهر ولب التجارة الإلكترونية، نذكر منه التشفير والتوقيع الإلكترونيين ومختلف وسائل الدفع الإلكتروني بالإضافة إلى المستهلك الإلكتروني، وكل هذه المفاهيم والآليات تستوجب الحماية من مختلف الاعتداءات التي تطالها عبر الإنترنت، وهذا ما سعى إليه المشرع الجزائري عن طريق تجريم الأفعال التي تمس بها والتي سوف نبيّنها على النحو التالي:

1-تجريم فض مفاتيح التشفير الخاصة بالتوقيع الالكتروني

رغم أن التشفير هو الوسيلة الفعالة لحماية بيانات التوقيع إلا أنه لا يؤمنه، حيث يمكن فك أو كشف مفتاح التشفير الذي نعني به المفتاح الخاص والحصول عليه من قبل أشخاص غير مخولين باستخدامه، لذلك وضعت الشركات المصدرة للتوقيع الإلكتروني سياسات خاصة يجب اتباعها للحفاظ على المفتاح الخاص[201].

تعد مشكلة تزوير التوقيع الإلكتروني من الجرائم القوية والمنتشرة بشكل كبير خاصة مع زيادة حالات النصب والاحتيال والتسلل والاختراق غير المشروع لأجهزة الحاسب الآلي عن طريق شبكة الإنترنت، والوصول للشفرة الخاصة بصاحب التوقيع الإلكتروني ثم القيام بنسخها ووضعها على محرر مصطنع واستعماله، حيث تكون طريقة الاعتداء على وسائل التشفير الضرورية من خلال تتبع التوقيع الإلكتروني لشخص ما اختراقه للبحث عن هويته الإلكترونية من أجل التوصل إليها ثم استنساخ التوقيع الإلكتروني الخاص به[202].

---

[201]– **لالوش راضية**، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012، ص 157.

[202] – **عبد العزيز محمد سعد البواردي**، السياسة الجنائية المعاصرة في حماية التجارة الإلكترونية دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2011، ص 113-114. أنظر كذلك:

- **Benoit DUPONT**, La coévolution du « vol d'identité » et des systèmes de paiment, criminologie, volume 43, numéro 2, les presses de l'université de Montréal, automne 2010, p 250.

2-تجريم استغلال المتعامل في البيع الالكتروني

الاستغلال بصفة عامة، هو أن يعمد شخص إلى أن يستفيد من أحد نقاط الضعف لدى شخص آخر فيجعله يبرم تصرفا معينا للحصول على مزايا لا تقابلها منفعة لهذا الأخير أو تتفاوت مع هذه المنفعة تفاوتا غير مألوف ولقد حصره المشرع في حالتي الطيش البيّن أو الهوى الجامح الذي يعتري المتعاقد بغرض دفعه إلى إبرام عقد يتحمل بمقتضاه التزامات لا تتعادل بتاتا مع العوض المقابل أو من غير عوض.

تتزايد تطبيقات الاستغلال في الوقت الحاضر مع زيادة عدد الباعة والمنتجين ومقدمي الخدمات عبر مواقع الإنترنت بما فيها الشركات غير الجادة والوهمية التي تمارس نشاطات بهدف تحقيق الربح السريع بغض النظر عن الوسيلة المستخدمة هذا من جهة، ومن جهة أخرى ارتفع أيضا عدد المستخدمين حتى من بين اللذين يملكون تعليما بسيطا وتنقصهم الخبرة اللازمة للتعامل على شبكة الإنترنت[203].

تظهر الحكمة من تجريم استغلال المتعامل في عقود البيع الالكترونية في حماية المتعاقدين في هذه العملية وبشكل أخص المشتري في هذا العقد، لأن البائع غالبا ما يكون الطرف الأقوى في العلاقة التعاقدية[204]، الأمر الذي يجعل الطرف الآخر مدفوعا للتعاقد على نحو يتضمن غبنا واقعا عليه[205].

---

[203] – **سيار عز الدين**، «**تأثير البيئة الإلكترونية على صحة رضا المستهلك**»، المجلة الجزائرية للحقوق والعلوم السياسية، العدد الثالث، معهد العلوم القانونية والإدارية، جامعة تيسمسيلت، جوان 2017، ص 69.

[204] – تعتبر طبيعة عقود التجارة الالكترونية عقود اذعان وذلك راجع إلى أن المتعاقد لا يملك إلا أن يضغط على عدد من الخانات الموجودة أمامه في موقع المتعاقد الآخر على مواصفات معينة، وهي مواصفات السلعة وثمنها المحدد سلفا، فهو لا يملك إمكانية المناقشة أو المفاوضة تجاه المتعاقد الآخر حول شروط العقد الواردة على الموقع، فلا يملك إلا قبول العقد، أو رفضه كما هو أنظر في ذلك: **خميخم محمد**، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية –دراسة مقارنة–، أطروحة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017–2018، ص 20. أنظر كذلك: **جلول دواجي بلحول**، الحماية القانونية للمستهلك في ميدان التجارة الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2014–2015، ص 43 وما يليها.

[205] – **خليفي مريم**، مرجع سابق، ص 360.

تعتبر جريمة الاحتيال الالكتروني من بين مظاهر استغلال المتعامل في البيع الإلكتروني، حيث يكون المستهلك في كثير من الاحيان عرضة للاحتيال بعدم حصوله على السلعة أو الخدمة التي تعاقد من أجلها[206]، ويتم ذلك بتشجيع المستهلك على شراء السلع أو الخدمات عن طريق بوابة إلكترونية، غير أنه لا يحصل على هذه السلع أو الخدمات المتفق عليها، ويحصل الاحتيال على المستهلك عن طريق الإحالة إلى موقع منتحل على شبكة الانترنت كطرف ثالث يمثل وسيلة للدفع الالكتروني مدعيا أنه يتم شحن السلع أو سيتم تنفيذ الخدمات إلى المستهلك بمجرد أن يتم تحويل الأموال إلى البائع، وعادة ما يكون موقع بوابة الدفع مزور لنفس جهة الاحتيال[207].

3-الاستخدام غير المشروع لوسائل الدفع الإلكتروني

يمثل الاعتداء على وسائل الدفع الإلكتروني[208] تهديدا مباشرا وفوريا وسريعا للاقتصاد العالمي والوطني وحقوق الأفراد، بغض النظر على موقعهم في العالم، أي أنه يمكن القول أن تقليد العملات الورقية والشيكات يمثل تهديدا موضعيا محدودا يمكن التحكم فيه، أما تقليد بطاقة الائتمان فإنه يمثل تهديدا سرطانيا يتأثر به حامل البطاقة في أي موقع من العالم[209].

---

[206]- **HALIM Rami**, op-cit, p 391.

[207] – **خميخم محمد**، مرجع سابق، ص ص 104-105.

[208]– نصّ المشرع الجزائري من خلال الفقرة 02 من المادة 27 من القانون رقم 18-05 على أن تتم تسوية المعاملات التجارية الإلكترونية عن طريق الدفع الإلكتروني إلى جانب الدفع غير الإلكتروني إما عن بعد أو عند تسليم المنتوج وذلك باستعمال كل وسائل الدفع المرخص بها في ظل التشريع الوطني، وعليه يمكن استخدام وسائل الدفع الإلكترونية للوفاء في المعاملات التجارية الإلكترونية التي تتم داخل حدود التراب الوطني، كما يمكن استخدامها في تسوية المعاملات التجارية الإلكترونية العابرة لحدود التراب الوطني حسب الفقرة 03 من المادة 27 السابقة الذكر. أنظر في ذلك: **أمينة بن عميور**، **«متطلبات نظام الدفع الإلكتروني في مجال المعاملات الإلكترونية في إطار القانون 18-05»**، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد ب، عدد 52، ديسمبر 2019، ص 100.

[209] – **رياض فتح الله بصلة**، جرائم بطاقة الائتمان دراسة معرفية تحليلية لمكوناتها وأساليب تزييفها وطرق التعرف عليها، الطبعة الأولى، دار الشروق، القاهرة، 1995، ص 85.

يتجسد الاستخدام غير المشروع لوسائل الدفع الإلكتروني –المتمثلة في البطاقات البنكية المختلفة– في حالات استخدامها بعد انتهاء مدة صلاحيتها، أو بعد إلغائها، أو بعد التصريح بسرقتها أو ضياعها[210].

أخضع المشرع من أجل التصدي لهذه الجريمة من خلال نص المادة التاسعة وعشرون 29 من القانون رقم 18–05 المتعلق بالتجارة الإلكترونية خضوع منصات الدفع الإلكتروني لرقابة بنك الجزائر وذلك من أجل متطلبات الأمن القانوني وسرية المعاملات والبيانات وسلامتها وأمنها[211].

الفرع الثالث

مكافحة الجريمة المرتكبة عبر الإنترنت في ظل قانون البريد والاتصالات الإلكترونية

أمام التغيرات العالمية المتسارعة التي يشهدها قطاع البريد والمواصلات السلكية واللاسلكية نتيجة التطور التكنولوجي، وكذا تطور السوق التنافسية لنشاط البريد والاتصالات تدخل المشرع سنة 2018 لسد الثغرات القانونية التي كشف عنها تطبيق أحكام القانون 2000–03 المتضمن القواعد الخاصة بالبريد والاتصالات السلكية واللاسلكية[212] من خلال إصدار القانون 18–04[213] المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الذي جاء مواكبا للتطورات التي يعرفها عالم البريد والاتصالات بصفة عامة، وخير دليل على ذلك تغيير تسمية هذا القانون، من قانون البريد والاتصالات السلكية واللاسلكية إلى قانون البريد والاتصالات الإلكترونية، وذلك تماشيا مع عصر الشبكات

---

[210]– **خشة حسيبة**، وسائل الدفع الحديثة في القانون الجزائري، مذكرة لنيل شهادة الماجستير، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة المسيلة، 2016، ص 110.

[211]– **أمينة بن عميور**، مرجع سابق، ص 110.

[212]– قانون رقم 2000–03 مؤرخ في 5 غشت 2000، يتضمن تحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر عدد 48، صادر في 6 غشت 2000 (ملغى).

[213]– قانون رقم 18–04 مؤرخ في 10 مايو 2018، يتضمن تحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر عدد 27، صادر في 13 مايو 2018.

الاتصالية وخاصة الإنترنت، لذا سعى المشرع الجزائري من خلال هذا القانون إلى حماية مستعملي هذه الشبكة عن طريق تدابير حمائية **(أولا)**، ليتبعها بتدابير ردعية بسنّه لعقوبات تطبق على اعتداء في هذا النطاق **(ثانيا)**

أولا: التدابير الحمائية من الجرائم المرتكبة عبر الإنترنت

عرف المشرع في نص المادة 10 فقرة 01 من القانون رقم 18-04 الاتصالات الإلكترونية بـ:

"**يقصد بالاتصالات الإلكترونية في مفهوم هذا القانون، 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 كهرومغناطيسة**".

في حين عرف في نص المادة 10 فقرة 21 شبكات الاتصالات الإلكترونية من بـ:

"**كل منشأة أو مجموعة منشآت تضمن إما إرسالا، أو أرسال 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 إلكترونية خصوصا: شبكات الأقمار الصناعية والشبكات الأرضية والأنظمة التي تستعمل الشبكة الكهربائية شريطة أن تستعمل لإيصال الاتصالات الإلكترونية"[214].

كما عرف شبكة الإنترنت والتي يمكن اعتبارها كمثال للشبكات الإتصالية التي تدخل في إطار التنظيم والحماية المقررة بمقتضى القانون رقم 18-04 في الفقرة 5 من المادة 10 بـ:

[214]- أنظر المادة 10 من قانون رقم 18-04 ، مرجع سابق

"شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية خاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال ip وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها".

ولقد أحاط طريقة إنشاء واستغلال هذه الشبكات بعدة إجراءات، وذلك سعيا منه إلى ضمان تقديم أحسن الخدمات من جهة، ومن جهة أخرى حماية مستعمليها من مختلف الاعتداءات التي يمكن أن تطالهم عبرها.

يأخذ نظام إنشاء واستغلال الشبكات الاتصالية الإلكترونية كما نصت عليه الفقرة الثانية من المادة 115 من القانون 18-04 شكل الرخصة[215] أو ترخيص عام[216] أو تصريح بسيط[217]، وفق شروط منافسة مشروعة وباحترام المتعاملين لمبدأ المساواة في معاملة المشتركين.

تلزم المادة 119 من القانون رقم 18-04 متعاملي الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها ضمان سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية، ويجب عليهم أن يطلعوا أعوانهم على التزاماتهم والعقوبات التي يتعرضون لها عند عدم احترامهم هذه الأحكام.

ثانيا: التدابير الردعية للجرائم المرتكبة عبر الإنترنت

دفع العالم الإفتراضي العديد من الدول إلى اتخاذ إجراءات لحماية سيادتها الافتراضية لأنها تؤثر عليها مباشرة، فمعظم الدول تسعى إلى إقتناء التقنية الخاصة بالأمن

---

[215]- أنظر المادة 123 من القانون رقم 18-04

[216]- تنص المادة 131 فقرة 1 على: "**يمنح الترخيص العام لكل شخص طبيعي أو معنوي يلتزم باحترام شروط إنشاء، واستغلال و/أو توفير خدمات الاتصالات الإلكترونية**"

[217]- تنص المادة 135 فقرة 1 على: "**يلزم كل شخص طبيعي أو معنوي يريد استغلال خدمة اتصالات إلكترونية خاضعة لنظام التصريح البسيط بإيداع تصريح برغبته في الاستغلال التجاري لهذه الخدمة، لدى سلطة الضبط**"

المعلوماتي[218]حماية لمصالحها الأساسية، ولقد نص القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية في المادة 10 فقرة 03 على الأمن السيبيراني الذي عرفه بـ:

"**الأمن السيبيراني، مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة**"

في هذا يكون المشرع قد كرّس مبدأ حماية الشبكات الإلكترونية من خلال الباب الرابع من القانون 18-04 تحت عنوان الأحكام الجزائية، حيث أقرّ عقوبات سالبة للحرية بالإضافة إلى غرامات مالية لكل متدخل في هذه الشبكات الاتصالية في حالة إخلاله بالقواعد المذكورة في هذا القانون.

تضمّنت المادة 164 أحكام جريمة التنصّت على الاتصالات الإلكترونية[219]، والمادتان 165 و166 على جريمة تحويل مضمون الاتصالات الإلكترونية[220]، بافشائها أو

---

[218]- **دلال مولاي ملياني، «الإنترنت والسيادة»**، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، المجلد 7، العدد 1، مارس 2020، ص 399-400.

[219]- تنص المادة 164 من قانون رقم 18-04 على :"**يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500,000 دج إلى 1,000,000 دج، كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها**".

[220]- تنص المادة 165 من القانون رقم 18-04 على: "**يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 1,000,000 دج إلى 5,000,000 دج أو بإحدى هاتين العقوبتين، كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال.**

تسري نفس العقوبات على كل منعامل للاتصالات الإلكترونية يحول، بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو يساعد في ارتكاب هذه الأفعال".

في حين تنص المادة 166 من نفس القانون على: " **يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 500,000 دج إلى 1,000,000 دج أو بإحدى هاتين العقوبتين، كل عون مستخدم من طرف متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال في إطار ممارسة مهامه.**

نشرها واستعمالها. وحسب المادة 187 يعتبر الشخص المعنوي مسؤولا جزائيا عن هذه الجرائم طبقا للقواعد المنصوص عليها في قانون العقوبات[221].

الملاحظ على نصوص هذا القانون أنها جاءت عامة من حيث استعمال المصطلحات من جهة، ومن ناحية نصوص التجريم من جهة أخرى، وأعتقد أن المغزى من ذلك هو رغبة المشرع إدخال كل ما يتعلق بالاتصالات الالكترونية في نطاق هذا القانون، والدليل على ذلك اعتماده على مصطلح الشبكات الاتصالية الذي يشمل كل الشبكات سواء الوطنية أو المتعدية للحدود الوطنية مثل الإنترنت.

غير أنّه ما يعاب من ناحية تعميم استعمال هذه المصطلحات خاصة مصطلح الشبكات الاتصالية هو عدم احترام خصوصية كل شبكة اتصالية وعدم التفريق بينها، حيث أن شبكة الانترنت على سبيل المثال تتميز بخصائص لا نجدها في الشبكات المحلية أو الوطنية لا من ناحية طريقة العمل و لا من ناحية خضوعها للنص القانوني، فالشبكة الاتصالية الوطنية لا تطرح أي إشكال فيما يخص تحديد الاختصاص والقانون الواجب التطبيق بما أنها كل التصرفات فيها تقع في نطاق جغرافي وطني، وهذا ما لا نجده في شبكة الانترنت التي لها خصوصية تتعدى الحدود الوطنية الأمر الذي يطرح بحدّة مسألة تنازع القوانين لهذا يجب وضع إطار قانوني متكامل يشمل تنظيم على كل شبكة على حدى.

المبحث الثاني

الآليات الإجرائية الوطنية لمكافحة الجريمة المرتكبة عبر الإنترنت

صاحب ظهور الثورة التكنولوجية في مجال الاتصالات العديد من الانعكاسات السلبية والتي تمثلت في الجرائم، الأمر الذي دفع بالمشرع إلى سن نصوص موضوعية حصر من

يعاقب بنفس العقوبات كل شخص مستخدم لدى متعامل للاتصالات الإلكترونية، يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في ارتكاب هذه الأفعال".

[221]– **روابح فريد**، ضمانات حرمة الحياة الخاصة أثناء إجراءات مراقبة الاتصالات الإلكترونية، مجلة الأبحاث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سطيف، المجلد 02، العدد 02، سنة 2020، ص 8-9.

خلالها هذه الجرائم وفق قالب قانوني تم من خلاله وضع استراتيجية فعالة لمكافحة هذا النوع المستحدث من الجرائم.

نصّ المشرع بالموازاة مع وضعه للإطار القانوني الموضوعي لمكافحة الجريمة المرتكبة عبر الإنترنت على آليات إجرائية يتم من خلالها تفعيل وتنفيذ ما سنّه في الجانب الموضوعي، وذلك إيمانا منه أن القاعدة الإجرائية هي الوسيلة الفعالة لتطبيق النصوص الموضوعية، وأنه إذا لم تصاحبها هذه القواعد الإجرائية تبقى مجرد حبر على ورق.

سعى في بادئ الأمر من أجل مكافحة الجريمة المرتكبة عبر الإنترنت إلى الاعتماد على الأساليب الإجرائية التقليدية **(مطلب أول)**، ولكن مع التطور الذي عرفته الجريمة قام باستحداث إجراءات جديدة تتماشى مع خصوصية هذه الجريمة **(مطلب ثان)**.

المطلب الأوّل

الآليات الإجرائية التقليدية لمكافحة الجريمة المرتكبة عبر الإنترنت

أثارت الجريمة المرتكبة عبر الإنترنت العديد من الإشكالات القانونية الموضوعية والإجرائية، فالطابع اللامادي للجريمة مع تعديها للحدود الجغرافية للدول أدى إلى صعوبة متابعتها من طرف سلطات التحقيق والاستدلال، لهذا سعى المشرع إلى تطبيق القواعد الإجرائية التقليدية المعروفة في قانون الإجراءات الجزائية وذلك بتعديلها وجعلها تتناسب مع خصوصية هذا النوع من الإجرام، ومن أهم هذه الإجراءات نجد المعاينة **(فرع أول)**، والتفتيش **(فرع ثان)**، والخبرة **(فرع ثالث)**.

الفرع الأول

المعاينة كإجراء لمكافحة الجريمة المرتكبة عبر الإنترنت

تعرف المعاينة بأنها الإجراء الذي يتضمن وصف مكان الحادث وما يحتويه من أشياء وأشخاص، والفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان والتي تشير إلى شخصيته أو شركائه وما قد يفيد في اثبات ارتكاب الجريمة وتوضيح قدرا

من الاستنتاجات المنطقية التي تشكل في حد ذاتها الأساس الذي يقام عليه التحقيق[222]، وسوف نبين ذلك من خلال التطرق إلى تبيان أهمية المعاينة **(أولا)**، ثم إظهار صورها **(ثانيا)** ، بالإضافة إلى التطرق إلى أسسها وقواعدها **(ثالثا)**.

أولا: أهمية المعاينة

تكمن أهمية المعاينة في أمرين، الأول جمع الأدلة الناتجة عن الجريمة (آثار الجريمة)، والثاني وقوف المحقق بنفسه على مسرح الجريمة لتتكون لديه فكرة واضحة عن كيفية وقوع الجريمة، وبهذا توصف المعاينة بأنها وسيلة من وسائل الإثبات المباشر تفوق في أهميتها اعتراف المتهم، إذ هي أقوى الإجراءات للوصول إلى الحقيقة التي يطمئن إليها المحقق لكونها لا تكذب ولا تحابي وتعبر عن الواقع تعبيرا صادقا[223].

والمعاينة رغم أهميتها، إلا أنها ليست لازمة في كل الجرائم، فهي ليست إجراء تلقائي في مباشرتها بل إجراء هادف غايته الكشف عن العناصر المادية التي تتعلق بالجريمة، فإذا انعدم ذلك الهدف كما هو الحال في جريمة السب مثلا لم يكن ثمة مجال لإجرائها.

وإذا كانت المعاينة تتم بالانتقال إلى محل الواقعة الاجرامية كقاعدة إجرائية عامة مقررة، إلا أنه في إطار جرائم الإنترنت فإن الانتقال لا يكون بالضرورة عبر العالم المادي وإنما عن طريق العالم الافتراضي، فيستطيع عضو التحقيق أن يقوم بالمعاينة من مكتبه بالمحكمة من خلال حاسبه الآلي أو من مقهى الإنترنت أو من مقر مزود الخدمة الذي يعتبر أفضل مكان يتم من خلاله إجراء المعاينة، كما يجب أن يجعل بإجرائها خشية ضياع الأدلة[224]، ويتم ذلك عن طريق برمجيات خاصة بالتحقيق.

222– **محمد بن نصير السرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، د س ن، ص 76.

223 – **محمد حماد مرهج الهيتي**، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2006، ص 75.

224– **بن فردية محمد**، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2015/12/07، ص 122–123.

ثانيا: صور معاينة مسرح الجريمة المرتكبة عبر الإنترنت

تختلف صور معاينة مسرح الجريمة المرتكبة عبر الإنترنت عن معاينة مسرح الجريمة التقليدية، وهذا الاختلاف نابع من الخصوصية التي تتسم بها هذه الجريمة والتي استمدتها من الطبيعة اللامادية لشبكة الإنترنت، فالجريمة التي ترتكب في هذا النطاق تتكون من مسرحين، الأول مادي والثاني افتراضي غير محسوس وهو ما سنوضحه فيما يأتي:

1-مسرح الجريمة التقليدي

هو مسرح يقع خارج بيئة الحاسوب والإنترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، يترك فيها الجاني آثار كالبصمات، ويتم من خلاله معاينة الأماكن والأشخاص والأشياء المكونة للحاسب الآلي[225].

تتمثل المكونات المادية للحاسب الآلي في جميع الأجهزة ذات الكيان المادي المحسوس واللازمة لعمله ولإنجاز مهامه، سواء تلك التي تدخل في تكوينه، أو التي يتطلبها عمله بشكله النهائي، أي الأجهزة التي ترتبط به ويتطلبها إنجاز عمله أو مهمته، وتسمى المكونات المادية في صناعة الحاسب بالأجهزة الإلكترونية والأجهزة المساعدة الملحقة كالطابعات وقارئات البطاقات، وما إلى ذلك من أجهزة داخلية تدخل في تكوين الحاسب الآلي أو خارجية تتصل به ويتطلبها عمله أو المهمة الموكلة له[226].

ليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل مأموري الضبط القضائي والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت

---

[225]- **بوعناد فاطمة الزهراء**، «**مكافحة الجريمة الإلكترونية في التشريع الجزائري**»، مجلة الندوة للدراسات القانونية، مجلة إلكترونية خاصة تعنى بنشر الدراسات القانونية، العدد الأول، 2013، ص 68.

[226]- **محمد حماد مرهج الهيتي**، مرجع سابق، ص 34.

المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، مع إخطار النيابة العامة بذلك[227].

2-مسرح الجريمة الافتراضي

تشمل عملية فحص أو معاينة أنظمة الاتصال بشبكة الإنترنت بالأساس فحص مسار الإنترنت أو ما يعرف ببروتوكول الإنترنت، والنظام الأمني للشبكات، وكذا فحص الخادم، فلا يكفي أحيانا معاينة مكونات الحاسب وحدها لاستخلاص الدليل الإلكتروني، وإنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الإنترنت كذلك[228].

ثالثا: أسس وقواعد المعاينة

نص قانون الإجراءات الجزائية على المعاينة كإجراء يجب أن تحترم فيه بعض القواعد والأسس من أجل أن يكون لها أثر قانوني، فضابط الشرطة القضائية المكلف بمعاينة مسرح الجريمة يجب عليه احترام هذه القواعد والتي تتمثل في: الانتقال فورا إلى مسرح الجريمة والاستعانة بالأساليب العلمية والمحافظة على مكان المعاينة وفي حالة وجود أمور تقنية عليه الاستعانة بالخبراء، بالإضافة إلى تسجيل المعاينة التي قام بها.

1- الانتقال الفوري إلى مسرح الجريمة

تقتضي المعاينة سرعة الانتقال إلى مكان وقوع الجريمة كي لا يدخل الشك على الدليل المستخرج منها، وذلك إذا ما انقضت الفترة بين وقوع الجريمة وإجراء المعاينة التي تسمح بأن

---

[227]– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 182.

[228] – **براهيمي جمال**، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018، ص 64.

يتمكن الجاني من إزالة بعض الآثار المادية التي تفيد في كشف الحقيقة التي هي في النهاية الهدف النهائي من الاثبات عن طريق الدليل[229].

2- الاستعانة بالأساليب العلمية

أفرز التطور السريع للوسائل التقنية الحديثة تطورا آخر في مجال الجريمة، من خلال استحداث أساليب علمية وفنية في ارتكاب الجرائم، وهو ما زاد من الحاجة إلى الاستعانة بالوسائل العلمية الحديثة لاكتشافها، ومع أهمية الضمانات القانونية التي تهدف إلى ضمان الحرية الشخصية للإنسان، وعدم التعد عليها، وتحديد آلية الحصول على الدليل ليصبح مقبولا أمام القضاء.

تبرز أهمية الخبراء الذين يستخدمون الوسائل العلمية الحديثة لاستنتاج الدليل والتأكد منه، والاستعانة بالتجارب والمقارنات العملية التي تجعل الدليل مقبولا أمام القضاء، وهذا لا يتم إلا باستخدام الاجهزة الحديثة، والمعمل الجنائي الذي يستخدم كافة النظريات العلمية الحديثة في مجال مكافحة الجريمة والعلوم المساعدة الأخرى، التي تهدف جميعها إلى المساهمة في تقديم الدليل العلمي الذي يساعد في كشف الحقيقة بالطرق القانونية الصحيحة[230].

3- المحافظة على مكان المعاينة

يقوم رجل الضبطية القضائية وبمعرفة المحقق بالتحفظ على الأجهزة المشتبه باستخدامها في الجريمة وما يرتبط بها من مكونات مادية بهدف ابعادها عن أيدي الجاني

---

[229] – **عمرو حسين عباس**، أدلة الإثبات الجنائي والجرائم الإلكترونية (المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد خلال الفترة 26-2008/04/27، بمقر جامعة الدول العربية، القاهرة، ص16.

[230] – **ناصر بن محمد البقمي**، «**أهمية الأدلة الرقمية في الاثبات الجنائي (دراسة وفق الأنظمة السعودية)**»، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، العدد 80، المجلد 21، سنة 2012، ص ص 34-35.

والحفاظ عليها من التدمير أو التلف، ويتم تأمين نقلها بمعرفة الخبير الفني والذي يتولى عملية التفتيش بالحاسب الآلي واستخلاص الأدلة من الحاسب ونسبتها إليه[231].

4- الاستعانة بالخبراء

تقتضي عمليات البحث والتحقيق ومعاينة جرائم الإنترنت الاستعانة بخبرات عديدة ولكي تنتج آثارها القانونية يجب الاعتماد على الخبراء الذين لديهم دراية بنوعية الأساليب المستخدمة في التلاعب بالبيانات والبرامج الأساسية أو برامج التطبيقات، والغش أثناء نقل وبث البيانات، وتزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.

يتعين على الخبير في الجرائم المرتكبة عبر الإنترنت أن يزود المحقق الجنائي في هذه الجريمة بكل المعلومات الدقيقة عن العملية في أقرب وقت ممكن وذلك في تقرير خبرة مفصل، بما في ذلك الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بيّنة أو قرينة، كما يجب على المحقق الجنائي أن يشرح للخبراء الجوانب القانونية لطبيعة عملهم مع التأكد من ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة[232].

كلّما ارتفعت كفاءة الخبير كان من الممكن تكليفه بجزء من أعمال الضبط لخبرته العالية في التعامل مع الاجهزة الإلكترونية إذ يمكنه ممارسة دور إشرافي على فريق الضبط والحرص على نقل الأجهزة الإلكترونية للمعمل بشكل سليم[233].

---

[231] – **سلامة محمد المنصوري**، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال الحصول على درجة الماجستير في القانون، كلية الحقوق، قسم القانون العام، جامعة الإمارات العربية المتحدة، نوفمبر 2018، ص 31.

[232] – **رابح وهيبة**، «**الجريمة المعلوماتية في التشريع الإجرائي الجزائري**»، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، العدد الرابع، ديسمبر 2014، ص ص 328-329.

[233] – **سلامة محمد المنصوري**، مرجع سابق، ص 40.

5- تسجيل المعاينة

تشكل مسألة تسجيل المعاينة إحدى أهم الخطوات التي يتعين على الضابط المعاين لمسرح الجريمة القيام بها، وذلك لأن محضر المعاينة يستقي منه كافة الوقائع والماديات المتعلقة بها.

كما أن إثبات معاينة مسرحها يساعد على تصور حالة الجريمة وقت حدوثها، والمكان الذي ارتكبت فيه والإجراءات التي اتخذت بواسطة المتخصصين والخبراء ورجال الشرطة[234].

نستشف أن للمعاينة دور فعال في إثبات الجريمة المرتكبة عبر الإنترنت رغم صعوبة معاينة مسرح الجريمة الافتراضي، إلاّ أنه يمكن لضابط الشرطة القضائية إن كان كفؤاً ومكوّناً في مجال شبكات الاتصال والنظم المعلوماتية الوصول إلى الدليل القاطع شريطة احترامه للإجراءات المنصوص عليها في القانون، دون أن ننسى أن للجريمة المرتكبة عبر الإنترنت مسرح تقليدي مادي الذي يسمح للضابط المعاين التأكد أكثر من وجود أدلّة مادية تساعده في الوصول إلى الحقيقة.

الفرع الثاني

التفتيش كإجراء لمكافحة الجريمة المرتكبة عبر الإنترنت

يعتبر التفتيش إجراء من إجراءات التحقيق الابتدائي، يهدف إلى ضبط الأشياء الناتجة من جناية أو جنحة عن طريق تفتيش الأشخاص والأماكن والأشياء، وهو من الاختصاصات الأصيلة لقاضي التحقيق الذي يمكن أن يخوله إلى ضباط الشرطة القضائية عن طريق الإنابة، ولقد أضحى من بين أهم الإجراءات المعتمد عليها لمكافحة الجريمة المرتكبة عبر الإنترنت نظرا لما ينتج عنه من أدلة قاطعة، غير أنه لا يمكن الاعتماد عليه إلاّ إذا توفرت شروط معينة **(أولا)**، بالإضافة إلى توفر محل التفتيش **(ثانيا)**

---

[234] –**ماينو جيلالي، «أسس وضوابط التعامل مع مسرح الجريمة للاستفادة من البصمة الوراثية في الاثبات الجنائي»**، مجلة البدر، جامعة بشار، الحجم 04، العدد 12، ديسمبر 2012، ص234.

أولا: شروط تفتيش النظم المعلوماتية

لكي يكون التفتيش صحيحا ومنتجا لآثاره القانونية يجب أن تتوفر فيه شروط موضوعية وشكلية:

أ- الشروط الموضوعية لتفتيش النظم المعلوماتية

حتى تتم عملية تفتيش نظم المعلوماتية يجب توفر شروط موضوعية وهي أن يكون السبب من وراء التفتيش **(1)** ووقوع الجريمة المعلوماتية **(2)** بالإضافة إلى التهمة الموجهة للشخص **(3)**.

1-سبب تفتيش النظم المعلوماتية

سبب التفتيش في العالم الافتراضي، أنه لا بد أن يكون بصدد جريمة إنترنت واقعة بالفعل سواء أكانت جناية أو جنحة، واتهام أشخاص أو شخص معين بارتكابها أو المشاركة فيها، وبتوفر قرائن قوية على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره[235].

يعتبر تسبيب اللجوء إلى إجراء التفتيش سواء في الجرائم التقليدية أو في جرائم الإنترنت من الأمور الجوهرية الواجب توفرها من أجل القيام به من طرف قاضي التحقيق أو ضابط الشرطة القضائية، وبدونه يعتبر تعسفا وخطأ في إجراءات التحقيق.

2-وقوع جريمة معلوماتية

فإذا كان الهدف من إجراء التفتيش هو الحصول على أدلة تساهم في كشف حقيقة الواقعة الإجرامية وإسنادها إلى مرتكبها، فإن المنطق القانوني والعقلي يقتضي ضرورة وقوع الجريمة بصورة قطعية سواء أكانت جناية أو جنحة، وتستبعد المخالفات لضآلة خطورتها، ومن ثم لا يجوز إجراءه لضبط جريمة مستقبلا أو لمجرد ورود معلومات تشير إلى إمكانية وقوع الجريمة مستقبلا حتى ولو كانت الدلائل كافية على أنها ستقع بالفعل[236].

---

[235] – **مرنيز فاطمة**، مرجع سابق، ص 239.

[236] – **بن خليفة إلهام**، مرجع سابق، ص 282.

3-توجيه التهمة إلى شخص وإسنادها إليه

يتعين للقيام بإجراء التفتيش بالإضافة إلى وقوع الجريمة أن يكون هناك اتهام موجه إلى شخص أو عدة أشخاص سواء بصفته فاعلا أو شريكا أو حائزا لأشياء تتعلق بجريمة من جرائم تكنولوجيا الإعلام والاتصال، معنى ذلك أن تتوفر في حق المراد تفتيشه دلائل قوية وكافية تدعو إلى الاعتقاد بأنه ساهم في ارتكاب الجريمة المعلوماتية ولا يقتصر الأمر على مجرد تجميع القرائن والأدلة التي تفيد وقوع الجريمة ونسبتها إلى فاعلها، بل يجب أن تتضمن كذلك المعلومات والقرائن التي تعزز موقف المشتبه فيه وتنفي عنه ارتكابه للجريمة[237].

ب- الشروط الشكلية لتفتيش النظم المعلوماتية

حتى تنتج عملية تفتيش النظم المعلوماتية آثارها لا بد من توفر شروط شكلية وهي أن يجري التفتيش بحضور أشخاص يحددهم القانون **(1)** وأن يصدر الإذن بالتفتيش من طرف جهة قضائية مختصة **(2)** مع احترام التوقيت القانوني للتفتيش **(3)** بالإضافة إلى وجوب تحرير محضر خاص بعملية التفتيش **(4)**.

1-أن يجري التفتيش بحضور أشخاص يحددهم القانون

لكي يكون التفتيش في الجرائم المرتكبة عبر الإنترنت أو غيرها من الجرائم صحيحا ومنتجا لأثاره، لا بد أن يتم من طرف سلطات التحقيق الأصلية باختلاف تشريعات الدول، مع مراعاة الاختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة، وإما بمكان إقامة المتهم، أو مكان القبض عليه.

غير أنه يجوز استثناء تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وذلك وفقا للشروط والإجراءات المنصوص عليها قانونا، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناء على إذن بالتفتيش صحيح، صادر من

---

237 – **هميسي رضا، «تفتيش المنظومات المعلوماتية في القانون الجزائري»**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 05، جوان 2012، ص 165.

هيئة مختصة، وفي غياب هذا الإذن، أو عدم صحته يصبح عدم مشروعية التفتيش أمرا مؤكدا[238].

وفي هذا يعد ضابط الشرطة القضائية هو المخول قانونا بتنفيذ أمر التفتيش وفقا لما تقضي به المادة 15 من قانون الإجراءات الجزائية حيث يقوم بتفتيش المكان وحجز ما له علاقة بالجريمة، يساعده في ذلك أعوان الضبط القضائي[239].

وبالإضافة إلى ذلك وحرصا على تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، تسهر التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم، أو من ينوب عنه معتبرين ذلك من القواعد الأساسية التي يترتب على مخالفتها البطلان، وهذا ما نصت عليه الفقرة 1 من المادة 45 من قانون الإجراءات الجزائية بأنه: "**إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته**".

يعتبر حضور المتهم أثناء القيام بإجراء التفتيش كأصل وكشرط حتمي في تفتيش الأشخاص على اعتبار التفتيش يقع عليه، وفي هذا الإطار لم تشترط التشريعات الإجرائية حضور الشهود عند تفتيشه، أما عندما يتعلق الأمر بتفتيش المساكن أو ملحقاتها[240]، فقد تباينت مواقف التشريعات الإجرائية بين من يشترط لصحة التفتيش حضور إما المتهم أو من يمثله أو شاهدين من غير المعنيين بالتحقيق، وبين من يستوجب إلى جانب حضور المتهم حضور شاهدين.

---

238 – **براهيمي جمال**، مرجع سابق، ص 38.

239 – **مرنيز فاطمة**، مرجع سابق، ص 185.

240– **بن طالب ليندا**، «**التفتيش في الجريمة المعلوماتية**»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 16، جوان 2017، ص 493.

2-توفر الإذن بالتفتيش

تنص المادة 44 من قانون الإجراءات الجزائية أنه لا يجوز القيام بإجراء التفتيش إلا بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق، ويشترط المشرع في هذا الإذن وجوب استضهاره قبل الدخول إلى المنزل والشروع في تفتيشه، وأن يتضمن بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز عليها، بمعنى أن يكون الإذن مسببا وعلة التسبيب هي بيان هدف التفتيش والتحقق من مشروعيته بثبوت أنها الغاية التي حددها القانون، ذلك أن الإذن -حسب المادة 44 السابقة الذكر- إذا لم يتضمن التسبيب يقع تحت طائلة البطلان، إذ أن اشتراط المشرع للتسبيب يتيح للقضاء تقدير صحة الأمر بالتفتيش وتقرير بطلانه إذا ثبت أنه يستهدف غاية أخرى غير ما حدده القانون، ولا يشترط المشرع في التسبيب أن يكون تفصيليا بل يكفي بيان الجرم بالاستناد إلى الدلائل التي استخلصتها الضبطية القضائية من تحرياتها[241].

3-احترام التوقيت القانوني المقرر للتفتيش

على الرغم من إلزام القانون لقاضي التحقيق بمراعاة مواعيد وأوقات إجراء التفتيش وفقا للمادة 47 من قانون الإجراءات الجزائية، إلا أنه عندما يتعلق الأمر بجرائم المعالجة الآلية للمعطيات فإنه أجاز إجراء التفتيش والمعاينة والحجز في كل مكان سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، بل ذهب المشرع إلى أبعد من ذلك عندما يتعلق الأمر بالجرائم السابقة بتمكينه لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني، أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك[242]

---

[241] - **بن خليفة إلهام**، مرجع سابق، 289.

[242] - **رويس عبد القادر**، «**أساليب البحث والتحري الخاصة وحجيتها في الاثبات الجنائي**»، المجلة الجزائرية للحقوق والعلوم السياسية، العدد الثالث، معهد العلوم القانونية والإدارية، جامعة تيسمسيلت، جوان 2017، ص 47.

4-تحرير محضر خاص بعملية التفتيش

لما كان التفتيش عملا تحقيقيا فإنه يتطلب محضر لإثبات ما تم من إجراءات، وما نتج عن التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقضي بأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الاجراءات التي اتخذت بشأن الوقائع التي يثبتها.

لهذا فإن الأمر ذاته يكون فيما يخص تفتيش نظم المعلوماتية وإن كان يستلزم بالاضافة إلى الشكليات السابقة ضرورة إحاطة القائم بالتفتيش بتقنية المعلومات فضلا على استعانته في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش بشخص يرافقه يكون متخصص في الحاسوب والإنترنت[243].

ثانيا: محل التفتيش

يتمثل محل التفتيش في المكان أو الوسط الذي يحتفظ فيه الشخص بأشيائه الخاصة وأسراره، حيث في هذا الصدد يتخذ محل تفتيش مسرح الجريمة الجريمة المرتكبة عبر الإنترنت عدة صور وهي:

أ- قابلية المكونات المادية للحاسب الآلي للتفتيش

يقصد بالمكونات المادية للحاسوب، الأشياء الملموسة من أجزائه وأدواته التي تعمل بشكل متكامل لآداء مهمة في معالجة البيانات آليا، وعليه يتكون الحاسوب من عدة وحدات إدخال كلوحة المفاتيح والقلم الضوئي وشاشات اللمس، ووحدة الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والبرامج، إضافة إلى وحدة المعالجة المركزية التي تقوم بالتنسيق بين الوحدات الاخرى وضبط التعليمات، وأخيرا وسائط إظهار نتائج التشغيل

[243]- **مليانى عبد الوهاب**، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2016-2017، ص 308.

كالشاشة والطابعة والسماعات والراسم والأقراص المرنة والصلبة والذاكرة الوميضية التي تعتبر من أشهر تخزين البيانات والمحافظة عليها، وعليه ليس هناك خلاف في أن الدخول إلى المكونات المادية للحاسوب بحثا عن دليل الجريمة يخضع للاجراءات التقليدية للتفتيش كتحديد طبيعة المكان الموجودة فيه تلك المكونات سواء كان عاما أو خاصا إضافة إلى حضور المعني أو من ينوب عنه[244].

وترتيبا على جواز تفتيش الكيانات المادية للحاسب الآلي يتوقف تفتيش تلك الأشياء على مكان وجودها[245]، إذا كان عاما أو خاصا، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكمه أي حكم المكان، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاتها والضمانات المقررة لها في التشريعات المختلفة.

في هذا تشترط المواد من 44 إلى 47 من قانون الإجراءات الجزائية للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها، الحصول على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش، على أن يتم التفتيش نهارا في الفترة الممتدة من الخامسة صباحا إلى الثامنة مساء وبحضور صاحب المسكن أو ممثله، وإن تعذر ذلك استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته.

أما إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء كانت عامة بطبيعتها كالحدائق العامة والطرق العامة، أم أماكن عامة بالتخصيص كمقاهي الإنترنت ومحلات بيع وصيانة الحواسيب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك

---

[244]– **يزيد بوحليط، «تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري»**، مجلة التواصل في الإقتصاد والإدارة والقانون، جامعة عنابة، عدد 48، ديسمبر 2016، ص 84.

[245]– **محسن العبودي، «المواجهة الأمنية لجرائم الإنترنت»**، مقال متوفر على الموقع التالي: www.eastlaw.comص 14.

الأماكن، ويستوي الأمر، بالنسبة للمكونات الموجودة بحوزة شخص ما، وبغض النظر عن صفة هذا الشخص، مبرمجا كان أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات القانونية المحددة لذلك[246].

ب- تفتيش المكونات المنطقية للحاسب الآلي

أثارت مسألة خضوع المكونات المنطقية للحاسوب (البرامج والبيانات) لإجراءات التفتيش أو الولوج في إطار إجراءات البحث والتحقيق الجنائي، جدلا فقهيا بين اتجاهين أساسيين في هذا المجال بين معارض **(1)** ومؤيد **(2)** لمسألة جواز اعتبار المكونات المنطقية للحاسوب محلا لإجراءات التفتيش[247].

1-الاتجاه المعارض لاعتبار المكونات المنطقية للحاسوب محلاً للتفتيش

تتمثل فكرته في عدم امكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته.

فهناك جانب من التشريعات الإجرائية قد حدد هدف التفتيش في البحث عن الأشياء وضبطها، وهذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس ولا يمتد في نطاق شموله إلى الكيانات المنطقية، وقد عملت الدول التي أخذت بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية[248].

---

[246] – **براهيمي جمال**، مرجع سابق، ص ص 16-17.

[247] – **ربيعي حسن**، مرجع سابق، ص 115.

[248] – **سعيداني نعيم**، مرجع سابق، ص 146.

2-الاتجاه المؤيد لاعتبار المكونات المنطقية للحاسوب محلا للتفتيش

أجاز أصحاب هذا الاتجاه ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الاجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة[249].

وهذا ما ذهب إليه المشرع في نص الفقرة الرابعة من المادة 47 من قانون الإجراءات الجزائية بأنه: "**إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا ونهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك**". حيث يفهم من نص هذه المادة أنه أجاز إمكانية التفتيش والضبط على المكونات المعنوية للحاسوب[250] خاصة باستعماله عبارة "**أية عملية تفتيش**".

ت- تفتيش شبكات الحاسب الآلي

أثارت عملية تفتيش شبكات الحاسب الآلي اشكالات وصعوبات عديدة بالنسبة للقائمين بهذا الإجراء، وذلك راجع إلى الطبيعة اللامادية لهذه الشبكات من جهة والتباعد بين مكان وقوع الجريمة والآثار المترتبة عنها من جهة أخرى، لهذا سوف نتطرق إلى حالة اتصال المتهم بحاسب آخر داخل الدولة **(1)** ثم إلى حالة اتصال المتهم بحاسب آخر خارج الدولة **(2)**

1- اتصال المتهم بحاسب آخر داخل الدولة

تنص المادة (05) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "**يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة**

---

[249] – **بوحزمة نصيرة، «التفتيش في جرائم تقنية المعلومات»**، مجلة حوليات جامعة بشار للحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة بشار، العدد 17، سنة 2017، ص 135.

[250] – لتفاصيل أكثر أنظر: **أمجدي بوزينة أمنة**، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، مقال موجه للملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص 63-64.

القضائية ، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها.

ب- منظومة تخزين معلوماتية".

يفهم من نص المادة أنه إذا كانت أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة أو جزء منها، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك[251]، وهو الأمر نفسه الذي حثت عليه الاتفاقية العربية لمكافحة تقنية المعلومات الدول الأعضاء فيها على اعتماده، وذلك من خلال الفقرة 02 من المادة 26.

نص في هذا السياق قانون الإجراءات الجزائية الفرنسي في المادة 1/57 منه على أنه: "**يمكن لضباط الشرطة القضائية، ومن هم تحت مسؤولياتهم أعوان الشرطة القضائية أثناء التفتيش الجاري والمحدد بالشروط المنصوص عليها في هذا القانون الدخول عن طريق نظام معلوماتي موجود في المكان أين يجري فيه التفتيش على معطيات تهم التحقيق والمخزنة في النظام المذكور أو في نظام معلوماتي آخر عندما تكون هذه المعطيات متاحة أو يمكن الدخول إليها انطلاقا من النظام الرئيسي**"، وهو أيضا ما أوصت به اتفاقية بودابست الدول الأعضاء فيها بمقتضى المادة 19 الفقرة 02[252].

[251]- **بن طالب ليندا**، التفتيش في الجريمة المعلوماتية، مرجع سابق، ص 491.

[252] - مشار لها لدى: **بن خليفة إلهام**، مرجع سابق، ص 286.

2- اتصال المتهم بحاسب آخر خارج الدولة

نقصد بها حالة اتصال المتهم بحاسب آخر موجود في مكان آخر خارج الدولة، حيث يقوم مرتكبوا الجرائم بتخزين بياناتهم في منظومة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعيدة مستهدفين عرقلة جهة التحقيق في جمع الادلة والتحقيقات[253].

يجوز في حالة تفتيش المعطيات التي تكون مخزنة في منظومة معلوماتية خارج الإقليم الوطني، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى للسلطات المختصة وكذا ضباط الشرطة القضائية تفتيش هذه المنظومة، ولا يعد ذلك أبدا انتهاكا لسيادة دولة أخرى طالما أن مقتضيات التعاون الدولي تستدعي محاصرة هذه الجرائم، وطلب مساعدة سلطات الدولة الأجنبية، طالما أن ذلك يتم في إطار الاتفاقيات الدولية الثنائية والمتعددة الأطراف التي أبرمتها الجزائر، وطبقا لمبادئ القانون الدولي والعلاقات الودية بين الدول التي تنص على مبدأ المعاملة بالمثل[254].

صدر عن المجلس الأوروبي توصيات تسمح بامتداد التفتيش خارج إقليم الدولة وهو ما نصت عليه التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات والتي ورد فيها: "**لسلطة التحقيق عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة، ما دامت مرتبطة بشبكة واحدة، وأن تضبط البيانات المتواجدة فيها مادام أنه من الضروري التدخل الفوري للقيام بذلك**"، كما أن التوصية رقم 17 نصت كذلك بامتداد نطاق التفتيش خارج إقليم الدولة إذا كان من الضروري اتخاذ

---

[253] – **رحال بومدين، سعداني نورة، «محل التفتيش في مجال التجارة الإلكترونية وفق القانون الجزائري»**، المجلة الجزائرية للحقوق والعلوم السياسية، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد بن يحيى الونشريسي، تيسمسيلت، المجلد الثالث، العدد السادس، ديسمبر 2018، ص 173.

[254] – **هميسي رضا**، مرجع سابق، ص 168.

إجراءات عاجلة في هذا الشأن، واشترطت أساس قانوني يجيز ذلك قائم على أساس موافقة الدولة التي يمتد التفتيش إليها[255].

خوّل المشرع على لسلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني، وذلك بنصه في المادة 3/5 من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "...**إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل**"[256].

الفرع الثالث

الخبرة التقنية كإجراء لمكافحة الجريمة المرتكبة عبر الإنترنت

تستعين الشرطة القضائية وسلطة التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي منذ ظهور الجرائم المرتكبة عبر الإنترنت، حيث إذا كانت الإستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق أو الحكم في الجرائم العادية، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع راي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيبا مستوجبا نقضه[257]، لهذا سوف نتطرق إلى أهمية الخبرة **(أولا)** ثم إلى نطاق الإستعانة بأصحاب الخبرة التقنية **(ثانيا)** بالإضافة إلى تبيان سلطة القاضي الجزائي في تقدير الخبرة **(ثالثا)**.

---

[255] – **بن فردية محمد**، مرجع سابق، ص 141.

[257] – **محمد أبو العلا عقيدة**، التحقيق وجمع الأدلة في الجرائم الإلكترونية، مقال متوفر على الموقع التالي: www.osamabahar.com

أولا: أهمية الخبرة التقنية

كثيرا ما تفشل جهات التحري والتحقيق في جمع الأدلة الرقمية مما يستدعي اللجوء إلى الخبرة الفنية[258]، بل كثيرا ما يتسبب المحقق في تدمير الدليل الرقمي إما نتيجة خطأ أو إهمال أو جهل في التعامل معه، وعموما يراعي في الخبير أن تتوافر لديه القدرات الفنية والإمكانيات العلمية في المسألة موضوع الخبرة، والتي تهدف إلى:

- الكشف عن الدليل الرقمي وإجراء الاختبارات اللازمة للتأكد من أصالته ومصدره كدليل يمكن قبوله أمام القضاء.
- إصلاح الدليل وتهيئته وإعادة تجميعه من المكونات المادية للحاسب، مع عمل نسخة أصلية من الدليل الرقمي للتأكد من سلامته أثناء عملية استخلاصه.
- استخدام الخوارزميات للتأكد من أن الدليل لم يتم العبث به، وتحريزه لإثبات أصالته وتحديد الخصائص المميزة لكل جزء من الأدلة الرقمية كالمستند الرقمي، الصور، الاتصالات[259].

ثانيا: نطاق الإستعانة بأصحاب الخبرة

يشمل نطاق الاستعانة بالخبراء قاعدتين أساسيتين تتمثلان في موضوع الخبرة **(1)** ثم إلى دورها في مراحل الدعوى **(2)** :

1-من حيث الموضوع

تحتل الخبرة مكانة هامة في العمل القضائي، باعتبارها طريقا مهما من طرق اثبات الحقوق في المنازعات القضائية، لاسيما في مواجهة التطور التقني في شتى المجالات، وإذا كان المبدأ القانوني يقضي انه على القاضي الإلمام بالتشريع والفقه ومواكبة تطوراتها على الصعيد الوطني، فإنه ليس بالضرورة أن يكون ملما بالفيزياء والهندسة والرياضيات

[258]- **PRZYSWA Eric**, Cybercriminalité et contrefaçon, fyp éditions, France, 2010, p 169.

[259]- **بن فردية محمد**، مرجع سابق، ص ص 165-166.

والميكانيك وعلم الفلك والطب، أو بالتشريع والفقه المقارن بالرغم من وجود آراء تصر على أن يكون للقاضي تكوينا في المسائل الفنية.

يعاين القاضي هيكل الحقيقة دون أن يكون لديه إمكانية الدخول إلى مضمونها، ومعرفة ذلك المضمون، لأن المسألة تستلزم معارف فنية اختصاصية لا يدركها إلا اهل الفن والاختصاص، لأجل هذا وجدت فكرة الخبرة لتكون وسيلة أو طريق من طرق البينات يلتمسها الخصوم لإثبات بعض الحقوق ذات الطبيعة المركبة من جهة، ولتكون وسيلة مساعدة للقاضي في إنارة طريق الوصول إلى الحقيقة تمهيدا لإقرار الحق لصاحبه في النزاع المعروض عليه للحكم فيه، وفصل الخصومات المستحكمة القائمة بين الأفراد[260].

2-من حيث مراحل الدعوى

لا يختلف رجال القانون في أن سلطة النيابة العامة تتمثل في تحريك ومباشرة الدعوى العمومية، غير أنه أحيانا تلجأ فيه النيابة إلى الاستعانة بالخبير من أجل توضيح بعض الجوانب ذات الطابع التقني والفني[261].

تلعب الخبرة الفنية دوراً كبيراً في مجال إثبات الجريمة المرتكبة عبر الإنترنت، لأنها تنير درب سلطات التحقيق والقضاء وسائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة وتحقيق العدالة الجنائية، لذلك ومنذ تفشي الجرائم المرتكبة عبر الإنترنت، تستعين سلطات التحقيق والاستدلال والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الإلكترونية من أجل كشف غموض الجريمة وتجميع أدلتها والتحفظ عنها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[262].

---

[260]- **محمد واصل، حسين بن علي الهلالي**، الخبرة الفنية أمام القضاء دراسة مقارنة، منشورات المكتب الفني للمحكمة العليا، سلطنة عمان، 2004، ص ص 27-28.

[261] - **فروحات سعيد**، «**السلطة التقديرية للقاضي الجنائي في التعامل مع الخبرة الجنائية**»، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 09، العدد 02، 2016، ص 128.

[262] - **براهيمي جمال**، مرجع سابق، ص 68.

ثالثا: سلطة القاضي الجزائي في تقدير الخبرة

يخضع تقدير تقارير الخبرة في المسائل الفنية إلى سلطة القاضي والتي سوف نتطرق إليها في تبيان مدى حجية الخبرة الفنية **(1)** ثم إلى الخبرة باعتبارها دليل إثبات قابل للمناقشة **(2)** بالإضافة إلى خضوع الخبرة الفنية لرقابة القاضي **(3)**

1-مدى حجية الخبرة

إذا كانت الاستعانة بخبير في المسائل الفنية البحتة في الجرائم التقليدية أمرا تقديريا على جهة التحقيق أو الحكم، فهي لازمة إذا استعصت عليه بعض المسائل الفنية في مجال استخلاص الدليل الرقمي لإثبات الجرائم المرتكبة عبر الإنترنت، لتعلقها بمسائل فنية آية في التعقيد لا يكشف غموضها إلا متخصص بارع في مجال تخصصه، ذلك لأن الذكاء والفن لا يكشفه و لا يفهمه إلا ذكاء وفن مماثلين.

تزايدت الحاجة إلى الخبرة الفنية للتحقيق في الجرائم المرتكبة عبر الإنترنت في الآونة الأخيرة نظرا للتحولات التكنولوجية التي مسّت وسائل الإعلام والاتصال، إذ تعددت أنواع ونماذج الحواسيب وشبكات الاتصال بينها، وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشعبة، والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب على المتخصصين تتبعها واستيعابها، بل يمكن القول أنه لا يوجد حتى الآن خبير يملك معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها، أو قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[263].

ترك المشرع للمحقق الحرية الكاملة وفي أية مرحلة من مراحل التحقيق انتداب أي خبير يرى فيه الكفاءة الفنية اللازمة للاستعانة بخبرته، كما أنه لا يوجد في القانون ما يلزمه بالاستجابة للمتهم و لا من الخصوم إذا طلبوا ندب خبير.

[263]- **براهيمي جمال**، مرجع سابق، ص 69.

نظرا للأهمية التي تكتسيها الخبرة الفنية نص المشرع في المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنه: "**يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها**".

قصد المشرع من خلال هذا النص الذي ورد بصيغة العموم "**كل شخص له دراية**"[264]، حتى يوسع دائرة المساعدة القضائية في مجال مكافحة الجرائم المرتكبة عبر الإنترنت لتشمل إلى جانب الخبير، جميع المتخصصين والعاملين في مجال تكنولوجيات الاعلام والاتصال، مثل المهندسين وذوي الشهادات العليا في الإعلام الآلي، ومقدمي خدمات الاتصالات الإلكترونية، كمزودي خدمة العبور إلى الإنترنت، ومزودي خدمة الإيواء، ومزودي خدمة الحوسبة وكل من لديه دراية في هذا المجال[265].

2-الخبرة دليل إثبات قابل للمناقشة

تظهر الممارسة العملية أن الخبرة هي دليل إثبات قابل للمناقشة والفحص من طرف القاضي، ولكن هل تمس هذه المناقشة الحقيقة العلمية التي جاءت بها الخبرة؟

لايمكن للقاضي أن يناقش هذه الحقيقة العلمية التي جاءت بها الخبرة بسبب أنها مسألة فنية لبيانها، ولكن الفحص يمس الظروف التي أحاطت بوجود الدليل العلمي الذي أفرزته الخبرة[266].

---

[264]- ذهب المشرع الجزائري إلى أكثر من ذلك بعد تعديل قانون الإجراءات الجزائية بمقتضى الأمر رقم 21-11 والذي بموجبه كرس القطب الوطني المتخصص في جرائم المعالجة الآلية للمعطيات الذي بدوره يحتوي على قضاة ذوي تكوين خاص في هذا النوع من الجرائم.

[265]- **براهيمي جمال**، مرجع سابق، ص 71.

[266] - **فروحات سعيد**، مرجع سابق، ص 132.

يقضي المبدأ العام أن يعلم الأطراف بتقرير الخبرة في الدعاوى الجزائية، الذين يكون لهم عندئذ إمكانية مناقشتها أو أن يطلبوا خبرة تكميلية أو خبرة مضادة، لهذا نصت بعض التشريعات على أنه يكون للمتهم حق الاستعانة بخبير استشاري على حسابه الخاص.

يتم عادة التفريق في مسألة الإخطار بين ما إذا كانت الخبرة جارية من قبل النيابة العامة أو من قبل قاضي التحقيق أو من قبل المحكمة، حيث يكون الإخطار من قبل النيابة العامة أو قاضي التحقيق مباشرة إلى المعنيين بها، أما الإخطار بها من قبل المحكمة فيتم بالطريقة التي تعلن فيها الخبرة في الدعاوى المدنية والتجارية، وفي جميع الأحوال فإنه في مرحلة المحاكمة يمكن للمجني عليه وللمتهم، وللادعاء العام أن يناقشوا نتائج الخبرة وأن يثيروا عند الاقتضاء أمر بطلانها، وأن يطلبوا خبرة إضافية أو خبرة مضادة كما أشرنا أعلاه، وأن يطلبوا دعوة الخبير لمناقشته في تقريره والنتيجة التي توصل إليها، وإذا دعي الخبير من قبل المحكمة فهو ملزم بالحضور، وبعد أدائه اليمين القانونية –إذا كان خبيرا غير محلف– عليه ان يجيب على جميع الأسئلة التي تطرح عليه[267].

3–الخبرة دليل إثبات يخضع لرقابة القاضي

يكون للقاضي الحرية الكاملة في تقدير القوة التدليلية لتقرير الخبرة والفصل فيها، فله أن يأخذ بها أو يطرحها سيما إذا راوده شك في النتيجة في النتيجة التي انتهى إليها كما له أن يفاضل بين تقارير الخبراء[268].

يتولى الخبير مهمته تحت رقابة القاضي الذي أمر بإجراء الخبرة[269] ولا يستلزم ذلك حضوره فعلا أثناء قيامه بأعماله بل يكفي أن يبقى على اتصال معه بهدف إحاطته علما بكل المستجدات التي تطرأ عليه في مجال عمله على اعتبار أن الخبير هو مساعد متخصص للقاضي، وفي حدود ما نص عليه أمر أو حكم الندب أثناء إجراء أعمال الخبرة،

---

[267]– **محمد واصل، حسين بن علي الهلالي**، مرجع سابق، ص ص 173–174.

[268]– **رحال بومدين، سعداني نورة**، مرجع سابق، ص 177.

[269]- **DE MUNAGORRI Rafael Encinas**, Les problèmes de preuve posés par l'évolution des sciences et des technologies, p 05, article disponible en ligne à l'adresse: https://halshs.archives-ouvertes.fr/halshs-01652004

ومن ذلك تكليف الخبير بإجراء أبحاث معينة أو سماع أي شخص معين باسمه قد يكون قادرا على مدهم بالمعلومات ذات الطابع الفني بأمر أو حكم الندب مع تحديد مهلة لإنجاز خبرته، فإذا لم يودع تقريره جاز للقاضي في الحال استبداله بغيره وعليه أن يقدم ما قام به من أبحاث، كما عليهم أيضا أن يردوا في ظرف ثمانية وأربعين ساعة جميع الأشياء والأوراق التي تكون في عهدتهم على ذمة انجاز مهمتهم، بل أكثر من ذلك يجوز أن تتخذ ضدهم تدابير تأديبية قد تصل إلى شطب أسمائهم من جداول الخبراء بقرار من وزير العدل إذا نسب إليهم إهمال ما[270].

المطلب الثاني

الآليات الإجرائية المستحدثة لمكافحة الجريمة المرتكبة عبر الإنترنت

أثرت الشبكة العنكبوتية للإنترنت على نوعية الجرائم التي ترتكب عبرها، حيث أفرزت هذه الشبكة الاتصالية العالمية جرائم جديدة لم تكن تعرفها الساحة القانونية من قبل، هذا التأثير امتد إلى الآليات التي وضعت قصد مكافحتها، ولعل الجانب الإجرائي نال الجزء الأكبر من تأثير هذه الأخيرة على النظم القانونية بصفة عامة، حيث لم تعد الإجراءات التقليدية تف بالغرض في متابعة تطورات هذه الجريمة المستحدثة.

لهذا عمد المشرع شأنه شأن سائر مشرعي دول العالم إلى وضع آليات إجرائية مستحدثة من شأنها وضع أسس متابعة فعالة للجريمة المرتكبة عبر الإنترنت، تمثلت في: التسرب **(فرع أول)**، والمراقبة الإلكترونية **(فرع ثان)**، وحفظ المعطيات المتعلقة بحركة السير **(فرع ثالث)**.

[270]– لمزيد من التفاصيل راجع: **مليايني عبد الوهاب**، مرجع سابق، ص 314.

الفرع الأول

التسرّب كإجراء لمكافحة الجريمة المرتكبة عبر الإنترنت

اعتمد المشرع أسلوب التسرّب كإجراء من إجراءات التحري والتحقيق عند تعديله قانون الإجراءات الجزائية بمقتضى القانون رقم(06-22[271]) مبرزا ماهية وضوابط إجرائه والآثار المترتبة عنه، وعليه سنتطرق إلى مفهوم عملية التسرب **(أولا)**، شروط صحة عملية التسرب **(ثانيا)**، ثم الحماية القانونية للمتسرب **(ثالثا)**.

أولا: مفهوم عملية التسرب

عرّف المشرع "التسرّب" في المادة 65 مكرر 12 من قانون الإجراءات الجزائية كما يلي: "**يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف**".

وعرّفه بعض الفقه بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسئولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنظمتهم الإجرامية وذلك بإخفاء الهوية الحقيقية، وبتقديم المتسرب على أنه فاعل أو شريك[272].

يعتبر التسرّب من أهم وأخطر طرق التحري وجمع المعلومات ولا يقوم بها إلا أعضاء التحري الأكفاء المدربين على ذلك، وينصح دائما بعدم اللجوء لذلك إلا بعد دراسة الوضع من كافة زواياه وتقدير الظروف والتأكد من أن هذا الأسلوب هو الوسيلة الوحيدة للوصول

---

[271]- قانون رقم 06-22 مؤرخ في 2006/12/20 يعدل ويتمم الأمر رقم 66-155 يتضمن قانون الإجراءات الجزائية، ج ر عدد 84، صادر بتاريخ 2006/12/24.

[272] - **بن خليفة إلهام**، مرجع سابق، ص 305.

إلى المعلومات المراد كشفها، وذلك لاحتمال انكشاف ظروف التحري والمساس بسرية المأمورية وبالتالي تعريض حياة الضابط للخطر[273].

ثانيا: شروط صحة عملية التسرب

لكي يكون لإجراء التسرب آثار قانونية يجب أن يتم وفق شروط شكلية **(1)** وأخرى موضوعية **(2)**

1-الشروط الشكلية لصحة التسرب

تتمثل الشروط الشكلية للتسرب في:

أ- تحرير محضر مسبق من طرف ضباط الشرطة القضائية

ألزم المشرع بموجب نص المادة 65 مكرر 13 من قانون الإجراءات الجزائية، ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب أن يحرر تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم، باستثناء الجرائم التي قد تعرض أمن الضابط أو العون المتسرب للخطر، وكذا الأشخاص المسخرين المنصوص عليهم في المادة 65 مكرر 14 هذا يعني أن يتضمن التقرير البيانات التالية، علاوة على عناصر **معاينة الجريمة، تحديد هوية العناصر المشتبه في تورطهم في العملية، "أسماؤهم وألقابهم المستعارة، الأفعال المجرمة"، الوسائل المستعملة "نوعيتها، تحديدها كالسيارات والآلات"، الأدلة المحجوزة وتحديدها، تحديد الأماكن والعناوين التي تم استعمالها "أماكن التخزين وطرق التوزيع"، تحديد كيفيات مخادعة رجال الأمن أو بعبارة أدق رصد كل مجريات عمليات الجريمة من بدايتها إلى**

[273] -**داود سليمان الصبحي**، أساليب البحث والتحري، بحث مقدم إلى الدورة التدريبية إجراءات التحري والمراقبة والبحث الجنائي، المنعقدة بكلية التدريب قسم البرامج التدريبية بجامعة نايف العربية للعلوم الأمنية، الرياض، خلال الفترة 25-29/أفريل/2009، ص15.

نهايتها، وتبقى الهوية الحقيقية للمتسربين مجهولة حتى بالنسبة لوكيل الجمهورية وقاضي التحقيق والنائب العام وكل القضاة[274].

1-صدور إذن قضائي بمباشرة العملية:

يجب أن يصدر الإذن بعملية التسرب من طرف وكيل الجمهورية إن لم يكن قد افتتح التحقيق في القضية أو من قبل قاضي التحقيق إذا كان التحقيق قد أفتتح، ويجب أن يكون الإذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب[275].

2-الشروط الموضوعية لصحة التسرب

تتمثل الشروط الموضوعية للتسرب في:

أ- مبررات اللجوء لعملية التسرب

طبقا لنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية فإن التسرب كإجراء جديد وحديث للتحري أوجدته ضرورات قضائية في التشريع وحسب النص السالف الذكر فإن اللجوء لهذا الإجراء يكون **(عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المنصوص عليها في المادة 65 مكرر 5).**

---

274 – **مجراب الدوادي**، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام، كلية الحقوق، جامعة الجزائر، 2015-2016، ص 337.

275– **شرف الدين وردة، «مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية –في التشريع الجزائري–** »مجلة المفكر العدد 15، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، د.س.ن، ص 546.

بمعنى أن مباشرة هذا الإجراء يكون عند الضرورة الملحة في جميع البيانات والاستدلالات الجنائية وأيضا لصنف محدد من الجرائم فالدافع هو الضرورة أولا و طبيعة الجرائم ثانيا[276]

ب- سرية عملية التسرب

يقصد بها كتمان سرّ عن كل ما يتعلق بالعملية، وتكون السرية عاملا يضمن عدم المساس بسلامة العنصر المتسرب من جهة، ويضمن إبقاء النشاط الإجرامي للشبكة في سريان عادي دون أن يشك المجرم بأنه تحت المراقبة، كما أن لها دور فعال في ضمان أمن وسلامة المتسرب وحسن سير العملية[277].

يخفي ضابط أو عون الشرطة القضائية المتسرب هويته الحقيقية وصفته أثناء القيام بالمهمة[278]، وهو عمل أجازه المشرع بنص المادة 65 مكرر 16 من القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، التي تنص "**لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات**".

ج-الجرائم التي تستدعي عملية التسرب

نص المشرع على هذه الجرائم بموجب المادة 65 مكرر 05 من القانون رقم 06-22 المعدل والمتمم لقانون الاجراءات الجزائية والذي حصرها في سبع جرائم هي:

- جرائم المخدرات
- الجريمة المنظمة العابرة للحدود الوطنية
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

---

[276]- **قريشي حمزة**، الوسائل الحديثة للبحث والتحري في ضوء قانون 06-22 دراسة مقارنة، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، ورقلة، 2012، ص 75.

[277]- **عنتر أسماء**، «**مكافحة الجرائم المستحدثة في التشريع الجزائري** "**التسرب نموذجا**"»، مجلة القانون العام الجزائري والمقارن، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 06، سنة 2017، ص 79.

[278] - لمزيد من التفاصيل أنظر: **مجراب الدوادي**، مرجع سابق، ص 332.

- جرائم تبييض الأموال
- جرائم الإرهاب
- الجرائم المتعلقة بالتشريع الخاص بالصرف.
- جرائم الفساد

تجدر الإشارة هنا إلى أن هذه الجرائم المستحدثة لا يعني بالضرورة أنها حديثة، وإنما قد تكون معروفة وسائدة من قبل، لكن ثمة تغييرات كثيرة طرأت عليها لتظهر بمظهر وشكل جديدين، سواء تعلق الأمر بنشأتها، أركان تأسيسها، أو التحقيق فيها[279].

ثالثا: الحماية القانونية للمتسرب

أقرّ المشرع بعض الضوابط الرامية إلى حماية القائم بعملية التسرب والتي تتمثل في:

1-انعدام المسؤولية الجنائية

المقصود بها أن ضابط الشرطة القضائية أو العون المتسرب غير مسؤول جزائيا عن الأعمال التالية:

- اقتناء أو تسليم أو إعطاء أو نقل مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذلك وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

نجد أن المشرع رفع المسؤولية الجزائية عن هذه الأفعال الإجرامية التي يقوم بها المتسرب حتى يكسب ثقة التنظيم الإجرامي، ما عدا في حالة تحريضه عن ارتكاب جرائم فيكون مسؤولا جنائيا عنها[280].

---

[279] – **شيخ ناجية، «إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة»**، مجلة معارف، جامعة البويرة، العدد 25، ديسمبر 2018، ص ص 11-12.

[280] – لمزيد من التفاصيل راجع: **عنتر أسماء**، مرجع سابق، ص 87.

2-المسؤولية الجنائية للمعتدي على المتسرب أو كاشف هويته

أقر قانون الإجراءات الجزائية عقوبة في حق كل من يكشف هوية المتسرب أو يعتدي عليه أو على أهله وذلك بمقتضى المادة 65 مكرر 16، التي نستشف من خلال استقرائها ثلاثة حالات هي:

أ- الكشف على هوية المتسرب دون وقوع ضرر له يعاقب عليه بالحبس من سنتين إلى خمس سنوات وغرامة مالية من (50,000 إلى 200.000 دج)

ب- الكشف على هوية المتسرب المفضي إلى أعمال عنف في حق المتسرب أو ذويه وهم زوجة أو أبناء أصوله المباشرين يعاقب عليه بالحبس من (05) سنوات إلى (10) سنوات وغرامة من (200.000) إلى (500.000 دج)

ت- الكشف المفضي إلى وفاة المتسرب أو أحد ذويه المذكورين سابقا تكون العقوبة من (10) سنوات إلى (20) سنة والغرامة من (500.000) إلى (1000.000 دج) دون الإخلال عند الإقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.

الفرع الثاني

المراقبة الإلكترونية كإجراء لمكافحة الجريمة المرتكبة عبر الإنترنت

يقصد بالمراقبة الإلكترونية ذلك الإجراء الذي ينصب على مراقبة الاتصالات السلكية واللاسلكية عن طريق اعتراضها، حيث يعد من بين أهم الإجراءات المستحدثة التي وضعها المشرع لمتابعة الجرائم المرتكبة عبر شبكات الاتصال خاصة المرتكبة عبر شبكة الإنترنت، وسوف نتطرق لذلك من خلال تبيان شرعية اللجوء إلى المراقبة الإلكترونية **(أولا)**، حالات اللجوء إلى المراقبة الإلكترونية **(ثانيا)**، ثم غلى ضمانات تنفيذ المراقبة الإلكترونية **(ثالثا)**.

أولا: شرعية اللجوء إلى المراقبة الإلكترونية

تباينت الآراء بخصوص مدى شرعية استخدام طرق المراقبة الالكترونية، فبالرغم من إقرارها قانونا إلاّ أنّها أثارت جدلا في الفقه:

1- الرأي المعارض للمراقبة الإلكترونية

ذهب اتجاه فقهي إلى القول بعدم شرعية استخدام هذه الطرق نظرا لمخالفتها للدستور وللمبادئ العامة للقانون والاتفاقيات الدولية، ونظرا لما في ذلك من اعتداء على خصوصية الفرد وإرادته وسرية حياته الشخصية.

من جانب آخر يرى أنصار هذا الاتجاه أن استخدام مثل هذه الطرق من شأنه أن يؤدي إلى التعسف في استعمالها والاعتداء على خصوصية الأفراد[281].

2- الرأي المؤيد للمراقبة الإلكترونية

على عكس الاتجاه الأول يرى أنصار هذا الاتجاه بمشروعية استخدام هذه الأساليب في البحث والتحري عن الجرائم والبحث عن المجرمين، ومن ثم فإن لهذه الأساليب فائدة عملية وعلمية، مما دفع بالكثير من التشريعات إلى انتهاج هذه الوسائل لمكافحة الجريمة وترصد المجرمين ولم يتوقف الأمر عند هذا الحد، بل حتى الدول التي تنادي بحماية حقوق الإنسان اعتمدت على هذه الأساليب ونادت بضرورة استخدامها الاتفاقيات الدولية في ظل التطورات الخطيرة التي يشهدها الإجرام المنظم، وجرائم المخدرات وتبييض الأموال والفساد وغيرها[282].

3- موقف المشرع الجزائري من المراقبة الإلكترونية

لم يبق للمشرع أمام استفحال الجرائم الخطيرة سوى القبول بإجراء المراقبة وذلك في حدود الضرورة، ونظرا لخطورة هذا الاجراء، وبما أنه استثناء عن الأصل العام المتمثل في

---

[281]- مشار لهذا الرأي لدى: **باخويا دريس، رواق عمرية، «أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الإنسان»**، مجلة الدراسات القانونية والسياسية، جامعة عمر ثليجي الأغواط، العدد 05، المجلد 01، جانفي 2017، ص 81.

[282]- مشار لكل ذلك لدى: **بولافة سامية، ساسي مبروك، «الأساليب المستحدثة في التحريات الجزائية»**، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، العدد التاسع، جوان 2016، ص 393.

حظر إجراء التنصت فقد أحاط هذه الإجراءات بمجموعة من الضمانات والشروط معا، لإقامة توازن دقيق بين الحق في الحياة الخاصة وبين حق المجتمع في العقاب[283].

ونص على مشروعية أجهزة المراقبة بموجب المواد من 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، الواردة في الفصل الرابع من الباب الثالث تحت عنوان "**في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور**".

كما تدخل كذلك بمقتضى القانون رقم 09-04 لتكملة وتنظيم المحادثات التي تتم عن طريق الإنترنت وأجاز بموجب المادة الثالثة منه اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل محتواها خاصة البريد الإلكتروني باعتباره أهم وسيلة تقنية في مجال التراسل الإلكتروني وبالتالي عملية المراقبة تنصب عليه[284].

ثانيا: حالات اللجوء إلى المراقبة الإلكترونية

يجوز القيام بعمليات المراقبة المنصوص عليها في المادة 04 من القانون 09-04 المتعلق بجرائم الإعلام والاتصال ومكافحتها في الحالات التالية:

1- الوقاية من الافعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة: يفهم من مصطلح الوقاية أن الجريمة لم ترتكب بعد ولكن المشرع سمح في هذا النوع من الجرائم بإجراء مراقبة على الاتصالات الإلكترونية لأشخاص أو مجموعات يحتمل تورطهم مستقبلا[285].

2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة أو الإقتصاد الوطني.

---

[283]- **بن لاغة عقيلة**، حجية أدلة الإثبات الجنائية الحديثة، مذكرة لنيل شهادة الماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2011-2012، ص 86.

[284]- **بن طالب ليندا**، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2019، ص 114-115.

[285]- **بن فردية محمد**، مرجع سابق، ص 196.

3- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية.

ثالثا: ضمانات تنفيذ المراقبة الإلكترونية

حتى ينتج إجراء المراقبة الإلكترونية آثاره أحاطه المشرع بعدة ضمانات هي:

1- استصدار إذن قضائي مكتوب

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة سالفا والمتعلقة بأمن الدولة ومؤسساتها والدفاع الوطني وكذلك تنفيذ المساعدات القضائية الدولية إلا بإذن مكتوب من السلطة القضائية المختصة، وبالتالي يشترط لإجراء المراقبة الإلكترونية أن يكون مكتوبا تحت طائلة البطلان، وذلك أن الأصل في العمل الإجرائي الكتابة، ولم يكتف المشرع بذلك بل اشترط أن يكون صادرا من سلطة قضائية مختصة، بأن يكون مصدره مختصا نوعيا ومكانيا أصلا بالبحث أو التحقيق في الجريمة التي صدر الإذن بشأنها، ووفقا للقواعد العامة يتحدد الاختصاص النوعي بحسب نوعية الجريمة، أما الاختصاص المكاني فيتحدد بمحل الواقعة، أو مكان ضبط المتهم أو محل إقامته[286].

ويشترط في الإذن حتى يكون شرعيا العناصر التالية:

- التعريف بالعملية: أي ذكر نوعية وتحديد الاتصالات المطلوب اعتراضها.
- الأماكن المقصودة ومحل الاعتراض والمراقبة.
- طبيعة الجريمة التي تبرر هذا الإجراء.

[286]- **بن فردية محمد**، مرجع سابق، ص 197.

- تسليم الإذن كتابة، وتحديد المدة التي لا يجب أن تتعدى 04 أشهر قابلة للتجديد[287]، غير أنه إذا تعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أجاز المشرع للنائب العام لدى مجلس قضاء العاصمة أن يمنح إذنا مكتوبا بإجراء المراقبة الإلكترونية لمدة لا تتجاوز 06 أشهر قابلة للتجديد لضباط الشرطة القضائية المعينين في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[288].

2- تسخير عون مؤهّل للمراقبة الإلكترونية

يجوز لوكيل الجمهورية، أو قاضي التحقيق، أو لضابط الشرطة القضائية أن يسخر عون مؤهل لدى هيئة مكلفة بالاتصالات سواء كانت عامة، أو خاصة للقيام بهذا الإجراء، كما يمكنه طلب المساعدة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، لأن من ضمن مهام هذه الهيئة قانونا هي مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنلوجيات الإعلام والاتصال[289].

3- سرية إجراءات المراقبة الإلكترونية

الأصل أن إجراءات التحري والتحقيق سرية، لذلك فإن القانون يلزم من ساهم في التحقيق أو اتصل به بشكل أو بآخر كتمان سرية الإجراءات المتبعة، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات[290]، بل ذهب إلى أكثر من ذلك بالنسبة

---

[287] – أنظر في ذلك المادة 65 مكرر 07 فقرة 2 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن تعديل قانون الإجراءات الجزائية،

[288]– أنظر في ذلك المادتين 04 و13 من قانون رقم 09-04 المؤرخ في 05 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[289]– **جبار فطيمة**، «**مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري**»، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة الشلف، العدد الثالث، ديسمبر 2016، ص 19.

[290]– **مذكور عائشة**، الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون العقود، كلية الحقوق والعلوم السياسية، جامعة آكلي محند أولحاج، البويرة، 2018، ص 174.

للترتيبات وتنفيذ المراقبة الإلكترونية، حيث نصت المادة 65 مكرر 6 من قانون الإجراءات الجزائية أن هذه الإجراءات لا تتم إلاّ إذا التزم القائم بها بمبدأ كتمان السر المهني وعدم إذاعة أسرار التحري والتحقيق المنصوص عليه في نص المادة 47 من نفس القانون.

4- حماية المعطيات المتحصل عليها

تنص المادة التاسعة من القانون رقم 09-04 بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، في حالة استعمال هذه المعطيات خارج الحدود أي التحريات، أو التحقيقات القضائية[291].

5- عدم المساس بالحرية الشخصية

تنص المادة 107 من قانون العقوبات الجزائري أنه "**يعاقب الموظف العمومي بالسجن المؤقت من خمس 5 سنوات إلى عشر 10 سنوات إذا أمر بعمل تحكمي أو ماس بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر**".

نشير هنا إلى أن ضابط الشرطة القضائية ملزم بالإجراءات التي وضعها القانون حماية لحقوق الأفراد وحرياتهم الشخصية، كما أنه ملزم بالتقيد بالإذن المقدم له سواء من قبل قاضي التحقيق أو وكيل الجمهورية، وأي خروج على فحوى الإذن ينتج عنه مساس بالحرية الشخصية يعرض ضابط الشرطة القضائية إلى العقوبة السالفة الذكر[292].

الفرع الثالث

حفظ المعطيات المتعلقة بحركة السير

استحدث المشرع هذا الإجراء طبقا للقانون رقم (09-04) المتضمن الوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك عن طريق وضع العديد من

[291]- أنظر المادة 09 من قانون رقم 09-04 المتضمن جرائم تكنولوجيا الإعلام الاتصال ومكافحتها.

[292]- **جبار فطيمة**، مرجع سابق، ص 19.

الالتزامات على عاتق مزودي خدمات الإنترنت والمتعلقة بحفظ كل المعطيات المجمعة عبر الإنترنت وإفشائها إلى رجال الضبطية القضائية إذا احتاجوا لها أثناء استدلالهم حول جريمة من الجرائم المرتكبة في هذا النطاق، وسنتطرق هنا إلى مفهوم حفظ المعطيات المتعلقة بحركة السير **(أولا)**، مفهوم مزودي خدمات الإنترنت **(ثانيا)** ثم إلى التزامات مزودي خدمات الإنترنت **(ثالثا)**.

أولا: مفهوم حفظ المعطيات المتعلقة بحركة السير

يعتبر حفظ البيانات اداة تحقيق في إطار جرائم الحاسوب والجرائم المرتبطة بها، حيث تكون البيانات محلا للتلاعب، مما يؤدي بالدليل إلى الضياع بسهولة من خلال الإهمال في التخزين، أو التلاعب العمدي أو الحذف المصمم بتدمير الدليل، أو الحذف الروتيني للمعلومات التي لم تعد لها حاجة، ولذلك يجب أن يكون المسؤول عن حفظ البيانات جديرا بالثقة يمكن معه تأمين مصداقية البيانات استنادا إلى أمر حفظ البيانات، كما أن الكم الهائل من التراسل والاتصالات يمكن أن يؤدي إلى تداخل المعطيات، فيصبح تحديد مصدر الاتصال أو جهة إرساله مهم جدا لمعرفة هوية مرتكبي الجريمة، ولهذا فحفظ حركة البيانات المتعلقة بالاتصالات هو أمر لازم لأنه هو الذي يسمح بتتبع الاتصال ومعرفة مصدره، فيكون الإجراء أفضل من التفتيش والضبط المعلوماتي[293].

عرّف المشرع حفظ المعطيات المتعلقة بحركة السير من خلال المادة 02 من قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال بأنها: "**أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا من حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة**".

[293]– **روابح فريد**، مرجع سابق، ص 11.

ثانيا: مفهوم مزودي خدمات الإنترنت

يتطلب تشغيل شبكة الإنترنت وجود مجموعة من الأشخاص القائمين على تشغيل هذه الشبكة، وذلك لأن تشغيل الإنترنت واستغلال خدماتها في حاجة إلى أنشطة وأدوات متعددة في تشغيل أجهزة وتخزين المعلومات وبثها وعرضها، وهؤلاء الاشخاص هم الذين يمكن أن نطلق عليهم مصطلح "الوسطاء في خدمة الإنترنت أو المهنيين".

يتمثل دور مزودي خدمات الإنترنت في تمكين المستخدم من الدخول والتجول فيها والاطلاع على ما يريد، وكذلك منهم ناقل خدمة الإنترنت، ومنهم من يمكن المستخدم من الدخول إلى موقع الإنترنت المطلوب، ومنهم من يخزن المعلومات أو ينتجها أو يوردها[294].

ثالثا: التزامات مزودي خدمات الإنترنت

تقع على عاتق مزودي خدمات الإنترنت العديد من الالتزامات نذكر أهمها:

1-حفظ البيانات المتعلقة بحركة السير

تنص المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على: "**مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدموا الخدمات بحفظ:**

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج-الخصائص التقنية وكذا تاريخ ووقف ومدة كل اتصال.

د-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها".

---

[294] – **مرنيز فاطمة**، الإعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013، ص 12.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة أ من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه..." [295].

يفهم من ذلك أن إجراء الحفظ يتم بعد قيام مقدمي الخدمات بإجراء التجميع والتسجيل ثم الحفظ ليقدم في النهاية إلى يد السلطات المكلفة بالتحريات القضائية، وتكتسي هذه الإجراءات أهمية بالغة من حيث كونها أداة تنقيب وتحري مفيدة من أجل تحديد مصدر الاتصال ومآله عن طريق أرقام الهاتف، كما توفر بيانات مرتبطة بالساعة والتاريخ والمدة المتعلقة بأنواع الاتصال غير المشروعة[296].

2-اتخاذ الاحتياطات الأمنية الكافية

ألزم المشرع مزودي خدمات الإنترنت بأخذ الاحتياطات الأمنية الكافية وذلك بتصفية المواقع وبيان نوعها وذلك بنصه في المادة 12 من القانون رقم 09-04 على أنه: "**زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه يتعين على مقدمي خدمات الإنترنت ما يلي:**

أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة، وإخبار المشتركين لديهم بوجودها".

3-الالتزام بمدة التخلص من المعطيات

بما أن حفظ المعطيات إجراءاً وقتياً فقد لجأ المشرع واحتراما للحق في الخصوصية إلى وضع التزام على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها وذلك بعد سنة ابتداء من تاريخ التسجيل[297]، وهو ما يستفاد بمفهوم المخالفة من نص المادة 11 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات

---

[295]- أنظر المادة 11 من القانون رقم 09-04، السالف ذكره.

[296]- **بن خليفة إلهام**، مرجع سابق، ص 327.

[297] -**مليانى عبد الوهاب**، مرجع سابق، ص 344.

الإعلام والاتصال ومكافحتها كما يلي: "...**تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة من تاريخ التسجيل...**"

4-مساعدة العدالة

يقتضي الأمر أن يقوم مزود الإنترنت بتقديم كافة البيانات التي تساهم في تحديد هوية المؤلف إلى السلطات[298]، وفي هذا السياق ألزم المشرع مزود خدمات الإنترنت وبموجب المادة 1/10 من القانون رقم 09-04 "...**يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها...**"

5- مسؤولية مزودي خدمات الإنترنت عن إهمال حفظ المعطيات

إن إخلال مزودي الخدمات بأحد الالتزامات الملقاة على عاتقهم بموجب القانون رقم 09-04 بما في ذلك الالتزام بالتحفظ على المعطيات المتعلقة بحركة السير، من شأنه أن يعرقل عمل السلطات المكلفة بالتحريات القضائية، مما يؤدي إلى قيام المسؤولية الجزائية للمخالف، فضلا عن قيام مسؤولية إدارية[299]، وذلك ما نصت عليه الفقرتين الأخيرتين من المادة 11 من القانون رقم 09-04 والتي جاء فيها:

"**دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.**

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقرر في قانون العقوبات".

---

[298] – **مرنيز فاطمة**، مرجع سابق، ص 31-32. أنظر كذلك:

- **BOSSAN Jerome**, Le droit pénal confronté à la diversité des intermédiaires de l'internet, revue de science criminelle et droit pénal comparé, n° 2, vol 2, 2013, p 306, disponible en ligne à l'adresse: https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2013-2-page-295.htm

[299]– **مذكور عائشة**، مرجع سابق، ص 181.

نستخلص مما سبق أن المجتمع الدولي قد تنبه إلى خطورة الجريمة المرتكبة عبر الإنترنت كظاهرة إجرامية مستحدثة لم يعرفها القانون من قبل، حيث أن هذه الأخيرة كل المصالح الأساسية للدول والحسابات الشخصية للأفراد عرضة للكثير من الاعتداءات، الأمر الذي أدى إلى وضع الآليات القانونية اللازمة لمكافحتها والتي كانت جد فعالة في مجملها.

بدأت أولى بوادر وضع الآليات القانونية لمكافحة الجريمة المرتكبة عبر الإنترنت في محاولة المجتمع الدولي في حصر هذه الجريمة وفق قالب قانوني يحدد مفهومها وأساليب تجريمها، وذلك تبعا لخطورتها والأثار الجسيمة المترتبة عنها، حيث نجح هذا الأخير إلى أبعد الحدود في وضع ترسانة قانونية سواء في شقها الموضوعي أو الإجرائي سمحت له بوضع استراتيجية فعالة لمكافحة هذا النوع المستحدث من الجرائم.

وخير دليل على ذلك الاعتماد على إبرام العديد من الاتفاقيات الدولية التي تعنى بمكافحة هذه الظاهرة الإجرامية على غرار اتفاقية بودابست التي يمكن اعتبارها الإطار الأمثل لمكافحة الجرائم المرتكبة عبر الإنترنت، وذلك لأنها تحصر وتشمل على أهم نصوص التجريم من جهة، وتحفّز على التنسيق والتعاون في مجال مكافحة هذه الجرائم سواء على المستوى الإقليمي أو الدولي.

كما حذت هذا النهج أغلب مشرعي دول العالم ومن بينها المشرع الجزائري الذي واكب التطورات المتسارعة للجريمة في حد ذاتها من جهة، و تحول السياسة التشريعية على المستوى الدولي من جهة أخرى، فقام بوضع آليات قانونية موضوعية وإجرائية سواء بتعديل القواعد القانونية التقليدية لتواكب هذه الجريمة المستجدة، أو وضع نصوص قانونية خاصة والتي كان لها دور كبير في الحد من آثارها.

ذهب المشرع إلى أكثر من ذلك ولم يكتف بتحيين النصوص القانونية التي تعنى بالجرائم الواقعة في إقليم الدولة، بل تعداه إلى البعد الدولي وذلك مرده إلى الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت المتعدية للحدود الوطنية، فقام بوضع آليات تعنى بالتعاون الدولي خاصة في الجانب الإجرائي والمتمثل بوضعه لآليات التعاون القضائي والأمني

الدولي خاصة في مجال الإنابات القضائية وتبادل المعلومات وتسليم المجرمين والتي كانت عن طريق انضمامه للعديد من الاتفاقيات الدولية وإبرامه لاتفاقيات ثنائية.

غير أن الملاحظ في هذا الصدد ورغم فعالية هذه اللآليات الموضوعة لمكافحة الجريمة المرتكبة عبر الإنترنت، إلا أنه واجهتها العديد من التحديات والصعوبات خاصة من الناحية العملية وهذا ما سنراه في الباب الثاني من دراستنا هذه.

الباب الثاني

قصور الآليات المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت

ألغت الشبكة العالمية للإنترنت معالم الحدود الجغرافية للدول افتراضيا، فهي لا تعير الاعتبار لفكرة الزمان والمكان فيما يخص العلاقات التي تربط المتعاملين عبرها، هذه الخاصية التي تتميز بها الشبكة ضف إليها التركيز الكبير عليها من طرف المتعاملين في قضاء معاملاتهم والانتشار الواسع لاستعمالها في الإتيان بالكثير من المعاملات أثار العديد من التحديات والإشكالات القانونية.

ولعل من بين أهم الظواهر المنجرة عن هذه الشبكة هي الجريمة، التي قام الجناة بنقلها من العالم التقليدي إلى هذا العالم الافتراضي، والتي أدت بالدول والمجتمع الدولي إلى محاولة وضع أسس الحماية القانونية من أجل مكافحة هذه الظاهرة الإجرامية المستحدثة، من خلال –كما سبق وأن رأينا في الباب الأول– وضع ترسانة قانونية موضوعية وإجرائية تكفل معالجة هذه الجريمة.

غير أن الملاحظ في هذا الصدد أن الجهود المبذولة سواء على المستوى الدولي أو الوطني، اصطدمت بالعديد من العراقيل التي حدت من فعالية أساليب مكافحة الجريمة المرتكبة عبر الإنترنت، والتي تعتبر بمثابة تحديات للقائمين على مكافحة هذه الظاهرة الإجرامية المستحدثة، والتي يجب عليهم تجاوزها من أجل وضع أسس أكثر فعالية لمكافحتها.

تتجلى التحديات التي واجهت آليات مكافحة الجريمة المرتكبة عبر الإنترنت في مسائل عديدة، جعلتها تبدوا غير فعالة في مكافحة هذا النوع المستحدث من الإجرام رغم تفعيلها على أرض الواقع.

نلاحظ أن خصوصية الجريمة المرتكبة عبر الإنترنت تعتبر من العقبات الأولى التي اصطدمت بها محاولات مكافحتها، حيث أن اختلاف البيئة التي ترتكب فيها هذه الجريمة عن مسرح الجريمة التقليدية أعطاها خصوصية لم يعرفها القانون من قبل، بل هذه الصعوبة ذهبت إلى أكثر من ذلك خاصة مع تميز شبكة الإنترنت بالبعد الدولي والعالمي، الأمر الذي

انجر عنه صعوبة تطبيق القواعد القانونية الوطنية على هذا النوع من الجرائم وذلك لاصطدامها بمبدأ سيادة الدول على إقليمها **(فصل أول)**.

كما يعتبر موضوع الخصوصية أو الحق في الحياة الخاصة من المفاهيم التي أثرت على مكافحة الجريمة المرتكبة عبر الإنترنت، فالحق في الخصوصية الرقمية يعتبر من المواضيع المطروحة بشدة عبر الساحة القانونية في الوقت الراهن، وذلك لاعتباره حق أصيل من حقوق الإنسان، غير أن هذا الحق الذي كرسته أغلب التشريعات الوطنية والدولية كان بمثابة حاجز يحول بين الجريمة ومكافحتها، وذلك عن طريق منع التعدي على هذا الحق إلا عن طريق إجراءات قانونية تتسم بالطول والتعقيد، وهذا ما لا يماشى مع السرعة الفائقة التي تتميز بها الجريمة المرتكبة عبر الإنترنت **(فصل ثان)**.

الفصل الأول

قصور ناتج عن خصوصية الجريمة المرتكبة عبر الإنترنت

أثارت الجريمة المرتكبة عبر الإنترنت انتباه المجتمع الدولي نظرا للخطورة التي تميزت بها واستوعب حجم الخسائر المنجرة عنها، فسعي لمكافحتها عن طريق سن العديد من النصوص القانونية ووضع الكثير من الآليات التي أثبتت فعاليتها في بادئ الأمر، غير أن خصوصية هذه الجريمة وسرعة تطورها جعل أمر مكافحتها يتسم بالصعوبة.

اعترت الآليات القانونية التي تعنى بمكافحة الجريمة المرتكبة عبر الإنترنت الكثير من الصعوبات، فمن الناحية النظرية وفي بداية استخدامها بصورها المختلفة سواء موضوعية أو إجرائية كانت توحي بأنها تفي بالغرض، غير أنه من الناحية الواقعية والعملية اصطدمت هذه الآليات بعدة عقبات وعراقيل راجعة إلى سببين رئيسيين.

تعد الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت من بين أكبر الصعوبات التي واجهت آليات مكافحتها، فالجريمة في حد ذاتها تتميز بعدة صفات جعلت منها جريمة مستعصية على جهات إنفاذ القانون، حيث أن خفاء الجريمة والسرعة في تنفيذها ومحو الدليل فيها كلها مميزات عرقلت من آليات مكافحتها **(مبحث أول)**.

اكتسبت الجريمة المرتكبة عبر الإنترنت البعد عبر الوطني الذي استمدته من الطبيعة العالمية لشبكة الإنترنت التي لا تعترف بالحدود الجغرافية والسياسية بين الدول، إن هذه الخاصية حدت من فعالية آليات مكافحة هذه الجريمة خاصة بالنسبة للإجرائية منها التي تعنى بمتابعة المجرمين، حيث أن هذه الأخيرة كثيرا ما تصطدم بمبدأ إقليمية النص الجزائي بما أن المجرم متواجد خارج الحدود الوطنية **(مبحث ثان)**.

المبحث الأول

من حيث الطبيعة التقنية للجريمة المرتكبة عبر الإنترنت

تختلف الجريمة المرتكبة عبر الإنترنت عن الجرائم المرتكبة في العالم التقليدي، وذلك لتميزها بعدة خصائص جعلت منها جريمة أكثر خطورة، حيث أن هذه الخصوصية التي تتميز بها هذه الجريمة المستحدثة أدت إلى ظهور عدة عقبات وصعوبات حدّت من فعالية الآليات القانونية الموضوعة لمكافحتها.

أدت الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت إلى صعوبة اكتشافها واثباتها مقارنة بتلك المرتكبة في العالم التقليدي، فهذه الأخيرة ترتكب في عالم مادي يمكن الوصول إلى الدليل فيه عن طريق إجراءات المعاينة المادية، الأمر الذي لا يمكن تحقيقه بالنسبة لاكتشاف وإثبات الجريمة المرتكبة عبر الإنترنت التي يكون مسرحها عبارة عن أرقام ورموز لا علاقة لها بالطابع المادي **(مطلب أول)**.

تتسم كذلك آليات مكافحة الجريمة المرتكبة عبر الإنترنت بالقصور نظرا للخصوصية التي يتميز بها الأطراف المتدخلين في هذه الجريمة سواء بالنسبة للجاني أو المجني عليه وحتى سلطات التحقيق فيها، حيث أن المجرم المعلوماتي يتميز عن المجرم التقليدي بالمهارة والذكاء، بالإضافة إلى أن المجني عليه فيها يتميز بنقص الخبرة وعدم التبليغ عن هذه الجرائم، إما لعدم علمه أصلا بحدوثها أو خوفا على سمعته، بالإضافة إلى ذلك أن سلطات التحقيق فيها في الغالب متأخرين عن مواكبة التطورات الكبيرة التي تعرفها هذه الجريمة المستحدثة **(مطلب ثان)**.

المطلب الأول

من حيث اكتشاف وإثبات الجريمة المرتكبة عبر الإنترنت

تعتبر مسألة اكتشاف الجريمة المرتكبة عبر الإنترنت من بين أكبر العقبات التي واجهت آليات مكافحتها، ويعود السبب في ذلك أن هذه الأخيرة ترتكب في فضاء افتراضي ليس له وجود مادي ملموس مثل الجريمة التقليدية، ضف إلى ذلك أن المجرم فيها يسعى إلى إخفائها حتى لا يتم الوصول إليه، بل إن المجني عليه في هذه الحالة له دور كبير إما عن طريق عدم التبليغ أو لنقص خبرته في هذا المجال **(فرع أول)**.

كما أن إثبات الجريمة المرتكبة عبر الإنترنت عن طريق آليات الإثبات المختلفة يعد أمراً صعباً، لأن الدليل فيها يختلف عن الدليل المادي المنجر عن الجرائم التقليدية التي يكون مسرحها مادي محسوس، فالدليل في هذه الجرائم يعتبر من الأدلة غير المحسوسة والتي تكون عبارة عن رموز وأرقام يصعب فهمها ويسهل محوها وتشفيرها من طرف الجناة **(فرع ثان)**.

الفرع الأول

اكتشاف الجريمة المرتكبة عبر الإنترنت

تتميز الجريمة المرتكبة عبر الإنترنت بصعوبة اكتشافها مقارنة بالجريمة التقليدية، حيث أن أغلب الجرائم التي ترتكب عبر العالم الافتراضي غالبا ما تكتشف بالصدفة، وذلك راجع إلى عدة أسباب نذكر منها إحجام المجني عليهم عن التبليغ **(أولا)**، نقص الخبرة لدى مصالح الاستدلال **(ثانيا)**، لا تخلّف آثاراً مادية **(ثالثا)**، بالإضافة على ذلك فإن الجناة يضربون حاجزا بينهم وبين أفعالهم لكي لا يتم اكتشافها (رابعا).

أولا: إحجام الجهات المتضررة عن إبلاغ السلطات المختصة

يعد عدم إدراك خطورة الجرائم المرتكبة عبر الإنترنت من قبل المسؤولين بالمؤسسات إحدى معوقات اكتشاف الجريمة، إذ تحرص الجهات المجني عليها والتي غالبا ما تكون مصرفا، أو مؤسسة مالية، أو شركة، أو مشروعا صناعيا ضخما، على الإحجام عن الإبلاغ

عن الجريمة بسبب الحفاظ على سمعة المؤسسات ومصداقيتها وثقة عملائها وعدم رغبتها في الظهور بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني ولم تتخذ الإحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي يجعلهم يفضلون الترضية المالية لعملائهم حتى لا يفقدوهم، ولا تتأثر سمعتهم المالية بدلا من البحث عن الجناة، فهذه المؤسسات لا تكتفي في إطار ذلك بالإحجام عن الإبلاغ، وإنما إلى جانب ذلك تلجأ إلى الترضية الودية فيما بينها وبين الجناة[299].

ثانيا: نقص جاهزية سلطات الاستدلال

اعتاد أعضاء الضبطية القضائية البحث والتحقيق في الجرائم العادية التي تقع في الواقع المادي، حيث يكون من السهل التنقل إلى مكان وقوع الجريمة والبحث عن الأدلة والاستدلال على مرتكبي الجرائم، والقبض عليهم والتحقيق معهم، وهي عملية تتطلب جاهزية ومهارة بدنية بشكل أساسي، حتى ظهرت الجرائم الإلكترونية التي تختلف تماما عن الجرائم التقليدية من حيث كيفية الوقوع والآثار المترتبة عنها والوسائل المستعملة لارتكابها، فأحدث طوارئ في أجهزة الضبط القضائي والتحقيق، وعندها تعالت الأصوات لإنشاء أجهزة خاصة للبحث والتحري في مثل هذه الجرائم والتي لا تعتمد على التدريبات المادية والفيزيولوجية، وإنما تعتمد على مستوى علمي وفكري معين ومهارات خاصة في مجال الاتصال والإنترنت، حتى يستطيع المحقق التحري والاستدلال في العالم الافتراضي ومطاردة المجرمين في البيئة الالكترونية[300].

---

[299]– **بثينة حبيباتني**، «**معوقات مكافحة الجريمة المعلوماتية**»، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، العدد 50، المجلد أ، ديسمبر 2018، ص 86.

[300]– **عمر عبد العزيز موسى الدبور**، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشاء ضبطية خاصة بالجرائم الإلكترونية، مقال موجه للمؤتمر الدولي: الجرائم الإلكترونية، المنعقد بطرابلس، بتاريخ 24–25 مارس 2017، منشورات مركز جيل البحث العلمي، لبنان، ص 217.

ثالثا: فقدان الآثار التقليدية للجريمة

مسرح الجريمة هو المكان الذي انتهت فيه أدوار النشاط الاجرامي ويبدأ منه نشاط المحقق الجنائي وأعوانه، بقصد البحث عن الجاني من واقع الآثار التي خلفها في مسرح الجريمة والتي تعد بمثابة الشاهد الصامت، الذي إذا أحسن المحقق الجنائي استنطاقه حصل على معلومات مؤكدة تساهم بشكل كبير في الكشف عن الحقيقة.

إلا أن مسرح الجريمة المرتكبة عبر الإنترنت يختلف تماما عن مسرح الجرائم التقليدية، فإذا كانت هذه الأخيرة تقع في واقع ملموس وحدود معينة، فإن الجريمة الإلكترونية تقع في واقع افتراضي لا حدود له، حيث لا تدع المجال لتحديد الفعل من عدمه، مما يجعل الأمر يزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة[301].

يخلق الطابع الافتراضي للجريمة المرتكبة عبر الإنترنت العديد من الإشكالات الواقعية والقانونية للمحققين، فبعد ظهور المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى إمكانية وقوع الجريمة في أماكن متعددة وفي زمن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل من الإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[302].

تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم القتل والمخدرات والسرقة والسطو المسلح وقطع الطريق، وهذا بخلاف الجرائم المتصلة بالحاسب

---

[301]– **فريجة محمد هشام**، «**النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني**»، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، العدد 24، جوان 2018، ص 148.

[302] – **عمر عبد العزيز موسى الدبور**، مرجع سابق، ص ص 223–224.

فإنها لا تتطلب عنفا، فنقل بيانات من حاسب آلي إلى آخر، أو السطو الإلكتروني على أرصدة بنك ما، لا تتطلب أي عنف أو تبادل لإطلاق النار مع رجال الأمن[303].

رابعا: فرض الجناة لتدابير أمنية

يتعمد الجناة فرض تدابير أمنية من أجل إخفاء جرائمهم وإزالة آثارها عن طريق التلاعب بالقواعد والبيانات والبرامج في الكمبيوتر، خاصة وأن التخزين الإلكتروني غير مرئي ومكتوب بلغة الأرقام، أو فرض تدابير احترازية من أجل عدم تسهيل إجراءات التفتيش التي يتوقع الجناة حدوثها كاستخدام كلمات السر، أو إعطاء تعليمات خفية بين هذه البيانات أو تشفيرها حتى يستحيل على جهات التحري والبحث الوصول إلى كشف هاته الأفعال غير المشروعة، مما يشكل عقبة أمام إقامة الدليل على الجريمة الإلكترونية وإثباتها[304].

الفرع الثاني

إثبات الجريمة المرتكبة عبر الإنترنت

يعد إثبات الجريمة المرتكبة عبر الإنترنت من بين أكبر التحديات التي تواجه الضبطية القضائية والنيابة العامة، فإن كان إثبات الجرائم التقليدية ميسورا نظرا لما تخلفه من دلائل مادية محسوسة يمكن معاينتها بالعين المجردة، يبقى إثبات الجريمة المرتكبة عبر الإنترنت يتميز بصعوبة بالغة لأنها ترتكب في عالم افتراضي غير محسوس والدليل فيها يكون عبارة عن أرقام فقط يصعب فهمها وتحصيلها، وسنتطرق قصد تبيان هذا إلى غياب الدليل ضد متهم معين **(أولا)**، إعاقة الوصول إلى الدليل **(ثانيا)**، ضخامة البيانات المتعين فحصها **(ثالثا)**، لا محدودية شبكة الإنترنت **(رابعا)**، فهم الدليل المتحصل من الجريمة **(خامسا)**، و إجراءات الحصول على الدليل الرقمي **(سادسا)**.

---

[303] – **محسن بن سليمان الخليفة**، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام (جريمة استنساخ برامج الحاسب اللآلي وبيعها وإنتاج الفيروسات ونشرها)، رسالة مقدمة استكمالا للحصول على درجة الماجستير، كلية الدراسات العليا، قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، د.س.ن، ص 44.

[304] – **فريجة محمد هشام**، مرجع سابق، ص 151.

أولا: غياب الدليل ضد متهم معين:

يكون دليل الإثبات في الجرائم التقليدية مرئيا مثل السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب وكذلك المادة السامة التي استعملت في القتل أو المحرر ذاته الذي تم تزويره أو النقود التي زيفت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو االمحقق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه[305]، ولكن في الجريمة المعلوماتية الدليل فيها يكون غير مرئي.

حيث أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة[306]، وبمجرد غلق جهاز الكمبيوتر أو قطع التيار الكهربائي عليه، يتسبب في محو المعلومات من الذاكرة، بمعنى فقدان كافة العمليات التي كان يتم تشغيلها، واتصالات الشبكة، وأنظمة الملفات الثابتة[307].

يتم تسجيل هذه البيانات إلكترونيا بكثافة بالغة وبصورة مرمزة غالبا ما تكون على دعائم أو وسائل للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها، وإن كانت قابلة للقراءة من قبل الأدلة نفسها ولا يترك التعديل أو التلاعب فيها أي أثر مما يقطع أي صلة بين المجرم وجريمته، ويحول دون كشف شخصيته وكشف وتجميع ادلة بهذا الشكل لإثبات وقوع الجريمة ونسبتها إلى مرتكبيها[308] وهو أحد أهم المشاكل التي يمكن أن تواجه جهات التحري والملاحقة[309].

---

[305]– **خيرت علي محرز**، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012، ص 36.

[306]- **DIOUF Ndiaw**, Infractions en relation avec les nouvelles technologies de l'information et procédure pénale: l'inadaptation des réponses nationales face à un phénomène de dimension internationale, afrilex n° 4, p 273, http://www.afrilex.u-bordeaux4.fr

[307]– **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص 115.

[308]– أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في "اوسلو" بالنرويج في الفترة ما بين 29-2000/05/31 موضوع عدم امكانية البنية التحتية للإنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة، أو المصدر الحقيقي لها، وموقعه على وجه التحديد، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالإنترنت والمستعمل كوسيلة لارتكاب الجريمة، أي ما يعرف اختصارا في النظام التقني (IP)، الذي يشير إلى رقم يعين الحاسوب الموصول على

ثانيا: إعاقة الوصول إلى الدليل :

يصعب الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تحول دون الوصول إليها أو ترميزها أو تشفيرها[310] لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها، بحيث أن البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال تحاط بجدار من الحماية الفنية[311].

يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول

الإنترنت، مثل هذا الرقم الذي يحدد هوية الحاسوب الذي استخدم في ارتكاب جرائم الاعتداء على نظم المعالجة الآلية إنما يفيد حال التوصل إليه واتخاذ إجراءات التحفظ بقصد ضبطه، ولكن في مقابل ذلك، فإن هذا الرقم ليس موحدا على المستوى العالمي، إذ أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية، ففي= =الولايات المتحدة أو كندا وبعض الدول الأخرى يمكن للشخص فيها اقتناء (IP) خاص به يشير إلى كونه أحد أعضاء الإنترنت ومن ثم يمكن تحديد هذا الشخص بكل سهولة لتبدأ بعد ذلك سلسلة إثبات ارتكابه للجريمة من عدمه.

إلا أنه في دول أخرى مثل أغلب الدول العربية فإن مصداقية الهوية عبر الإنترنت (IP) تتقلص كثيرا إذا علمنا أن كل خط هوية على الإنترنت يصادفه عدد من الهويات التي يمكن أن تكون محل للتغاير بين أعضاء الإنترنت المشتركين في مزود إنترنت واحد، وهنا يمكن القول أن مجرد وجود شخص في الجزائر أو في سوريا فإنه يملك فورا هوية رقمية محددة حقا حال وجوده على الإنترنت، إلا أنه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الإنترنت فإن الهوية السابقة لن تكون له وإنما لغيره، إذ من الممكن جدا –بل وهو الأمر المعتاد– أن يتواجد بهوية (IP) أخرى، أنظر في ذلك: **بوكر رشيدة**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012، ص 475.

[309] – **الطيبي البركة، حاج سودي محمد، «إشكالية الإثبات في الجرائم الإلكترونية»**، مجلة آفاق علمية، جامعة تمنراست، المجلد 11، العدد 01، سنة 2019، ص 269.

[310] – لمزيد من المعلومات حول التشفير راجع في ذلك الفرع الأخير من بحثنا هذا والمعنون بالتشفير

[311] - يلجأ المجرم المعلوماتي إلى هذه الأساليب لإعاقة جهات التحقيق إلى الدليل الذي يمكن أن يدينه لأن هذا الأخير يعلم بأن من الصعب التخلص من الدليل الإلكتروني وذلك راجع إلى أن الكمبيوتر يسجل كذلك نشاط الجاني عند محوه للدليل هذا من جهة، ومن جهة ثانية فإنه وللتخلص النهائي منه على الجاني الرجوع لمسرح الجريمة وتفكيك الجهاز وأخذ القرص الصلب الذي يحتوي على كل شيء وإلا لن يمكنه التخلص منه عن بعد حتى وإن أرسل برمجيات خبيثة لمسح النظام، فرجال الضبطية اليوم على دراية بكيفية استرجاع تلك الملفات حتى وإن تم مسح النظام، أنظر في ذلك: **بعقيقي عبير، نسيغة فيصل، «الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04»**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص 38.

إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها وضبطها، لذا فإن استخدام تقنيات التشفير لهذا الغرض يعد أحد العقبات الكبرى التي تعيق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة[312].

كما يلجأ المجرم المحترف إلى القيام بمجموعة من الإجراءات الفنية على الحاسب الآلي من خلال مجموعة من التطبيقات والبرمجيات والتي تؤدي إلى إخفاء الهوية أو استبدالها بهوية أخرى أثناء التصفح أو ارتكاب الجريمة وهذا يشكل عائق ضخم أمام رجال الضبط الجنائي[313].

ثالثا: ضخامة البيانات المتعين فحصها

ينتج عن إخضاع الحاسب الآلي للضبط والتفتيش في محتوياته كم كبير وضخم من البيانات المخزنة على الحاسب أو على وسائل تخزين خارجية، ويحتاج المحقق أو الفنيين لوقت وجهد كبيرين لفحص واختيار ما هو مفيد من البيانات والمعلومات للمساهمة في استخلاص أدلة الجريمة المعلوماتية ونسبتها لشخص محدد[314].

لذلك يشكل الكم الهائل من البيانات التي يجري تداولها في الأنظمة المعلوماتية إحدى الصعوبات البارزة التي تعيق التحقيق في الجرائم التي تقع عليها أو بواسطته[315]ا، إذ عادة ما يتطلب البحث عن الأدلة في حاسب واحد، الاطلاع والفحص الدقيق لكل المعطيات التي تتضمنها آلاف الملفات المخزنة في ذاكرته، ويكلف المحقق وقتا وجهدا كبيرين، وهو ما قد ينعكس سلبا على مردود سلطات البحث والتحقيق بسبب الضجر والملل ويؤدي بهم إلى التخلي عن مواصلة البحث والتحقيق.

---

312 – **الطيبي البركة، حاج سودي محمد**، مرجع سابق، ص 273.

313 – **سلامة محمد المنصوري**، مرجع سابق، ص 38. أنظر كذلك:

- **Y.Akdeniz, J.Bell**, La vie privée et l'internet prespectives du Royaume-Uni, groupe d'études société d'information et vie privée, chapittre 8, p 156, disponible sur le site: http://asmp.fr

314 – **سلامة محمد المنصوري**، مرجع سابق، ص 37.

315– **هشام محمد فريد رستم**، أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، مقال مقدم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص 430.

تزداد المسألة تعقيدا، حينما يكون محل البحث هو الشبكة العنكبوتية للإنترنت، إذ يصبح ضبط الدليل والبحث عنه أمرا في غاية الصعوبة، وإن لم يكن مستحيلا، على اعتبار أن التفتيش والضبط في هذا الفضاء اللامتناهي يستدعي من المحقق تصفح عدد هائل من مواقع وصفحات الإنترنت وفحص كم ضخم من البيانات الأمر الذي قد يسبب له إرهاقاً شديداً يدفعه إلى الخروج عن الضوابط القانونية للبحث وتحصيل الدليل، ما يجعل القضاء لا يكترث بالدليل الرقمي المستخلص من هذه العملية لافتقاده للشروط المشروعة والمصداقية التي تجعله جدير بالثقة.

لا تضفي عملية البحث والتحري إلى نتيجة رغم الجهد والوقت الكبيرين المبذولين من طرف المحقق، بسبب تواضع مستواه الفني والتقني في فنون وتقنيات استخدام وسائل الاعلام والاتصال الحديثة من ناحية، وعدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يتسن الوقوف على البيانات غير المشروعة وضبطها من جهة أخرى، مما يؤثر سلبا على معنويات المحقق، ويفقده الثقة في مؤهلاته وقدراته[316].

رابعا: لا محدودية شبكة الإنترنت

يزداد حجم جرائم الإنترنت وتتنوع أساليب ارتكابها وتتعاظم خسائرها وأخطارها، وذلك لما تتميز به من خصائص لا تتوفر في الجرائم التقليدية (لا في أسلوبها ولا في طريقة ارتكابها)، ومن أبرزها أنها جرائم لا تعترف بالحدود الجغرافية، وذلك أن شبكة الإنترنت ألغت كل الحواجز والحدود السياسية، وتخطت الفواصل الطبيعية، واستعصت على الضوابط الأمنية، فبضغطة زر أو إشارة بالفأرة ينتقل المستخدم –وهو قابع على مقعده– من أقصى الأرض إلى أقصاها، دون أن يمر بدائرة الجوازات، ولا بمصلحة الجمارك[317].

وهنا يطرح إشكال جوهري حول طبيعة جرائم الإنترنت وفقا لهذه الخاصية فهل تعتبر جرائم داخلية، أم جرائم دولية، أم جرائم ذات بعد دولي؟

---

316 – **براهيمي جمال**، مرجع سابق، ص ص 217–218.

317 – **علي بن عبد الله عسيري**، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 23.

تعتبر جرائم الإنترنت من الجرائم التي لها عدة أبعاد: يتجسد البعد الأول لها في النطاق المحلي، مما يعني أن الاختصاص ينعقد فيها للمشرع الجنائي الداخلي.

يتجسد بعدها الثاني في النطاق الدولي، ويتحقق عندما يكون مرتكب الجريمة دولة أو أحد مؤسساتها أو أحد أشخاص القانون الدولي، أو أن تكون الجريمة موجهة ضد دولة ما كما حدث في التجسس الذي قامت به الولايات المتحدة الأمريكية، إذ استخدمت الأسلحة المعلوماتية الفتاكة أثناء القصف الجوي للحلف الأطلنطي في كوسوفو عن طريق انتهاك أنظمة حاسوب أعدائها، كما أنه قد تكون ذات بعد دولي، عندما ترتكبها عصابات إجرام أو منظمات إجرامية أو أفراد، من ذلك مثلا جريمة ترويج المواد المخدرة عبر الإنترنت، وكذلك العدوان الذي باشره القاتل الإلكتروني الصيني بنسفه لقاعدة بيانات السفارة الأمريكية في بكين وبلغراد إثر قصف الولايات المتحدة للسفارة الصينية في بلغراد إبان الحرب الأمريكية الصربية[318].

نستخلص مما سبق أن من الصعوبات التي تواجه سير الإثبات في الجرائم المعلوماتية، هو أن شبكة الإنترنت ليست لها حدود دولية، فهي لا تعترف بتلك الحدود القائمة بين الدول، كما أنها ليست مملوكة لأحد، وبالتالي فليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، فالإنترنت ظاهرة دولية تنعدم مركزيتها وتتساوى أمامها الدول الكبيرة والصغيرة دون المساس بسيادة الدول، ما يخلق صعوبة كبيرة أمام الجهات التي تقوم بتعقب دليل الإثبات عبر هذه الشبكة[319].

---

[318]– تجدر الإشارة إلى أن موضوع تدويل ظاهرة الإختراق تثار في ظل الجريمة الدولية والجريمة ذات البعد الدولي في إطار الإنترنت، لكونها جريمة يمكن أن يتأثر بها المجتمع الدولي برمته، كما هو الشأن في جريمة إغراق الخوادم الذي حدث في شهر فيفري 2000 وانتشرت انتشارا دوليا، وكذلك بالنسبة لدودة الحب والشفرة الحمراء، مشار إليه لدى: **علي بن عبد الله عسيري**، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص ص 40–41.

[319]– **بثينة حبيباتني**، مرجع سابق، ص 89.

خامسا: فهم الدليل المتحصل من الجرائم المعلوماتية

تعني هذه الخاصية أنه على الرغم من أن الدليل الإلكتروني في أساسه متحد التكوين بلغة الحوسبة فإنه مع ذلك قد يتخذ أشكالا مختلفة، فمصطلح الدليل الإلكتروني أو الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني.

لايوجد شك في أن إثبات وفهم الأمور المادية التي تترك آثار ملحوظة يكون سهلا ميسورا[320]، غير أن خاصية التنوع التي يتمتع بها الدليل الإلكتروني تعني أنه يمكن أن يظهر في هيئات مختلفة الشكل كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل، كما هو الشأن في حالة المراقبة عبر الشبكات، وقد يكون الدليل مفهوما للبشر كما لو كان وثيقة معدة بنظام المعالجة الألية للكلمات بأي نظام، كما يمكن أن تكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري، أو تكون مخزنة في نظام البريد الإلكتروني، كما يمكن أن تكون عبارة عن بيانات مشفرة وغيرها من الأنواع والأشكال التي قد يتخذها، وهذا التنوع إنما يعد تعبيرا عن اتساع قاعدة الدليل الإلكتروني، حيث يمكنه بهذه الصورة أن يشمل أنواع متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لأن تكون دليلا بالإدانة أو البراءة.

أما عن كون الدليل الإلكتروني دليل متطور، فهي خاصية تكاد تكون تلقائية، نظرا للتطور المتواصل في عالم تكنولوجيا المعلومات، ولذلك فمن الضروري مواكبة هذا التطور الحاصل في البيئة التقنية، حتى لا يكون ذلك عائقا أمام الحصول على دليل إلكتروني يفيد في كشف الواقعة بأشخاصها الحقيقية.

320– **غازي عبد الرحمان هيان الرشيد**، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص 539.

يترتب على هذه الخاصية أن أي محاولة فقهية أو قضائية لتقسيم الدليل الإلكتروني يمكن أن تكون محل جدل فقهي نظري، وذلك بسبب التطور المستمر الذي يطرأ على البيئة التقنية التي يعيش فيها هذا الدليل، مما يجعله من الأدلة المتطورة بطبيعتها لا سيما وأن العالم الافتراضي لا يزال في بدايته[321].

سادسا: إجراءات الحصول على الدليل الرقمي

لا تقف صعوبة إثبات الجرائم المرتكبة عبر الإنترنت عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها وإنما تمتد لتشمل إجراءات الحصول عليها، لأن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب، فهم قد يزيدون من صعوبة إجراءات التفتيش التي يتوقع حدوثه للبحث عن الأدلة التي قد تدينهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها قد يستحيل على غيرهم الاطلاع عليها[322].

بالإضافة إلى ذلك فإن الطرق التي يلجأ إليها ضباط الشرطة القضائية في التحري حول هذا النوع المستحدث من الجرائم، هي في الغالب طرق تقليدية مثل التفتيش والمعاينة وضبط الأشياء، حيث أن هذه الطرق لا تفي بالغرض نظرا للخصائص التي يتمتع بها الدليل الإلكتروني مثل اللامادية وصعوبة تحديد مكانه[323].

321– **مذكور عائشة**، مرجع سابق، ص ص 134–135.

322 – **عبد الله بن حسين آل حجراف القحطاني**، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية دراسة على المحققين في هيئة التحقيق والادعاء العام بمدينة الرياض، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014، ص 72.

323- **DIOUF Ndiaw**, op-cit, p 273.

فإذا ما حصّل دليل تقني وفق الطرق السابقة يمكن أن يشوبه عيب أو أن يدخل الشك حوله بسبب عدم تماشي إجراءات الحصول عليه مع طبيعة هذه الجريمة،[324]، حيث نصّت المادة 191 من قانون الإجراءات الجزائية على أنه: "**تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها...**"

المطلب الثاني

من حيث أطراف الجريمة المرتكبة عبر الإنترنت وسلطات التحقيق فيها

إنجرّ عن ظهور الجريمة المرتكبة عبر الإنترنت بروز طائفة جديدة من المجرمين الذين يختلفون عن المجرمين التقليديين سواء من حيث الدوافع والصفات، أو من حيث الطريقة التي من خلالها يرتكبون بها جرائمهم، هؤلاء المجرمين ألقوا بضلالهم على مختلف الآليات الموضوعة لمكافحة هذه الجريمة المستحدثة نظرا لما يتمتعون به من مهارة وذكاء وحب لتحدي نظم المعلوماتية **(فرع أول)**.

ظهر كذلك في نوع آخر من المجني عليهم الذين يتميزون بعدة صفات جعلت منهم بمثابة عراقيل تحد من فعالية آليات مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك راجع إلى موقفهم السلبي منها، إما عن طريق عدم الإبلاغ عنها لخوفهم على سمعتهم ومكانتهم الاجتماعية متناسين في ذلك حجم الخسائر التي يتكبدونها يوميا في صمت، أو لقلة خبرتهم ووعيهم في مجال تقنيات الاتصال، بالإضافة إلى ذلك ظهرت في خضم هذا التطور في الجريمة فئة من المحققين الذين يعتبرون حجر عثرة بالنسبة للآليات المستحدثة لمكافحة هذه الجريمة وذلك راجع لنقص خبرتهم في هذا المجال نظرا لعدم مواكبتهم لأهم التطورات التي تعرفها هذه الجريمة المستحدثة **(فرع ثان)**.

[324]– **بوكر رشيدة**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، مرجع سابق، ص 494.

الفرع الأوّل

الجاني في الجريمة المرتكبة عبر الإنترنت

يطلق على المجرم الذي يرتكب الجريمة المرتكبة عبر الإنترنت بالمجرم المعلوماتي، والذي يعتبر من بين أخطر المجرمين نظرا لما يتميز به عن المجرم التقليدي، فإذا كان ارتكاب الجرائم التقليدية لا يحتاج إلى مستوى تعليمي معين، فإن ارتكاب الجريمة عبر الإنترنت بصفتها جرائم فنية وتقنية يكون المجرم فيها من ذوي الاختصاص والمعرفة التقنية العالية، حيث تعتبر هذه المميزات التي يتمتع بها المجرم المعلوماتي من بين أصعب التحديات التي تواجه مكافحة هذا النوع من الجرائم وسنتطرق في تبيان ذلك إلى أصناف المجرمين المعلوماتيين **(أولا)**، ثم إلى أهم الصفات التي يتمتعون بها **(ثانيا)**.

أولا: أصناف المجرمين المعلوماتيين

تتمثل مختلف أصناف المجرمين المعلوماتيين في عدة فئات هي:

1-فئة القراصنة

تعتبر القرصنة عبر الإنترنت من أكثر الجرائم ارتكابا في العالم الافتراضي[325]، حيث يقوم بها أشخاص يتفاوتون فيما بينهم في المستوى ودرجة الخطورة الإجرامية ويمكن حصرهم في فئتين هما:

أ- **القراصنة الهواة (Hackers)**

هم أشخاص بارعون في استخدام الحاسب الآلي وبرامجه ولديهم فضول في استكشاف حاسبات الآخرين بطرق غير مشروعة[326].

[325]- **DOUZET Frédérick, SAMAAN Jean-loup, DESFORGES Alix**, Les pirates du cyberespace, revue hérodote, vol 03, n° 134, p 179, disponible en ligne à l'adresse: https://www.cairn.info/revue-herodote-2009-3-page-176.htm

[326]- **CHAWKI Mohamed**, Essai sur la notion de la cybercriminalité, p 32, voir le site : www.iehei.org

فالهاكرز، كما يدل على ذلك اسمهم، هم متطفلون يتحدّون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات[327].

ب- القراصنة المحترفون (Crackers)

تعكس الاعتداءات التي تقوم بها هذه الفئة أن لها ميولات إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرارا كبيرة.

يعود المجرم المحترف في ارتكاب الجريمة المعلوماتية في الغالب إلى ارتكاب الجريمة مرة أخرى، حيث تزداد سوابقه القضائية وهو يعيش لسنوات طويلة من عائد جرائمه، وهذا المجرم لا يفضل الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح الشخصية[328].

2-فئة الحاقدين

يغلب على هذه الطائفة عدم توافر أهداف وأغراض الجريمة لديها، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة في نشاطهم[329].

3-فئة المتطرفين

يعتبر "المتطرفون الفكريون" طائفة من الناس نزلت المتعصبين لأفكارهم وآرائهم، ومتجاوزون بذلك كل الحدود المعقولة والمقبولة للتحاور والنقاش، وذلك بخصوص قضية أو

327- **محمد حمدان عاشور**، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الأمنية، الشئون الأكاديمية، قسم المناهج، فلسطين، 2010، ص 270.

328- **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 84.

329- **محمد حمدان عاشور**، مرجع سابق، ص 272.

غاية ليس لها علاقة بمصالحهم الشخصية، وهم في سبيل تحقيق ما يعتقدونه على استعداد لارتكاب أنشطة إجرامية مختلفة تخلف وراءها أضرار جسيمة سواء على أفراد من المجتمع أو على قطاعات كاملة منه هادفين من ذلك تحول المجتمع إلى الأفضل من جهة نظرهم بدون قيد أو شرط.

يختلف المجرم العادي عن المجرم المعلوماتي المتطرف، فالأول لا يبغي سوى تحقيق منفعته الشخصية، أما الثاني فيكون مدفوعا ببعض البواعث التي قد تكون ذات طبيعة سياسية أو إقتصادية أو تتعلق بحقوق الإنسان أو مرتبطة بشؤون البيئة أو دينية[330].

4-طائفة الموظفون في مجال المعلوماتية

يشكل النظام المعلوماتي مجال العمل الأساسي بالنسبة لهذه الفئة من المجرمين، ولهذا فهم يقترفون جرائم تمكنهم من تحقيق أهدافهم الشخصية، هؤلاء يعودون إلى مقر عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو اتلافه أو سرقته، وقد يجد نفسه أحيانا مرتكبا لجريمة إلكترونية صدفة ودون تخطيط مسبق لها[331].

5-طائفة الدول والحكومات الأجنبية

قد يظن البعض أن الإجرام المعلوماتي يقتصر على الأفراد أو الشركات والمؤسسات، ولكن مما لا شك فيه أن تجسس الحكومات على بعضها البعض يضرب بجذوره في أعماق التاريخ، فالدول تبحث عن المعلومات[332] لدى الغير سواء كان من الأعداء أم لا من أجل

---

[330]- **حمزة بن عقون**، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012، ص 41. أنظر كذلك:

- **AKMOUCHE Walter, HEMERY Henri**, La propagande jihadiste sur internet dignostic et perspectives, cahiers de la sécurité, n° 6, INHES, paris, octobre-décembre 2008, p 54.

[331]- **عبد السلام محمد المايل، عادل محمد الشربجي، علي قابوسة، «الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم -الأسباب- سبل المكافحة مع التعرض لحالة ليبيا»**، مجلة آفاق للبحوث والدراسات، المركز الجامعي إيليزي، العدد 04، جوان 2019، ص 248.

[332]- **Claire FENERON, Laurent KLEIN, Julien LE CLAINCH, Michèle BATTISTI, Matthieu BERGUIG**, Droit de linformation, documentaliste-sciences de l'information, vol 49, n° 4, 2012, p 18. Disponible en ligne à l'adresse: https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2012-4-page-16.htm

تفادي المخاطرة والتفوق عليه، وكان التجسس في ما مضى يرتكز على الأمور العسكرية، ولكن في الوقت الحاضر لم يعد التفوق العسكري وحده الفاصل في المعارك، وإنما يلزم التفوق الاقتصادي والتكنولوجي، ولذلك فإن التجسس يرتكز الآن على التطور التكنولوجي في أكثر صوره، وذلك تجسيدا للتقدم الصناعي، والمتمثل في ثورة المعلومات[333].

ثانيا: صفات المجرمين المعلوماتيين

يتصف المجرمين المعلوماتيين بعدة صفات مشتركة بينهم، كما يتصف البعض منهم بصفات تميزهم عن غيرهم من المجرمين خاصة إذا كانوا ينتمون إلى منظمات إجرامية.

1- **الصفات المشتركة للمجرمين المعلوماتيين**

تتمثل الصفات المشتركة لدى المجرمين المعلوماتيين في:

أ- **الذكاء والمهارة**

يتمتع مجرمي المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والإنترنت، بل إن بعضهم متخصصين في مجال المعلومات آليا كما يتميز غالبا بالذكاء، حيث أن هذا النوع من الإجرام يحتاج إلى مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليهم، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى العنف أو الاتلاف المادي، بل يحاول أن يحقق أهدافه بهدوء، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة مع الإجرام العادي الذي يميل إلى العنف[334].

يصنف المجرم في جرائم الكمبيوتر والإنترنت ضمن نوابغ المجرمين أو نوابغ المعلوماتية فهو ليس مجرما عاديا، خاصة الأحداث الجانحون منهم، والذين يخشى عليهم

---

[333]–**حمزة بن عقون**، مرجع سابق، ص 45. أنظر كذلك:

- **FREYSSINET Eric**, Botnets: illustrationde nouvelles formes de criminalité organisée, revue du groupe de recherches actions sur la criminalité organisée (crasco), 2013, p 7, article disponible sur le site: https://hal.archives-ouvertes.fr/hal-01077117

[334] – **موفق علي عبيد، ساهر ماضي ناصر**، المرجع السابق، ص 215.

من التحول من مجرد الهواية إلى الاحتراف في أفعال إختراق النظم، وقد تتربص به منظمة غير مشروعة تعتمد المعلوماتية في جرائمها وتقوم بتجنيده الأمر الذي يجعله مجرما معلوماتيا محترفا[335].

ب- مجرم ذو طابع اجتماعي

لا يضع المجرم المعلوماتي نفسه في حالة عداء مع المجتمع الذي يحيط به، فهو يتوافق ويتصالح معه، وتزداد خطورته الإجرامية كلما زاد تكيفه الإجتماعي مع توافر الميول الإجرامي لديه، فشعوره بأنه محل ثقة وأنه خارج إطار الشبهات يدفعه إلى التمادي في ارتكاب جرائمه والتي لا تكتشف عادة[336].

يعتبر المجرم المعلوماتي إنسان يستطيع التوافق والتصالح مع مجتمعه، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف، ولا يقصد بذلك التقليل من شأن المجرم المعلوماتي، بل أن خطورته الإجرامية قد تزداد إذا زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه[337].

يمارس المجرم المعلوماتي عمله في المجال المعلوماتي أو ومجالات أخرى أيضا، وتطبيقا لذلك ترتكب الكثير من الجرائم المعلوماتية بدافع النصب أو الحسد أو بدافع اللهو أو لإضهار مدى ما يتمتع به من قدرة على التفوق في مواجهة أمن الأنظمة المعلوماتية[338].

د- الصبر والحذر الشديد

يتطلب الوصول إلى أنظمة المعلومات واختراق تحصيناتها الدفاعية والرقابية في الغالب إجراء عدة محاولات تستغرق مدة طويلة، كما أن أكثر الاختراقات تتم عن طريق

---

335 – **خزار لمياء**، مرجع سابق، ص 168.

336 – **ربيعي حسين**، «**المجرم المعلوماتي شخصيته وأصنافه**»، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015، ص 289، أنظر كذلك:

- **HUMBERT Jean-Philippe**, Les mondes de la cyberdélinquance et images sociales du pirate informatique, thèse pour le doctorat en sciences de l'information et de la communication, université paul verlaine, metz, 2007, p 137.

337 – **بن عقون حمزة**، مرجع سابق، ص 30.

338 – **عطوي مليكة**، «**الجريمة المعلوماتية**»، مجلة حوليات، جامعة الجزائر، العدد 21، جوان 2012، ص 12.

تقنية المحاولة والخطأ، والتي تستلزم إجراء عدد من المحاولات، واستخدام عدد كبير من الأدوات والبرامج للقيام بذلك، كما أن اختيار التقنية المناسبة والعدد والبرامج التي تتطلبها مثل هذه الاختراقات، واختيار الوقت والمكان المناسبين لإجراء الاختبارات، اتباع الطرق المناسبة لتفادي عمليات تتبع آثاره كالانتقال من شبكة إلى أخرى حتى الوصول إلى الهدف كل ذلك يتطلب درجة عالية من الذكاء والصبر لدى منفذ مثل هذه العمليات[339].

هـ- التمتع بالسلطة اتجاه النظام المعلوماتي

يقصد بالسلطة هو أن يكون للمجرم المعلوماتي حقوق ومزايا تجاه نظام المعلومات الذي يستهدف من قبله بالشكل الذي تجعله مسيطرا ومتحكما به إلى حد ما، وهذه السلطة قد تكون مباشرة في حالة الشخص الذي لديه الشفرة الخاصة والتي تمكنه من الدخول إلى النظام المعلوماتي الذي يحتوي على المعلومات، أو تكون غير مباشرة في حالة الشخص الذي لديه التصريح في دخول الغرفة أو المكان الذي توجد فيه الأنظمة.

فيما يخص المعرفة فإنها تتمثل في الدراية والمعرفة بكافة الظروف التي تحيط بالجريمة المراد ارتكابها، وكذلك احتمالات الفشل أو النجاح، وبتلافي ما هو غير متوقع من الأمور من خلال التصور الكامل للجريمة في ذهنه، ويعود ذلك إلى البيئة التي ترتكب فيها الجريمة[340].

2- الصفات التي تتميز بها الجماعات الإجرامية في ارتكاب جرائم الإنترنت

تتمثل هذه الصفات في:

---

339 – **محسن بن سليمان الخليفة**، مرجع سابق، ص 54.

340– **خليل يوسف جندي، «المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني دراسة مقارنة»**، مجلة كلية العلوم القانونية والسياسية، د.ب.ن، المجلد 07، العدد 32، سنة 2018، ص 95.

أ- التنظيم والتخطيط

يعتبر عنصر التنظيم حجر الزاوية في الجريمة المنظمة[341]، وسميت الجريمة بهذا الاسم للزوم وجود هذا العنصر فيها، فمن غيره لا يمكن تصور حدوثها، ويقصد به: ترتيب وتنسيق وجمع الأعضاء داخل بنيان شامل ومتكامل على درجة عالية من الدقة، بحيث يكون قادرا على القيام بأعمال إجرامية، وهذا ما أشارت إليه إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، حيث نصت في المادة الثانية على أنه "**جماعة ذات هيكل تنظيمي تتألف من ثلاثة أشخاص فأكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول بشكل مباشر على منفعة مادية أخرى**"[342].

كذلك يعتبر عنصر التخطيط عنصرا بارزا في هذا النوع من الجرائم، فالجريمة التي ترتكب من غير تخطيط لا تدخل في نطاق الجريمة المنظمة، وهذا العنصر ليس بالأمر السهل فهو يحتاج إلى عدد من محترفي الإجرام الذين يتصفون بقدرة عالية من الذكاء ويملكون خبرة دولية ودراية وثقافة جنائية تمكنهم من رسم الخطط الناجحة وسد جميع الثغرات القانونية والاقتصادية التي يمكن أن تؤدي إلى اكتشاف الجريمة قبل ارتكابها أو أثناء تنفيذها، وهذا ما يصعب من إمكانية اكتشافها والقضاء عليها[343].

ب- التكيف الاجتماعي والروابط الدولية

تعتبر هذه الخاصية امتدادا لسمة التخطيط والتنظيم، حيث إن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، فتنشأ بالتالي بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي إلى المجال الدولي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي.

---

[341]- **RAUFER Xavier**, Cyber-criminologie, cnrs éditions, paris, 2015, p 118.

[342]- نقلا عن: **شرف الدين كامل**، الجريمة المنظمة، الطبعة الأولى، دار النهظة العربية، القاهرة، 2000، ص 62.

[343] - **أحمد عبد الرحمن المجالي**، «**الظواهر الإجرامية الحديثة والجريمة المنظمة**»، مجلة العلوم الإنسانية، جامعة بسكرة، العدد الثاني والثلاثون، نوفمبر 2013، ص ص 224-225.

ولا شك أن إقامة المؤتمرات الدولية بين هؤلاء المجموعات خير دليل على وجود تلك الصلات والروابط الدولية بينهم[344].

ج- التطور في السلوك الإجرامي

تسعى منظمات الجريمة المنظمة إلى تطوير أساليب عملها باستمرار بما يحقق أهدافها وغاياتها[345]، والعوامل المساعدة في تطوير هذه المنظمات لطرق عملها الموائمة المالية والاقتصادية التي تتمتع بها، فهي تسعى دوما إلى استغلال الوسائل التقنية الحديثة في القيام بنشاطاتها، فاستفادت هذه المنظمات عبر سنوات عملها من أحدث وسائل الاتصال حتى تؤمن الترابط بين أفرادها وجماعاتها[346].

الفرع الثاني

المجني عليه وسلطات التحقيق في الجريمة المرتكبة عبر الإنترنت

تعتبر النتيجة الإجرامية من ارتكاب الجريمة عبر الإنترنت العامل الأساسي من ارتكابها، فكما يمكن أن ترتكب ضد أشخاص طبيعيين، فهي ترتكب ضد مؤسسات حكومية واقتصادية ومالية، الأمر الذي يجعل نتائجها جسيمة مما لا يجعل مجال إلاّ لضرور التبليغ عليها، غير أنه من الناحية العملية نرى في الغالب اتخاذ موقف سلبي من طرف المجني عليهم حيث لا يقومون بالتبليغ عليها إما خوفا على سمعتهم أو لقلة خبرتهم في مجال

---

[344]- يعتبر أول مؤتمر لقراصنة المعلومات هو الذي عقد في شهر أغسطس سنة 1989 في أمستردام بهولندا، واشترك فيه نحو مائتي شخص، وكان شعاره "عيد مجرات القراصنة" وكان ينادي بحملة احتكار المعلومات، وقد عقد في قاعة مسرح كبير نصبت عليه شاشة عملاقة، وكان المشاركون في المؤتمر معظمهم من الشباب حبث تتراوح أعمارهم ما بين عشرين إلى ثلاثين سنة، وتم فيه الحوار بين أحد الأشخاص وبين أعضاء شبكة قرصنة معلومات في نيروبي (بدولة= =كينيا)، وكان الحوار يدور حول اختراق شبكات المعلومات، وكانت الأسئلة والأجوبة تتناول طريقة وأساليب القيام بعمليات القرصنة وشبكات الاتصالات المنتظمة وردود فعل السلطات المحلية عليها، **أنظر في ذلك: أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة جرائم المعلوماتية، د.د.ن، د.س.ن، 2005، ص ص 16-17.

[345]- **VERGNE Jean-Philippe, DURAND Rodolphe**, Cyberespace et organisations « virtuelles »: l'état souvrain a-t-il encore un avenir, revue-regards-croises-sur-l-economie, n° 14, vol 1, 2014, p 133, disponible en ligne à l'adresse: https://www.cairn.info/revue-regards-croises-sur-l-economie-2014-1-page-126.htm

[346]- **نهلا عبد القادر المومني**، مرجع سابق، ص 87.

المعلوماتية، بل بالإضافة إلى ذلك أن سلطات الاستدلال حول هذه الجريمة لا تواكب في الغالب التطور السريع لها، نظرا للتباين بين مرتكب الجريمة الذي يطوّر قدراته باستمرار، وبين سلطات الاستدلال التي يكون أسلوبها مختلف في هذا المجال، حيث أن كل هذه العوامل أضحت بمثابة عراقيل تحد من فعالية آليات الجريمة المرتكبة عبر الإنترنت، ومن أجل تبيين ذلك سوف نتطرق إلى المجني عليه **(أولا)**، ثم إلى سلطات الإستدلال **(ثانيا)**.

أولا: المجني عليه في الجريمة المرتكبة عبر الإنترنت

تتمثل الصعوبات المتعلقة بالمجني عليه في:

1-نقص الخبرة التقنية:

ينخدع كثير من المجني عليهم في الجرائم المرتكبة عبر الإنترنت بالعروض التجارية الوهمية، حيث ينتحل بعض الأشخاص مواقع لمنظمات تجارية مشهورة، ويقدمون سلعا وخدمات بأسعار زهيدة، مما يجعل المجني عليهم ينجذبون إليها ويقومون بملأ النموذج الإلكتروني للشراء، ويتضمن هذا النموذج أرقام بطاقات الائتمان، والبنك الذي أصدرها، فيقوم الجناة بالدخول على أنظمة البنك والتعامل بأرقام البطاقة واستخدامها في عمليات الشراء أو التحويل من حساب لآخر[347].

إن قلة الخبرة التي يعاني منها بعض مستخدمي الشبكة تجعلهم صيدا سهلا للجناة من خلال منحهم الفرصة للاستيلاء على البيانات المهمة بسهولة، ويرجع ذلك إلى عدة عوامل أهمها العشوائية في استقبال البريد الإلكتروني الذي قد يتضمن فيروسات تسيطر على الحاسب الآلي للمجني عليه وتمكن المخترقين من الدخول وقتما شاءوا، فضلا عن الانخداع بالتخفيضات الوهمية من قبل الجناة الذين يستخدمون هذه التخفيضات كوسيلة لإغراء المجني عليهم لطلب الشراء، ومن ثم معرفة بياناتهم، أو تتبع ال (Ip) الخاص بهم واختراق مواقعهم والاستيلاء على أموالهم[348].

---

[347]- **عبد الله بن سعود محمد السراني**، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 236

[348]- **عبد الله بن سعود محمد السراني**، مرجع سابق، ص 236.

2-عدم اتخاذ الحيطة والحذر

يعتبر ضعف رقابة نظم الحواسيب ولامبالاة العاملين عليها من أكبر الصعوبات التي تعترض اكتشاف الجريمة المرتكبة عبر الإنترنت[349]، وهو ما يسميه البعض بالدور غير المباشر للمجني عليه في ارتكاب الجريمة، وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للجريمة المرتكبة عبر الإنترنت مرتفع بشكل كبير[350].

يهمل الكثير من ضحايا الجرائم المرتكبة عبر الإنترنت اتخاذ الحيطة والحذر اللازمين لاكتشاف مثل هذه الجرائم في حال وقوعها[351]، فأغلب الأفراد من مستخدمي شبكة الانترنت لا يستخدمون برامج وتقنيات للحماية ضد الاختراق والتجسس والوقاية من الفيروسات ما يترتب على ذلك عدم إمكان اكتشافهم للجريمة الواقعة لحظة ارتكابها وقد يكتشفونها بعد مرور مدة طويلة، وهذا الأمر يشمل حتى المؤسسات والشركات المالية والتجارية، فهي لا تقوم بمراجعة حساباتها المالية والتجارية يومياً ولا حتى شهرياً لتكتشف مثل هذه الجرائم قبل فوات الأوان، وحتى ولو قامت بمثل هذه المراجعة فأنها غالباً ما تعتبر المفارقات الحاصلة في حساباتها مجرد مفارقات عادية ناجمة عن خسائرها الاعتيادية أو عن عمليات دفع أجله.

كما أن هذه المؤسسات غالباً ما تتسابق مع بعضها البعض في توفير خدماتها للعملاء بأكبر قدر ممكن من التسهيلات بحيث توجه اهتمامها إلى تحسين وتسهيل الحصول على خدماتها على حساب نظامها الأمني، مما ينجم عنه بالتالي سهولة اختراق نظامها الأمني وفي الغالب من دون أن يكتشف أمر الاختراق.

---

[349]- **FEVRIER Rémy**, Les collectivités territorialesfaceauxmenaces numériques, revue gestion et management public, volume 01, n° 03, 2013, p 27, Disponible en ligne à l'adresse: https://www.cairn.info/revue-gestion-et-management-public-2013-1-page-24.htm

[350]- **معاشي سميرة، «الجريمة المعلوماتية، دراسة تحليلية لمفهوم الجريمة المعلوماتية»**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 17، جوان 2018، ص 413.

[351]- **VALLET Caroline**, Le dévoilement de la vie privée sur les sites de réseaux social. Des changements significatifs, revue droit et société, n° 80, vol 01, 2012, p 174. disponible en ligne à l'adresse: https://www.cairn.info/revue-droit-et-societe1-2012-1-page-163.htm

3- التكتم عن الجريمة

تظل الجريمة المرتكبة عبر الإنترنت مستترة ما لم يتم الإبلاغ عنها، والصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية وذلك لصعوبة اكتشافها من قبل الاشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجنيا عليها، أو لأن هذه الجهات تحاول درء الأثر السلبي للابلاغ عما وقع وحرصا على ثقة العملاء فلا تبلغ تلك الجرائم التي ارتكبت ضدها[352]، حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت في حقهم، خاصة المؤسسات والشركات التجارية، حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها هذا النوع من الجرائم، ويمكن أن يرجع هذا الإحجام عن التبليغ لعدة أسباب أهمها[353]:

- عدم ادراكهم بأن هذه الأفعال تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة في إقليم الدولة أو المطبقة دوليا.
- خوف الجهات التي وقعت عليها الجرائم، خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث على سمعتها وثقة السوق قي قدرتها.

---

[352]- **حفصي عباس**، جرائم التزوير الإلكترونية دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم الإسلامية تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران، 2015، ص 50.

[353]- في دراسة أجراها المعهد الوطني للعدالة التابع لوزارة العدل الأمريكية وشملت 127 من العاملين في مجال التحقيق في جرائم الحاسوب والإنترنت يمثلون 114 وكالة رسمية وغير رسمية، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسوب والإنترنت التي يتم اكتشافها لا يبلغ عنها للشرطة.

كما توصلت دراسة أخرى أجراها معهد أمن الحاسوب بالاشتراك مع مكتب التحقيق الفدرالي في الولايات المتحدة الأمريكية إلى أن حوالي 70 %من الجرائم التي يتم اكتشافها لا يتم الإبلاغ عنها لسلطات انفاذ العدالة، ويذهب بعض الباحثين إلى أن كثيرا من المنشآت تتكتم على ما تتعرض له أنظمتها الحاسوبية من اختراقات حيث تشير الإحصائيات إلى أن 11% فقط من جرائم الحاسوب والإنترنت يتم الإبلاغ عنها، في حين يرى البعض الأخر أن نسبة الجرائم المرصودة التي يتم الإبلاغ عنها للسلطات أو حتى للعامة لا تتجاوز 10% من اجمالي الجرائم التي تقع على الحاسوب، أنظر: **محمد بن نصير محمد السرحاني**، مرجع سابق، ص ص 66-67.

- خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق.
- قد تساور بعض الضحايا الشكوك حول قدرة الشرطة على التعامل مع جرائم الحاسوب والإنترنت، من حيث توفر الخبرة الفنية لدى ضباطه أو توفر المعدات والتجهيزات اللازمة للتحقيق في هذا النوع من الجرائم.

4- عدم إدراك خطورة الجرائم المعلوماتية

يمكن تفسير زيادة ضحايا الجريمة المرتكبة عبر الإنترنت من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور الإنترنت تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة...الخ، فالجميع يستخدم المحتويات الرقمية والبرمجيات وشبكة الإنترنت، من خلال التصفح وإرسال البريد الإلكتروني والمشاركة في المحادثات والمنتديات، دون أن يدركوا مدى السهولة التي يمكن لطرف ثالث الحصول على البيانات والمعلومات الخاصة بهم[354].

خلقت التغيّرات في أنشطة الناس الروتينية، مثل استخدام الإنترنت وشبكات التواصل الاجتماعي مثل الفيسبوك والإميل والمواقع وغيرها فرصا للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة[355] من جهة، وعدم إدراك المتعاملين عبر هذا الفضاء لخطورة هذه الجرائم من جهة أخرى، حيث تعد كل هذه العوامل إحدى معوقات اكتشاف الجريمة[356].

354- **محمد سيد سلطان**، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، د.ب.ن، 2016، ص 20.

355- **ذياب موسى البداينة**، الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية مقدمة للملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المنعقد بكلية العلوم الإستراتيجية، عمان، بتاريخ 2-2014/09/4، ص 12.

356- **بثينة حبيباتي**، مرجع سابق، ص 86.

ثانيا: سلطات البحث والتحقيق في الجريمة المرتكبة عبر الإنترنت

تتمثل الصعوبات المتعلقة بسلطات التحقيق في:

1- إشكالات التعليم والتدريب الأمني

أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذي تلجأ له السلطات لتحقيق أهدافها باعتباره عنصرا حيويا لا بد منه لبناء الخبرات والمهارات المتجددة[357]، غير أنه في مجال مكافحة الجريمة المرتكبة عبر الإنترنت تجلى نوع من التباين بين تدريب عناصر الضبطية القضائية وسرعة تطور ارتكاب هذه الجريمة مما أدى الحد من فعالية مكافحتها ولعل من أبرز الاشكالات التي تواجه التعليم والتدريب الأمني تتمثل في[358]:

- عدم كفاءة بعض الطلاب الملتحقين بالتعليم الأمني، فالأفراد يشكلون المدخلات الرئيسية لنظام التعليم، وإذا كانت معايير هذه المدخلات غير دقيقة فسوف تكون مخرجاتها غير دقيقة كذلك.
- غالبية الكليات الأمنية تركز بشكل كبير على التدريب العسكري الذي يأخذ جهد وطاقة الطالب مما يجعله غير قادر على استيعاب المادة العلمية.
- قتل روح الابداع، حيث تقوم غالبية الكليات العسكرية على تعويد الطالب على الطاعة العمياء والالتزام بالأوامر العسكرية مما يجعل آداء الطالب الابداعي محدودا إن لم يكن معدوما.

2- نقص الخبرة

تختلف الجرائم المرتكبة عبر الإنترنت عن غيرها من الجرائم المادية الأخرى في أن عملية ضبط الأدلة فيها عملية تقنية محضة تتطلب اتباع استراتيجيات خاصة ومهارات وذكاء كونها في مواجهة تقنيات الحاسب الآلي، ويقابل ذلك نقص الخبرة لدى رجال الضبط

---

[357]- **يوسف حسن يوسف**، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 176.

[358] - **عبد الله بن عبد العزيز اليوسف**، أساليب تطوير البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص ص 92-93.

القضائي وأجهزة العدالة الجنائية فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة المعلوماتية وكيفية التعامل معها على الأقل في البلدان العربية نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته جاءت متأخرة عن أوروبا وأمريكا، ومن هنا تظهر الدعوة في مجال تأهيل المحققين ورجال العدالة بصفة عامة[359]، كما أن الكثير من الدول أصبحت تستوعب من رجال الشرطة المتخصصين في المعلوماتية ورغم ذلك تبقى مواجهة الجرائم المرتكبة عبر الإنترنت قائمة واستنباط الدليل الرقمي صعبة، وهذا راجع إلى التطور المذهل الذي يشهده العالم الرقمي وانتشار الحواسيب وتفشيها في الأماكن العامة والخاصة، ومما يزيد الأمر صعوبة افتقار شبكة الإنترنت إلى الرقابة وضوابط التدقيق والمراجعة فضلا عن كون هذا النوع من الجرائم عابر للحدود كثيرا ما تفشل جهات التحقيق في تعقب الجاني، بل جهات التحري قد تدمر الدليل بخطأ منها أو نتيجة إهمال[360].

وهذا ما لاحظه جانب كبير من الفقه الجنائي، ذلك أن البحث والتحقيق في الجريمة المرتكبة عبر الإنترنت هي مسألة في غاية الأهمية والصعوبة، ولا سيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي، ذلك أن حداثة هذه الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها، فلا يكفي أن يكون لديهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لا بد من الإلمام بخبرة فنية في مجال الجريمة الإلكترونية عن طريق الحاسب الآلي[361].

يعد التباين بين سرعة تطور أساليب ارتكاب الجريمة المرتكبة عبر الإنترنت وقدرات رجال الأمن والمحققين العاملين في مجال مكافحتها في بعض الدول خير معين لمرتكبيها،

359- **OK Eric**, La preuve numérique un défi pour l'enquete criminelle du 21e siècle, revue les cahiers du numirique, n° 3, vol 4, 2003, p 212, disponible en ligne à l'adresse: https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

360 – **بن فردية محمد**، مرجع سابق، ص 226-227.

361– مشار له لدى **ثنيان ناصر آل ثنيان**، إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 129.

وقد أثبتت الوقائع أن هنالك جرائم متعلقة بالإنترنت ارتكبت على مرأى ومسمع من رجال الأمن، بل قام بعض رجال الأمن من تقديم يد المساعدة لمرتكبي جرائم الحاسب الآلي دون قصد وعن جهل، أو على سبيل واجبات المهنة التي يلزمهم بها القانون، فإذا كان هذا حال الأشخاص المناط بهم إنفاذ القوانين وحماية المجتمع من الأشرار فإننا نحسب أن الكثيرين من عامة الناس قد تقع في حقهم، أو في حضورهم أو بتسهيلات منهم جرائم التقنية العالية[362].

3- التكاليف الكبيرة للرقابة الأمنية

يوجد سباق دائم بين رجال الأمن والمجرمين، ومهما كانت وسائل الأمن فإنها لا تصل إلى حد التأمين الكامل للأفراد أو الممتلكات، وينطبق ذلك على نظم المعلومات وشبكة الإنترنت، فإنه لا يمكن وضع نظام للتأمين الكامل لهذه النظم، ولذلك فإن المنظمات تقوم بدراسة جدوى هذه النظم بمقارنة التكلفة والعائد للوصول إلى قرار بالنسبة لزيادة وسائل الأمن وأساليبه[363].

يحتاج وضع نظام أمن للمعلومات إلى تقدير التكاليف اللازمة لذلك وبالتالي تحديد ميزانية مالية والتي تكون في الغالب كبيرة جدا، ولذلك يجب معرفة التكاليف والنفقات التي يحتاجها النظام، وهذا يعتمد على[364]:

362- **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 107.

363- **محسن بن سليمان الخليفة**، مرجع سابق، ص 58.

364- تقسم تكاليف تصميم النظام الأمني إلى:

1- تكاليف أولية:

- تكاليف دراسة ووضع السياسات والإجراءات الخاصة بالنظام المقترح.
- تكاليف الإجراءات الفيزيائية التي من خلالها يعرف المستفيد نفسه للنظام وإثبات شخصيته.
-تكاليف إجراءات الاختبارات اللازمة للبرمجيات والملفات وفحصها.

2- تكاليف التشغيل:

- تكاليف الإجراءات الإدارية (مثل الوقت المستغرق في عملية تحليل وتصميم النظام الأمني الجديد).
- تكاليف المعدات: وهي مرتبطة بالأجهزة التي ستساعد في تصميم النظام الأمني.

- طبيعة الإجراءات الأمنية التي سيتم تنفيذها.
- طبيعة الأجهزة والمعدات التي تساعد على تصحيح النظام.
- أهمية ونوعية المعلومات ودرجة الأمن المطلوبة له.
- طبيعة وعدد المستفيدين من النظام.

المبحث الثاني

من حيث الطبيعة الدولية للجريمة المرتكبة عبر الإنترنت

اكتسبت الجريمة المرتكبة عبر الإنترنت خاصية البعد عبر الوطني الذي استمدته من الطبيعة العالمية لشبكة الإنترنت التي ألغت كل المفاهيم المتعلقة بالحدود الجغرافية والسياسية بين الدول، الأمر الذي خلق عدة إشكالات بالنسبة لتطبيق القواعد القانونية التي تعنى بمكافحة هذه الجريمة.

يعد أسلوب التعاون الدولي من القواعد الراسخة التي رسى عليها العرف الدولي، حيث استعملها المجتمع الدولي للقضاء على كل الإشكالات ذات البعد عبر الوطني ومنها الجريمة، غير أنّه بظهور الجريمة المرتكبة عبر الإنترنت تبيّن أن هذه القواعد لم تعد تفي بالغرض نظرا لعدم مواكبتها للتطورات والسرعة التي تعرفها هذه الجريمة **(مطلب أول)**.

أدّت الجريمة المرتكبة عبر الإنترنت كذلك إلى ظهور إشكالية الاختصاص القضائي فتعديها للحدود الوطنية جعل أمر تحديد القانون الواجب التطبيق عليها والمحكمة المختصة بشأنها يتسمان بصعوبة كبيرة، وذلك لظهور تنازع في هذا المجال مما أعجز المبادئ التقليدية في الاختصاص عن حلها **(مطلب ثان)**.

– تكاليف الأعمال المضافة إلى الذاكرة الرئيسية للحاسوب ووحدة المعالجة المركزية.

– تكاليف الصيانة والخزن الإضافي لعمليات التسجيل التي سيستخدمها النظام المقترح، أنظر في ذلك: **محمد دباس الحميد، ماركو إبراهيم نينو**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، 2006، ص 56.

المطلب الأوّل

صعوبة تجسيد التعاون الدولي في مجال الجريمة المرتكبة عبر الإنترنت

يعد التعاون الدولي من بين أهم الآليات التي يسعى من خلالها المجتمع الدولي لحل أكثر الإشكالات القانونية حدّة على هذا المستوى، ولعل أهم هذه المجالات نجد الشق الجزائي الذي يعنى بالنظر في الجرائم العابرة للحدود الوطنية مثل الجريمة المرتكبة عبر الإنترنت، والتي لا يمكن للدول أن تكافحها منفردة.

غير أن آلية التعاون الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت عرفت إشكالات كبيرة، فمن الناحية الموضوعية تجلى وجود اختلافات تشريعية بين الدول وقصور في المعاهدات والاتفاقيات بينهم **(فرع أول)**.

لم يسلم الجانب الإجرائي الذي يكفل المكافحة الإجرائية للجريمة المرتكبة عبر الإنترنت هو الآخر من الإشكالات التي فرضتها خصوصية هذه الجريمة على الآليات الموضوعة لمكافحتها، حيث اصطدم التعاون الدولي في هذا المجال بمبادئ سيادة الدول على إقليمها الأمر الذي جعل التعاون الإجرائي يبدو قاصرا خاصة وأن الجريمة في هذا المجال تتسم بالسرعة في الإرتكاب والخفاء **(فرع ثان)**.

الفرع الأول

الصعوبات الموضوعية في تجسيد التعاون الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

تتحدى الجريمة المرتكبة عبر الإنترنت القواعد التقليدية للتجريم والعقاب على المستوى الدولي، لذلك فإن هذه الظاهرة الإجرامية تثير العديد من الإشكالات القانونية والعملية من الناحية الموضوعية، حيث أن ما يميزها عن الجرائم المرتكبة في العالم التقليدي أنها تتسم بالفراغ التشريعي **(أولا)** وقصور المعاهدات الدولية التي تعنى بهذا الشأن **(ثانيا)**، وحتى وإن تم سد هذا النقص نلاحظ دائما وجود تباين بين الدول وخير دليل على ذلك عدم الاتفاق على نموذج موحد للنشاط الإجرامي **(ثالثا)** وانعدام التجريم المزدوج **(رابعا)**.

أولا: الفراغ التشريعي لدى بعض الدول

أصبح مفهوم مبدأ إقليمية القانون، والقانون الواجب التطبيق، وطرق الإثبات، من المفاهيم التي تحتاج إلى مراجعة مع ظهور الإنترنت، فباعتبارها ظاهرة عالمية أوجدت ثورة في هذه المفاهيم، وألغت كل الحواجز المكانية واستخدمت أدوات جديدة في التعامل والتعاقد طغت على الأدوات القديمة[365].

ينتج في بعض الأحوال عن الجرائم المرتكبة عبر الإنترنت أضرار كبيرة، ولكن الجرائم في هذه الحالة لا تقع في دائرة التجريم من جانب القانون الجنائي لدول عديدة[366]، فجرائم الإنترنت لها خصوصية تجعل التشريع يقف عاجزا عن تكييفها قانونيا أو إخضاعها لمواد القانون الجنائي، من هذه الخصوصية أن جرائم الإنترنت لا تقع على أرض دولة معينة بحيث يختص قضاء هذه الدولة بالنظر فيها، فقد يستخدم شخص ما الحاسب الشخصي في دولة ما لكي يعتدي على نظام الحاسب في دولة أخرى قصد الحصول على المعلومات أو تدميرها أو تزويرها، هذه السهولة في عبور النشاط الإجرامي للحدود يجب أن تجعلنا ننظر بشكل مختلف إلى جرائم الإنترنت[367].

لذلك كان من الطبيعي وجود فراغ في الأنظمة والقوانين القديمة عند محاولة تطبيقها على ما يحصل في عالم الإنترنت فمثلا التزوير كان يستهدف محررات ملموسة أما في عالم الإنترنت فهو يستهدف رموزا إلكترونية، لذا يجب النّص على عقوبة التزوير الإلكتروني حتى يصبح بالإمكان ردع القائمين به.

ومما زاد الأمر صعوبة، الصيغة الدولية للإنترنت إذ لو فرضنا وجود قوانين متكاملة للوقاية من أخطار الإنترنت في بلد من البلدان فإن المعتدي يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة لشن اعتداءاته في بلدان أخرى توجد فيها تلك القوانين الصارمة

---

[365]– **علي بن عبد الله عسيري**، مرجع سابق، ص 61.

[366]- **Alix DESFORGES**, La coopiration internationale et bilatérale en matière de cybersécurité: enjeux et rivalités, laboratoire de IRSEM, Paris, 2013, p 12.

[367]– **حسن طاهر داود**، جرائم نظم المعلومات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 210.

فتعجز البلد التي وقع عليها الاعتداء عن تطبيق قوانينها، ومن الأمثلة على ذلك (فيروس الحب) الذي انتشر أواخر عام 2000 وكلف آلاف الشركات حول العالم خسائر تجاوزت المليارات وعندما تم تحديد هوية الفاعل وجد أنه طالب في الفلبين وأنه لا يوجد في الفلبين قانون يمكن محاكمته على أساسه[368].

ثانيا: قصور المعاهدات الثنائية أو الجماعية بين الدول في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

يعد القصور الموجود في المعاهدات الثنائية والجماعية بين الدول من بين أبرز الإشكالات في تحقيق الحماية المطلوبة من الجريمة المرتكبة عبر الإنترنت خاصة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الإنترنت، مما جعل التعاون الدولي في هذا المجال لا يؤتي نتائجه[369].

يرجع كذلك قصور المعاهدات الدولية في الحد من ظاهرة الجريمة المرتكبة عبر الإنترنت إلى الاختلاف في الرؤى الموجود بين الدول، فكل دولة لها نظرتها فيما يخص الحماية اللازمة لمنظومتها المعلوماتية، وذلك راجع إلى التشبث بمفهوم سيادة كل دولة على إقليمها من جهة، والتخوف من المساس بمصالحها الأساسية إذا تفتحت على المجتمع الدولي من جهة أخرى[370].

368– **علي بن عبد الله عسيري**، مرجع سابق، ص 62.

369– **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 145. أنظر كذلك:

- **KELLO Lucas**, Traduit de l'anglais par **RICHARD Thomas**, Les cyberarmes: dilemmes et futurs possibles, revue-politique-etrangere, n° 4, institut français des relations internationales, 2014, p 142, disponible en ligne à l'adresse: https://www.cairn.info/revue-politique-etrangere-2014-4-page-139.htm

370- **BARAT-GINIES Oriane**, Existe-t-il un droit international du cyberespace?, revue hérodote, vol 01, n° 152-153, p 202, disponible en ligne à l'adresse: https://www.cairn.info/revue-herodote-2014-1-page-201.htm

ثالثا: عدم وجود نموذج موحد للنشاط الإجرامي

لم تتفق الأنظمة القانونية في بلدان العالم قاطبة على صورة محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها[371]، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه وذلك لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي، فيمكن اعتبار فعل من الأفعال مباحا في دولة، بينما تقوم دولة أخرى بتجريمه، ومرد ذلك إلى طبيعة النظام القانوني السائد في كل بلد من البلدان[372].

حيث وبنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجريمة المعلوماتية، يتضح لنا عدم وجود اتفاق عام مشترك بين الدول حول نماذج الأفعال التي يقوم بها الأشخاص الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كإختلاف البيئات والعادات والتقاليد، والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر[373].

وعليه فإن عدم توفر تعريف موحد للجريمة المرتكبة عبر الإنترنت يضفي عادة إلى إحداث ثغرات في منظومة القانون الدولي في مجال مكافحة تلك الجرائم وإضعاف فعاليته، وإبقاء أفعالا إجرامية خطيرة دون تجريم ولا عقاب، مما يسهل إفلات الجناة من المسؤولية الجزائية لأن نص التجريم هو بمثابة الركن الشرعي لقيام الجريمة وانتفائه يؤدي بالضرورة إلى انتفاء المسؤولية الجنائية.

تثار مسألة عدم الاتفاق على نموذج موحد للنشاط الإجرامي بقوة، حينما يتعلق الأمر بتسليم المجرمين، الذي يعتبر إجراءً دولياً تتخلّى الدولة بموجبه عن شخص متواجد لديها

371- **GODEBERGE Céline**, La coopération judiciaire en matière pénale après le traité de lisbonne, mémoire master de droit pénal et sciences pénales, Université Panthéon-Assas, Paris 2, 2013, p 69.

372– **حفصي عباس**، مرجع سابق، ص 52.

373– **فنور حاسين**، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مذكرة من أجل الحصول على شهادة الماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر، 2012.2013، ص124.

لسلطات دولة أخرى تطالب بتسليمه بغرض محاكمته عن جريمة ارتكبها أو لتنفيذ حكم صادر ضده، إذ يخضع التسليم كما هو معلوم لشرط جوهري يتمثل في التجريم المزدوج، بمعنى أن يكون الفعل المطلوب التسليم من أجله مجرم في قانون الدولة المطلوب منها التسليم والدولة الطالبة للتسليم، أما إذا كان هذا الفعل غير مجرم في نظر قانون إحدى الدولتين فإنه لا يجوز المطالبة بتسليم الفاعل قصد محاكمته أو معاقبته على سلوك مباح وفقا لقانون هذه الدولة[374].

ولعل عدم الاتفاق بين الأنظمة القانونية المختلف على صور موحدة للسلوك الإجرامي في الجريمة المرتكبة عبر الإنترنت يغري قراصنة الحاسب الآلي على تنظيم أنفسهم وارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة[375]

رابعا: التجريم المزدوج للسلوك الإجرامي

يعد التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته هذه يبقى عقبة أمام التعاون الدولي في مجال تسليم المجرمين سيما بالنسبة للجرائم المعلوماتية، إذ أن معظم الدول لا تجرم هذا النمط الإجرامي بالإضافة إلى أنه من الصعوبة تحديد فيما كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أو لاعتبارها من الجرائم المنظمة مثلا، الأمر الذي يعيق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالجريمة العابرة للحدود[376].

ولا يتوقف تسليم المجرمين على توفر شرط التجريم المزدوج فقط، بل لا بد أن تكون الجرائم المراد التسليم من أجلها تحمل الوصف القانوني نفسه وتشترك في الحد الأدنى من

374- **براهيمي جمال**، مرجع سابق، ص 234.

375- **خيرت علي محرز**، مرجع سابق، ص 104.

376- **قارة أمال**، «**تفعيل آليات تسليم المجرمين في إطار المنظمة الدولية للشرطة الجنائية**»، المرجع السابق، ص 900.

العقوبة بمنظور قانون كل من الدولة طالبة التسليم والدولة المطلوب منها التسليم، فبالرجوع إلى المادة الثانية من الاتفاقية الأوربية الخاصة بتسليم المجرمين المبرمة في 13 ديسمبر 1957 فإنها تشترط بالإضافة إلى شرط التجريم المزدوج أن تكون العقوبة المقررة للجريمة المطلوب التسليم من أجلها تساوي على الأقل عامين حبس في قانون الدولتين المعنيتين بالتسليم، وهذا الشرط غالبا ما لا يتحقق بسبب الاختلاف الشاسع بين تشريعات دول العالم فيما يخص الوصف القانوني للجرائم المرتكبة عبر الإنترنت والعقوبة المقررة لها، فما يشكل جنحة في قانون دولة ما يمكن أن يشكل مخالفة في قانون دولة أخرى وبالتالي لا يتم التسليم[377].

الفرع الثاني

الصعوبات الإجرائية في تجسيد التعاون الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

أضفى البعد عبر الوطني للجريمة المرتكبة عبر الإنترنت عدة صعوبات وإشكالات إجرائية قيدت الجهود المبذولة في مجال مكافحتها على المستوى الدولي، وهذه الإشكالات تتعلق بالأساس في اختلاف النظم القانونية الإجرائية **(أولا)** وعدم وجود قنوات اتصال بين الدول **(ثانيا)**، وحتى وإن وجدت فإنها دائما ما تصطدم بالقيود المفروضة على المساعدات القضائية الدولية **(ثالثا)** والتعاون الأمني الدولي **(رابعا)** بما أنها دائما ما تتماشى مع مفهوم سيادة الدولة على إقليمها وأفرادها.

أولا:اختلاف النظم القانونية الإجرائية بين الدول

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي ثبتت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دوله أخرى أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية، والتسليم المراقب , والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع

[377]–مشار إليه لدى: **براهيمي جمال**، مرجع سابق، ص ص 234–235.

الاستدلالات أو التحقيق أنها قانونية في دوله معينة قد تكون ذات الطريقة غير مشروعه في دوله أخرى، وبالتالي فان الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي انه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعه، حتى وان كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع[378].

كل هذه الاختلافات تشكل صعوبات كبيرة لمنظمة الأنتربول في مكافحة الجريمة المرتكبة عبر الإنترنت، خاصة أثناء اصطدامها بترسانة من النظم القانونية الإجرائية المختلفة بين الدول في مجال تحديد المجرم الدولي المرتكب للجريمة عبر الإنترنت المطلوب تسليمه من عدمه.

لهذا تعمل منظمة الأنتربول من أجل تحقيق أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، بالحصول على المعلومات والبيانات المتعلقة بالنظم القانونية الإجرائية عن طريق التنسيق مع المكاتب المركزية للشرطة في الدول، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة بناءا على ما هو مسموح به في النظم القانونية للدول الأعضاء في منظمة الأنتربول، لهذا يعتبر هذا النظام مهم جدا في مجال مكافحة الجريمة المرتكبة عبر الإنترنت وفي حالة انعدامه يؤدي إلى عدم القدرة على جمع الأدلة من أجل مكافحة هذه الجريمة المستحدثة[379].

ثانيا: عدم وجود قنوات اتصال دولية

أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لازماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدله معينة أو

---

[378] – **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص 52.

[379]– **فنور حاسين**، مرجع سابق، ص 125.

معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالباً ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون[380].

تضع بعض الدول قيودا على تداول المعلومات، إذ تطلب في حالة انتقال هذه المعلومات إلى دولة أخرى، أن تلتزم هذه الدولة بنفس مستوى الحماية المفروضة على هذه المعلومات، وربما كان هذا في حق الدولة ولكن امتداد القيود عبر الدول مع اختلاف قوانينها يسبب مشاكل كثيرة فيما يخص تبادل المعلومات عبر العالم[381].

ثالثا: الصعوبات الخاصة بتبادل المساعدات القضائية الدولية

يتم إرسال طلب الإنابة القضائية كما هو معهود عبر القنوات الدبلوماسية، وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت[382].

تتمثل هذه الصعوبات في التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب[383].

ما يزيد الأمور تعقيدا فيما يخص المساعدة القضائية الدولية، هو فتح غالبية الاتفاقيات والمعاهدات الدولية الثنائية والجماعية المجال واسعا لإمكانية رفض واستبعاد تنفيذ الإنابة القضائية الدولية في مجال الجرائم السياسية والجرائم التي تمس بسيادة الدولة وتلك التي تمس بمصالحها الأساسية، كما هو وارد في المادة 27 فقرة 4 من اتفاقية بودابست التي تنص على أنه: "**بالإضافة إلى الشروط أو أسباب الرفض المنصوص عليها في الفقرة الرابعة من المادة 25 فإنه يمكن رفض طلب المساعدة من قبل الطرف الموجه إليه إذا:**

---

380 – **الطيبي البركة، حاج سودي محمد**، مرجع سابق، ص 279.

381– **حسن طاهر داود**، مرجع سابق، ص 211.

382 – **مرنيز فاطمة**، مرجع سابق، ص 205

383 – **محمد أحمد سليمان عيسى**، مرجع سابق، ص 62.

أ- كان موضوع طلب المساعدة ينصب على جريمة يعتبرها الطرف المطلوب منه جريمة سياسية أو جريمة مرتبطة بجريمة سياسية.

ب- إذا كان الطرف الموجه إليه طلب المساعدة يعتقد بأن تنفيذ هذا الطلب من شأنه المساس بسيادة دولته أو نظامها العام الداخلي، أو مصالحه الأساسية الأخرى".

والجدير بالذكر هو أن مفهوم النظام العام يختلف من دولة إلى أخرى، كما أن المصالح الأساسية للدولة مثلما صرحت اللجنة الأوروبية للمشكلات الجنائية في تقرير لها أعدته في عام 1990 هي غير معروفة وغير محددة بمفهوم القانون الدولي، مما سمح للدول استغلال هذه الثغرات في القانون لرفض الإنابة القضائية كلما سنحت لها الفرصة[384].

رابعا: الصعوبات الخاصة بالتعاون الأمني الدولي

تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف الجرائم المرتكبة عبر الإنترنت ومعاقبة مرتكبيها، لذا فإن التحقيقات في هذه الجرائم وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة والتعاون الأمني بين الدول، الذي أولى له الفقه الجنائي اهتماما بالغا لتحقيق القدرة على التصدي للإجرام العابر للحدود وسد أوجه القصور القانوني الذي ساعد المنظمات الإجرامية على اختراق النظم القانونية، فقد يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأن أجهزة الأمن في هذه الدولة يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها، فمتى ما فر المجرم خارج حدود الدولة يقف جهاز الأمن عاجز عن ملاحقته[385].

كما نجد من بين الصعوبات في مجال التعاون الأمني الدولي ما يتعلق خاصة بتدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الإنترنت، ومنها عدم رغبة بعض القيادات

---

[384] – مشار إليه لدى: **براهيمي جمال**، مرجع سابق، ص ص 238-239.

[385] – **فكيري أمال، «إشكالات الإثبات والاختصاص في جرائم تكنولوجيا الاعلام والاتصال العابرة للحدود»**، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 17، جانفي 2018، ص 645.

الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربين في الدورات التدريبية وما اكتسبوه من خبرات.

ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين، وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الافراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال، حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال[386].

المطلب الثاني

الصعوبات المتعلقة بتنازع الاختصاص في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

يعتبر تحديد معايير الاختصاص من بين أهم الآليات التي تسمح للدولة من بسط ولايتها على الجرائم التي ترتكب في إقليمها، غير أن هذا الأمر يتسم بصعوبة كبيرة بالنسبة للجرائم المرتكبة عبر الإنترنت التي أثارت عدة اشكالات سواء على المستوى الوطني أو الدولي، بالرغم من أن تحديد الاختصاص على المستوى الوطني لا يكون مطروحا بحدة وذلك بالرجوع إلى المعايير التقليدية، إلا أنه يبقى مطروحاً بصورة شديدة على المستوى الدولي.

أثارت الجريمة المرتكبة عبر الإنترنت عدّة إشكالات فيما يخص تحديد القانون الواجب التطبيق، وذلك راجع إلى تشعب ركنها المادي عبر العديد من الدول، الأمر الذي أدى إلى ظهور تنازع بين قوانينها **(فرع أول)**.

كذلك الأمر بالنسبة لتحديد القضاء المختص بالنظر في الجرائم المرتكبة عبر الإنترنت الذي اتسم بصعوبة كبيرة، وذلك مرده إلى أن هذه الأفعال تبقى غير واضحة لأن أغلبها ترتكب من طرف مجرمين متواجدين خارج حدود الدولة **(فرع ثان)**.

386 – **مرنيز فاطمة**، مرجع سابق، ص 206.

الفرع الأول

صعوبات تحديد القانون الواجب التطبيق في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

غالبا ما يتحدد السريان المكاني للقانون الجنائي الوطني وفقا لأحد المبادئ الأربعة: مبدأ الإقليمية، ومبدأ الشخصية، ومبدأ العينية، ومبدأ العالمية، وتتفاوت أهمية هذه المبادئ فيما بينها، وتتدرج في أهميتها بحسب ترتيبها، وتأخذ معظم التشريعات الجنائية بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى[387]، غير أن محاولة تطبيق هذه المبادئ على الجرائم المرتكبة عبر الإنترنت أظهر العديد من الصعوبات نظرا لطبيعتها الخاصةن وسوف نتطرق في هذا المجال إلى مبادئ تطبيق النص الجزائي **(أولا)**، ثم إلى صعوبات تطبيق المبادئ التقليدية على الجريمة المرتكبة عبر الإنترنت **(ثانيا)**.

أولا: مبادئ تطبيق النص الجزائي على الجرائم بصفة عامة

تتمثل مبادئ تطبيق النص الجزائي في:

1- مبدأ إقليمية النص الجزائي (المبدأ الأصلي)

يقتضي مبدأ الإقليمية أن يخضع كل من يرتكب عمل اجرامي على إقليم الدولة للقانون الوطني لتلك الدولة[388]، ولا فرق في ذلك بين مواطن أو أجنبي، وتطبيقا للمبدأ نص قانون العقوبات الجزائري في المادة الثالثة على أنه: "**يطبق قانون العقوبات على كافة الجرائم التي ترتكب على أراضي الجمهورية**"

يعني هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل الإقليم الوطني بغض النظر عن جنسية مرتكبها أو المجني عليه، وينعقد الاختصاص وفقا له بتحقق أحد العناصر المكونة للجريمة سلوكا ونتيجة ولو كان الفعل غير معاقب عليه في البلد الأصلي،

---

[387] – **مفتاح بو بكر المطري**، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا، المنعقد بجمهورية السودان، في 23-2012/09/25، ص 21.

[388]- **TITOYCHE Radia,** op-cit, p 29.

ومن ثم يجب تطبيق قانون العقوبات الوطني. كما يمكن بناء على هذا مبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل الوطن[389].

2- مبدأ شخصية النص الجزائي

أخذ المشرع بمبدأ شخصية النص الجزائي من خلال نص المادة 582 من قانون الإجراءات الجزائية التي نصت على أن كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري ارتكبها جزائري خارج الجمهورية يجوز أن يتابع ويحاكم في الجزائر.

كما نص على ذلك فيما يخص الجنح من خلال المادة 583 على أنّه: "**كل واقعة موصوفة بأنّها جنحة سواء في نظر القانون الجزائري أم في نظر تشريع القطر الذي ارتكبت فيه يجوز المتابعة من أجلها والحكم فيها في الجزائر إذا كان مرتكبها جزائريا**"

3- مبدأ عينية النص الجزائي

أخذ المشرع بمبدأ العينية في نص المادة 588 من قانون الإجراءات الجزائية والتي تنص على أن كل أجنبي ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية...تجوز متابعته ومحاكمته وفقا للقانون الجزائري إذا ألقي عليه القبض في الجزائر أو حصلت الدولة على تسليمه لها[390].

4- مبدأ عالمية النص الجزائي

يطبق النص الجنائي وفقا لهذا المبدأ على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني، فالدولة التي تضبط المجرم عليها بمعاقبته ومحاسبته بحسب قانونها الوطني[391]، غير أن الملاحظ في هذا المبدأ أن أغلب

---

[389]- أنظر المادة 586 من قانون الإجراءات الجزائية الجزائري.

[390]- تنص المادة 588 من أمر رقم 15-02 المؤرخ في 23 يوليو 2015 المتضمن تعديل قانون الإجراءات الجزائية على أنه : " تجوز متابعة ومحاكمة كل أجنبي، وفقا لأحكام القانون الجزائري، ارتكب خارج الإقليم الجزائري =بصفته فاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات= الدبلوماسية والقنصلية الجزائرية أو أعوانها، أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري".

[391]- **آمال فكيري**، مرجع سابق، ص 642.

مشرعي دول العالم لم تعمل به نظرا لتعارضه مع مبدأ سيادة الدولة على إقليمها ورعاياها ومن بينها المشرع الجزائري الذي لم ينص عليه.

ثانيا: صعوبات تطبيق المبادئ التقليدية على الجريمة المرتكبة عبر الإنترنت

لا يخلو إعمال السريان المكاني للقانون الجنائي بخصوص الجرائم المرتكبة عبر الإنترنت وفقا لأحد المبادئ الأربعة السالفة الذكر من صعوبات، تفضي تارة إلى إثارة تنازع إيجابي في الاختصاص بين أكثر من تشريع وطني، وتارة أخرى يقوم تنازع سلبي في الاختصاص يخرج معه اختصاص أي من الدول بملاحقة الجاني، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد اختصاصها وفقا لمعايير الاختصاص المعروفة.

أما في حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة ما إذا ثار فيها التنازع كما في الجرائم عبر الوطنية ومنها جرائم الإنترنت التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، أو في حالة تجرد بعض عناصر هذا السلوك من خاصيتها المادية، كما هو الحال في القرصنة في مجال الحوسبة، وصور المساهمة الجنائية التي تتم باستخدام أجهزة الاتصالات الحديثة، مثل هذه الظاهرة تفرض تنازعا في الاختصاص بل غموضا في تحديد معياره، تتطلب بطبيعة الحال حلولا مستحدثة وابتكار لمفاهيم قانونية جديدة دون الإخلال بمبادئ الشرعية الجنائية التي ترتكز عليها معظم النظم الجنائية الوطنية[392].

ثار جدل بخصوص مسألة تخزين المعلومات او البيانات المعالجة إلكترونيا خارج إقليم الدولة، حيث ظهر رأيان: الرأي الأول يرى إنه من غير المشروع أن تقوم سلطات دولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى، بهدف كشف وضبط أدلة لإثبات جريمة كانت قد وقعت على أراضيها وذلك إستنادا إلى مبدأ إقليمية القانون، أما الرأي الثاني، فإنه يعول على أن القانون الدولي يمكن أن يتشكل من خلال توافق الآراء على

[392]– **مفتاح بو بكر المطري**، مرجع سابق، ص 22.

الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية[393].

واجه مبدأ إقليمية النص الجزائي صعوبة كبيرة من حيث التطبيق بالنسبة للجرائم المرتكبة عبر الإنترنت، وهذا بالنظر لطبيعتها والخصائص التي تميزها عن الجريمة التقليدية، خصوصا صعوبة تحديد مكان وقوعها وارتكابها بدقة وكذا زمان حدوثها، فتطبيق المبدأ هنا يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي باعتباره شرط أولي لعقد الاختصاص للقاضي الوطني[394].

ضف إلى ذلك أنه يترتب على تطبيق مبدأ إقليمية قانون العقوبات عدم اهتمام الدولة إلا بالجرائم التي تقع على إقليمها، فلا يمتد إلى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدولة، غير أن هذه النتيجة قد لا تتفق مع حماية مصالح الدولة، خاصة فيما يتعلق بالجرائم التي ترتكب عبر الإنترنت، وذلك راجع إلى البعد الدولي، بل العالمي لنشاط الشبكة، حيث يضع دول مختلفة في حالة اتصال دائم عن طريق البيانات والمعلومات التي يتم إدخالها وتحميلها على الشبكة، بحيث تكون متاحة لأي مستخدم في تلك الدول[395].

كما ورد على مبدأ شخصية القانون الجزائي عدة قيود بصفة عامة، وبالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج بل يجب علم النيابة العامة بها، كما أنه لا يجوز محاكمة الشخص على نفس الفعل الواحد مرتين وهذه الإجراءات طويلة ومكلفة وتقيد تطبيق مبدأ الاختصاص الشخصي.

والملاحظ أن مبدأ الشخصية يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف عن جنسيته، وهذه المعلومات تعد صعبة وعسيرة في جرائم الإنترنت أين يستعمل التشفير والأسماء المستعارة بالإضافة إلى اللغة الصعبة والمعقدة في كشفها

---

393 – **مفتاح بو بكر المطري**، مرجع سابق، ص ص 22-23.

394 – **فكيري أمال**، مرجع سابق، ص ص 640-641.

395 – **فريجة محمد هشام**، مرجع سابق، ص 156.

والتعامل معها، كما أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة ومعقدة ومكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام الصادرة في الخارج[396].

يصادف كذلك مبدأ عينية النص الجزائي في الواقع العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص الجريمة المرتكبة عبر الإنترنت حيث لا تظهر ماديتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع النظم القانونية في العالم واختلافها مما يترتب عليه البطء والتعقيد وطول مدة الإجراءات[397].

بالإضافة إلى ذلك أن من بين المشكلات التي تعيق تنفيذ مبدأ عينية النص الجزائي تعارض تطبيق القانون الجنائي وفقا لمبدأ العينية مع تطبيق القانون وفقا لمبدأ الإقليمية في حالة ما إذا كانت الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص والقانون الواجب التطبيق بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية والدول الأخرى التي تعد الجريمة من الجرائم التي يناط بقضائها النظر فيها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على فعله مرتين[398].

كما لا يخلو تطبيق مبدأ عالمية النص الجزائي على إطلاقه من الإشكالات القانونية العديدة، حيث أن تطبيق قانون العقوبات على كل مجرم يقبض عليه في إقليم الدولة، أيا كانت الدولة التي ارتكب فيها الفعل الإجرامي وأيا كانت جنسية الجاني قد يؤدي إلى تعارض بين قوانين الدول، إذ يجعل لكل دولة اختصاص بالنظر في أية قضية هي بالأصل من اختصاص قانون آخر، ويتعارض مع مبادئ قانون العقوبات نفسه الذي هو بالأصل قانون إقليمي، كل هذا يجعل تطبيق المبدأ أمرا صعبا من الناحية العملية، ولذا فقد درج البعض

396 – **لموسخ محمد**، «**تنازع الاختصاص في الجرائم الإلكترونية**»، مجلة دفاتر السياسة والقانون، العدد الثاني، كلية الحقوق والعلوم السياسية، جامعة ورقلة، جوان 2009، ص 158.

397 – **المرجع نفسه**، ص 159.

398– **بثينة حبيباتي**، مرجع سابق، ص 93.

على تقييد المبدأ لينطبق على بعض الأنواع من الجرائم، منها جرائم الإنترنت العابرة للحدود، فتضافرت الجهود في مكافحة هذا النوع من الإجرام تشريعيا وقضائيا وتنفيذيا[399].

على الرغم من أن المبادئ العامة التي تحكم التجريم والعقاب من حيث المكان في القانون الجزائري، سواء تلك الواردة في قانون العقوبات أو الإجراءات الجزائية قد جاءت قاصرة على مبدأ الإقليمية كمبدأ أصلي ومبدأي الشخصية والعينية كمبادئ احتياطية دون أية إشارة إلى تبني مبدأ عالمية النص الجنائي في مكافحة الجريمة المرتكبة عبر الإنترنت، إلا أنه ومن الناحية العملية نجد أن وزارة العدل تسعى جاهدة إلى عقد عدة اتفاقات ونشاطات سواء على المستوى العربي أو الدولي لأجل مكافحة الإجرام المعلوماتي، غير أن هذه الاتفاقات إن لم تدعم بمبدأ عالمية النص الجنائي الذي ينبغي تبنيه والنص عليه من طرف المشرع، قد تبقى عاجزة عن مواجهة ظاهرة الإجرام المرتكب عبر الإنترنت إذا كانت الجريمة المرتكبة لا تخضع لسلطان القانون الجزائري بمقتضى مبدأ الإقليمية أو الشخصية أو العينية[400].

الفرع الثاني

صعوبات تحديد المحكمة المختصة في مجال مكافحة الجريمة المرتكبة عبر الإنترنت

أثارت الجريمة المرتكبة عبر الإنترنت إشكالات قانونية في تحديد القضاء الذي تعود له الولاية متابعة هذا النوع من الجرائم، ويعود أساس هذا الإشكال إلى التباين بين المعايير المعتمد عليها من طرف الدول في تحديد الاختصاص القضائي، لهذا سوف نتطرق إلى تبيين معايير تحديد المحكمة المختصة **(أولا)**، ثم إلى صعوبات تطبيق المبادئ التقليدية للاختصاص القضائي على الجرائم المرتكبة عبر الإنترنت **(ثانيا)**

أولا: معايير تحديد المحكمة المختصة

تتمثل معايير تحديد المحكمة المختصة في:

399- **آمال فكيري**، مرجع سابق، ص 642.

400- **فنور حاسين**، مرجع سابق، ص 133.

1- معيار الاختصاص المكاني

يرتبط الاختصاص الجنائي –سواء من الناحية الموضوعية (المرتبطة بالإباحة والتجريم) أو من الناحية الإجرائية– بسيادة الدولة، أو ما يسمى بمبدأ إقليمية القانون، وبالتالي فإنه لا ينفذ في إقليم الدولة إلا قوانينها ولا يطبق بشأن الجرائم المرتكبة في هذا الإقليم إلا الأحكام الواردة في هذه القوانين، وتصير محاكمها هي صاحبة الولاية بمحاكمة المتهم، وفي المقابل تحترم الدولة سيادة الدول الأخرى وحقها في إعمال قوانينها[401].

لا يستثنى من هذه الأحكام إلا حالات الضرورة، والحالات التي استقر العرف الدولي على الأخذ بها –كتطبيق القانون الجنائي للدولة التي ترفع السفارة أو السفينة أو الطائرة علمها على ما يقع داخلها من جرائم– أو الحالات التي ترتبط بمتطلبات التعاون الدولي لمكافحة العمليات الإجرامية وخاصة الإجرام المنظم.

تطبق ذات الأحكام على الدعوى العمومية المتعلقة بالجريمة المرتكبة عبر الإنترنت، بمعنى أنه يتحدد الاختصاص المكاني للمحكمة الجنائية المختصة بنظرها وفقا للمكان الذي وقعت فيه الجريمة المعلوماتية أو الذي يقيم فيه مرتكبها، أو يقبض عليه فيه خاصة إذا لم يكن له مكان إقامة معروف[402].

2- معيار القانون الأكثر ملائمة

بني هذا المعيار على الأخذ بعين الاعتبار نقطة الاتصال المميزة والسلطة الفعلية، أي باختصاص قضاء الدولة التي قانونها هو الأكثر تعرضا للانتهاك بسبب الفعل الجرمي، ومن أمثلة ذلك ما أصدرته إحدى المحاكم الأمريكية، التي قررت فيه أنه لا يمكن الارتكاز

401- **DIOUF Ndiaw**, op-cit, p 265.

402– **طارق عفيفي صادق أحمد**، الجرائم الإلكترونية جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص ص 231–232. أنظر كذلك:

- **BRAULT Nicolas**, Le droit applicable à internet de l'abime aux sommets, revue-legicom, n° 12, vol 2, 1996, p 11, disponible en ligne à l'adresse: https://www.cairn.info/revue-legicom-1996-2-page-1.htm

على مجرد النفاذ، أو الاتصال بهذا الموقع، أو المورد انطلاقا من الأراضي الأمريكية، حيث قضت باختصاص قضاء الدولة من منطلق وقوع الضرر الفعلي لا الاحتمالي[403].

3- معيار الضرر المرتقب

صاحب ظهور شبكة الإنترنت وجود عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، وهذا العالم الافتراضي لا يخضع لأي سلطة إقليمية، وبالتالي يترتب على هذه الحالة أن الضرر الذي تسببه الجريمة المرتكبة عبر الإنترنت يمكن أن يحدث في أي دولة تكون متصلة بالإنترنت، وهذا هو معيار "الضرر المرتقب أو الإفتراضي".

قدم المجلس الأوروبي تفسيرا خاصا بشأن مفهوم قاعدة اختصاص محل وقوع أو حدوث الفعل الضار، وذلك بالتأكيد على حق المتضرر، باللجوء حسب خياره إلى محكمة محل ارتكاب الفعل، أو إلى محل وقوع الضرر، ولكن مع إضافة قيد هام، أو أساسي في حالة لجوء المتضرر إلى محكمة محل وقوع الضرر، يقضي بحجب اختصاص هذه المحكمة، إذا أثبت المدعى عليه، أنه لم يكن قادرا على الارتقاب بصورة معقولة، وإن الفعل أو الامتناع كان من شأنه إحداث أو انتاج ضرر مماثل في دولته[404].

---

[403]- **فريد منعم جبور**، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010، ص 207.

[404]- ورد في حيثيات هذا القرار أن المعلومات المنشورة في شبكة الإنترنت يمكن معاينتها من قبل جميع الدول الموصولة بها، ومن دون أن تكون موجهة بالضرورة محددة، لكن طبيعة هذه الوسيلة الإعلامية الجديدة لا يجب أن ينتج عنها تطبيق لجميع القوانين الموجودة بل يجب أن نطبق معيار (الإرتقاب)، على المسؤول عن المعلومات الضارة فيها، وهذا المعيار لا يمكن إيجاده إلا من خلال إيجاد صلة أو علاقة للقانون المختص مع مبدأ موضوعي، وذلك بمعزل عن تذرع كل دولة باختصاصها المحتمل، أنظر في ذلك: **صغير يوسف**، الجريمة المرتكبة عبر الإنترنت، مذكرة مقدمة للحصول على شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2013، ص ص 145-146.

4- **المعيار المختلط**

أمام الإنتقادات التي تعرض لها كلا الإتجاهين السابقين، برز اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط (العمل التنفيذي)، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققه فيه، وهذا الاتجاه حظي بمباركة أغلب الفقه، ويجد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي الفعل (النشاط)، والنتيجة، وعلاقة السببية، ما يعني أن الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة على حد سواء[405].

قد يرتكب المجرم جريمته في دولة (أ) وتتحقق النتيجة في دولة اخرى (ب) ثم يفر إلى دولته التي يحمل جنسيتها تملصا من المسؤولية، فلا تستطيع هذه الأخيرة معاقبته على أساس عدم تحقق أحد العناصر المكونة للجريمة على إقليمها[406].

ثانيا: صعوبات تطبيق المبادئ التقليدية للاختصاص على الجرائم المرتكبة عبر الإنترنت

بما أن جرائم الإنترنت تعتبر من الجرائم العابرة للحدود، فإنه تثار مشكلة الاختصاص على المستوى الدولي بسبب اختلاف التشريعات والنظم القانونية[407]، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل اجنبي، فهنا تكون الجريمة خاضعة لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل حينها في اختصاصها استنادا لمبدأ العينية، كما قد تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، لذلك تعتبر مسألة الإقليمية من أهم الصعوبات التي تعترض ماهية التعاون الدولي في سبيل

---

405 – **موسى مسعود أرحومة**، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، خلال الفترة 28-2009/10/29، طرابلس، ليبيا، ص 16.

406 – **شرف الدين وردة، بشير سليم**، مرجع سابق، ص 129.

407- **HARIVEL Jean**, op-cit, p 91.

مكافحة الجريمة المرتكبة عبر الإنترنت خاصة في حال تمسك الدولة بهذا الإجراء واعتبرته مساسا صارخا بسيادتها الوطنية[408].

لذلك ثار خلاف حول تحديد المحكمة المختصة بنظر هذه الجرائم، فذهب الجانب الأول منه إلى أن الاختصاص ينعقد في الجرائم المعلوماتية إلى محاكم الدولة التي تم فيها تحميل البيانات، كون عملية جمع البيانات والأدلة ستكون سهلة لكونها دولة المصدر، كما أن بنك معلومات محل التحميل يكون أكثر ثباتا[409].

وجهت العديد من الانتقادات لأصحاب هذا الرأي يتمثل أهمها في:

أن المذهب لا يعير اهتماما للمكان الذي تحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فيه، فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلا، كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها[410]

بالإضافة إلى ذلك أن بعض هذه الأفعال قد لا يكون معاقبا عليها في دولة التحميل وبالتالي تكون فعلا مباحا ولا يعاقب عليه القانون، لذلك ظهر جانب آخر من الفقه يتجه لإعطاء الاختصاص لمكان وقوع النتيجة الجرمية لتعدد دول التحميل مما يعقد الاختصاص لأكثر من دولة مما يؤدي لضياع السؤولية خصوصا إذا كانت دولة التحميل لا تعاقب على مثل هذه الأفعال، ولكن كان على هذا الرأي مآخذ أيضا حيث لم يضع في الحسبان مصلحة المتهم بأن تطبق عليه قوانين غير قانون الدولة التي يحمل جنسيتها مما يزيد من كلفة المحاكمات في هذه الجرائم، وزيادة مدة وأجل المحاكمة.

---

408 – **حاج مخناش نوال**، مرجع سابق، ص 1131

409– **حنان ريحان مبارك المضحكي**، مرجع سابق، ص 373.

410 – **شرف الدين وردة، بشير سليم**، المرجع السابق، ص128.

استدعت كل هذه المبررات ظهور اتجاه ثالث يرى بانعقاد الاختصاص القضائي لمكان المعتدى عليه فهو المكان الذي تحققت فيه النتيجة الإجرامية ومرتبط بشخص المعتدى عليه، وهو يتجنب السلبيات والانتقادات التي وجهت للاتجاهين السابقين[411].

[411]– **حنان ريحان مبارك المضحكي**، مرجع سابق، ص 374.

الفصل الثاني

قصور ناتج عن تأثير الحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت

تعتبر الشبكة العالمية للإنترنت –كما أسلفنا الذكر– سلاحا ذو حدين، فكما تحمل في طياتها جانبا إيجابيا من خلاله سهلت مختلف التعاملات التي يقوم بها المتعاملين عبرها في مختلف المجالات التعليمية والاقتصادية والتجارية وحتى الترفيهية، فلها جانب سلبي مظلم من خلاله يتم الاعتداء على العديد من حقوق الأفراد، ولعل أهمها الاعتداء على حقهم في الحياة الخاصة.

تجمع الشبكة العالمية للإنترنت العديد من البيانات عن الأفراد والجماعات في مختلف المجالات السياسية والاجتماعية والاقتصادية وحتى الصحية، كما أنها تسهل على إظهار حياة الفرد خلال لحظات وجيزة، وتمكّن الغير من الاطلاع على مختلف المعلومات المتعلقة به، والتي كانت في السابق يكسوها طابع الحجب، الأمر الذي أدى بالتشريعات إلى سن قوانين تحمي هذه الخصوصية سواء في شقها الموضوعي أو التقني، وذلك بالتطرق خاصة إلى تحديد ما يعتبر من الحياة الخاصة للأفراد **(مبحث أول)**.

غير أن هذه الحماية المفروضة من طرف التشريعات المختلفة على الحق في الحياة الخاصة أدت إلى التعارض مع الأساليب المتبعة في مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك عن طريق فرض أن تكون هذه الآليات مشروعة وتتم وفقا للقانون ولا تمس بالحياة الخاصة للفرد سواء في جانبها القانوني أو التقني **(مبحث ثان)**.

المبحث الأول

ماهية الحق في الحياة الخاصة وطرق الاعتداء عليه عبر الإنترنت

يعتبر الحق في الحياة الخاصة من بين أقدم وأهم حقوق الإنسان، حيث يعد حقاً متصلا اتصالا وثيقا بحرية الشخص وكرامته، الأمر الذي أدّى إلى ضرورة حمايته من مختلف الاعتداءات وذلك ما كرسته أغلب التشريعات الوطنية والدولية، غير أنّه بظهور الشبكات الاتصالية وخاصة الشبكة العالمية للإنترنت، فتحت آفاق جديدة لممارسة هذا الحق من طرف الأفراد.

جعل التطور الذي عرفته شبكة الإنترنت مفهوم ممارسة الحق في الحياة الخاصة يتسم هو الآخر بالتطور والتغير، وذلك بظهور حقوق أخرى متصلة به لم يكن يعرفها الإنسان من قبل أساسها التقنية العالية **(مطلب أول)**.

أدّى هذا التطور في مفهوم الحياة الخاصة في العصر الرقمي إلى الاختلاف في ممارسة هذا الحق، غير أنه سهل من طرق الاعتداء عليه والمساس به بما يضر بصاحبه، وذلك راجع إلى الخصوصية التي تتميز بها شبكة الإنترنت التي لا تخضع لأي سلطة **(مطلب ثان)**.

المطلب الأول

مفهوم الحق في الحياة الخاصة

أدى التطور الذي عرفه مفهوم الحق في الحياة الخاصة عبر شبكة الإنترنت إلى ظهور العديد من التضاربات فيما يخص تحديد المقصود بهذا الحق، وذلك نظرا لما اكتنفه من غموض وتعقيد في هذا النطاق، وأمام صعوبة تحديد هذا المفهوم وعدم الاتفاق على تعريف موحد له ارتأينا تحديد المقصود منه من خلال نقطتين هما:

مظاهر الحق في الحياة الخاصة **(فرع أول)**، وخصائص الحق في الحياة الخاصة **(فرع ثان)**.

الفرع الأول

مظاهر الحق في الحياة الخاصة

يتميز تحديد مظاهر الحق في الحياة الخاصة تحديداً دقيقاً بالصعوبة، وذلك راجع إلى تعدد صور هذا الحق من جهة، واختلافه من مكان إلى آخر ومن زمان إلى آخر من جهة أخرى، ومن أجل تبيين ذلك سوف نتطرق إلى الحق في حرمة المسكن **(أولا)**، حرمة المحادثات والمكالمات والمراسلات الشخصية **(ثانيا)**، حرمة الشرف والاعتبار **(ثالثا)**، حرمة الحياة العائلية **(رابعا)**، حرمة الحياة الصحية والرعاية الطبية **(خامسا)**، حرمة الذمة المالية **(سادسا)**، ثم حرمة اسم الشخص **(سابعا)**:

أولا: الحق في حرمة المسكن

تعتبر حرمة المسكن أول وأهم مظاهر الحق في الحياة الخاصة بحكم الوظيفة التي يتمتع بها باعتباره مستودع أسرار الأفراد المادية والمعنوية، وفيه يتحرر الفرد من قيود التعامل وضوابط اللباس مع الآخرين، وهو محل سكينته التي ينشد فيها عزلته بعيدا عن أعين ومسمع الآخرين[409].

اعترف المشرع بحرمة المسكن بداية بدستور 1963[410] الذي نصت المادة 14 منه بأنه:

"لا يجوز الاعتداء على حرمة المسكن، ويضمن حفظ سر المراسلة لجميع المواطنين"[411]

ونظرا لأهمية وخطورة الاعتداء عليه باعتباره جوهر ممارسة الحياة الخاصة فقد تدارك في الدساتير اللاحقة ضرورة إحاطته بالضمانات القانونية التي تكفل احترامه، حيث خص التفتيش باعتباره من أخطر الاجراءات الماسة بحرمة المسكن بجملة من الإجراءات التي

---

[409]- **JAMMET Adrien**, La prise en compte de la vie privée dans l'innovation technologique, thèse pour obtenir le grade de docteur en droit, l'université Lille 2- droit et santé, p 68.

[410]– دستور الجمهورية الجزائرية الديموقراطية الشعبية لسنة 1963، ج ر، عدد 64، صادر في 10 سبتمبر 1963.

[411]– كما نص على ذلك دستور 2020 في المادة 48 على أنه: "تضمن الدولة عدم انتهاك حرمة المسكن".

يجب توافرها لتفتيش المسكن وهي وجوب أن يكون الأمر الذي يقضي بالتفتيش مكتوبا، وصادر من سلطة قضائية مختصة[412].

ثانيا: حرمة المحادثات والمكالمات والمراسلات الشخصية

خص المشرع المحادثات والمكالمات والمراسلات الشخصية بحماية وذلك لاعتبارها من مظاهر الحق في الحياة الخاصة للفرد التي لا يجوز الاعتداء عليها، بل اعتبرها حق دستوري يحميه القانون.

1- حرمة المحادثات والمكالمات

حيث يجب حماية أسرار الحياة الخاصة التي تنبعث من خلال الأحاديث الشخصية ضد جميع وسائل التنصت والإستماع والنشر، فلا يجب مطلقا تسجيل الأحاديث الشخصية والمكالمات الهاتفية أو مراقبتها والتنصت عليها بأية وسائل كانت، ويعتبر هذا القيد مهما لا يمكن خرقه إلا في الحدود والحالات التي ينص عليها القانون[413].

2- حرمة المراسلات

تتمثل المراسلات التي كفلتها الحماية بمقتضى القانون فيما يلي:

أ- المراسلات العادية:

عرف المشرع المراسلات وبين مضمونها وحدد أشكالها بموجب المادة 09 الفقرة السادسة عشر من قانون 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية بأنها: "**اتصال مجسد في شكل كتابي على دعامة مادية مهما كانت طبيعتها**

412- **بن حيدة محمد**، حماية الحق في الحياة الخاصة في التشريع الجزائري، رسالة مقدمة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2016-2017، ص ص 114-115.

413- **يوسفات علي هاشم، «الحق في الحياة الخاصة وآليات التعويض عن المساس به في التشريع الجزائري»**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، العدد 17، سنة 2006، ص 279.

يتم إيصاله وتسليمه إلى العنوان المبين من طرف المرسل نفسه أو بطلب منه لا تعد الكتب والفهارس والجرائد كمادة مراسلات"[414].

كفل المشرع حماية حرمة المراسلات بمقتضى مواد القانون السالف ذكره، حيث أقرّ عقوبات تتراوح بين عقوبات سالبة للحرية والغرامة المالية لكل شخص أو متعامل في البريد يقوم بانتهاك حرمة المراسلات وذلك طبقا لنص المادة 164 منه وما يليها والتي تضمنها الباب الرابع والمعنون بالأحكام الجزائية.

ب- **البريد الإلكتروني:**

لم يعد مفهوم المراسلات يقتصر على الرسائل المكتوبة في الوقت الحاضر، بل شمل جميع أشكال التراسل بما في ذلك الإنترنت، وبذلك فرض الحق في المراسلات الخاصة التزاما على الدولة بضمان تسليم الرسائل الإلكترونية وغيرها من أشكال المراسلات عبر الإنترنت إلى المتلقي المنشود بالفعل، دون أي تدخل أو تفتيش من قبل أجهزتها أو أي جهة ثالثة[415].

ثالثا: حرمة الشرف والاعتبار

يحق لكل انسان أن يحظى باحترام كرامته التي يعتز بها، وبالتقدير الذي يرى أنه يستحقه من قبل المجتمع في ضوء مكانته الإجتماعية، وهذا يطلق عليه قانونا بالحق في الشرف والاعتبار[416].

---

[414]- قانون رقم 18-04، مؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر عدد 27، صادر في 13 مايو سنة 2018.

[415] - **بن حيدة محمد**، حماية الحق في الحياة الخاصة في التشريع الجزائري، مرجع سابق، ص 122. أنظر كذلك:
- **KAMENI Guy marcel**, La vie privée en droit camerounais, Thèse en vue de l'obtention du doctorat, université de toulouse 1 capitole, 2013, p 170.

[416]- **سليم جلاد**، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، مذكرة لنيل شهادة الماجستير في الشريعة والقانون، تخصص حقوق الإنسان، كلية العلوم الإنسانية والحضارة الإسلامية، قسم العلوم الإسلامية، جامعة وهران، 2012-2013، ص 93. أنظر كذلك:
- **METILLE Sylvain**, Le Droit au respect de la vie privée les défis digitaux une perspective de droit comparé, union européenne, Bruxelles, 2018, p 17.

كفل المشرع حرمة الشرف في موضع كفالة حرمة الحياة الخاصة حسب المادة 39 من الدستور وورد فيها: "**لايجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون**"[417]، وهذا فيه دلالة على وجود العلاقة بين الحياة الخاصة والشرف والاعتبار إلى جانب العناصر الأخرى المتمثلة في سرية المراسلات والاتصالات وحرمة المسكن، ويعضد ذلك ما ذهب إليه بعض الفقه والقضاء من أن توافر المساس بالحياة الخاصة مع الاعتداء على حق الشخص في شرفه واعتباره يشكلان تعددا صوريا بين الجريمتين، إضافة إلى التصريح المباشر في المادة السالفة الذكر، هناك تصريح غير مباشر بحرمة الشرف والاعتبار[418]، وذلك ما نص عليه المشرع الجزائري في المادة 34 من الدستور بقوله: "**تضمن الدولة عدم انتهاك حرمة الانسان، ويحظر أي عنف بدني أو معنوي أو أي مساس بالكرامة**"، وكذا المادة 35 ونصها: "**يعاقب القانون على المخالفات المرتكبة ضد الحقوق والحريات، وعلى ما يمس الانسان البدنية والمعنوية**"[419].

رابعا: حرمة الحياة العائلية

تنشأ بموجب الحياة العائلية الكثير من الأمور التي تستوجب السرية والكتمان والعديد من الأسرار التي تستوجب الحفظ كالحالة الصحية للزوجين والحياة العاطفية والمراسلات بينهما، وقد ذهبت المحكمة الدستورية المصرية العليا في إحدى أحكامها المؤرخة في 18 مارس 1995 إلى أن الحق في الزواج والحقوق المتفرعة عنه لم ينظمها الدستور لأنها مندرجة ضمن الحق في الخصوصية باعتباره مكملا للحرية الشخصية[420].

---

[417]– أنظر المادة 39 من دستور 1996، ج ر عدد 74، صادر في 28 ديسمبر 1996.

تنص المادة 39 من دستور الجزائر لسنة 2020 على أنه: "تضمن الدولة عدم انتهاك حرمة الإنسان"

[418]– **سليم جلاد**، مرجع سابق، ص 94

[419]– أنظر المواد 34 و35 من دستور 1996، مرجع سابق، أنظر كذلك الفقرة 2 والفقرة 3 من المادة 39 من تعديل الدستور لسنة 2020

[420]– مشار إليه لدى : **بن حيدة محمد**، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مذكرة لنيل شهادة الماجستير، تخصص حقوق وحريات، كلية الآداب والعلوم الإنسانية، قسم العلوم القانونية والإدارية، جامعة أدرار، 2009–2010، ص 64

كما أدرج جانب من الفقه الفرنسي الحياة العائلية وكل ما يرتبط بها من بنوة وزواج وطلاق وحياة عاطفية ضمن الحق في الخصوصية، بل إن الأمور العاطفية للبنات تعتبر من أدق مظاهر الحياة الخاصة ولا يجوز الكشف عنها سواء كانت حقيقة أو مجاز، ويرى أن الحياة الأسرية تندرج ضمنها ثلاث حقوق، الحق في تأسيس أسرة، والحق في العيش معها، والحق في احترام خصوصيات الأسرة باحترام السير الطبيعي لها والذي يندرج ضمن الحقوق الأساسية للخصوصية[421].

وباعتبار الأسرة هي الكيان الأول للفرد فقد أثير جدل حول التعدي على خصوصيات الفرد هل يشكل اعتداء على الأسرة أم لا؟ وهو ما أجاب عليه القضاء الفرنسي بأن الكشف والمساس بالحياة الخاصة للقاصر إنما يعد مساسا بالحياة الخاصة للأسرة التي ينتمي إليها كما أن الذكريات الشخصية لا يجوز نشرها إلا بموافقة الشخص الذي تتعلق به[422].

خامسا: حرمة الحياة الصحية والرعاية الطبية

تعد الحياة الصحية وما يرتبط بها من رعاية طبية داخل المؤسسات العلاجية أو خارجها من أهم مظاهر الحياة الخاصة، وذلك أن الأصل العام هو حماية أسرار المرضى واعتبار ذلك من صميم الحياة الخاصة، حيث اعتبرها الفقه الحديث أنها من الأمور التي يجب سترها، فإفشاؤها يسيء إلى المرضى خاصة إذا ذكرت أسماؤهم[423].

---

[421]- **MATTATIA Fabrice**, Internet et les réseaux sociaux : que dit la loi ? 2e édition, éditions eyrolles, Paris, 2015, p 101.

[422] – نقلا عن **بن حيدة محمد**، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مرجع سابق، ص 65.

[423] – **بن سعيد صبرينة**، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال"، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2014-2015، ص56.

سادسا: حرمة الذمة المالية

من أهم ما يتصل بالخصوصية هي الأمور المتعلقة بالذمة المالية للشخص، ومن ثم يعد من قبيل انتهاك الخصوصية نشر كل ما من شأنه الكشف عن عناصر الذمة المالية، سواء أثناء حياة الشخص أو بعد وفاته[424].

تعتبر ثروة الفرد ورصيده المالي من الأمور التي يشكّل الكشف عنها مساسا بالحق في الحياة الخاصة، وهو ما أقره القضاء الفرنسي في الكثير من الأحكام القضائية، حيث أدرج الذمة المالية ضمن مظاهر الحق في الحياة الخاصة، وأن كل كشف لها يعتبر مساسا به، فنشر ضريبة الشخص وكشف مقدار تركة المتوفي كلها من المسائل التي تسهل معرفة حجم ثروته[425].

سابعا: حرمة إسم الشخص

يعتبر الاسم أحد الحقوق الملازمة لشخصية الانسان والمكونة لها، وهو الذي يمنح الشخص ذاتيته ويميزه عن غيره من الأشخاص، فهو واجب يفرضه القانون على الشخص كنظام يميزه عن غيره، وحق من الحقوق يمنحه القانون وقف الاعتداء عليه[426].

اعترف المشرع الجزائري بالحق في الاسم من خلال المادة (48) من القانون المدني "لكل من نازعه الغير في استعمال اسمه دون مبرر، ومن انتحل الغير اسمه أن يطلب وقف هذا الاعتداء، والتعويض عما يكون قد لحقه من ضرر".

---

424 – **عاقلي فضيلة**، الحماية القانونية للحق في حرمة الحياة الخاصة دراسة مقارنة، بحث مقدم لنيل شهادة دكتوراه علوم تخصص قانون، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2011–2012، ص 98.

425 – **بن حيدة محمد**، حماية الحق في الحياة الخاصة في التشريع الجزائري، مرجع سابق، ص 141.

426 – **بن حيدة محمد**، مرجع نفسه، ص 134.

الفرع الثاني

خصائص الحق في الحياة الخاصة

يعتبر الحق في الحياة الخاصة للأفراد من الحقوق المتصلة اتصالا وثيقا بشخصيتهم، والتي بدورها تنقسم إلى عدة مظاهر منها ما هو متعلق بالجانب المادي للإنسان مثل سلامته الجسدية، ومنها ما هو مرتبط بالجانب المعنوي مثل الحق في الشرف والسمعة، وعليه من هذا المنطلق يمكن لنا دراسة خصائص الحق في الحياة الخاصة من خلال التطرق إلى السرية **(أولا)**، النسبية **(ثانيا)**، حق شخصي **(ثالثا)**، حق من حقوق الانسان **(رابعا)**، حق ملكية خاصة **(خامسا)**:

أولا: السرية

عرف البعض الحياة الخاصة تعريفا إيجابيا مرتبطا بفكرة السرية[427]، حيث إن شراح القانون والقضاء المقارن قد اعترف بالحق في سرية الحياة الخاصة قبل الكلام عن الحق في احترامها[428]. فالحق في الخصوصية أن يضرب الإنسان على نفسه ستارا من السرية، ولتحديد مفهومه ومدى تمتع الخبر أو الواقعة به ظهرت عدة معايير في ذلك:

1- معيار الضرر

يرى أنصار هذا المعيار بأن السر هو كل أمر يضر إفشاءه بسمعة صاحبه أو يمس بكرامته، وأن إفشاءه يعتبر نوعا من السب في حالة وجود مصلحة يحميها، فمتى كان إفشاء الواقعة أو الأمر يشكل ضررا أعتبر سرا[429].

427- « La vie privée est cette partie de la vie n'est pas cosacrée à une actévité publique et ou les tiers n'ont pas accés, afin d'assurer à la personne le secret et la tranquillité auxquels elle a droit », voir: **PHILIPPE Xavier**, Vie privée et nouvelles technologies, annuaire international de justice constitutionnelle, cours international de justice constitutionnelle, 18-2002,2003, p 434.

428- **سليمان بن عبد الله بن سليمان العجلان**، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي دراسة تطبيقية مقارنة، رسالة مقدمة استكمالا لنيل درجة الماجستير في العدالة الجنائية، تخصص سياسة جنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005، ص 46.

429 - **بن حيدة محمد**، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مرجع سابق، ص ص 48-49.

1- معيار المصلحة

يرى أصحاب هذا المعيار بأن السر هو كل مصلحة يحميها القانون، أي بمفهوم آخر أن الشخص صاحب المعلومة أو الواقعة إذا أراد أن يحتفظ بهذه الأخيرة بمثابة سر، فمعناه أن هناك مصلحة له في ذلك، فإذا تم الاعتداء عليها يتدخل القانون من أجل فرض التدابير اللازمة لحمايتها[430].

2- معيار الإرادة

يعد سرا إذا أراد من أودعه كتمانه، فالسر يتوقف على إرادة صاحبه في أن ينحصر نطاق العلم بالواقعة في أشخاص محدودين، فالشرط الجوهري لنظرية الإرادة هو علم صاحب السر وسواء كانت هذه الإرادة ضمنية أو صريحة[431]، وهو ما ذهب إليه المشرع الجزائري من خلال المادة 301 الفقرة الأولى من قانون العقوبات التي تنص: "**يعاقب بالحبس....الأطباء والجراحون والصيادلة والقابلات وجميع الاشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك**".

ثانيا: النسبية

تعد النسبية من أهم خصائص الخصوصية أو الحياة الخاصة، يتأكد ذلك من خلال اختلافها من مكان إلى آخر ومن زمان إلى آخر، ويضيق نطاقها ويتسع من وقت إلى آخر، كما تتضح النسبية باختلاف الأشخاص، من شخص عادي إلى شخص مشهور أو شخصية عامة، ولا شك في أن النسبية يعزى إليها عدم اتفاق الفقه على مفهوم محدد لماهية الحق في الحياة الخاصة، وإن تم الاتفاق على بعض عناصره أو نطاقه[432].

---

[430]- **CHEVALIER Michael**, Les enjeux juridiques concernant les nouveaux modèles d'affaires basés sur la commercialisation des données, Mémoire présenté en vue de l'obtention du grade de L L M en droit des technologies de l'information, université de montréal, 2015, p p 22-23.

[431] – **بن حيدة محمد**، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"مرجع سابق، ص ص 49-50.

[432]– **محمد نور الدين**، «**الحماية الجنائية للحق في خصوصية المكالمات الهاتفية دراسة تحليلية نقدية للقنونين الكويتي والإماراتي**»، مجلة دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد 43، ملحق 04، سنة 2016، ص 1691.

ثالثا: حق شخصي

يذهب الرأي الراجح في فرنسا حديثا، إلى اعتبار الحق في الحياة الخاصة من قبيل الحقوق الشخصية ولو أن نظرية الحقوق اللصيقة بالشخصية لم تجد مكانها في كتابات الفقه إلا مع مطلع هذا القرن، حيث كان تحليل المفهوم القانوني لهذه الفكرة محلا للعديد من الدراسات الهامة[433].

يعرف الفقه الحقوق اللصيقة بالشخصية على أنها: "الحقوق التي تنصب على مقومات وعناصر الشخصية في مختلف مظاهرها الطبيعية والمعنوية والفردية والاجتماعية، بحيث تعبر عما للشخص من سلطات مختلفة واردة على المقومات وعلى تلك العناصر بقصد تنمية هذه الشخصية وحمايتها من اعتداء الغير"، وتشمل الحقوق الشخصية حق الفرد في كماله البدني، كما تشمل أيضا حقه في كماله المعنوي أي ما يتعلق بذاتية الفرد، لذا فهي تنقسم إلى قسمين[434]:

الأول: الحقوق الواردة على المقومات المادية للشخصية، أي تلك التي تستهدف الكيان المادي للإنسان كالحق في سلامة الجسم والحق في الحياة، كما تهدف إلى تأكيد حماية الجسم سواء في مواجهة الغير أو في مواجهة الشخص نفسه حيا كان أو ميتا.

الثاني: الحقوق التي ترمي إلى حماية المقومات المعنوية للإنسان، فشخصية المرء ليست منحصرة في كيانه المادي فقط، وإنما تشمل أيضا بعض المقومات المعنوية مثل حق الإنسان في السمعة والشرف والاعتبار والمعتقدات، وكذلك مشاعره ورغباته.

---

[433]– أورده : **طارق عثمان**، الحماية الجنائية للحياة الخاصة عبر الإنترنت دراسة مقارنة، مذكرة مقدمة لنيل شهادة الماجستير ، فرع القانون الجنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2006–2007، ص 20.

[434] – **طارق عثمان**، مرجع سابق، ص 20.

رابعا: حق من حقوق الإنسان

ترتبط مجموعة حقوق الإنسان بكيان الشخص وآدميته، بانعدامها تنعدم صفته الإنسانية، والحق في الخصوصية هو نوع من هذه الحقوق وأحد مقوماتها الأساسية فوجود هذا الحق والمحافظة عليه يضمن العيش في سكينة وأمان[435].

خامسا: حق ملكية خاصة

يعتبر الإنسان مالكا لحرمة حياته الخاصة ومن ثم لا يجوز الاعتداء على خصوصياته بأي صورة من صور التعدي، كما يستطيع التصرف في حياته الخاصة كيفما يشاء.

تعتمد هذه الفكرة على النظرية التي تقول بأن للإنسان حق ملكية على جسمه، ولما كانت الصورة تعتبر جزء لا يتجزأ من جسم الإنسان، فقد أمكن اعتبار الحق في الصورة من قبيل الحق في الملكية، فالشكل (الصورة) يتكون شأنه شأن الجسم من مجموعة من العظام والجلد والأوردة والعضلات، وهذه الأجزاء مجتمعة تعطي كل شخص شكلا خاصا يتميز به عن غيره من البشر[436].

المطلب الثاني

الاعتداء على الحق في الحياة الخاصة عبر الإنترنت

رغم الحماية التي أقرتها مختلف التشريعات الدولية والوطنية للحق في الحياة الخاصة، إلا أن الاعتداء عليه هذا الحق يعرف منحى متصاعد ومتسارع، خاصة في مجال شبكات الاتصال، حيث أفرزت هذه الشبكات وخصوصا شبكة الإنترنت مناخا مثاليا لمختلف الاعتداءات على كل ما يرتبط بالحق في الحياة الخاصة للأفراد مثل المعطيات والبيانات والمعلومات المتعلقة بهم.

---

[435] – **عيدة بلعابد**، «**الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية**»، مجلة آفاق علمية، جامعة تمنراست، المجلد 11، العدد 01، سنة 2019، ص 144.

[436] – **عاقلي فضيلة**، مرجع سابق، ص 100.

اتخذت الاعتداءات على الحق في الحياة الخاصة عبر الشبكة العالمية للإنترنت طرقا عديدة منها ما يتعلق بالمراسلات الشخصية خاصة عبر البريد الإلكتروني، ومنها ما يتعلق بالمساس بسمعة وشرف الأشخاص عبر المواقع التي توفرهم الشبكة **(فرع أول)**.

تعددت الأسباب التي أدت إلى تزايد الاعتداءات على الحق في الحياة الخاصة عبر الشبكة العالمية للإنترنت، وذلك راجع للخصوصيات التي تتميز بها هذه الشبكة، حيث أن التجميع السهل للمعلومات عبر الحواسيب المترابطة عبرها تعد من الأسباب التي سهلت الاعتداء على هذا الحق **(فرع ثان)**.

الفرع الأول

صور الاعتداء على الحق في الحياة الخاصة عبر الإنترنت

أخذت الاعتداءات على الحق في الحياة الخاصة صورا عديدة، فكما أن لهذا الحق مظاهر كثيرة ومختلفة مثل حرمة الاعتبار والشرف والصورة...الخ، تعددت صور الاعتداء عليه عن طريق ما تقدمه شبكة الإنترنت من تسهيلات جعلت من المجرمين باستطاعتهم الحصول على مختلف البيانات والمعطيات المتعلقة بالأشخاص ليستعملوها بطرق غير مشروعة، وسوف نتطرق إلى ذلك من خلال تبيين الاعتداءات ضد سرية البيانات الشخصية **(أولا)**، اعتداءات ضد سلامة البيانات الشخصية **(ثانيا)**، التنصت على الاتصالات **(ثالثا)**، اعتراض المراسلات الإلكترونية **(رابعا)**، جريمة نشر أخبار أو صور أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية **(خامسا)**، ثم إلى جريمة الجمع والتخزين غير المشروع للبيانات الشخصية **(سادسا)**:

أولا: اعتداءات ضد سرية البيانات الشخصية

تأخذ الاعتداءات ضد سرية البيانات الشخصية عدة صور نذكر منها:

1- جريمة الافشاء غير المشروع للبيانات الشخصية

نص المشرع على هذه الجنحة في المادتين 46 و85 من قانون الإجراءات الجزائية، حيث تعاقبان بنفس عقوبة الحبس والغرامة على إفشاء الوثائق المتحصلة من التفتيش الذي يقوم به ضباط الشرطة القضائية والتفتيش الذي يتولاه قضاة التحقيق[437]

فقد نصت المادة 46 المتعلقة بصلاحية الشرطة القضائية على ردع "**كل من أفشى مستندا ناتجا من التفتيش أو أطلع عليه شخصا لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه، ما لم تدع ضرورات التحقيق إلى غير ذلك**"، ومن جهتها نصت المادة 85 الواردة بشأن مهام قاضي التحقيق، في ألفاظ ومعان مقاربة لنص المادة 46، بنصها: "**كل من أفشى أو أذاع مستندا متحصلا من تفتيش شخص لا صفة له قانونا في الاطلاع عليه وكان ذلك بغير إذن من المتهم أو من خلفه أو الموقع بامضائه على المستند أو الشخص المرسل إليه، وكذلك كل من استغل ما وصل إلى علمه منه ما لم يكن ذلك من ضرورات التحقيق القضائي**".

الظاهر من هذين النصين أن ردع هذه الجنحة يولي مكانة كبرى لهدف حماية الحياة الخاصة، دون استبعاد هدف هام آخر يهدف إليه هذا الردع في نفس الوقت، هو سرية البحث والتحقيق[438].

نص كذلك المشرّع على هذه الجريمة بمقتضى القانون رقم 18-05 المتضمن قواعد التجارة الإلكترونية وذلك في المادة 26 على أنه: "**ينبغي للمورد الإلكتروني الذي يقوم بجمع المعطيات ذات الطابع الشخصي ويشكل ملفات الزبائن المحتملين، ألا يجمع إلا البيانات الضرورية لإبرام المعاملات التجارية، كما يجب عليه:**

- الحصول على موافقة المستهلكين الإلكترونيين قبل جمع البيانات.

---

[437]- أنظر المادة 46 والمادة 85 من قانون الإجراءات الجزائية.

[438] - **نويري عبد العزيز**، الحماية الجزائية للحياة الخاصة -دراسة مقارنة-، أطروحة لنيل شهادة دكتوراه علوم، شعبة القانون الجنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2010-2011، ص 290.

- ضمان أمن نظم المعلومات وسرية البيانات.

الالتزام بالأحكام القانونية والتنظيمية المعمول بها في هذا المجال"

كما نص في المادة 31 من الفصل السابع المتعلق بالإشهار الإلكتروني حيث تنص على أنّه: "**يمنع الاستبيان المباشر اعتمادا على إرسال الرسائل عن طريق الاتصالات الإلكترونية باستعمال معلومات شخص طبيعي، بأي شكل من الأشكال، لم يبد موافقته المسبقة لتلقي استبيانات مباشرة عن طريق الاتصال الإلكتروني**"

2- جريمة معالجة بيانات لأشخاص سبق تصنيفهم

يتضمن الركن المادي في هذه الجريمة صورتين: فأما الصورة الأولى تتعلق بمعالجة بيانات خاصة بأشخاص سبق تصنيفهم من حيث أصولهم العرقية او معتقداتهم السياسية أو الفلسفية أو الدينية وكذلك الانتماءات النقابية لهم، وكذلك ما يتعلق بأخلاقهم، أما الصورة الثانية للركن المادي في هذه الجريمة فتتعلق بمعالجة بيانات لأشخاص سبق تصنيفهم باعتبار الجرائم التي ارتكبوها أو أحكام الإدانة أو التدابير التي سبق صدورها أو اتخاذها ضدهم.

يعود السبب في تجريم هذه الأفعال، استبعاد أي تمييز يقوم على الأصل العرقي أو الدين أو السياسة الأمر الذي يخل بمبدأ المساواة، وذلك من أجل حماية الفكر والرأي والتعبير والعقيدة والانتماء النقابي، فضلا عن أن هذه المسائل تدخل في نطاق الحياة الخاصة –بمعناها الواسع– والتي يحظر معالجة البيانات الخاصة بها.

لا يجوز حفظ أو معالجة المعلومات الإسمية المتعلقة بالجرائم والعقوبات إلا بالنسبة للحاسب الآلي التابع للجهات القضائية أو السلطات العامة، وذلك في حدود اختصاصاتها القانونية، ولذلك يحظر على غير الجهات السابقة معالجة مثل هذه البيانات في الحاسب الآلي الخاص، والعلة في هذا الحظر هي حماية سمعة واعتبار الشخص، وهذا الحظر يتفق إلى حد ما مع قانون صحيفة الحالة الجنائية الذي ينظم أي الجرائم يظهر كسابقة في صحيفة الحالة الجنائية وأيها لا يظهر في هذه الصحيفة[439].

[439] – **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 79–80.

ثانيا: اعتداءات ضد سلامة البيانات الشخصية

قد يرتكب الشخص المعالج للبيانات الشخصية للأفراد اعتداءات على هذه الأخيرة لهذا اعتبرها المشرع الجزائري جرائم معاقب عليها بمقتضى القانون ويمكن ذكرها في مجملها في: جريمة جمع أو معالجة بيانات شخصية بدون ترخيص وجريمة الإنحراف عن الغرض وجريمةالحفظ غير المشروع للبيانات الشخصية.

أ- جريمة جمع أو معالجة بيانات شخصية بدون ترخيص

فيما يتعلق بالبيانات الشخصية الحساسة[440]، لا يكفي التصريح، بل غالبا ما تفرض إجراءات أكثر تعقيدا، كأن يفترض الحصول على إذن خاص، من السلطة المعنية بحماية البيانات، ويفرض هذا الإجراء الإداري الخاص، بناء لطبيعة البيانات (جينية، أحكام جزائية...)، أو بسبب كون الأهداف محددة وخاصة (حرمان بعض الأشخاص من حق ما)، وأما بسبب النية في نقل البيانات إلى خارج الحدود الوطنية، ويمكن أن يصدر هذا الإذن عن الهيئة أو بموجب قرارات وزارية، أو عن هيئة قضائية، ولكن دائما بعد إعطاء الهيئة المختصة رأيها.

تقر بعض القوانين إجراءات إدارية مختلفة باختلاف طبيعة الجهة مقدمة طلب الحصول على إذن، كأن تكون من القطاع العام، أو القطاع الخاص، إلا أنها تتلاقى على ضرورة تشديد شروط المعالجة وإعلام أصحاب البيانات نسبة إلى المخاطر التي تمثلها، على مستوى الحقوق والحريات.

تذهب كذلك بعض القوانين إلى إقرار عقوبات جزائية على عدم التقيد بالإجراءات الإدارية، دون التمييز بين عدم التقيد المقصود أو غير المقصود، كأن يكون المسؤول عن المعالجة قد نسي التصريح، أو أن يكون قد قصد عدم القيام به، وكان الاجتهاد الفرنسي قد

[440]- **MATTATIA Fabrice**, internet et les réseaux sociaux : que dit la loi ?, op-cit, p 63.

اتخذ عددا من القرارات في هذا الاتجاه معتبرا أن مجرد عدم إتمام الاجراءات المفروضة سبب كاف للإدانة[441].

عالج المشرع الجزائري هذه الجريمة بمقتضى المادة 14 من القانون رقم 18-07 المتضمن حماية المعطيات ذات الطابع الشخصي، فطبقا لنص المادة السالفة الذكر أن كل معالجة لمعطيات ذات طابع شخصي يجب أن تكون بمقتضى طلب مقدم إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مع احترام البنود المذكورة في المادة المذكورة أعلاه وأي تخلف لهذا الشرط يكون الشخص القائم بالمعالجة لهذه المعطيات قد ارتكب جريمة معالجة معطيات شخصية دون ترخيص[442].

ب- جريمة الانحراف عن الغرض

تتخذ هذه الجريمة صورة استخدام البيانات التي تم جمعها عن الأفراد في غير الغرض المخصص لها[443]، أو استخدامها في غير ما يلائم صاحبها أو يوافق عليه أو دون رضاه، بالإضافة إلى جمع بيانات دون سبب مشروع، حيث يعد انتهاكا للحياة الخاصة وتهديدا للحريات الفردية، وهذا ما يفرض ضرورة وضع التشريعات الخاصة لحماية البيانات الشخصية وضمان عدم اساءة استخدامها في الغرض المعدة له[444].

تعد هذه الجريمة بدورها من الجرائم العمدية التي تقوم بالقصد الجنائي العام، بعنصريه العلم والإرادة، ومن ثم لا يعاقب عنها بوصف الخطأ، ومتى توافر للجريمة ركنيها المادي والمعنوي على نحو المتقدم عوقب الجاني طبقا لنص المادة 394 مكرر 2 من قانون العقوبات الجزائري بالحبس من شهرين لثلاث سنوات والغرامة من مليون إلى 10 مليون دينار جزائري[445].

---

[441] – **منى الأشقر جبور**، **محمود جبور**، مرجع سابق، ص 98.

[442]– أنظر نص المادة 14 من قانون رقم 18-07 مؤرخ في 10 جوان 2018، يتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشحصي، ج ر، عدد 34، صادر في 10 جوان 2018.

[443]- **PRADEL Jean**, Les infractions relatives à l'informatique, revue internationale de droit comparé, vol 42, n° 2, avril-juin 1990, p 820, dispnible en ligne à l'adresse: https://www.persee.fr/doc/ridc_0035-3337_1990_num_42_2_1994

[444] – **طارق عثمان**، الحماية الجنائية للحياة الخاصة عبر الإنترنت دراسة مقارنة، مرجع سابق، ص 85.

[445] – نقلا عن **حمودي ناصر**، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 114.

ت- جريمة الحفظ غير المشروع للبيانات الشخصية

يقصد به إمساك الجاني واحتجازه لتسجيل مستند لشخص أو أشخاص آخرين عن قصد مع علمه بمحتواه، مع ضرورة أن يكون قد تم الحصول على التسجيل أو المستند عن طريق الاستماع أو التسجيل أو نقل الأحاديث الخاصة أو التقاط أو تسجيل أو نقل صورة المجني عليه، المعتدى على حرمة حياته الخاصة في مختلف هذه الأشكال، وقد يحتفظ المعتدي بالبيانات الشخصية –المستندات أو التسجيلات– لحسابه الخاص أم لحساب غيره.

فإذا كان الاحتفاظ لحسابه الخاص، فلابد أن يكون له هدف من وراء ذلك، وهو إما معنوي كالانتقام من المعتدى عليه، او مادي وهو الحصول على مقابل مالي، وفي هذه الحالة الأخيرة تكون الجنحة إما بمبادرة منه أو بتحريض من الغير الذي يعرض مبالغ مغرية، ولا يتصور أن يعلم المعتد عليه بهذا الفعل، والمعتدي يكون قد قام به بطريق غير قانوني.

أما إذا كان الاحتفاظ لحساب الغير، في هذه الحالة يقوم المعتدي بالتقاط البيانات الشخصية أو تسجيلها ثم يعهد بها لشخص آخر يحتفظ بها، فيكون هذا الأخير مودعا لديه إما حسن النية –وهي حالات نادرة قد تعفيه من المسؤولية– أو شريكا –وهي الحالات الغالبة– تجعله مسؤولا مسؤولية كاملة تماما كالفاعل الأصلي، وذلك وفقا لما يقرره قانون العقوبات، والمشاركة في ارتكاب الجنحة قد تكون معتادة بين الفاعلين الأصلي والشريك وقد تكون عرضية[446].

ثالثا: التنصت على الاتصالات

يعتبر محل جريمة التنصت كل صوت له دلالة التعبير عن معنى أو مجموعة من المعاني والأفكار المترابطة[447]، ويستوي أن يكون دلالة الحديث مفهومة للناس كافة أو لفئة محدد منهم، مؤدى ذلك أنه لايشترط لغة معينة يجري بها الحديث، كالحديث الذي يتم

---

[446] – **بشاتن صفية**، الحماية القانونية للحياة الخاصة دراسة مقارنة، رسالة لنيل شهادة دكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012، ص 374.

[447]- **MAITROT DE LA MOTTE Alexandre**, Le droit au respect de la vie priveé, groupe d'études société d'information et vie privée, p 264. Disponible sur le site: http://asmp.fr

بلغة أجنبية أو باستعمال الشيفرة، وينتفي عن الصوت وصف الحديث كما لو كان لحنا موسيقيا أو صيحات ليس لها دلالات لغوية.

والأحاديث أسلوب من أساليب الحياة الخاصة للناس، تستمد حرمتها من حرمة الحياة الخاصة لأصحابها، فيها يهدأ المتحدث لمحدثه، سواء بطريق مباشر أم بواسطة من الوسائط الإلكترونية دون حرج أو خوف من تنصت غيره، وفي مأمن من فضول استراق السمع.

يحرص الأشخاص على سرية محادثاتهم، ويعمل كل شخص بحذر حتى لا يتم البوح بأسراره إلى غيره دون علمه، إلا أن تطور وسائل التنصت الحديثة جعلت من السهل استراق السمع والنظر إلى خصوصيات شخص آخر، مما جعل أغلب التشريعات تجرم انتهاك سرية المحادثات الخاصة، فاختلفت التشريعات في تحديد معيار معين للتمييز بين ما يعد حديثا خاصا، وما يعد حديثا عاما، بعض التشريعات أخذت بطبيعة المكان الذي يدور فيه الحديث أي التفرقة بين المكان الخاص والمكان العام، وبعضها اعتمد على طبيعة الحديث ذاته[448].

رابعا: اعتراض المراسلات الإلكترونية

يعرفها البعض بأنها عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب الجريمة[449].

وتتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات، والتي هي عبارة عن بيانات قابلة للانتاج أو التوزيع أو التخزين أو الإستقبال أو العرض.

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني فيكون الثاني بطلب أو برضا

---

[448] – **محمد أمين الخرشة، إبراهيم سليمان القطاوية**، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الإماراتي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 13، العدد 01، سنة 2016، ص ص 68-69، أنظر كذلك:

- **JEAN-MEIRE Caroline**, Les nouvelles technologies et la lutte contre la délinquance: regards croisés France/ryaume-uni, thèse pour le doctorat en droit, école de droit de la sorbonne, université de Paris 01 Panthéon-Sorbonne, 2016, p 386.

[449] – **بولافة سامية، ساسي مبروك**، مرجع سابق، ص 396.

صاحب الشأن ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك[450].

خامسا: جريمة نشر أخبار أو صور أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية[451]

لتتحقق هذه الجنحة لا بد من:

1- **النشاط إجرامي:** وتتحقق صوره التي أوردها المشرع في المادة 303 مكرر 1 من قانون العقوبات[452] في:

أ- **الاحتفاظ بالتسجيل أو الصور أو الوثائق:**

ويعتبر هذا الفعل جنحة مستمرة، لذلك لا يسري في شأنه التقادم إلا من توقفه وانقطاعه، ويصلح هذا الحكم في شأن الاحتفاظ بالمعلومات المتحصل عليها عبر الإنترنت.

وحتى يعتبر هذا الفعل جنحة، لا بد أن يكون الجاني قد تحصل على موضوعه بالكيفية المنصوص عليها في المادة 303 مكرر من قانون العقوبات، وهي التقاط أو تسجيل أو نقل إما الأحاديث أو المكالمات الخاصة أو الصورة.

---

[450] – **عبد الرحمان خلفي**، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس، الجزائر، 2015، ص 101.

[451]– الأخبار: هي المعلومات والوقائع التي تتعلق بأسرار الحياة الخاصة للأفراد، وتقوم الجريمة سواء كانت هذه المعلومات تمس الحياة الخاصة للمجني عليه بصورة واضحة ومباشرة أو على سبيل التلميح.

الصورة: هي امتداد ضوئي لجسم الشخص، ولا تعبر عن فكرة ولا دلالة لها غير أنها تشير إلى شخصية صاحبها

التعليقات: هي التي تتم من الآخرين تجاه المجني عليه بشرط أن تتعلق بأسرار الحياة الخاصة للمجني عليه، وسواء كانت هذه الأخبار أو الصور أو التعليقات التي تتصل بأسرار الحياة الخاصة أو العائلية للأفراد تمس الحياة الخاصة للمجني عليه بصورة واضحة ومباشرة أو على سبيل التلميح، وتقوم هذه الجريمة حتى لو كانت هذه الاخبار أو الصور أو التعليقات صحيحة. أنظر في ذلك: **محمد أمين الخرشة، إبراهيم سليمان القطاوية**، المرجع السابق، ص 81.

[452]– ورد نص المادة على النحو التالي: "**يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون**".

ب- الوضع في متناول الجمهور:

يبدأ الجاني في هذه المرحلة في تنفيذ الجنحة فعلا لأنها هي التي تسمح بعلم عدد من الأشخاص بمحتوى التسجيل أو الوثائق أو الصور[453]، ولا يهم عدد الأشخاص من الجمهور الذين يطلعون على المنتوج، وذلك أن إذاعته قد تكون عامة لعلم عدد غير محدود من الأشخاص بمحتواه، وقد تكون خاصة لأنها معلنة على عدد خاص ضيق، وقد أكد المشرع على هذا المعنى حين نص في المادة 303 مكرر 1 من قانون العقوبات على أنه: "**توضع في متناول الجمهور أو الغير**".

ت- السماح بالوضع في متناول الجمهور:

يفترض في هذه الجنحة أن يقوم بها أكثر من فاعل واحد، إلا أن ذلك لا يعني أن واحدا أو بعضا من المعتدي على حرمة الحياة الخاصة للغير بهذه الصورة يقوم بالفعل بصفته شريكا أو شركاء في الجنحة، وإنما تكون مسؤولية الجميع مسؤولية فاعلين أصليين وفقا للمادة 303 مكرر 1 من قانون العقوبات الجزائري.

ث- استخدام التسجيل أو الصور أو الوثائق:

تعتبر الحالة الغالبة من حالات ارتكاب الجنحة، إذ يهدف المعتدي على حرمة الحياة الخاصة للغير بهذا الفعل المجرم إلى تحقيق هدف معين، عاما كان أم خاصا ولغرض مالي أو معنوي[454].

2- عدم رضاء الضحية بهذه الأفعال

لا يكفي لتحقق الركن المادي لهذه الجريمة أن يلتقط الجاني أو يسجل أو ينقل صورة للمجني عليه وهو في مكان خاص، وإنما يجب علاوة على ذلك أن لا يكون صاحب الشأن راض بهذا الالتقاط أو النقل أو التسجيل فرضاء صاحب الشأن يحول دون تحقق الركن المادي للجريمة كونه يزيل عن التدخل في الحياة الخاصة صفة عدم المشروعية، ولكي ينتج الرضا أثره ينبغي أن يكون صحيحا أي صادرا عن إرادة حرة مدركة غير مشوبة بأي عيب

---

[453]- **CHILSTEIN David**, op-cit, p 579.

[454]- **بشاتن صفية**، مرجع سابق، ص 407.

من عيوب الرضا، وأن يكون الرضا سابقا على وقوع السلوك الإجرامي أو ملازما له فالرضا اللاحق لا يمحو الجريمة، كما يجب أن يكون الرضا خاصا ومحددا ويقتصر على الوقائع والموضوع محل الرضاء ولا يتعداها إلى غيرها[455].

3- توفر قصد الإضرار بالضحية

يؤكد الفقه أن جريمة نشر أخبار أو صور أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية من الجرائم العمدية التي يأخذ الركن المعنوي فيها صورة القصد الجنائي، بعنصريه العلم والإرادة، بمعنى علم الجاني بالصفة الخاصة للمحادثة محل الجريمة، وأن من شأن الجهاز الذي يستعمله أن ينقل الحديث أو يسجله، مع اتجاه إرادته إلى ارتكاب الفعل وتحقيق النتيجة التي يبغيها وهي الوصول إلى المحادثة أو الاحتفاظ بها أو تحويلها لغير أطرافها[456].

سادسا: جريمة الجمع والتخزين غير المشروع للبيانات الشخصية

يقصد بعملية جمع وتخزين البيانات الشخصية قيام الفاعل بكل أفعال من شأنها تحقيق التقاط وتسجيل أو احتفاظ أو تخزين أو معالجة للبيانات باستعمال نظام معلوماتي أو الحاسوب أو بنوك المعلومات، وتلحق صفة عدم المشروعية البيانات الشخصية من جراء الطرق الملتوية للحصول على البيانات أو مضمون وطبيعة البيانات ذاتها، كما إذا كانت حساسة لا يجوز تداولها قانونا، أو لا يوجد مبرر مشروع لجمعها أو تم تجاوز المدة القانونية للاحتفاظ بها أو دون موافقة صاحبها[457].

يتمثل فعل الانتهاك للحق في الحياة الخاصة في هذا المعنى عملية جمع وتخزين بيانات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو

---

[455]- **عثمان طارق، «حماية الأطفال من الاستغلال في المواد الإباحية عبر الإنترنت في التشريع الجزائري»**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد الثالث عشر، د.س.ن، ص ص 433-434.

[456]- **محمد نور الدين**، مرجع سابق ص 1696. أنظر كذلك:

- **PRADEL Jean,** op-cit, p 819

[457] - **بشان عبد النور**، مرجع سابق، ص 274. أنظر كذلك:

- **MATTATIA Fabrice**, Le droit des données personnelles, 2e édition, Editons Eyrolles, Paris, 2016, p 162.

التخزين صفته غير المشروعة إمّا من الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات والمعلومات، أو من طبيعة مضمونها[458].

عاقب المشرع الجزائري على هذه الجريمة بمقتضى القانون رقم 18-07 المتضمن حماية المعطيات ذات الطابع الشخصي طبقا لنص المادة 59 حيث تنص على أنه: "يعاقب كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة".

الفرع الثاني

أسباب الاعتداء على الحق في الحياة الخاصة عبر الإنترنت

أفرز الحاسب الآلي العديد من التقنيات التي لم يكن يعرفها الإنسان من قبل، الأمر الذي أدى إلى التهافت في استعماله نظرا لما يقدمه من خدمات مثل الذاكرة الواسعة لهذ الأخير والتي تسمح بتجميع كم هائل من المعلومات، وما زاد كثرة الاعتماد عليه ترابطه عن طريق شبكات اتصالية ضخمة أبرزها شبكة الإنترنت التي سمحت بإنشاء بنوك للمعلومات وإرسال هذه الأخيرة وتشعبها عبرها، غير أن هذه المزايا التي قدمها الحاسوب وشبكاته كان له أثر عكسي، حيث أعتبرت من بين أهم الأسباب التي أدت إلى الاعتداء عل الحق في الحياة الخاصة، وسوف نتطرق لذلك من خلال تبيين لا محدودية ذاكرة الحاسب **(أولا)**، مخاطر الثقة في الحاسوب **(ثانيا)**، مخاطر الثقة في بنوك المعلومات **(ثالثا)**، الجمع الكبير للبيانات **(رابعا)**، تشعب البيانات **(خامسا)**، النقل الرقمي للبيانات **(سادسا)**، بنوك ومراكز المعلومات الشخصية المنشئة من قبل الدول **(سابعا)**، المعلومات غير الدقيقة وغير المكتملة **(ثامنا)**.

[458]- **نهلا عبد القادر المومني**، مرجع سابق، ص 174.

أولا: لا محدودية ذاكرة الحاسب

يتمتع الحاسوب الآلي بقدرة فائقة على حفظ واسترجاع قدر كبير من البيانات عن مختلف أوجه الحياة سواء عن الأفراد أو الجماعات، الأمر الذي يجعل الحصول على هذه البيانات أمرا يسيرا، بعد أن كان من الصعب بل من المستحيل في بعض الأحيان الحصول على معلومات كاملة عن حياة الشخص بهذه السرعة والسهولة، مما أضحى يهدد الحياة الخاصة للأفراد وحرياتهم ويؤدي إلى ازدياد الحاجة إلى السرية كي يتسنى حماية الحياة الخاصة من خطر العلانية.

قبل ظهور الحاسوب الآلي كانت البيانات الشخصية توضع في ملفات ورقية، وكانت بالطبيعة محدودة العدد وموزعة في أماكن عدة، أما بعد ظهوره واستخدامه كبنوك للمعلومات فقد أمكن تجميع عدد أكبر من البيانات الشخصية للأفراد، كما أن سهولة الاتصال بين الحاسبات الآلية التي تتبع نظاما واحدا قضى على مسألة تفرق البيانات الشخصية وتشتتها، ولقد كان هذا التشتت في حد ذاته ضمانة للحياة الخاصة للأفراد[459].

ثانيا: مخاطر الثقة في الحواسيب

يقصد بها أن الحاسوب هو الذي يتخذ القرارات الهامة التي تهم الأشخاص وتؤثر مباشرة على مساراتهم، نظرا للثقة التامة الممنوحة لبنوك المعلومات، وهذا ما يكون له الأثر البالغ على الحق في حرمة الحياة الخاصة، ذلك أن الاعتماد على جهاز لعقلنة الخيارات يعرض مفهوم الديموقراطية للخطر، والسبب هو أن الخيارات المتخذة وفقا لمبادئ حسابية تستبعد الحالة النفسية والاجتماعية للفرد، وحتى إذا أدرجت هذه الاعتبارات، كعامل مساعد في المعلومات التي يغذّي بها الحاسوب، فيجب أن لا تكون إلا ذات أهمية ثانوية[460].

---

[459]– **طارق عثمان**، الحماية الجنائية للحياة الخاصة عبر الإنترنت دراسة مقارنة، مرجع سابق، ص 83.

[460]– يقول Robert M.Bowie: "إن التقنوقراطية، وهي تملك الكمبيوتورات قد تصبح على درجة بالغة من القوة بحيث تحبس الحياة الخاصة داخل حدود ضيقة، وتكيف حياة الفرد وأسرته بهذه الأجهزة في اللحظة التي تكون لها في ذلك مصلحة اقتصادية أو اجتماعية، وبذلك يصبح الإنسان معاملا كالأرقام في جهاز مسلوب الإرادة في اتخاذ قراراته بوعي واستغلال، ومفرغا أخيرا من شخصيته"، نقلا عن: **بن سعيد صبرينة**، مرجع سابق، ص 135.

تمكن هذه القدرة الهائلة للحاسبات الآلية من مزج البيانات المختلفة المتعلقة بالشخص وتحليلها، بحيث تعطي في النهاية صورة كاملة عن الشخصية وجوانبها المختلفة، وتزداد الخطورة إذا تمت معالجة البيانات من أجل استخلاص حكم أو تقييم للشخصية من واقع ما وضع داخل الحاسب الآلي من بيانات، والتوصل إلى نتائج انطلاقا من البيانات المتفرقة من دون دراسة شخصية الإنسان محل التقويم، مما يهدد باستخلاص نتائج غير دقيقة سواء من حيث سلوك الشخص أو صفاته أو سمعته، كما قد يؤدي إلى تلويث شخصيته[461].

ثانيا: مخاطر الثقة في بنوك المعلومات

يقصد بمصطلح بنك المعلومات، تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة[462].

تحتوي مثل هذه البنوك على معلومات مالية أو وطنية أو أمنية...الخ، ويتم جمعها من خلال الأخبار والأنباء والبيانات، ثم يتم تسجيلها على شرائط أو أسطوانات ثم يتم إدخالها إلى الحاسب الآلي وتخزينها[463].

تبرز خطورة الأنظمة المعلوماتية وبنوك المعلومات على الحق في الحياة الخاصة بشكل خاص من الثقة الكاملة للأفراد في نتائج المعالجة الآلية التي يستخلصها الحاسوب من المعلومات الإسمية المخزنة فيه[464]، وتكون هذه الخطورة على الحق في الخصوصية أكثر وضوحا إذا تمت معالجة البيانات من أجل استخلاص حكم أو تقييم للشخصية من واقع ما غذي به الحاسوب من معلومات، فمن أخطر ما يهدد الانسان استخلاص أحكام قيمية على أساس بيانات دون دراسة شخصية الإنسان نفسه محل التقييم الأمر الذي ينتج عنه

---

[461]– **طارق عثمان**، الحماية الجنائية للحياة الخاصة عبر الإنترنت دراسة مقارنة، مرجع سابق، 83.

[462]- **Métille Sylvain,** Mesures technique de surveillance et respect des droits fondamentaux en particulier dans le cadre de l'instruction pénale et du renseignement, op-cit, p p 73-74.

[463]– **محمود أحمد عبابنة**، جرائم الحاسوب وأبعدها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 74.

[464]- **VALLET Caroline,** op-cit, p 174.

استخلاص نتائج غير دقيقة عن سلوكه أو صفاته أو سمعته مما يؤدي إلى المساس به[465].

تظهر كذلك خطورة بنوك المعلومات على الحياة الخاصة عند حدوث أخطاء، سواء كانت بشرية متمثلة في تغذية الحاسوب بالمعلومات أو عند إعادة تنظيمها أو تقويمها أو كانت أخطاء تقنية ناتجة عن عيوب ميكانيكية، كعيب فني في الجهاز أو عيوب كهربائية كاختلال الضغط في الكهرباء[466].

ثالثا: الجمع الكبير للبيانات

شهدت الإنترنت نماء التوجه نحو جمع البيانات[467] المتوفرة في العالم الحقيقي باعتبارها تصبح تصبح أكثر سهولة في بيئة الإنترنت من حيث قدرة الوصول إليها، وأكثر ملاءمة للتبويب بسبب تقنيات الحوسبة، وتصبح أسهل للتبادل في ضوء وسائل تبادل المعلومات بكل أشكالها التي أتاحتها الإنترنت وبرمجيات التصفح والتبادل والنقل.

فالبيئة التي تمر عبرها رحلة البيانات المتبادلة تغيرت بسبب الإنترنت، وترك الأفراد خلفهم الوسائل التقليدية في الوصول للمعلومات وأصبح اعتمادهم أكثر فأكثر على الإنترنت، لأن هذه الأخيرة مصدر غني بالمعلومات حول كل شيء، وفي نطاق مسائل الخصوصية

---

[465]– **نهلا عبد القادر المومني**، مرجع سابق، ص 172.

[466]– **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004، ص 65.

[467]– توصلت دراسة أجرتها إحدى جمعيات المستهلكين في أمريكا إلى أن شركات عدة جمعت معلومات شخصية جدا وغير ضرورية عن المستهلكين، وقالت هذه الجمعية أن احترام الحياة الشخصية حق معترف به كحق أساسي من حقوق الإنسان لكن مع ذلك اكتشفنا أن كثير من الشركات جمعت كمًّا وافرا من المعلومات الشخصية جدا وغير الضرورية بخصوص المستهلكين، وأكدت أن ثلثي المواقع الأمريكية التي شملتها الدراسة ما زالت تطلب من مستخدمي الشبكة تزويدها بمعلومات شخصية، ثم تقوم بعد ذلك باستخدام هذه المعلومات كما هي أو خارج إطارها، أنظر في ذلك: **محمد عبيد الكعبي**، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهظة العربية، القاهرة، د.س.ش، ص 150.

تحديدا فإن المعلومات عن الأفراد وعاداتهم وهوياتهم وسلوكياتهم وآرائهم واتجاهاتهم في التسوق أصبحت متوفرة في ظل الإنترنت[468].

رابعا: تشعب البيانات

لا يعرف الشخص إلى أي مدى يتم استعمال بياناته الموجودة في الحواسيب الآلية وشبكة الإنترنت وفي أي نطاق، وهذا يمثل خطرا على حرمة الحياة الخاصة للفرد حتى وإن كانت هذه البيانات صحيحة، وهذا ما أكده أحد القضاة الفرنسيين بأن أحد الأنظمة الدكتاتورية في أمريكا اللاتينية استخدمت التحليلات التي أجريت بواسطة الحاسب للإجابة عن أسئلة تم وضعها في شكل بريء يخص باطنه الذي يهدف إلى كشف خفايا نفوس المعتقلين على ذمة قضايا[469].

خامسا: النقل الرقمي للبيانات

تتدفق المعلومات في بيئة الإنترنت عبر الحدود دون أي اعتبار للجغرافيا والسيادة، والأفراد يعطون معلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية[470]، وقد لا تخدم القوانين الوطنية كثيرا في هذا الفرض، كما أن تضمينها نصوصا بشأن السيطرة على نقل البيانات قد لا يكون فاعلا في ظل غياب التنسيق وضمان أن يكون نقل البيانات محكوما باتفاقيات تكفل حمايتها أو تضمن توفر حماية مماثلة في الدولة المنقول لها البيانات[471].

---

[468]– **منى تركي الموسوي، جان سيريل فضل الله، «الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها»**، مجلة كلية بغداد للعلوم الإقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص 309.

[469]– **بن سعيد صبرينة**، مرجع سابق، ص 136.

[470]- Un journaliste scientifique américain. Charles PRATT, écrivait en 1993: « maintenant que mon credit rating, le montant de mes impots, mon profil de consommation et mes antécédents médicaux sont disponibles on-line et que les agences fédérales sont pretes à saisir ma voiture, mon bateau et ma maison en cas de désaccord fiscal, j'ai vraiment quelques raisons de me sentir en insécurité », voir: **VOISSET Michèle**, Droit au respect de la vie privée et société de l'information, groupe d'études société d'information et vie privée, chapitre 16, p 253, disponible sur le site: http://asmp.fr

[471]– **منى تركي الموسوي، جان سيريل فضل الله**، مرجع سابق، ص 310.

سادسا: بنوك ومراكز المعلومات الشخصية المنشئة من قبل الدول

تظهر خطورة بنوك المعلومات كذلك عندما تقوم الدول بإنشاء بنوك أو مراكز للمعلومات تجمع فيها ما تشاء من البيانات عن الأفراد وتقوم بتحليلها وتنظيمها والربط بينها ومن ثم تخزينها في النظام المعلوماتي[472]، مما يتيح للدول فرض رقابة على مواطنيها ومعرفة أدق تفاصيل حياتهم مما يشكل مساسا بحقهم في الخصوصية.

تعالت الاحتجاجات في بعض الدول –كفرنسا والولايات المتحدة الأمريكية وألمانيا– ضد إنشاء النظام الموحد للمعلومات، والمقصود بهذا النظام امكانية جمع المعلومات المتصلة بالفرد في حاسوب مركزي واحد، فيمكن بالتالي جمع المعلومات الضريبية والاجتماعية والدينية والسياسية والحالة الصحية والمالية والنشاط الحزبي والنقابي لهذا الفرد حتى أوقات تسليته وفراغه والأماكن التي يرتادها....الخ، الأمر الذي دفع بعض الدول إلى تحريم إيجاد نظام موحد للمعلومات فيها كما هو الحال في البرتغال والنمسا[473].

سابعا: المعلومات غير الدقيقة وغير المكتملة

تعتبر المعلومات غير الدقيقة وغير المكتملة من الأخطار الجسيمة للبنوك المعلوماتية على حقوق وحريات الإنسان[474]، فعلى سبيل المثال، كلف مكتب التقنية في الولايات المتحدة في عام 1981 الدكتور (لوردن)، وهو عالم في مجال الجريمة، بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات وكالة الشرطة الفدرالية وقد وجد أن النسبة عالية من البيانات كانت غير كاملة وغير دقيقة ومبهمة، ويتضمن العديد منها اعتقالات لم تؤد إلى إدانة، أو أنها متعلقة بجنح بسيطة تمت في الماضي القديم، وأكد على أن أصحاب العمل لم يوظفوا في الغالب مثل هؤلاء الأشخاص لسجلاتهم الإجرامية غير الدقيقة، واعترفت

472- **HARIVEL Jean**, op-cit, p p 461-462

473– مشار له لدى: **نهلا عبد القادر المومني**، مرجع سابق، ص 171.

474- **JAMMET Adrien**, La prise en compte de la vie privée dans l'innovation technologique, Thèse pour obtenir le grade de docteur en droit, université Lille 2-droit et santé, 2018, p 91.

أربع من خمسة ولايات أمريكية تم الاتصال معها بواسطة مكتب تقييم التقنية أنها لم تتأكد أبدا من دقة البيانات في ملفاتها ولم تقم بتحديث نوعي منتظم[475].

المبحث الثاني

كيفيات تأثير الحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت

أدّت الشبكة العالمية للإنترنت بمختلف التقنيات التي أفرزتها إلى توسيع مفهوم الحق في الحياة الخاصة، الأمر الذي دفع بمختلف التشريعات عبر دول العالم إلى توسيع مجال الحماية المقررة لذا الحق، فانطلاقا من الحماية المقررة للحق في الحياة الخاصة بمنظوره التقليدي مثل حرمة المسكن وصولا إلى تكريس مبادئ حماية هذا الحق في مجال التقنية مثل الحق في سرية المراسلات الإلكترونية التي تتم عبر البريد الإلكتروني، تعد من بين الأسباب التي حدت من فعالية الآليات الموضوعة لمكافحة الجريمة المرتكبة عبر الإنترنت.

واجهت آليات مكافحة الجريمة المرتكبة عبر الإنترنت الكثير من العقبات التي كانت نتيجة الإجراءات الموضوعة لحماية الحق في الحياة الخاصة، حيث أن هذه الأخيرة قامت بتعطيل هذه الآليات، وذلك عن طريق فرض احترام حق الفرد في حياته الخاصة أثناء الاستدلال والتحقيق حول جريمة تكون شبكة الإنترنت مسرحا لها، الأمر الذي يجعل آليات مكافحة الجريمة المرتكبة في هذا المجال تبدوا قاصرة نظرا للسرعة التي تتميز بها هذه الجريمة.

اختلفت أنماط تأثير الحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت تبعا لنوعية إجراءات حماية هذا الحق، فمنها ما هو قانوني **(مطلب أول)**، ومنها ما أفرزته الشبكة من تقنيات **(مطلب ثان)**.

---

[475] – مشار له لدى: **بن سعيد صبرينة**، مرجع سابق، ص 138.

المطلب الأوّل

التأثير القانوني للحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت

سعت غالبية الدول إن لم نقل كلها إلى تكريس مبادئ الحماية للحق في الحياة الخاصة عن طريق وضع نصوص قانونية عديدة تكفل هذا المجال، ولم يكن يعلم مشرعي هذه النصوص أنه في يوم من الأيام سوف يكون تأثيرها عكسي، حيث أن كان تأثيرها على الشق الجزائي من القانون تأثيرا كبيرا، خاصة مع ظهور الجريمة المرتكبة عبر الإنترنت.

أثرت النصوص القانونية الموضوعة لحماية الحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك عن طريق عرقلة الاستدلال والتحقيق في هذه الجريمة، فالضمانات المكرسة قانونا للأفراد أثناء استخدام الوسائل التقنية في الاثبات وقفت كحاجز في وجه الإجراءات المتبعة لمكافحة هذه الجريمة الأمر الذي لا يتماشى مع سرعتها **(فرع أول)**، بالإضافة إلى مبدأ المشروعية الذي كان له دور كبير في التأثير على مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك بفرض التحقق أن تكون الأدلة المستمدة من الوسائل التقنية تتسم بالمشروعية **(فرع ثان)**.

الفرع الأول

ضمانات حقوق الفرد أثناء استخدام الوسائل التقنية في الإثبات

يعطي الشخص المرتكب لجريمة من الجرائم الحق للدولة لكي تمارس سلطتها المطلقة في حماية المجتمع من الجريمة وتوقيع العقاب عليه عن طريق مختلف الأجهزة التي توضع لذلك، ويسمح لها بالمساس بحريته الشخصية بشرط أن يتم ذلك في إطار القانون، وهذا ما يطلق عليه ضمانات الفرد في الإجراءات الجزائية، غير أن هذه الضمانات كان لها دور سلبي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت لأنها تطيل مرحلة التحقيق والاستدلال، الأمر الذي لا يتماشى مع سرعة ارتكاب وإخفاء هذه الجريمة. من هذا المنطلق

سوف نتطرق إلى ذلك إلى تبيان ضمانات حقوق الفرد أثناء استخدام الوسائل التقنية في الاثبات على المستوى الدولي **(أولا)**، ثم على المستوى الوطني **(ثانيا)**.

أولا: على المستوى الدولي

يتمتع الفرد على المستوى الدولي بحماية كبيرة لحقه في الحياة الخاصة وذلك عن طريق العديد من المعاهدات الدولية التي كرست هذا الحق، حيث اعتبرتها هذه المواثيق الدولية من أهم الحقوق التي يمكن أن يتمتع بها الإنسان ولا يجوز في أي حال من الأحوال الاعتداء عليها، وإن تحتم ذلك في إطار التحري والاستدلال والتحقيق حول وقوع جريمة من الجرائم أن يتم ذلك وفقا للقانون، ويمكن أن نوضح ذلك على النحو التالي:

1- الإعلان العالمي لحقوق الإنسان

يتضمن الإعلان العالمي لحقوق الإنسان الصادر سنة 1948[476] مجموعة من المبادئ التي تنادي باحترام الحقوق الأساسية للإنسان، والتي تهدف إلى المحافظة على قيمة الإنسان، وهذه الحقوق يكتسبها الإنسان بسبب إنسانيته دون النظر إلى أي اعتبارات أخرى كالجنس أو اللون أو العقيدة أو اللغة، ويطالب هذا الإعلان الدول التي وقعت عليه باحترام ما ورد فيه من مبادئ وقيم[477].

تنص المادة 03 من الإعلان العالمي لحقوق الإنسان على: "لكل فرد الحق في الحياة والحرية وسلامة شخصه"، وأضافت المادة 12 من نفس الإعلان على أنه "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"[478].

---

[476]- أعتمد الإعلان العالمي لحقوق الإنسان بموجب قرار الجمعية العامة رقم (217 ألف) د-3) المؤرخ في 10 ديسمبر 1948.

[477] - **سليمان بن عبد الله بن سليمان العجلان**، مرجع سابق، ص 73.

[478]- أنظر المواد 03 و12 من الإعلان العالمي لحقوق الإنسان، مرجع سابق.

2- العهد الدولي للحقوق المدنية والسياسية

تضمنت هذا العهد مجموعة من المبادئ والقيم التي تعني بالمحافظة على حقوق الإنسان، ويمتاز هذا العهد عن الإعلان العالمي لحقوق الإنسان الصادر سنة (1948)، باعتبارها تقنينا دوليا لحقوق الإنسان يفرض التزامات قانونية محددة على الدول بضرورة احترام ما تضمنته من حقوق، بخلاف الإعلان الذي يقتصر على فرض التزامات أدبية باحترام ما تناولته من قواعد تتعلق بحقوق الإنسان[479].

أشارت الفقرة الأولى من المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة 1966[480] على لأنه: "**لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته**"، و تنص المادة 19 فقرة ثانية منه "**لكل إنسان حق في حرية التعبير، ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها**".

ثانيا: على المستوى الوطني

انقسم الفقه بين مؤيد ومعارض بشدة لاستعمال أساليب التحري على الجرائم المرتكبة عبر الإنترنت وذلك من وجهين

أ- **الرأي المعارض:** انتقد المعارضون بشدة أساليب التحري الخاصة وذلك من وجهين:

---

[479]- مشار له لدى: **سليمان بن عبد الله بن سليمان العجلان**، المرجع نفسه، ص ص 73-74.

[480]- اعتمد العهد الدولي الخاص بالحقوق المدنية والسياسية وعرض للتوقيع والتصديق والانظمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف(د-21) المؤرخ في 16 ديسمبر 1966.

1- من حيث حجيتها:

فهي وسائل غير مضمونة لأنها لا تعكس دائما الحقيقة، نظرا لإمكانية تغيير أو حذف أي مقاطع أو صور عن بعضها البعض، أو على العكس من ذلك تركيبها بشكل يغير الحقيقة، وينطبق هذا الأمر على الصوت والصورة.

2- من حيث مشروعيتها

نصت المادة 39 من دستور سنة 1996 على أنه: "**لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، سرية المراسلات الخاصة بكل أشكالها مضمونة**"[481].

كما يقضي قانون العقوبات بحرمة الرسائل البريدية والبرقيات على فضها أو تسهيل ذلك، كما يجرم ويعاقب على المساس بحرمة الحياة الخاصة للمواطن فيما يتعلق بالمكالمات والصور[482].

3- الرأي المؤيد

يعتقد مؤيدو هذا التوجه بمشروعية أساليب التحري الخاصة في مجال كشف وتتبع الجرائم المرتكبة عبر الإنترنت، وهذا لأن المصلحة العامة تقتضي وضع حد للجرائم الخطيرة المتفشية في المجتمع بالاستعانة بالوسائل التكنولوجية الحديثة، لعدم نجاعة الأساليب التقليدية في البحث والتحري، خاصة وأن الإجرام قد تطور بتطور وسائل ارتكابه، واستفاد المجرمون من هذا التطور، لذلك فإنه لا يوجد ما يمنع السلطة القضائية من تسخير هذه

---

[481]- قام المشرع الجزائري بتحيين هذه المادة في دستور الجمهورية الجزائرية الديموقراطية الشعبية الصادر في الجريدة الرسمية عدد 82، بتاريخ 30 ديسمبر 2020، والتي جاء نصها على النحو التالي: "**تضمن الدولة عدم انتهاك حرمة الإنسان.**

يحظر أي عنف بدني أو معنوي، أو أي مساس بالكرامة.

يعاقب القانون على التعذيب، وعلى المعاملات القاسية، واللاإنسانية أو المهينة، والاتجار بالبشر"

[482] – **شرف الدين وردة**، مرجع سابق، ص 552.

الوسائل العلمية الحديثة في سبيل كشف الجريمة وضبط الجناة حتى ولو ترتب على ذلك مساس طفيف بالحقوق والحريات، فمصلحة الدولة أولى بالرعاية من مصلحة الأفراد.

كما أن ضمان الحق في الحياة الخاصة للأفراد ومراسلاتهم واتصالاتهم ليس ضمانا مطلقا بل نسبيا ومقيدا، فالمصلحة العامة تقتضي تبجيل مصلحة الدولة والمجتمع على مصلحة الفرد الخاصة، وبالإضافة إلى ذلك، فإن واجب الدولة في مكافحة الجريمة والوقاية منها يحتم عليها في بعض الاحيان الاطلاع على خصوصيات الأشخاص والمساس بحقوقهم وحرياتهم الفردية، وذلك بمنح ضابط الشرطة القضائية المأذون لهم أو في إطار الإنابة القضائية القيام بالتحري في الجرائم المتلبس بها أو في حالة فتح تحقيق قضائي الحق في اعتراض المكالمات الهاتفية وتسجيلها وإباحة التصنت والتقاط الصور، وهنا نكون أمام حقين متناقضين، الأول حق الدولة في حماية أمنها وأمن المجتمع، والثاني هو حق الفرد في حرمة حياته الخاصة[483].

إعتنقت الجزائر مبدأ الدفاع عن الخصوصية الفردية بموجب دساتيرها المتعاقبة بدءا من دستور 1963 بموجب المادة 11 منه[484]، كما انضمت الجزائر إلى الإعلان العالمي لحقوق الإنسان الصادر سنة 1948، وانضمت بعد ذلك إلى العهد الدولي للحقوق المدنية والسياسية لسنة 1966، بمقتضى المرسوم الرئاسي رقم 89-67، المؤرخ في 1989/05/16[485] وهذا إيمانا منها بحماية حق الأفراد في الخصوصية[486].

---

[483] – **حاحة عبد العالي، يعيش تمام آمال، «الترصد الإلكتروني كآلية للتحري عن جرائم الفساد بين متطلبات حماية الحقوق والحريات وضرورات الكشف عن الجريمة»**، مجلة كلية القانون الكويتية العالمية، ملحق خاص بأبحاث المؤتمر السنوي الدولي الخامس المنعقد بتاريخ 09-10 ماي 2018، العدد 03، الجزء الثاني، أكتوبر 2018، ص 373.

[484]– تنص المادة 11 من دستور 1963 على: "**توافق الجمهورية على الإعلان العالمي لحقوق الإنسان وتنظم إلى كل منظمة دولية تستجيب لمطامح الشعب الجزائري وذلك اقتناعا منها بضرورة التعاون الدولي**"

[485]– مرسوم رئاسي رقم 89-67 مؤرخ في 16 مايو سنة 1989 يتضمن الانظمام إلى العهد الخاص بالحقوق الاقتصادية والاجتماعية والثقافية والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية الموافق عليها من طرف الجمعية العامة للأمم المتحدة يوم 16 ديسمبر سنة 1966، ج ر عدد 20، صادر بتاريخ 17 مايو سنة 1989.

أكّد المشرع في المادة 303 مكرر من قانون العقوبات حين جرّم المساس بحرمة الحياة الخاصة للأشخاص وبأية تقنية كانت وكذا ما تضمنته المادة 14 حين صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتجريم فعل الاعتداء على الحياة الخاصة للأفراد بواسطة تقنية المعلوماتية[487].

ما يلاحظ أن المشرع لم ينص صراحة على اعتبار المعلوماتية على إطلاقها محلا يصلح للحماية في إطار الحياة الخاصة، وإنما منع الاعتداء على الحياة الخاصة باستعمال التقنية المعلوماتية، فمن خلال مضمون المادة 303 مكرر من قانون العقوبات يمكن اعتبار، التقاط الأحاديث أو المكالمات الخاصة أو السرية وكذا صور الأشخاص اعتداء على حرمة الحياة الخاصة حتى ولو كان باستعمال التقنية المعلوماتية، إذ أن النص جاء فاتحا المجال إلى استعمال أية تقنية هذا من جهة، ومن جهة أخرى يلاحظ عدم إشارة النص لا من قريب ولا من بعيد إلى شمولية البيانات والمعلومات بالحماية من باب اعتبارها تدخل ضمن الحياة الخاصة، الأمر نفسه ملاحظ في نص المادة 14 سالفة الذكر.

وعليه يمكن القول أنه بالرغم من وجود نص المادة 303 مكرر من قانون العقوبات وكذا المادة 14 إلا أن المشرع سها في البداية عن إدراج المعلومات والبيانات كمحل يدخل ضمن الحياة الخاصة للأشخاص، ولعل هذا الأمر من الأسباب التي جعلته لا يضع تعريفا للحق في حرمة الحياة الخاصة بصفة عامة، ولحرمة الحياة الخاصة المعلوماتية بصفة خاصة، ليتدارك الأمر من خلال القانون رقم 18-07[488] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[489].

---

[486] – **جبار فطيمة، «مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري»**، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة الشلف، العدد 03، ديسمبر 2016، ص 14.

[487]– أنظر المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر سنة 2014، مرجع سابق.

[488]– قانون رقم 18-07 مؤرخ في 10 جوان 2018، يتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، صادر في 10 جوان 2018.

[489]– **بشان عبد النور**، مرجع سابق، ص ص 260-261

الفرع الثاني

مدى مشروعية الدليل المستمد من الوسائل التقنية

تعتبر مشروعية الحصول على الدليل ووجوده وإخضاعه لرقابة القاضي من بين أهم الإجراءات التي وضعتها أغلب التشريعات لحماية حقوق الأفراد خاصة في حقهم في الحياة الخاصة، فالأدلة التي يتم التحصل عليها عن طريق المراقبة والتنصت والتلصص دون سند قانوني تعتبر غير مشروعة وماسة بخصوصية الأفراد، وبالتالي يتم استبعادها، فمبدأ المشروعية بهذا الوصف يمكن اعتباره بمثابة قيد ينصب على آليات مكافحة الجريمة المرتكبة عبر الإنترنت لعدم مسايرته للتطورات المتسارعة لهذه الجريمة المستحدثة، ومن هذا المنطلق سوف نتطرق إلى مشروعية وجود الدليل الرقمي **(أولا)**، مشروعية الحصول على الدليل الرقمي **(ثانيا)**، أن يكون الدليل الإلكتروني يقيني **(ثالثا)**، وأن تتم مناقشته أمام قاضي الحكم **(رابعا)**.

أولا: مشروعية وجود الدليل الرقمي

يقصد بمشروعية الدليل الرقمي أن يكون الدليل معترفا به، بمعنى أن يجيز القانون للقاضي الاستناد إليه لتكوين عقيدته بالإدانة أو البراءة[490]، فالقاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه يلتزم ببيان الأدلة التي استمد منها اقتناعه، فليست الحرية أن نطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر فقط في استخلاص الحقيقة من أي مصدر مشروع[491].

يتمثل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي في طبيعة نظام الاثبات المعمول به في الدولة، إذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يأخذ بها في الاثبات وتقبل كأساس للحكم

---

[490] – **بهنوس أمال**، «**الدليل الرقمي في الإجراءات الجنائية**»، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، مجلد 16، عدد 02، سنة 2017، ص 179.

[491] – **علوي سالم**، أدلة الاثبات في التحقيق الجنائي، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق جامعة الجزائر 01، 2017/2016، ص195.

بالإدانة بحسب الاتجاه الذي تتبناه، والحقيقة أن هناك اتجاهين رئيسيين في نظام الاثبات الجنائي عرفتهم التشريعات الاجرائية الجزائية، الأول يدعى بنظام الأدلة القانونية والثاني نظام الاثبات الحر، وسنتناول كل منها على حدة لبيان موقف المشرع الجزائري منهما:

1- نظام الأدلة القانونية (الإثبات المقيد)

يعني هذا النظام أن يتقيد القاضي في حكمه سواء بالإدانة أو البراءة بأنواع معينة من الأدلة طبقا لما يرسمه التشريع، فوفقا لهذا النظام المشرع هو الذي يحدد حصرا الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، وذلك من خلال التحديد المسبق للأدلة المقدمة في الدعوى والتي يستند إليها القاضي الجزائي في حكمه بناء على قناعة المشرع بها لا قناعة القاضي، وبالتالي يكون القاضي مقيدا في ظل هذا النظام، إذ لا سبيل له إلى الاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، وبالتالي ينحصر دوره على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون[492].

2- نظام الإثبات الحر (الاقتناع القضائي)

يمنح هذا النظام للقاضي حرية الاستعانة بكافة طرق الإثبات التي يراها موصلة إلى الكشف عن الحقيقة في أمر الدعوى المطروحة عليه، فباب الإثبات مفتوح على مصراعيه، وليست هناك أدلة محددة يكون وجودها كافيا ولازما لاقتناع القاضي، وتخلفها يتخلف عنه – حتما- عدم اقتناع القاضي، فكل الأدلة سواء، ولذا سمي هذا النظام بحرية الاثبات، الذي يمنح القاضي سلطة قبول جميع الأدلة، والاعتراف له بتقدير كل دليل، وتقدير قيمة الأدلة مجتمعة، واستخلاص النتيجة التي تمثل اقتناعه الشخصي، وجوهر هذا النظام هو تخلي المشرع عن السلطات التي كان يستأثر بها في نظام الأدلة القانونية، ونقل هذه السلطات للقاضي، فإذا كانت الحقيقة بغيته فعلية أن ينشدها أنى وجدها، ومن أي سبيل يجده مؤديا

[492]- **تومي يحيى**، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيا الاعلام والاتصال، أطروحة من أجل نيل شهادة الدكتوراه علوم، تخصص قانون، كلية الحقوق، جامعة الجزائر، 2017-2018، ص ص 255-256.

إليها، ولا رقيب عليه في ذلك غير ضميره وحده، وعلى ذلك فهو مبني على إطلاق الأدلة، وحرية القاضي، ودوره الإيجابي[493].

3- النظام المختلط

يقوم هذا النظام عن طريق تحديد القانون لأدلة معينة للإثبات في بعض الجرائم من خلال تقييد سلطة القاضي في الإثبات[494]، ومثال ذلك منح حجية للمحاضر المحررة في بعض المخالفات بالنسبة لما ورد فيها إلى أن يثبت العكس، وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة.

يعتمد النظام المختلط على تحديد القانون لأدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطا في بعض الأحوال[495].

تنص المادة 212 من قانون الإجراءات الجزائية على أنه " **يجوز اثبات الجرائم بأي طريق من طرق الاثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه** ".

كما تنص المادة 307 من قانون الإجراءات الجزائية أيضا "...**إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها.....وأن يبحثوا باخلاص ضمائرهم في اي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم....**"

يتبين لنا من خلال النصين المعروضين أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائي، واستثناء نجده قد أخذ بنظام الأدلة القانونية في

---

[493]- **ناصر بن محمد البقمي**، مرجع سابق، ص ص 27-28.

[494]- **FRIEDRICH Cyrielle**, Les sciences et les techniques comme moyens de preuve dans la procedure pénale aspects techniques et juridiques de ces moyens de preuves, Thèse de doctorat, faculté de droit, université de Genève, 2016, p 13.

[495]- **لعوارم وهيبة**، مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي، مجلة الفقه والقانون، مجلة إلكترونية شهرية تعنى بنشر الدراسات الشرعية والقانونية، العدد العشرون، سنة 2014، ص 103، أنظر كذلك: **علي جبار الحسيناوي**، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، 2011، ص 124.

اثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر، وفي هذا لا يكون للقاضي الجزائي دور في تقدير القيمة الإقناعية للدليل فيتقيد القاضي وفق هذا النظام بالأدلة التي رسمها المشرع سلفا.

كرس المشرع الجزائري وذلك بالرجوع إلى المادة 212 من قانون الإجراءات الجزائية قاعدتين تكمل إحداهما الاخرى، قاعدة الاقتناع الشخصي الحر للقاضي الجزائري وقاعدة حرية اختيار وسائل الاثبات من جهة أخرى وهو المعمول به في الواقع القضائي[496].

ثانيا: مشروعية الحصول على الدليل الرقمي

يلتزم في هذا الصدد ضابط الشرطة القضائية بالإجراءات التي وضعها القانون حماية لحقوق الأفراد وحرياتهم الشخصية، كما أنه ملزم بالتقيد بالإذن المقدم له سواء من قبل قاضي التحقيق أو وكيل الجمهورية، وأي خروج على فحوى الإذن ينتج عنه مساس بالحرية الشخصية يعرض ضابط الشرطة القضائية[497] إلى المساءلة والعقوبة كما جاء في نص المادة 107 من قانون العقوبات الجزائري[498].

يكون الدليل الجنائي نتاج مجموعة من الإجراءات القانونية التي تهدف للوصول إليه، ويقتضي الوصول إليه وفق مجموعة من القواعد القانونية التي أقرّها المشرع بداية من محاولات الاستدلال ثم التنقيب والتفتيش عن الدليل والوصول إليه والحفاظ عليه بوضعه تحت أنظار السلطة العامة وسلطة المحكمة، ليقول القاضي كلمته النهائية في هذا الدليل إذا كان قد اقتنع به من عدمه أو أخذ جزء منه وترك البقية[499].

فمشروعية الدليل بصفة عامة شرط أساسي للوصول إلى اليقين القضائي عند الإدانة، ومعيار مشروعية الأدلة يكمن في احترام ضمانات الحرية الشخصية التي نص عليه القانون لاحترام حرية الفرد بوصفه بريئا إلى أن تثبت إدانته بحكم بات، وبالتالي فلا يجوز للقاضي

---

496 – **تومي يحيى**، مرجع سابق، ص ص 257–258.

497 – **جبار فطيمة**، مرجع سابق، ص ص 19–20.

498 – "يعاقب الموظف العمومي بالسجن المؤقت من خمس سنوات إلى عشر سنوات إذا أمر بعمل تحكمي أو ماس سواء بالحرية الشخصية للفرد أو بالحقوق الوطنية للمواطن أو أكثر".

499 –**سلامة محمد المنصوري**، مرجع سابق، ص 51.

الجنائي أن يعتمد على دليل باطل أو مجرد من قيمته القانونية ويستمد منه قناعته الذاتية ويدخل في مدلول الدليل الباطل ذلك الدليل الذي لم يستوف شرطا من الشروط التي يتطلبها القانون فيه كي تكون له قوة إقناعية للقاضي.

يجب أن يكون إقتناع القاضي مبنيا على دليل مستمد من إجراء صحيح ومشروع، أما إذا بني هذا الاقتناع على أدلة باطلة أو إجراءات غير مشروعة، كان مؤديا إلى بطلان الحكم تطبيقا لقاعدة "ما بني على باطل فهو باطل"، ولذا يجب أن تكون تلك الإجراءات مطابقة للقانون غير متعارضة مع المبادئ الأخلاقية والعلمية[500].

وعليه يجب أن تكون الأدلة الرقمية التي تم الحصول عليها من الوسائل الإلكترونية بصورة مشروعة غير مخالفة لأحكام الدستور أو قانون الإجراءات الجزائية، فمثلا مشروعية الدليل الإلكتروني تتطلب صدقه في مضمونه، وعلى ذلك يجب أن تكون إجراءات جمع الأدلة الرقمية ضمن الإطار العام الذي حدده القانون وإلا فإنه يتعرض للبطلان، لذا ينبغي أن لا يؤسس القاضي الجزائي حكمه على دليل ناتج عن حاسب إلكتروني لحقه سبب يبطله ويعدم آثاره[501].

ثالثا: أن يكون الدليل الإلكتروني يقيني

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، وذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها، إلا عندما يصل القاضي إلى درجة من القناعة تتسم بالجزم واليقين.

واليقين في النظم الإجرائية هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى وما يتطبع في ذهنه من تصورات واحتمالات ذات درجة

---

[500] – **محمودي نور الهدى**، مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي، –دراسة مقارنة–، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة 1، 2017–2018، ص ص 200–201.

[501] – **بن فردية محمد**، مرجع سابق، ص 251.

عالية من التأكيد ويمكن الوصول إلى اليقين عن طريق نوعين من المعرفة إحداهما حسية تدرك بالحواس، والأخرى معرفية تدرك بالعقل عن طريق التحليل والاستنتاج[502].

إلا أنه في نطاق الجزم بوقوع جرائم الاعتداء على نظم المعالجة الآلية ونسبتها إلى المتهم يستدعي نوعا آخر من المعرفة ألا وهي المعرفة العلمية في مجال المعلوماتية، وهو ما يلقي المزيد من الأهمية على تدريب القضاة، وتكمن هذه الأخيرة في كون الجهل بها قد يؤدي في بعض الاحيان إلى التشكيك في قيمة الدليل التقني[503].

رابعا: أن تتم مناقشته أمام قاضي الحكم

من المتعارف عليه فقها وقضاء أن إجراءات المحاكمة لدى مختلف الدول في العالم تتم في شكل مرافعة شفوية وحضورية، والمقصود بالمرافعة هنا جميع إجراءات التحقيق النهائي الذي تجريه المحكمة، ومفهوم هذا المبدأ يعني أن القاضي لا يمكن له أن يؤسس اقتناعه إلا على العناصر الاثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[504]، ولا يختلف الأمر بالنسبة للأدلة الرقمية بوصفها أدلة إثبات إذ إثبات إذ ينبغي أن تطرح في الجلسة وأن يتم مناقشتها في مواجهة الأطراف.

حتى يتمكن القاضي من بناء قناعته، وهو ما يعبر عنه بشرط وضعية الدليل ما معناه أن يكون للدليل أصل ثابت في أوراق الدعوى ثم يطرح للمناقشة بعد اطلاع الخصوم عليه[505].

لا يكفي أن يكون الدليل ضمن أوراق الدعوى المقدمة أمام القاضي، فمناقشة الدليل من قبل أطراف الدعوى أمر هام، إذ يؤدي للتأكد من جدية الدليل وصلاحيته للإثبات في

---

[502] – **ربيعي حسن**، مرجع سابق، ص 267.

[503]- **بوكر رشيدة**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، مرجع سابق، ص 518.

[504]- **BOLZE Pierre**, Le droit à la preuve contraire en procedure pénale, Thèse en vue de l'obtention du grade de docteur en droit, faculté de droit, sciences économique et gestion, université Nancy 2, 2010, p 237.

[505]– **إلهام شهرزاد روابح، «الدليل الرقمي بين المشروعية وانتهاك الخصوصية المعلوماتية»**، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة البليدة، العدد العاشر، د س ن، ص 195.

الدعوى، فالخصوم كافة يجب أن يكونوا على بينة من الأدلة المقدمة قبل الحكم بالدعوى ليتسنى لهم مواجهتها والرد عليها وتفنيدها[506].

يعد مبدأ المواجهة بين أطراف الدعوى من أهم المبادئ التي يجب أن يؤسس القاضي اقتناعه في ضوئها، حيث يتطلب هذا المبدأ طرح الأدلة في الجلسة، وأن تتاح الفرصة أمام القاضي في الدعوى الجنائية، لمناقشة الأدلة المقدمة من كل منها، وتنفيذها، ويرتبط هذا المبدأ بالمبدأ القانوني العام، المتمثل في ضرورة احترام حقوق الدفاع، الذي يعد أحد المظاهر الأساسية لدولة القانون، والنظم الديمقراطية.

يقتضي مبدأ المواجهة ضرورة حضور كل خصم في الدعوى، وأن يطلع خصمه على ما لديه من أدلة وأن يواجهه بها، وأن يناقش كل منهما الآخر، ومبدأ المواجهة، يتطلب نوعين من الضمانات.

النوع الأول: يكون سابقا على عملية المواجهة بين الأطراف، ويتضمن إحاطة المتهم علما بالتهمة المنسوبة إليه، وإعطائه الوقت الكافي، والوسائل اللازمة لكي يدافع عن نفسه.

أما النوع الأخر: من الضمانات، فيكون أثناء عملية تقديم أدلته سواء مستندات، او سؤال الشهود، أو الخبراء، وتقديم المذكرات وغيرها، ومن ثم يناقش كل طرف أدلة الطرف الآخر ويحاول أن يدحضها، وعلى ضوء المناقشات التي تحصل يبني القاضي الجنائي اقتناعه على النتيجة النهائية لهذه المناقشات[507].

وعليه فإن الأدلة الرقمية مهما كانت صورتها سواء في شكل مطبوعة أو بيانات معروضة على شاشة الحاسب أم كانت بيانات مدرجة في حاملات البيانات، فإنه يجب مناقشتها وتحليلها، وكقاعدة عامة فإن مبدأ وجوب مناقشة الدليل الجزائي سواء كان دليلا تقليديا أم كان ناتجا عن الحاسب الآلي تعتبر ضمانات مهمة وأكيدة للعدالة[508].

---

[506]– **سلامة محمد المنصوري**، مرجع سابق، ص 50.

[507]– **سامي جلال فقي حسين**، مرجع سابق، ص 117.

[508]– **محمودي نور الهدى**، مرجع سابق، ص 199.

المطلب الثاني

التأثير التقني للحق في الحياة الخاصة على آليات مكافحة الجريمة المرتكبة عبر الإنترنت

نتج عن التطورات التي عرفتها شبكة الإنترنت والاستعمال الواسع لها العديد من المفاهيم التي أصبحت بمثابة حقوق للأشخاص بل أضحت من حرمة حياتهم الخاصة، وكما انبثقت هذه المفاهيم الجديدة ظهر نوع جديد من آليات حماية هذه الحقوق تمثلت في تقنيات عديدة، غير أن هذا التحول في مفهوم حماية الحق في الحياة الخاصة لم يمر بسلام، بل كان له تأثير كبير على آليات مكافحة الجريمة المرتكبة عبر الإنترنت، وذلك عن طريق استغلال هذا الوضع من طرف المجرمين والجماعات الإجرامية وقيامهم باستعمال هذه التقنيات في حجب المعلومات الخاصة بهم من أجل الحيلولة دون وصول سلطات الاستدلال والتحقيق للأدلة التي بمقتضاها تتم إدانتهم.

يعتبر التوقيع الإلكتروني من بين أهم التقنيات التي أفرزتها التقنية العالية والتي يعتمد عليها المجرمون في حجب البيانات الخاصة بهم، حيث لا يمكن لأي أحد الوصول إليها من جهة، ويتم عقاب المعتدي على هذا التوقيع دون موافقة المعني من جهة أخرى **(فرع أول)**.

لا نغفل كذلك تقنية التشفير وما هو في حكمه التي تعتبر من بين أكثر التقنيات استعمالا من طرف المجرمين نظرا لفعاليتها بجعل البيانات محجوبة على كل من يريد أن يطلع عليها عن طريق رموز وأرقام لا يعرفها إلا واضعها **(فرع ثاني)**.

الفرع الأول

التوقيع الإلكتروني كآلية لحجب الأعمال الإجرامية

التوقيع الإلكتروني هو رقم أو رمز سري أو شفرة خاصة مما لا يفهم معناه إلا صاحبه ومن يكشف له عن مفتاحه[509]، حيث أن اللجوء إلى التوقيع الإلكتروني يرفع من مستوى الأمن والخصوصية للمتعاملين على شبكة الإنترنت، حيث يضمن سرية المعلومات والرسائل

[509]– **أحمد شرف الدين، «حجية الرسائل الإلكترونية في الإثبات»**، ص 03، مقال متوفر على الموقع التالي: www.eastlaw.com

والبيانات[510]، ويعتبر من بين أهم الوسائل التي يسعى من خلالها المجرمون لحجب أعمالهم الإجرامية ومنع سلطات التحري والتحقيق من الوصول إلى الأدلة التي تدينهم، وسوف نبين ذلك بالتطرق إلى الأسس القانونية للتوقيع الإلكتروني **(أولا)**، صور التوقيع الإلكتروني **(ثانيا)**، ثم إلى الحماية المقرر للتوقيع الإلكتروني **(ثالثا)**.

أولا: الأسس القانونية للتوقيع الإلكتروني

تتمثل الأسس القانونية للتوقيع الإلكتروني في:

1- على المستوى الدولي

أ- القانون النموذجي حول التجارة الإلكترونية، الصادر عن لجنة القانون التجاري الدولي لدى الأمم المتحدة بموجب القرار رقم 162/51 بتاريخ 1996/01/16 الذي أقر بالقوة الثبوتية للسند والتوقيع الإلكترونيين[511].

ب- التوجيه الصادر عن البرلمان الأوربي بتاريخ 1999/12/13 حول التوقيع الإلكتروني وتسهيل استعماله من أجل حسن سير العمل في السوق الداخلي الأوربي[512]، كما أقر البرلمان الأوربي توجيها آخر بتاريخ 2000/06/08 حول التجارة الإلكترونية والتأكيد على الاهتمام بتوقيع العقود بالطرق الإلكترونية[513].

---

[510] – **محمد زيدان، محمد حمو**، متطلبات أمن المعلومات المصرفية في بيئة الإنترنت، مداخلة مقدمة في المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية، البيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد بالرياض خلال الفترة 06-07 أفريل 2010، ص 12

[511]– أنظر في ذلك قرار الجمعية العامة للأمم المتحدة رقم 162/51 المتضمن القانون النموذجي بشأن التجارة الإلكترونية الذي اعتمدته لجنة الأمم المتحدة للقانون التجاري الدولي في الدورة الحادية والخمسون، البند 148 من جدول الأعمال، رقم A/RES/51/162.

[512]- Directive 1999/93/CE du parlement Européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

[513]– التوجيه النموذجي رقم EC/2000/31 للبرلمان والمجلس الأوروبي المؤرخ في 2000/06/08 بشأن بعض الجوانب القانونية لخدمات مجتمع المعلومات لاسيما في مجال التجارة الإلكترونية في السوق الداخلية (أمر توجيهي في مجال التجارة الإلكترونية).

ت- قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها 34 بتاريخ 2001/07/05، لتنظيم التوقيع الإلكتروني في سياق العلاقات ذات الطابع التجاري[514].

2- على المستوى الوطني

أدرج التوقيع الإلكتروني للمرة الأولى في الجزائر من قبل المشرع سنة 2005 بتعديل القانون المدني[515]، الذي تم من خلاله الاعتراف بالكتابة الالكترونية كوسيلة اثبات وذلك بإضافة المادتين 323 مكرر و232 مكرر 1.

كما قنّنت الجزائر بعد ذلك التوقيع الالكتروني بمقتضى المرسوم التنفيذي رقم 07-162[516]، ليليه الإفراج عن القانون رقم 15-04 المؤرخ في 01 فيفري 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[517]، قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة المواتية لتعميم وتطوير المبادلات الإلكترونية، وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق

---

[514]- قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع 2001، المنعقد بفيينا من 25يونيو-13 يوليو 2001 للدورة الرابعة والثلاثون، من طرف لجنة الأمم المتحدة للقانون التجاري الدولي رقم A/CN.9/493، أنظر كذلك: قرار الجمعية العامة للأمم المتحدة رقم 80/56 بناء على تقرير اللجنة السادسة (A/56/588)،= =المتضمن القانون النموذجي بشأن التوقيعات الإلكترونية الذي وضعته لجنة الأمم المتحدة للقانون النجاري الدولي، رقم A/RES/56/80.

[515]- قانون رقم 05-10، المؤرخ في 20 جوان 2005، يعدل ويتمم القانون المدني، ج.ر عدد 44، صادر بـ 26 جوان 2005.

[516]- مرسوم تنفيذي رقم 07-162، مؤرخ في 30 ماي 2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 ماي 2001، يتضمن نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37، صادر في 07 يونيو 2007.

[517]- قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يتضمن القواعد العامة للتوقيع والتصديق الإلكترونيين، ج.ر عدد 06، صادر في 10 فبراير 2015.

الإلكترونيين في الجزائر، يسمح بتعميم وتطوير التبادلات الإلكترونية بين المستعملين في مجالات القطاع العام والخاص[518].

ثانيا: صور التوقيع الإلكتروني

تتمثل صور التوقيع الإلكتروني في:

1- التوقيع البيومتري

يقصد بالتوقيع البيومتري التحقق من شخصية المتعامل بالاعتماد على الخواص الفيزيائية الطبيعية للأفراد، وهذه الصورة من التوقيع الإلكتروني صورة علمية حديثة ومتطورة، تدخل ضمن تكنولوجيا البصمات والخواص الحيوية والطبيعية.

يقوم التوقيع البيومتري على حقيقة علمية مفادها أن لكل إنسان صفاته الجسدية الخاصة التي تختلف عن أي شخص آخر، والتي تتميز بالثبات النسبي الذي يجعل لها قدرا كبيرا من الحجية في التوثيق والاثبات، وتشمل طرق التوقيع البيومتري ما يلي:

1-بصمة الأصابع.

2-بصمة العين وهي بصمة شبكية وقزحية العين.

3-بصمة معالم الوجه.

4-خواص اليد البشرية.

5-بصمة الصوت[519].

تتم كيفية التوقيع البيومتري من خلال استعمال تقنية خاصة، بها تؤخذ صورة لأحد أعضاء جسم الإنسان ويحتفظ بها في شكل شفرة داخل ذاكرة هذه التقنية يستطيع صاحب

---

518 – **درار نسيمة**، مرجع سابق، ص ص 190-191. أنظر كذلك:

- **ABDELSADOK kheira**, L'impact de nouvelle technologie de l'information sur les services bancaires en droit algérien, Thèse présentée pour l'obtention du diplôme de doctorat de sciences en sciences juridique, option droit privé, faculté de droit et sciences politique, département de droit, université de Batna 01, 2017/2018, p 122

519 – **إبراهيم بن سطم بن خلف العنزي**، التوقيع الإلكتروني وحمايته الجنائية، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الدكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص ص 54-55.

الشأن عند الرغبة في استعمال هذه الصورة في إبرام التصرفات والتعاقدات للرجوع إليها وتوثيق تصرفه وهذا من خلال برنامج داخل ذاكرة التقنية المستخدمة يمكن مقارنة الصورة المحفوظة بالصورة الملتقطة فإذا تطابقت الخصائص والسمات بين الصورتين تمكن الشخص صاحب الشأن من توثيق التصرف المراد القيام به[520].

2- التوقيع بالرمز السري

يتم توثيق المراسلات والتعاملات الإلكترونية بناء على هذه الطريقة باستخدام مجموعة من الأرقام والحروف يختارها صاحب التوقيع لتحديد شخصيته ولا تكون معلومة إلا منه أو من يبلغه بها، وتنتشر هذه الطريقة من التوقيع الإلكتروني في عمليات المصارف والدفع الإلكتروني بصفة عامة، وقد اعترف القضاء الفرنسي مبكرا بهذا النوع من التوقيع كونه يحاط بالضمانات الموجودة في التوقيع اليدوي التقليدي[521].

3- التوقيع الإلكتروني الرقمي

تعتبر هذه الصورة من صور التوقيع الإلكتروني الأرقى على الإطلاق، ومن أجل تنظيم هذه الصورة من التوقيع الالكتروني، صدرت أغلب القوانين الخاصة بالتوقيعات الإلكترونية وسميت بذلك، حتى استحوذت على هذا المسمى "التوقيع الإلكتروني" رغم أن هذا المسمى أشمل وأعم مما أرادت التشريعات، حتى تصور البعض أنه لا يوجد صورة من صور التوقيع الإلكتروني إلا هذه الصورة، وذلك لما يتحقق في هذه الصورة من الأمان والثقة لارتباطها بالتعاملات والصفقات التي تتم عبر شبكة الإنترنت[522].

---

[520] – **سعدي الربيع**، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015-2016، ص 62.

[521] – **جامع مليكة**، حماية المستهلك المعلوماتي، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية (القانون الخاص)، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2017-2018، ص 211.

[522] – **إبراهيم بن سطم بن خلف العنزي**، مرجع سابق، ص 57. أنظر كذلك:

- **Virginie ETIENNE**, Le développement de la signature électronique, mémoire master 2 recherche droit des affaires, université Paris 13, 2010/2011, p 19.

4- التوقيع باستخدام البطاقات الممغنطة

تعتبر هذه الصورة من صور التوقيع الإلكتروني الأكثر شيوعا لدى الجمهور، فاستخدامها لا يرتب عناءً كبيرا ولا يتطلب خبرة معينة، وبذلك تتيح هذه الطريقة إمكانية استخدامها لكل شخص، فهي لا تستلزم جهاز حاسب آلي خاص به، أو أن يكون جهازه متصلا بشبكة الإنترنت، فالبنوك ومؤسسات الإئتمان تقوم بإصدار هذه البطاقات، وهي على أنواع، فمنها ما هو ثنائي الأطراف (العميل+بنك) بحيث يستخدمها العميل لإجراء عملية السحب النقدي من خلال أجهزة الصراف الآلي، ومنها ما هو ثلاثي الأطراف (العميل+ البنك+ طرف ثالث) حيث تخول حاملها وفاء ثمن البضائع من سلع أو خدمات، والتي يحصل عليها من بعض التجار أو المحلات التجارية التي تقبلها بموجب اتفاق مسبق أبرمته مع الجهة المصدرة، وذلك يتم من خلال تحويل الثمن من حساب العميل المشتري (حامل البطاقة) إلى حساب التاجر البائع[523].

ثالثا: الحماية المقررة للتوقيع الإلكتروني

سبق القول بأن حماية المعطيات الشخصية والخصوصية في بيئة الإنترنت يولد الثقة في تعامل الأشخاص بالتعاملات الإلكترونية خاصة التجارية منها، التي تعد ركيزة أساسية من ركائز الاقتصاد في عالمنا اليوم، ولذلك تضمنت أغلب القوانين مبدأ ضمان حق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهو ما سار على إثره المشرع الجزائري

صدر قانون التوقيع الإلكتروني رقم 15-04 ليقر حماية خصوصية المعلومات في نطاق التعاملات الالكترونية وما يتعلق بها من معطيات ومعلومات يتم تداولها من خلال تجريم بعض الأفعال التي من شأنها المساس بها تحقيقا لمبدأ الردع العام والخاص في هذا المجال، وصور التجريم هذه تمثل حماية للمعطيات ابتداء قبل تسجيلها لدى الوسيط

[523]- **لملوم كريم**، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ملود معمري، تيزي وزو، 2011، ص 128.

النظامي في التعامل الإلكتروني أو كما يعرف بمزود خدمة التصديق الإلكتروني، ومنها ما تمثل حماية بعد هذا التصديق[524].

بالإضافة إلى ذلك أصدر المشرع الجزائري نصوص قانونية بموجب قانون العقوبات تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلاله جرم كل أنواع الاعتداءات التي تستهدف الدخول غير المشروع للأنظمة المعلوماتية، تغيير أو إتلاف المعطيات[525]، محددا بذلك الأفعال والسلوكات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم[526].

الفرع الثاني

استعمال التشفير وبرامج حماية المعطيات الشخصية لجب الأعمال الاجرامية

بالرغم من أن أسلوب التشفير وضع لحماية بيانات الأشخاص من التعدي عليها، إلا أنه أستعمل من طرف المجرمين والجماعات الإجرامية في حجب المعطيات والبيانات الناتجة عن جرائمهم، وذلك لتفادي وصول الضبطية القضائية وجهات التحقيق إلى الدليل الذي يدينهم، بل ذهب الجناة إلى أكثر من ذلك باستعمالهم العديد من التقنيات التي لها دور مثل التشفير بدافع عرقلة مسار التحقيقات حول جرائمهم والتي سوف نبينها من خلال التطرق إلى التشفير **(أولا)** ثم إلى التقنيات المشابهة له **(ثانيا)**

---

[524] – **بوكر رشيدة**، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص 124.

[525] –أنظر في ذلك الفرع الأول من المطلب الأول من المبحث الأول، من الفصل الثاني من الباب الأول من بحثنا هذا.

[526] – **لالوش راضية**، مرجع سابق، ص 167.

أولا: التشفير

إضافة إلى العوامل السابقة هناك عامل آخر قد يعقد من عملية التحقيق في الجرائم المعلوماتية وهو تكنولوجيا التشفير، والتي تحمي معلومات ضد أي شخص يريد الولوج أو الدخول وهذا من خلال كلمة سر[527].

1-تعريف التشفير

تقتضي التعاملات الإلكترونية عبر شبكة الإنترنت ضرورة تشفير البيانات المتداولة وذلك عن طريق تشفير الرسائل أو الملفات الخاصة، لضمان أمنها وسريتها[528].

عرف المشرع الفرنسي أدوات التشفير في القانون رقم 90-1170 الصادر بتاريخ 29 ديسمبر 1990 المتعلق بتنظيم الاتصالات عن بعد بأنها: "تشمل جميع التقنيات التي ترمي بفضل بروتوكولات سرية، إلى تحويل معلومات مفهومة إلى معلومات وإشارات غير مفهومة أو القيام بالعملية المعاكسة، وذلك بفضل استخدام معدات أو برامج مصممة لهذه الغاية".

ومن التعريفات التي أوردها الفقه، التشفير هو: "تحويل عملية النص إلى رموز وإرشادات غير مفهومة تبدو ذات غير معنى لمنع الغير من الاطلاع عليها، إلا الأشخاص المرخص لهم بالاطلاع على النص المشفر وفهمه، مما تنصب عملية التشفير على قيام بتحويل النصوص العامة إلى نصوص مشفرة، مع إمكانية إعادة النص المشفر إلى نص عادي[529].

---

[527] -**مزيود سليم، «الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها»**، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد 01، أفريل 2014، ص 100. (ص ص 94-107)، أنظر كذلك: **عبد الرحمان شعبان عطيات**، أمن الوثائق والمعلومات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 119 وما يليها.

[528]- **MATIGNON Emmanuelle,** op-cit, p 20. Voir aussi: **DIMITRIOU Philippe**, L'aplication du droit de la cryptologie en matière de sécurité des réseaux informatiques, Mémoire pour l'obtention du déplome de D E A défense nationale, option sécurité européenne et internationale, faculté des sciences juridiques, politiques et sociales, université de Lille 2-droit et santé, 2002, p 05.

[529] – مشار له لدى: **مرنيز فاطمة**، مرجع سابق، ص 51. أنظر كذلك: **أشرف السعيد أحمد**، القرصنة الإلكترونية، مطابع الشرطة، القاهرة، 2013، ص 111.

2-أهمية التشفير

يعتبر التشفير فن تغيير الشكل الظاهري للمعلومات بحيث يتم اخفاء معناها الحقيقي، وهو عامل مهم في أمن المعلومات إلا أنه متى ما تم استخدامه من قبل المجرمين والإرهابيين لتشفير اتصالاتهم وملفات المعلومات الخاصة بخططهم، فإنه يشكل معضلة بالنسبة لرجال الشرطة، فالتعامل مع الملفات المشفرة أمر صعب خاصة في ظل تطور تقنيات التشفير ووجود برمجيات ذات واجهة رسومية جعلت القيام به أمرا سهلا، بالإضافة إلى التزايد الهائل في قدرة الحواسب الشخصية على معالجة البيانات ومن ثم سرعة تشفير الملفات مهما كان عددها كثيرا أو أحجامها كبيرة[530].

وضع التشفير وسمح باستعماله قانونا من طرف غالبية دول العالم وذلك نظرا للاعتداءات التي طالت الاشخاص والمؤسسات حماية لحياتهم الخاصة حتى سميت هذه التقنية بالتقنية الداعمة لحماية الحياة الخاصة[531]، غير أن هذه الوسيلة التقنية والقانونية الموضوعة أساسا للحماية تم استغلالها من طرف المجرمين من أجل إعاقة جهات انفاذ القانون من الوصول إلى الدليل الذي يثبت فعلهم ويدينهم أمام القضاء.

3-أساليب التشفير

تتعدد الأساليب المتبعة في تشفير المعطيات ذات الطابع الشخصي، والتي من خلالها يقوم الشخص بحجب بياناته الشخصية عن طريق استعمال رموز وإشارات لا يمكن لغيره فضها إلا إذا قام هو بذلك ويمكن لنا أن نوضح ذلك على النحو التالي:

---

[530] – **تركي بن عبد الرحمن المويشر**، مرجع سابق، ص 70.

[531] – **xavier philippe**, Vie privee et nouvelles technologies, annuair international de justice constitutionnelle, 18-2003, p 442.

أ- أسلوب الشبكة الخاصة الافتراضية:

يعتمد على بروتوكول (ipsec) الذي يسمح بإنشاء ممر آمن بين المرسل والمستقبل الذي من خلاله يتم تشفير كل البيانات والرسائل قبل تبادلها[532].

ب- الأمن من خلال البروتوكول (ssl):

طورت هذه التقنية من طرف شركة "نت سكيب" التي ساعدت على زيادة الثقة في التجارة الإلكترونية ومستوى الأمان فيها مما جعلها أساس التجارة الإلكترونية في العالم حيث قامت معظم الشركات المنتجة لمتصفحات الإنترنت بالأخذ بها وتزويد متصفحاتها بهذه التقنية.

يحتوي هذا البرنامج على بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة آمنة بحيث لا يمكن قرائتها إلا من طرف المرسل و المستقبل لأن قوة تشفيرها تكون قوية ويصعب فكها وهي تختلف عن طرق التشفير الأخرى في أمر واحد وهو أنه لا يطلب من المرسل البيانات تشفير المعلومات التي يريد حمايتها فقط عليه التأكد من أن البروتوكول مستخدم بالقوة المطلوبة[533].

يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم بجهاز الخادم الخاص بالموقع المراد الشراء منه وهذا طبعا إذا كان الخادم مزود بهذه التقنية أساسا، ويقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولا إلى جهاز الخادم الخاص بالموقع باستخدام بروتوكول التحكم بالارسال وبروتوكول الإنترنت وهو ما يعرف بـ

---

[532] – **منصور أحلام، «الحلول الحديثة لأمن المعلومات لمواجهة المخاطر الإلكترونية»**، مجلة دراسات في الاقتصاد والتجارة والمالية، المجلد 07، العدد 01، مخبر الصناعات التقليدية لجامعة الجزائر 3، سنة 2018، ص 321.

[533] – **صراع كريمة**، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة مقدمة لمتطلبات نيل شهادة الماجستير في العلوم التجارية، تخصص استراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2014، ص 78.

(TCP/IP) ولقد سميت بالطبقة الآمنة لأن هذا البرنامج يعمل كطبقة وسيطة بين بروتوكول التحكم بالنقل وبروتوكول (http://(hyper text transfer protocol)[534].

ت- التشفير التماثلي

يتميز هذا النظام بوجود مفتاح واحد يستخدم من طرف المرسل قصد تشفير الرسالة ويستعمل من طرف المرسل إليه قصد استعادة الرسالة في شكلها الواضح الأصلي[535]، يكون مفتاح الإغلاق والفتح فيها عبارة عن معادلة رياضية يمثلها نظام معين تعمل على تحويل البيانات إلى نص رقمي ذي رموز غير مقروءة، وآلية هذا النظام قائمة على تغيير تسلسل الأحرف، ولتبادل المحررات الإلكترونية ينبغي أولا إرسال المفتاح الذي أغلق به بيانات المحرر إلى المرسل إليه ليتسنى لهذا الاخير فتح المحرر والاطلاع عليه[536].

ث- التشفير غير التماثلي

يستلزم هذا النوع من التشفير استخدام نوعين من المفاتيح[537]، المفتاح الخاص والمفتاح العام، فالمفتاح الخاص يكون معرفا فقط من طرف جهة واحدة وهو الشخص القادر على تشفير المعلومات وفك شفرتها، أما المفتاح العام فيكون معرفا لدى أكثر من جهة ويستطيع فك شفرة الرسالة التي شفرتها المفتاح الخاص، إذن المبدأ الذي يقوم عليه هذا النوع من التشفير وهو أن المعلومة التي يتم تشفيرها من أحد المفاتيح لا يتم فك شفرتها إلا من طرف المفتاح الآخر[538].

---

[534] – **خبازي فاطمة الزهرة**، جرائم الدفع الإلكتروني وسبل مكافحتها، مقال موجه للملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص 38.

[535]- **GHERAOUTI Solange**, Cybersécurité sécurité informatique et réseaux, 5e édition, Dunod, Paris, 2016, p 156

[536] – **سعدي الربيع**، مرجع سابق، ص 58.

[537]- **BOUTROS Mickael**, Le droit du commerce électronique: une approche de la protection du cyber consommateur, Thèse pour obtenir le grade de docteur en droit privé, université de Grenoble, 2014, p 120.

[538]– **صراع كريمة**، مرجع سابق، ص 79.أنظر كذلك: **لملوم كريم**، مرجع سابق، ص ص 169-170.

ثانيا: برامج حماية المعطيات الشخصية

1-الشهادات الإلكترونية

هي عبارة عن وثائق إلكترونية تثبت هوية المستخدمين عبر شبكة الإنترنت ويتولى إصدار هذه الشهادات جهة موثوق فيها تسمى سلطة إصدار الشهادات، تحتوي كل شهادة رقمية يتم اصدارها على معلومات مهمة تتعلق بمالكها وبالسلطة التي أصدرت هذه الشهادة[539].

2-أنظمة كشف الإختراق (برنامج المنظف)

من مميزات هذا البرنامج أنه ينبه صاحب الجهاز بوجود أي مخترق، بالإضافة لإمكانية تنظيف الجهاز وإخراج المخترق منه ويعتبر هذا البرنامج من أكثر البرامج فائدة في هذا المجال[540].

3- ضبط الوصول إلى الشبكة وإتاحة مواردها

أدى تزايد المخاطر الناشئة عن إنشاء شبكة الإنترنت وما سهلته للمخربين والمتسللين من اقتحام الشبكة وارتكاب كافة الجرائم إلى التفكير في ضرورة التغلب على هذه العقبة من خلال شبكات الاتصال ولذلك ظهر على السطح ما يعرف باسم "الشبكات الافتراضية".

تعتمد فكرة عمل الشبكة الافتراضية على نقل البيانات عن طريق توثيقها وتشفيرها باستخدام أكواد ومفاتيح سرية تكون معلومة لدى مختلف أطراف الشبكة الخاصة، وبالتالي يصعب على أي طرف خارجي الاطلاع على محتوى تلك البيانات وقراءتها حتى يصل إلى غايته[541]

---

[539] – **صراع كريمة**، مرجع نفسه، 82.

[540] – **سالم بن حامد بن علي البلوي**، مرجع سابق، 163.

[541]– تنقسم المتطلبات والبروتوكولات المطلوبة لإتشاء الشبكة إلى ما يلي:

– بوابة الشبكة (vpn gate way) ومعدات وبرمجيات الشبكة المطلوبة وذلك لكي تؤدي الشبكة الوضائف المطلوبة منها بفاعلية.

– البرامج التي سيتم تحميلها على الأجهزة أو محطات العمل وتقوم هذه البرامج بأداء الوظائف والأعمال على الشبكة.

– الحوائط النارية وهي البرامج والأجهزة اللازمة لتمكين الشبكة من القيام بمهامها بأمان.

4- جدران الحماية

تعتبر هذه الطريقة الأفضل لحماية الشبكات الداخلية من أخطار الشبكة، حيث أن الشبكة المراد حمايتها تجعل جميع بياناتها الداخلية تمر عبر الجدران التي تقوم بنقلها من وإلى الشبكة بعد فحصها.

يحتوي جدار النار على اثنين من الموجهات المرشحة للحزم وبوابة للتطبيقات حيث تمر جميع البيانات الداخلية والخارجية من الحاسب عبر هذين الموجهين الذين يعتبران ممرين عاديين مضاف إليهم بعض الوظائف الخاصة، وتتلخص طريقة عمل هذه الجدران في أن جميع الحزم تمر عن طريق الوجه الأول الذي يقوم بعمل محض لهذه الحزم ولا يسمح بمرور أي حزمة إلا لتلك التي تتفق مع معيار محدد من قبل واضع جدار النار، أما الحزم التي تفشل في هذا الفحص يتم اسقطها، وبعدما تمر الحزم الناجحة عبر بوابة التطبيقات التي تقوم بعمل اختبارات أخرى ومن ثم تتجه إلى الموجة الثانية التي يقوم بالتأكد من أنها خضعت لعملية الفحص ثم يمررها إلى المكان المرسلة إليه[542].

وتكمن أهمية جدران الحماية فيما يلي[543]:

1-قلة كمية البيانات المرسلة عبر الشبكات نسبيا مقارنة بالموجودة على الأجهزة، ومن هنا تكمن أهمية حماية البيانات الموجودة على الأجهزة.

- الموجات اللازمة لقيام الشبكة بوظائفها في نقل البيانات من نقطة لأخرى. أنظر في ذلك، **أيمن عبد الحفيظ**، مرجع سابق، ص 162.

[542] - **سالم بن حامد بن علي البلوي**، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2009، ص 161.

[543] - **منصور بن سعيد القحطاني**، مهددات الأمن المعلوماتي وسبل مواجهتها دراسة مسحية على منسوبي الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008، ص 58.

2-يتم أخذ الحذر عند إرسال البيانات عبر الشبكات، وتشفيرها إذا كانت بيانات خاصة وسرية، بينما تقل درجات الحذر للبيانات المخزنة في الأجهزة.

3-قد لا يدرك مستخدمي الحاسبات المرتبطة بشبكات محلية أن هذه الشبكات مرتبطة بشبكات أكبر، ولذلك لا يتخذون الاحتياطات اللازمة لحماية بياناتهم المخزنة في أجهزتهم.

4-يتوقف اختيار نوع جدار الحماية على حاجة المنظمة ومجال عملها، حيث توجد عدة أنواع من جدران الحماية لكل منها مميزات وإمكانيات مختلفة عن الأخرى، ومن أهم هذه الأنواع الموجهة الحاجب، الوسيط، والحارس.

نلاحظ أنه بالرغم من الجهود المبذولة من طرف الدول والمجتمع الدولي في مكافحة الجريمة المرتكبة عبر الإنترنت والتي توجت بوضع العديد من الآليات القانونية الموضوعية والإجرائية التي كانت في بداية تطبيقها جد فعالة، إلا أن فعاليتها تبقى نسبية وذلك راجع إلى نقص مواكبتها للتطورات التي تعرفها هذه الجريمة وذلك لاصطدامها بعدة عراقيل وتحديات.

تحدت الجريمة المرتكبة عبر الإنترنت عن طريق الخصوصية التي تتميز بها مختلف الإجراءات الموضوعة لمكافحتها، وذلك بإفرازها لمفاهيم جديدة في القانون الجزائي لم يكن يعرفها من قبل، حيث ألغت أهم المبادئ التي يقوم عليها هذا الشق من القانون وكرست مبادئ جديدة على المجتمع الدولي أخذها بعين الاعتبار.

تجلت الصعوبة في مكافحة الجريمة المرتكبة عبر الإنترنت في الطبيعة الخاصة لهذه الجريمة المتعدية للحدود الوطنية، والتي أثّرت على أساليب مكافحتها خاصة من حيث الجانب الإجرائي للقانون، فبالإضافة إلى التباين في التشريعات المجرّمة لهذه الأفعال بين الدول، هناك قصور كبير في الإجراءات المتّبعة لمتابعة هذه الجريمة على المستوى الدولي وذلك راجع لاصطدامها بعدّة مبادئ جامدة تعتمد عليها الدول في قوانينها الداخلية خاصة مبدأي السيادة وإقليمية النص القانوني، ضف إلى ذلك اعتماد الدول على القنوات

الدبلوماسية في تطبيق أغلب آليات التعاون الدولي سواء في شقه القضائي أو الأمني الأمر الذي لا يتماشى مع السرعة التي تتميز بها هذه الجريمة سواء من حيث الارتكاب أو من حيث سهولة التلاعب بالدليل في زمن قياسي.

بالإضافة إلى ذلك إن الإجراءات المتّبعة في مكافحة الجريمة المرتكبة عبر الإنترنت تشكّل خطرا على خصوصية الأفراد، وذلك لإمكانية اطلاع سلطات الاستدلال والتحقيق على أسرار متعلقة بالحياة الخاصة للأفراد سواء متعلقة بالمجرم أو أشخاص آخرين ليس لهم علاقة بموضوع الجريمة، الأمر الذي عجّل بمشرعيّ أغلب دول العالم ومنها المشرع الجزائري إلى وضع آليات قانونية وتقنية من أجل حماية الحق في الحياة الخاصة للأفراد، غير أن هذه الضمانات القانونية والتقنية أثّرت بطريقة سلبية على آليات مكافحة الجريمة المرتكبة عبر الإنترنت وذلك أن التقيّ دبها يحدّ من فعالية آليات مكافحة هذه الجريمة نظرا لاتسامها بالطول والتعقيد الأمر الذي لا يتماشى مع سرعة الجريمة.

وعليه فالمجتمع الدولي مدعو إلى إعادة النظر في الطريقة التي يتعامل بها مع هذا النوع المستحدث من الجرائم لتجاوز التحديات التي فرضتها هذه الأخيرة وعليه أن يتنازل على الكثير من المبادئ التقليدية التي كان يسير عليها، فالسيادة اليوم في هذا الفضاء الافتراضي ليس للدول بل لشبكة الإنترنت التي غيرت وجه العالم.

الخاتمة

الخاتمة

تبين لنا من دراستنا لموضوع آليات مكافحة الجريمة المرتكبة عبر الإنترنت أنها تعتبر ظاهرة إجرامية وليدة الثورة المعلوماتية التي عرفها العالم مؤخرا، فهي جريمة ترتكب في مجتمع يختلف كل الاختلاف عن المجتمع التقليدي الذي كنا نعرفه من قبل، والذي يتميز بخصوصيات وتقاليد تجعله مجتمع حديث بامتياز.

فمن خلال التطرق لمختلف الآليات القانونية الموضوعية أو الإجرائية التي سنتها مختلف التشريعات لمكافحة هذا النوع المستحدث من الجرائم، نجد أن المجتمع الدولي ومن ورائه الدول قد توصل إلى فكرة أنه من الضرورة اللجوء إلى قواعد خاصة لمكافحة هذه الجريمة بعد أن قام بتفعيل النصوص القانونية التقليدية القائمة لمكافحتها.

لاحظنا أن الجهود المبذولة على المستوى الدولي والرامية إلى مكافحة الجريمة المرتكبة عبر الإنترنت، لم يبق المجتمع الدولي مكتوف الأيدي بل سعى إلى مكافحة هذه الجريمة المستحدثة بكل جدية. وذلك عن طريق المنظمات الدولية المختلفة أهمها منظمة الأمم المتحدة.

انصبت مسألة مكافحة الجريمة المرتكبة عبر الإنترنت على المستوى الدولي منصبة على الجانب الموضوعي، وذلك من منطلق أن هذه الجرائم المستحدثة لم يعرفها القانون من قبل، وبالتالي سعى المجتمع الدولي عن طريق المنظمات الدولية إلى محاولة وضع آليات قانونية موضوعية فعالة في حصر هذه الجريمة ضمن قالب قانوني خاص، فكان تدخل المنظمات الدولية في هذا المجال عن طريق عقد المؤتمرات والمعاهدات الدولية وإرشاد الدول الأعضاء فيها للطريقة المثلى لمواجهة هذه الظاهرة الإجرامية.

لم تتوقف الجهود الدولية في هذا المجال عند هذا الحد بل امتدت إلى النطاق الإقليمي الذي كان له دور هام في وضع الآليات اللازمة لمكافحة الجريمة المرتكبة عبر الإنترنت، فرغم الفجوة الموجودة بين التكتلات الإقليمية، إلا أن جهودها كانت فعالة إلى أبعد الحدود، ونخص بالذكر جهود الإتحاد الأوروبي الذي وضع المعاهدة الخاصة بجرائم نظم المعلومات سنة 2001 ببودابست والتي تعتبر كمرجع بالنسبة لكافة الدول رغم أن منطلقها كان إقليمي وذلك لإلمامها بكل الجوانب المتعلقة بهذه الجريمة سواء من ناحية التجريم أو طرق المتابعة.

كما لا نغفل في هذا الصدد الجهود المبذولة على المستوى العربي والإفريقي، فرغم أنها جاءت متأخرة وتميز هذه الأخيرة بالتخلف في مجال تقنيات الاتصال مقارنة بالعالم المتقدم، إلا أنها تبقى محاولات جادة سعى من خلالها المشرعين في هذه الدول إلى مواكبة العالم المتقدم في تكريس هذه الآليات من أجل مكافحة هذا النوع المستحدث من الإجرام.

عاصرت الجهود الدولية الموضوعية جهود أخرى تمثلت في وضع آليات إجرائية تتماشى مع النصوص الموضوعية لضمان متابعة قانونية سليمة وفعالة لمرتكبي جرائم الإنترنت، والملاحظ في هذا الصدد أن هذه الآليات منصبة في مجملها حول التعاون الدولي سواء في شقه القضائي أو الأمني.

ركّز المجتمع الدولي على التعاون القضائي والأمني الدوليين باعتباره الطريقة المثلى لمكافحة الجريمة المرتكبة عبر الإنترنت العابرة للحدود، كون أن الدول لا تستطيع مكافحة هذه الجريمة منفردة، لهذا فعّل عدة آليات إجرائية قضائية دولية مثل المساعدة القضائية الدولية ونظام تسليم المجرمين، كما تم وضع الآليات التي بمقتضاها يتم التعاون الأمني بين الدول مثل التدريب الأمني المتبادل والقيام بعمليات مشتركة بين الدول، وخير مثال على ذلك الجهود المبذولة في إطار المنظمة الدولية للشرطة الجنائية في إطار مكافحة الجريمة المرتكبة عبر الإنترنت.

تكمن فعالية الآليات القانونية الرامية إلى مكافحة الجريمة المرتكبة عبر الإنترنت سواء موضوعية كانت أو إجرائية في الطريقة التي من خلالها وضف المجتمع الدولي هذه الأخيرة.

نلاحظ أن المجتمع الدولي سلك طريق المرافقة وإرشاد الدول إلى كيفية معالجة هذه الظاهرة الإجرامية المستحدثة، وخير دليل على ذلك ما قامت به المنظمات الدولية من عقد لمؤتمرات وتقديمها لإرشادات مهدت الطريق للدول الأعضاء فيها إلى وضع نصوص قانونية شاملة لكل جوانب هذه الجريمة، سواء من ناحية تحديد ماهيتها أو طريقة تجريمها، فرغم أن هذه الصكوك من الناحية النظرية لا تتميز بالإلزامية، إلا أنها من الناحية العملية كانت

العنصر الفعال في الساحة التشريعية الذي وضعت بمقتضاه أهم المبادئ الكفيلة بمكافحة هذه الجريمة.

تتجلى كذلك فعالية الآليات الإجرائية الدولية في هذا المجال في اعتماد المجتمع الدولي على طريق التعاون الدولي، وذلك لفهمه أن الدول لن تستطيع مكافحة هذه الجريمة المستحدثة منفردة، ونظرا لمساس هذه الأخيرة بمصالح العديد من الدول في آن واحد، فمغزى التعاون الدولي في هذا المجال هو عدم ترك ملاذ يمكن للجاني أن يلجأ إليه وبالتالي يفلت من المتابعة والجزاء، حيث تعتبر فعالية هذا التعاون كبيرة في إطاره الأمني عن طريق تبادل المعلومات الأمنية.

واكبت التشريعات الوطنية الحركية التشريعية التي انطلقت على المستوى الدولي، ووضعت الآليات القانونية اللازمة لمكافحة الجريمة المرتكبة عبر الإنترنت، وذلك عن طريق إسقاط وتكريس أهم المبادئ التي تعنى بمكافحة هذه الجريمة في قوانينها الداخلية سواء موضوعية كانت أو إجرائية ومن بينها التشريع الجزائري.

ساير المشرع التشريعات الدولية حتى وإن كان متأخرا في وضع المبادئ الأساسية لمكافحة هذه الظاهرة الإجرامية المستحدثة، حيث أن عقيدة المشرع في ذلك انبثقت من إيمانه أنه ليس بمعزل عن هذه الجرائم نظرا لتشعبها وتعديها للحدود الدولية من جهة، ومن جهة أخرى تفاقم الخسائر المنجرة عنها.

حاول المشرع في بادئ الأمر مكافحة الجريمة المرتكبة عبر الإنترنت عن طريق وضعها في إطار القوانين التقليدية القائمة وذلك بتحيينها وتعديلها، وخير مثال عن ذلك تعديله لقانون العقوبات بوضعه لباب في هذا الأخير سماه "جرائم المساس بأنظمة المعالجة الالية للمعطيات"، غير أن تطور الجريمة المرتكبة عبر الإنترنت جعله يغير من عقيدته التشريعية ليذهب إلى وضع نصوص قانونية جديدة.

كما تم تكريس أهم المبادئ الموضوعية على المستوى الدولي بعد مصادقته على معاهدات واتفاقيات دولية في مجال جرائم نظم المعلوماتية في قوانينه الداخلية، هذا التكريس انجر عنه وضع المشرع لقوانين خاصة بمكافحة هذه الجريمة المستحدثة، ولعل أهمها

القانون رقم 09-04 المتضمن قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، وكذلك قانون التجارة الإلكترونية وقانون البريد والاتصالات الإلكترونية الذين وضعوا آليات قانونية جد فعالة لمتابعة الجريمة المرتكبة عبر الإنترنت.

وقام كذلك بعد حصر الجريمة المرتكبة عبر الإنترنت في إطارها القانوني الموضوعي، بوضع آليات إجرائية لكي تكون هناك متابعة فعالة لهذه الجريمة، وذلك إيمانا منه أن القاعدة القانونية الموضوعية إذا لم تتبعها إجراءات سليمة تبقى حبر على ورق ولن تنتج عنها الآثار المرجوة منها.

فعّل في بادئ الأمر الآليات الإجرائية التقليدية المنصوص عليها في قانون الإجراءات الجزائية، وذلك عن طريق تحيينها لتواكب التطور الذي تعرفه الجريمة المرتكبة عبر الإنترنت، وأهمها التفتيش والمعاينة والخبرة، ليتبعها بوضع آليات إجرائية مستحدثة خاصة بهذا النوع الجديد من الجرائم، مثل اعتراض المراسلات السلكية واللاسلكية وإجراء التسرب وحفظ المعطيات المتعلقة بحركة السير والتي أثبتت فعاليتها ميدانيا، وخير دليل على ذلك الكم الهائل من القضايا التي تمت معالجتها من طرف الضبطية القضائية أو التي تم حلها من قبل الجهات القضائية المختصة بذلك.

نستنتج من النصوص الموضوعية التي وضعها المشرع بغرض تجريم الجريمة المرتكبة عبر الإنترنت أنها جد فعالة، وذلك – باستخلاص نية المشرع- راجع إلى سلوك هذا الأخير سياسة التجريم العام والشامل بهدف سد الثغرات القانونية التي تتولد عن التطور المستمر للجريمة، حيث تعتبر هذه الطريقة في نظرنا جد فعالة لتفادي خروج الأفعال الإجرامية الجديدة من دائرة التجريم.

أثبتت الآليات الإجرائية فعاليتها في مكافحة الجريمة المرتكبة عبر الإنترنت بالخصوص الإجراءات المستحدثة سواء المنصوص عليها في قانون الإجراءات الجزائية مثل التفتيش واعتراض المراسلات الإلكترونية، أو ما هو منصوص عليه في قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال مثل حفظ المعطيات المتعلقة بحركة السير، فهذه الإجراءات أدت إلى إمكانية مراقبة كل التصرفات الدائرة من خلال سبكات الاتصال بما فيها

الإنترنت من الناحية العملية، الأمر الذي سمح لضباط الشرطة القضائية إلى التوصل لمرتكبي الجرائم في هذا الفضاء الافتراضي بكل سهولة.

غير أن فعالية الآليات القانونية الموضوعية والإجرائية المتبعة في مكافحة الجريمة المرتكبة عبر الإنترنت على المستوى الدولي أو الوطني تبقى نسبية وقاصرة لاصطدامها بعدة صعوبات، وذلك لارتباطها ببعض المعايير، منها ما هو منصب على الطبيعة الخاصة للجريمة في حد ذاتها، ومنها ما يتعلق بالطابع المتعدي للحدود أو ما يتعلق بضرورة حماية الحق في الحياة الخاصة للأفراد، والتي تعتبر تحديات كبيرة للدول والمجتمع الدولي على حد سواء بحيث عليهم تجاوزها إن أرادوا الوصول إلى مكافحة كاملة الفعالية لهذا النوع المستحدث من الجرائم.

تتجلى أولى الصعوبات التي حدّت من فعالية آليات مكافحة الجريمة المرتكبة عبر الإنترنت في الطبيعة الخاصة لهذه الجريمة، فهي تختلف كل الاختلاف عن الجرائم المرتكبة في العالم التقليدي، بحيث إن كانت هذه الأخيرة ترتكب في وسط مادي محسوس، فجرائم الإنترنت ترتكب في عالم افتراضي غير مادي والذي انجر عنه غياب الدليل المادي الذي بمقتضاه تتم إدانة المتهم.

بالإضافة إلى ذلك فإن خصوصية الجريمة المرتكبة عبر الإنترنت ألقت بظلالها على كافة أطراف الجريمة وسلطات التحقيق فيها، فالمجرم المعلوماتي الذي يرتكب هذا النوع من الجرائم يختلف بدوره عن المجرم التقليدي وذلك بتمتعه بالمهارة والذكاء والعلم في مجال التقنية الذي يحيط دائما نفسه بحواجز تكنولوجية تجعل الوصول إليه أمر صعب للغاية، والعكس بالنسبة للمجني عليه الذي نجده في الغالب تنقصه الخبرة والمعرفة في هذا المجال، وأن كانت لديه فهو يحجم عن التبليغ خوفا على نفسه أو عائدات مؤسسته الأمر الذي يصعب اكتشاف هذه الجريمة، وما زاد الطين بلة أن سلطات التحقيق والاستدلال في هذه الجرائم تنقصهم الخبرة وذلك راجع لعدم مواكبتهم للتطورات التي تعرفها الجريمة المرتكبة عبر الإنترنت.

الخاتمة

يصطدم الطابع الدولي للجريمة المرتكبة عبر الإنترنت بمبدأ سيادة الدولة على إقليمها، فهذا المبدأ في نظرنا يعتبر من أكبر العراقيل التي تواجه الآليات الموضوعة لمكافحة هذه الجريمة، حيث أن المبدأ السالف ذكره يجعل الإتيان بإجراءات متابعة الجريمة أمر صعب للغاية، وذلك لعدم قبول أي دولة تطبيق نصوص قانونية غير وطنية على إقليمها، مما أدى بها إلى اللجوء إلى القنوات الدبلوماسية التي أثبتت طول إجراءاتها مقارنة بالسرعة في ارتكاب الجريمة عبر الإنترنت وكذلك سرعة تطور هذه الأخيرة.

تعتبر كذلك مشكلة تحديد القانون الواجب التطبيق والمحكمة المختصة بالنظر في الجريمة المرتكبة عبر الإنترنت من بين أهم الصعوبات التي انجرت عن الطابع الدولي لهذه الأخيرة، وذلك راجع لتشعبها عبر الحدود الدولية، الأمر الذي جعل تحديد مكان وقوعها ومكان تحقق النتيجة الإجرامية ومكان الإتيان بالسلوك الإجرامي فيها يتميز بصعوبات كبيرة.

يعتبر كذلك حماية الحق الحياة الخاصة للأفراد هو الآخر من بين العراقيل التي واجهت آليات مكافحة الجريمة المرتكبة عبر الإنترنت، وكان تأثير هذا الحق على الجانب الإجرائي كبيرا، وذلك سواء عن طريق التأثير القانوني المتمثل في ضرورة احترام حقوق وحريات الأفراد أثناء القيام بالبحث والاستدلال عن هذه الجريمة، الأمر الذي يحد من فعالية هذه الإجراءات بالنظر إلى السرعة التي ترتكب بها الجريمة وسهولة إخفائها عن سلطات التحقيق والاستدلال، أو عن طريق التأثير التقني، وذلك بالرجوع إلى السماح للأفراد باستعمال مختلف التقنيات التي تنتجها الشبكة لحجب المعلومات الخاصة بهم مثل التشفير، وذلك لحماية خصوصياتهم، غير أن في حالة ارتكاب جريمة من الجرائم في هذا النطاق يجعل هذه التقنيات من العقبات الكبيرة التي تحد من إجراءات البحث والاستدلال والتحقيق فيها.

ومن أجل تجاوز الصعوبات والعراقيل التي حدّت من فعالية الآليات المكرّسة لمكافحة الجريمة المرتكبة عبر الإنترنت وجعلتها تتسم بالقصور نقدم بعض الاقتراحات مساهمة منا في ايجاد الحلول والتي نعرضها على النحو التالي:

1-الحد من الفجوة الموجودة بين العالم المتقدم والعالم المتخلف في مجال تكنولوجيا الإعلام والاتصال والتشريعات الخاصة بها، من أجل التقليل من التباين الموجود بين تشريعات الدول والقضاء على إشكالية عدم وجود تجريم مزدوج فيها، لكي لا تتولد عن هذه الحالة خلق ملاذات للمجرمين داخل الدول التي لا تحتوي على نصوص تجرم هذه الأفعال.

2-حث المجتمع الدولي على تعزيز وتطوير آليات التعاون الدولي في مجال مكافحة الجريمة المرتكبة عبر الإنترنت سواء في شقه القضائي أو الأمني.

3-مطالبة المجتمع الدولي على تجاوز الإجراءات القضائية الدولية القائمة التي تتسم بطول مدتها، واللجوء إلى وضع إجراءات جديدة أكثر فعالية عن طريق ربط قنوات اتصال دولية مباشرة بين مختلف جهات إنفاذ القانون عبر العالم لمواكبة سرعة هذه الجريمة.

4-حث الدول على استعمال هذه الشبكة وما أفرزته من مواقع للتواصل الاجتماعي في توعية وتحسيس الأفراد من مخاطر الجريمة المرتكبة عبر الإنترنت، وحثهم كذلك عن التبليغ عليها.

5-التنسيق بين الدول وحثها على التعديل والتحيين المتواصل للنصوص القانونية سواء الموضوعية منها أو الإجرائية لكي تواكب التطورات السريعة التي تعرفها الجريمة المرتكبة عبر الإنترنت.

6-حث الدول على التقليل من التمسك بمبدأ سيادة الدولة على إقليمها لتسهيل إجراءات متابعة الجريمة المرتكبة عبر الإنترنت، بشرط أن تتم في إطار التبادل الشفاف للمعلومات، وفي إطار المعاملة بالمثل، لأن شبكة الإنترنت غيرت من مفهوم هذا المبدأ وأصبحت السيادة لمواقعها وليس للدول.

7-حث الدول على تفعيل مبدأ عالمية النص الجزائي تماشيا مع طبيعة عالمية شبكة الإنترنت.

8-ضرورة توسيع المشرع لنطاق اختصاص الضبطية القضائية وجعله اختصاصا وطنيا، أو استحداث جهاز يتميز بالاستقلالية لمكافحة الجريمة المرتكبة عبر الإنترنت بالنظر للتطورات

التي تعرفها هذه الأخيرة، يكون المنتسبون فيه من الأفراد المتخصصين والمكونين من الناحية القانونية والتقنية.

9- التكوين المستمر لجهات التحقيق والنيابة العامة وقضاة الحكم حول التطورات التي تعرفها الجريمة المرتكبة عبر الإنترنت وأهم التعديلات في النصوص التشريعية الموضوعة على المستوى الدولي أو على مستوى الدول التي تعرف تقدما في هذا المجال.

10- ضرورة تكوين أعضاء الهيئة التشريعية في مجال تقنية المعلومات وتكنولوجيا الإعلام والاتصال بما أنهم المعنيون بالجانب التشريعي الذي يكفل مكافحة الجريمة المرتكبة عبر الإنترنت.

11- ضرورة استحداث أقطاب جزائية جهوية خاصة بالنظر في الجرائم التي ترتكب عبر الإنترنت يكون القضاة فيها من المتخصصين في الجانب القانوني لهذه الجرائم والجانب الفني والتقني الخاص بها.

12- ضرورة استحداث تخصصات علمية في مجال تكنولوجيا نظم المعلوماتية ومكافحة الإجرام المنجر عنها على مستوى الجامعات ومراكز البحث الوطنية.

قائمة المراجع والمصادر

أولاً – باللغة العربيّة:

1 – الكتب

1. **أميمة معراوي**، التسوق الإلكتروني، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2020
2. **إياس بن سمير الهاجري**، أمن المعلومات على شبكة الإنترنت، ندوة حقوق الملكية الفكرية، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004
3. **محمد فتحي عيد**، الإنترنت ودوره في انتشار المخدرات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003
4. **غسان فطوم**، حقوق المؤلف والملكية الفكرية والحقوق المجاورة في العالم العربي والشرق الأوسط، منشورات الاتحاد الدولي للصحفيين، بروكسل، 2020
5. **عبد الله عبد الكريم عبد الله**، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دار الجامعة الجديدة، مصر، د س ن.
6. **منى الأشقر جبور**، **محمد جبور**، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، 2018.
7. **ليلى القجيري**، الدليل العلمي للمخاطر المرتبطة بجرائم الإنترنت المحدقة بالطفل، منشورات المنظمة الإسلامية للتربية والعلوم والثقافة، الرباط، 2012.
8. **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي دراسة مقارنة، دار الكتب القانونية، الإسكندرية، 2011.
9. **يوسف حسن يوسف**، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011.

10. **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، 2009.
11. **خثير مسعود**، الحماية لبرامج الكمبيوتر أسايب وثغرات، دار الهدى، عين مليلة، الجزائر، 2010.
12. **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2007.
13. **أمير فرج يوسف**، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
14. **سليم عبد الله الجبوري**، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011.
15. **مؤيد زيدان**، حقوق الملكية الفكرية، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2020.
16. **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004.
17. **رياض فتح الله بصلة**، جرائم بطاقة الائتمان دراسة معرفية تحليلية لمكوناتها وأساليب تزييفها وطرق التعرف عليها، دار الشروق، القاهرة، 1995.
18. **محمد حماد مرهج الهيتي**، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2006.
19. **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.
20. **محمد واصل، حسين بن علي الهلالي**، الخبرة الفنية أمام القضاء دراسة مقارنة، منشورات المكتب الفني للمحكمة العليا، سلطنة عمان، 2004.

21. **خيرت علي محرز**، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012.
22. **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، الإسكندرية، 2006.
23. **بوكر رشيدة**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012.
24. **علي بن عبد الله عسيري**، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
25. **علي بن عبد الله عسيري**، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
26. **محمد حمدان عاشور**، أساليب التحقيق والبحث الجنائي، أكاديمية فلسطين للعلوم الأمنية، الشئون الأكاديمية، قسم المناهج، فلسطين، 2010.
27. **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008.
28. **شرف الدين كامل**، الجريمة المنظمة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000.
29. **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة جرائم المعلوماتية، د.د.ن، د.س.ن، 2005.
30. **عبد الله بن سعود محمد السراني**، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

31. **محمد سيد سلطان**، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، د.ب.ن، 2016.
32. **عبد الله بن عبد العزيز اليوسف**، أساليب تطوير البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
33. **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
34. **حمد دباس الحميد، ماركو إبراهيم نينو**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، 2006.
35. **حسن طاهر داود**، جرائم نظم المعلومات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.
36. **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.
37. **طارق عفيفي صادق أحمد**، الجرائم الإلكترونية جرائم الهاتف المحمول دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.
38. **فريد منعم جبور**، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010.
39. **عبد الرحمان خلفي**، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس، الجزائر، 2015.
40. **محمود أحمد عبابنة**، جرائم الحاسوب وأبعدها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004.

41. **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004.
42. **محمد عبيد الكعبي**، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهظة العربية، القاهرة، د.س.ش.
43. **علي جبار الحسيناوي**، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، 2011.
44. **عبد الرحمان شعبان عطيات**، أمن الوثائق والمعلومات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
45. **أشرف السعيد أحمد**، القرصنة الإلكترونية، مطابع الشرطة، القاهرة، 2013.

2 – <u>الرسائل والمذكرات الجامعية</u>

أ- **<u>رسائل الدكتوراه:</u>**

1. **إسماعيل بن وصفي غانم الآغا**، سوء استخدام تقنية الإنترنت والجوال ودورها في انحراف الأحداث بدول مجلس التعاون الخليجي، أطروحة مقدمة استكمالا للحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العلوم الاجتماعية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009
2. **بن خليفة إلهام**، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه علوم في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2015-2016
3. **تركي بن عبد الرحمن المويشر**، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009

4. **بن حليمة ليلى**، الحماية القانونية لحقوق المؤلف بين التشريع الجزائري والتشريع الأردني، أطروحة مقدمة لنيل شهادة دكتوراه العلوم علوم قانونية، تخصص ملكية فكرية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2016-2017
5. **بوزيدي أحمد التيجاني**، حماية حق المؤلف في إطار النشر الإلكتروني -دراسة مقارنة-، أطروحة لنيل شهادة دكتوراه علوم تخصص ملكية فكرية، كلية الحقوق، جامعة الجزائر 1، 2019/2018.
6. **بشان عبد النور**، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2018/2017.
7. **بوكر رشيدة**، الحماية الجزائية للتعاملات الإلكترونية، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2017.
8. **درار نسيمة**، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني -دراسة مقارنة-، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015-2016.
9. **بوصلعة ثورية**، السياسة الجنائية والأمنية في مواجهة الجريمة العابرة للحدود، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.
10. **رابحي عزيزة**، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.

11. **بن زحاف فيصل**، تسليم مرتكبي الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي والعلاقات السياسية الدولية، كلية الحقوق والعلوم السياسية، جامعة وهران، 2011-2012.

12. **عصماني ليلى**، التعاون الدولي لقمع الجرائم الدولية، رسالة لنيل شهادة الدكتوراه في القانون الدولي، كلية الحقوق والعلوم السياسية، جامعة وهران، 2012-2013.

13. **ربيعي حسن**، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015-2016.

14. **خزار لمياء**، الحكومة الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون، تخصص قانون إداري وإدارة عامة، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة 1، 2017-2018.

15. **حابت آمال**، التجارة الإلكترونية في الجزائر، رسالة لنيل شهادة دكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2015.

16. **دعاس كمال**، حق المؤلف في ميدان المصنفات الرقمية، أطروحة دكتوراه علوم في القانون، كلية الحقوق، جامعة الجزائر 1، 2018.

17. **بن زواوي سفيان**، عقد الترخيص باستغلال براء الاختراع في التشريع الجزائري، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في القانون الخاص، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2020/2019.

18. **مخلوفي عبد الوهاب**، التجارة الإلكترونية عبر الإنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012.

19. **خليفي مريم**، الرهانات القانونية للتجارة الالكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011-2012.

20. **خميخم محمد**، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية -دراسة مقارنة-، أطروحة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.

21. **بلخير محمد آيت عودية**، الضبط الإداري للشبكات الاجتماعية الإلكترونية، أطروحة لنيل شهادة دكتوراه العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2019/2018.

22. **بن فردية محمد**، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2015.

23. **براهيمي جمال**، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018.

24. **ملياني عبد الوهاب**، أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2016-2017.

25. **مجراب الدوادي**، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام، كلية الحقوق، جامعة الجزائر، 2015-2016.

26. **بن طالب ليندا**، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2019.

27. **مرنيز فاطمة**، الإعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013.

28. **غازي عبد الرحمان هيان الرشيد**، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.

29. **حفصي عباس**، جرائم التزوير الإلكترونية دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم الإسلامية تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران، 2015.

30. **بن حيدة محمد**، حماية الحق في الحياة الخاصة في التشريع الجزائري، رسالة مقدمة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2016-2017.

31. **بن سعيد صبرينة**، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال"، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2014-2015.

32. **عاقلي فضيلة**، الحماية القانونية للحق في حرمة الحياة الخاصة دراسة مقارنة، بحث مقدم لنيل شهادة دكتوراه علوم تخصص قانون، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2011-2012.

33. **نويري عبد العزيز**، الحماية الجزائية للحياة الخاصة –دراسة مقارنة–، أطروحة لنيل شهادة دكتوراه علوم، شعبة القانون الجنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2010–2011.

34. **بشاتن صفية**، الحماية القانونية للحياة الخاصة دراسة مقارنة، رسالة لنيل شهادة دكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012.

35. **تومي يحيى**، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيا الاعلام والاتصال، أطروحة من أجل نيل شهادة الدكتوراه علوم، تخصص قانون، كلية الحقوق، جامعة الجزائر، 2017–2018.

36. **محمودي نور الهدى**، مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي، –دراسة مقارنة–، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة 1، 2017–2018.

37. **إبراهيم بن سطم بن خلف العنزي**، التوقيع الإلكتروني وحمايته الجنائية، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الدكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

38. **سعدي الربيع**، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015–2016.

39. **جامع مليكة**، حماية المستهلك المعلوماتي، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية (القانون الخاص)، كلية الحقوق والعلوم السياسية،

قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2017-2018.

ب- **مذكرات الماجستير**

1. **بن يطو أسامة**، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الإختراع، مذكرة مقدمة لاستكمال نيل شهادة الماجستير في القانون، تخصص قانون الملكية الفكرية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة 1، 2018.
2. **جلول دواجي بلحول**، الحماية القانونية للمستهلك في ميدان التجارة الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2014-2015.
3. **فتحي نسييمة**، الحماية الدولية لحقوق الملكية الفكرية، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012.
4. **بن ديدي جميلة**، الحماية الوطنية والدولية للمصنفات الأدبية، مذكرة مكملة لنيل شهادة الماجستير في القانون، تخصص الملكية الفكرية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2015-2016.
5. **خالد بن عبيد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

6. **ذنايب آسية**، الأليات الدولية لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة لنيل شهادة ماجستير في القانون العام، فرع علاقات دولية وقانون المنظمات الدولية، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، 2009-2010.
7. **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2012-2013.
8. **فنور حساين**، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مذكرة من أجل الحصول على شهادة الماجستير، تخصص القانون الدولي والعلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2012-2013.
9. **قارة آمال**، الجريمة المعلوماتية، مذكرة مقدمة من أجل الحصول على درجة الماجستير، كلية الحقوق، جامعة الجزائر، سنة 2001-2002.
10. **حمودي ناصر**، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة الماجستير، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2015.
11. **بوذراع عبد العزيز**، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2011-2012.
12. **بن عقون حمزة**، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012.
13. **خالد بن عبيد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية دراسة تحليلية مقارنة، بحث مقدم

استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

14. **لالوش راضية،** أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2012.
15. **عبد العزيز محمد سعد البواردي،** السياسة الجنائية المعاصرة في حماية التجارة الإلكترونية دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2011.
16. **خشة حسيبة،** وسائل الدفع الحديثة في القانون الجزائري، مذكرة لنيل شهادة الماجستير، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة المسيلة، 2016.
17. **محمد بن نصير السرحاني،** مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، د س ن.
18. **سلامة محمد المنصوري،** تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال الحصول على درجة الماجستير في القانون، كلية الحقوق، قسم القانون العام، جامعة الإمارات العربية المتحدة، نوفمبر 2018.
19. **قريشي حمزة،** الوسائل الحديثة للبحث والتحري في ضوء قانون 06-22 دراسة مقارنة، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي،

كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة قاصدي مرباح، ورقلة، 2012.

20. **بن لاغة عقيلة**، حجية أدلة الإثبات الجنائية الحديثة، مذكرة لنيل شهادة الماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2011-2012.

21. **مذكور عائشة**، الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون العقود، كلية الحقوق والعلوم السياسية، جامعة آكلي محند أولحاج، البويرة، 2018.

22. **محسن بن سليمان الخليفة**، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام (جريمة استنساخ برامج الحاسب اللآلي وبيعها وإنتاج الفيروسات ونشرها)، رسالة مقدمة استكمالا للحصول على درجة الماجستير، كلية الدراسات العليا، قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، د.س.ن.

23. **عبد الله بن حسين آل حجراف القحطاني**، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية دراسة على المحققين في هيئة التحقيق والادعاء العام بمدينة الرياض، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.

24. **حمزة بن عقون**، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2011-2012.

25. **ثنيان ناصر آل ثنيان**، إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير،

تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

26. **فنور حاسين**، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، مذكرة من أجل الحصول على شهادة الماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق، جامعة الجزائر، 2013/2012.

27. **صغير يوسف**، الجريمة المرتكبة عبر الإنترنت، مذكرة مقدمة للحصول على شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2013.

28. **سليم جلاد**، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، مذكرة لنيل شهادة الماجستير في الشريعة والقانون، تخصص حقوق الإنسان، كلية العلوم الإنسانية والحضارة الإسلامية، قسم العلوم الإسلامية، جامعة وهران، 2012-2013.

29. **بن حيدة محمد**، الحق في الخصوصية في التشريع الجزائري "دراسة مقارنة"، مذكرة لنيل شهادة الماجستير، تخصص حقوق وحريات، كلية الآداب والعلوم الإنسانية، قسم العلوم القانونية والإدارية، جامعة أدرار، 2009-2010.

30. **سليمان بن عبد الله بن سليمان العجلان**، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي دراسة تطبيقية مقارنة، رسالة مقدمة استكمالا لنيل درجة الماجستير في العدالة الجنائية، تخصص سياسة جنائية، كلية الدراسات العليا، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005.

31. **طارق عثمان**، الحماية الجنائية للحياة الخاصة عبر الإنترنت دراسة مقارنة، مذكرة مقدمة لنيل شهادة الماجستير ، فرع القانون الجنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2006-2007.

32. **علوي سالم**، أدلة الاثبات في التحقيق الجنائي، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق جامعة الجزائر 01، 2016/2017.

33. **لملوم كريم**، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2011.

34. **صراع كريمة**، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة مقدمة لمتطلبات نيل شهادة الماجستير في العلوم التجارية، تخصص استراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2014.

35. **سالم بن حامد بن علي البلوي**، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2009.

36. **منصور بن سعيد القحطاني**، مهددات الأمن المعلوماتي وسبل مواجهتها دراسة مسحية على منسوبي الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008.

3- المقالات:

1. **حفوظة الأمير عبد القادر، غرداين حسام،** «واقع جرائم تكنولوجيا الإعلام والاتصال وسبل التصدي لها محليا، عربيا ودوليا»، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي بتندوف، العدد الأول، جوان 2017، ص ص 158-186.
2. **مراد مشوش،** «الجهود الدولية لمكافحة الإجرام السيبراني»، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 12، العدد 02، 2019، ص ص 703-726.
3. **فيصل كامل نجم الدين،** «واقع الجريمة الإلكترونية في مواقع التواصل الإجتماعي الحماية النظامية في دول مجلس التعاون الخليجي»، المجلة الدولية للاتصال الإجتماعي، جامعة عبد الحميد ابن باديس، مستغانم، المجلد 05، العدد 04، سنة 2018، ص ص 07-31
4. **بن يطو أسامة، عبدلي حمزة،** «حماية برامج الحاسب الآلي في ضوء التشريع الجزائري والمواثيق الدولية»، مجلة معارف، قسم العلوم القانونية، جامعة البويرة، العدد 19، ديسمبر 2015، ص ص 122-153.
5. **موسى مرمون،** «أثر اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية trips في التشريع الجزائري في مجال براءات الإختراع الدوائية»، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد 31، عدد 4، ديسمبر 2020، ص ص 569-588.
6. **سعيداني سلامي،** «تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (واقع ومقاربات)»، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة المسيلة، العدد العاشر، المجلد الأول، سنة 2018، ص ص 190-205.

7. **بن قارة مصطفى عائشة**، «الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية»، المجلة العربية للعلوم ونشر الأبحاث، المركز القومي للبحوث، فلسطين، المجلد الثاني، عدد 5، يونيو 2016، ص ص 38-52.

8. **شوقي يعيش تمام، عزيزة شبري**، «تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية»، مجلة الإجتهاد القضائي، مخبر أثر الإجتهاد القضائي على حركة التشريع، العدد 15، جامعة محمد خيضر بسكرة، سبتمبر 2017، ص ص 92-102.

9. **حاج مخناش نوال**، «التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الإتمان»، مجلة العلوم القانونية والسياسية المجلد 10، العدد01، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، ص ص1118-1135.

10. **أحمد حمي، كيسي زهيرة**، «صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 10، العدد01، ص ص776-795.

11. **موفق علي عبيد، ساهر ماضي ناصر**، «ماهية جريمة الاحتيال المعلوماتي»، مجلة جامعة تكريت للعلوم القانونية، السنة 07، العدد 25، سنة 2015، ص ص 184-226.

12. **شرف الدين وردة، بشير سليم**، «حل مشكلة تنازع الاختصاص الدولي في مجال مكافحة جرائم التجارة الإلكترونية»، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر، بسكرة، المجلد 05، العدد 01، 2019، ص ص118-135.

13. **خديجة خالدي**، «آلية الاتحاد الإفريقي للتعاون الشرطي أفريبول»، مجلة العلوم الإجتماعية والإنسانية، العدد الخامس عشر، جامعة المسيلة، د.س.ن، ص ص 65-79.

14. **نقموش محمد، ميلودية أحمد**، «الجريمة المعلوماتية: المفهوم-حتمية تطوير آليات التعاون الدولي في مجال مكافحتها»، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، العدد 02، المجلد 04، جوان 2018، ص ص266-283.

15. **ربيعة فرحي**، «المساعدة القانونية المتبادلة كآلية للتعاون الدولي الأساس القانوني ومعوقات التفعيل»، مجلة المفكر للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة بسكرة، المجلد 03، العدد 04، ديسمبر 2020، ص ص 98-110.

16. **محمد أحمد سليمان عيسى**، «التعاون الدولي لمواجهة الجرائم الإلكترونية»، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، المجلد 14، العدد 2، 2016، ص ص 50-66.

17. **عصماني ليلى، صهيب سهيل غازي زامل**، «المساعدة القضائية الدولية كآلية للحصول على الدليل الإلكتروني»، مجلة القانون المجتمع والسلطة، المجلد 09، العدد 02، جامعة وهران 2، سنة 2020، ص ص 11-33.

18. **زغودي عمر**، «الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية»، مجلة البحوث القانونية والاقتصادية، المركز الجامعي آفلو، الأغواط، المجلد 02، العدد 02، ماي 2020، ص ص 101-118.

19. **جيلالي حسين**، «التعاون الجنائي الدولي في مكافحة الجريمة العالمية»، مجلة القانون، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد

زبانة غيليزان، المجلد 07، العدد 02، 2018، ص ص 08-27.

20. **علواش فريد**، «نظام تسليم المجرمين في الاتفاقيات الدولية»، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، العدد 05، المجلد 02، جانفي 2017، ص ص399-411.

21. **خرشي عثمان**، «تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية»، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، العدد العاشر، جوان 2018، ص ص 916-942.

22. **لعطب بختة**، «أشكال التعاون الدولي في مكافحة الجرائم الدولية»، مجلة المعيار، المركز الجامعي تيسمسيلت، العدد 04، ديسمبر 2011، ص ص 102-110.

23. **قارة أمال**، «تفعيل آليات تسليم المجرمين في إطار المنظمة الدولية للشرطة الجنائية»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص ص890-907.

24. **حسين بن سعيد بن سيف الغافري**، «الجهود الدولية في مواجهة جرائم الإنترنت»، مقال متوفر على الموقع التالي: www.minchawi.com

25. **لورنس سعيد الحوامدة**، «الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة»، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، المجلد الرابع، العدد الأول، 2017، ص ص 183-220.

26. **محمد أبو العلا عقيدة**، «التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية»، مقال منشور على الموقع: www.arablawinfo.com

27. **مايا خاطر**، «الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها»، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الثالث، سنة 2011، ص ص 509-526.

28. **عقون مصطفى**، «دور منظمة الشرطة الجنائية الدولية الإنتربول في مكافحة الجريمة المنظمة»، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، العدد الخامس، ديسمبر 2015، ص ص 210-229.

29. **معمر بن علي، عبد المالك الدح**، «الوسائل المتاحة لمنظمة الأنتربول لمجابهة الجريمة المنظمة»، مجلة البحوث القانونية والاقتصادية، المجلد 02، العدد 02، المركز الجامعي آفلو، الأغواط، ماي 2020، ص ص 130-143.

30. **قسمية محمد**، «الوسائل الفنية للمنظمة الدولية للشرطة الجنائية (الأنتربول) كآلية للتعاون الدولي الشرطي»، حوليات جامعة الجزائر، المجلد 34، العدد 02، سنة 2020، ص ص 124-137.

31. **بلعيور محمد نذير، بوعيشة بوغوفالة**، «دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة»، مجلة البحوث القانونية والاقتصادية، المركز الجامعي آفلو، المجلد 02، العدد 02، ماي 2020، ص ص 29-42.

32. **يوبي سعاد**، «الإنتربول كآلية دولية شرطية لمكافحة جريمة الفساد»، المجلة الإفريقية للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة أدرار، المجلد 03، العدد 01، جوان 2019، ص ص 109-122.

33. **عائشة عبد المجيد**، «النظام القانوني للمنظمة الدولية للشرطة الجنائية (الإنتربول) ودورها في مجال التعاون القضائي الشرطي»، المجلة الأكاديمية

للأبحاث والنشر العلمي، الإصدار الحادي عشر، 2002، متوفر على الموقع التالي: www.ajrsp.com

34. **بن عمر حاج عيسى**، «الأنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود»، مجلة الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد 03، جانفي 2016، ص ص 252-263.

35. **ناجية شيخ**، «حول مكافحة الجريمة الإلكترونية في التشريع الجزائري»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص ص 688-701.

36. **حمودي ناصر**، «الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري»، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية الحقوق والعلوم السياسية، جامعة بجاية، سنة 2016، ص ص 67-91.

37. **قلاتي دنيازاد**، «الحماية الجزائية للحق المعنوي للمؤلف على المصنفات الرقمية»، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 44، جوان 2016، ص ص 317-331.

38. **مشري راضية**، «الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف»، مجلة التواصل في العلوم الإنسانية والإجتماعية، جامعة عنابة، عدد 34، جوان 2013، ص ص 135-151.

39. **طارق بوبترة**، «الحماية القانونية الداخلية للعلامة التجارية»، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد 31، عدد 1، جوان 2020، ص ص 353-364.

40. **بدرة عمارة**، «الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية»، مجلة الفقه والقانون، مجلة إلكترونية شهرية تعنى بنشر الدراسات الشرعية والقانونية، العدد السادس والثلاثون، أكتوبر 2015، ص ص 54-78.

41. **بوعون زكرياء**، «دور الهيئة الوطنية للوقاية من الجرائم الإلكترونية في حماية المستهلك»، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد 1، عدد 49، جوان 2018، ص ص 419-431.

42. **أحمد بن خليفة، حفوظة الأمير عبد القادر**، «الجريمة الإلكترونية وآليات التصدي لها»، مجلة الامتياز لبحوث الاقتصاد والإدارة، المجلد 01، العدد 01، جامعة الأغواط، جوان 2017، ص ص 148-171.

43. **لشهب حورية**، «النظام القانوني للتجارة الإلكترونية دراسة مقارنة»، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 23، نوفمبر 2011، ص ص 25-43.

44. **سيار عز الدين**، «تأثير البيئة الإلكترونية على صحة رضا المستهلك»، المجلة الجزائرية للحقوق والعلوم السياسية، العدد الثالث، معهد العلوم القانونية والإدارية، جامعة تيسمسيلت، جوان 2017، ص ص 61-71.

45. **أمينة بن عميور**، «متطلبات نظام الدفع الإلكتروني في مجال المعاملات الإلكترونية في إطار القانون 18-05»، مجلة العلوم الإنسانية، جامعة قسنطينة، المجلد ب، عدد 52، ديسمبر 2019، ص ص 99-116.

46. **دلال مولاي ملياني**، «الإنترنت والسيادة»، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، المجلد 7، العدد 1، مارس 2020، ص ص 384-416.

47. **روابح فريد**، «ضمانات حرمة الحياة الخاصة أثناء إجراءات مراقبة الاتصالات الإلكترونية»، مجلة الأبحاث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سطيف، المجلد 02، العدد 02، سنة 2020، ص ص 01-30.

48. **بوعناد فاطمة الزهراء**، «مكافحة الجريمة الإلكترونية في التشريع الجزائري»، مجلة الندوة للدراسات القانونية، مجلة غلكترونية خاصة تعنى بنشر الدراسات القانونية، العدد الأول، 2013، ص ص 63-74.

49. **ناصر بن محمد البقمي**، «أهمية الأدلة الرقمية في الاثبات الجنائي (دراسة وفق الأنظمة السعودية)»، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، العدد 80، المجلد 21، سنة 2012، ص ص 15-74.

50. **رابح وهيبة**، «الجريمة المعلوماتية في التشريع الإجرائي الجزائري»، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، العدد الرابع، ديسمبر 2014، ص ص 320-331.

51. **ماينو جيلالي**، «أسس وضوابط التعامل مع مسرح الجريمة للاستفادة من البصمة الوراثية في الاثبات الجنائي»، مجلة البدر، جامعة بشار، الحجم 04، العدد 12، ديسمبر 2012، ص ص 228-237.

52. **هميسي رضا**، «تفتيش المنظومات المعلوماتية في القانون الجزائري»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 05، جوان 2012، ص ص 157-182.

53. **بن طالب ليندا**، «التفتيش في الجريمة المعلوماتية»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 16، جوان 2017، ص ص 488-495.

54. **رويس عبد القادر**، «أساليب البحث والتحري الخاصة وحجيتها في الاثبات الجنائي»، المجلة الجزائرية للحقوق والعلوم السياسية، العدد الثالث، معهد العلوم القانونية والإدارية، جامعة تيسمسيلت، جوان 2017، ص ص 38-50.

55. **بوحزمة نصيرة**، «التفتيش في جرائم تقنية المعلومات»، مجلة حوليات جامعة بشار للحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة بشار، العدد 17، سنة 2017، ص ص 132-144.

56. **يزيد بوحليط**، «تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري»، مجلة التواصل في الإقتصاد والإدارة والقانون، جامعة عنابة، عدد 48، ديسمبر 2016، ص ص 82- 94.

57. **محسن العبودي**، «المواجهة الأمنية لجرائم الإنترنت»، مقال متوفر على الموقع التالي: www.eastlaw.com

58. **رحال بومدين، سعداني نورة**، «محل التفتيش في مجال التجارة الإلكترونية وفق القانون الجزائري»، المجلة الجزائرية للحقوق والعلوم السياسية، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد بن يحيى الونشريسي، تيسمسيلت، المجلد الثالث، العدد السادس، ديسمبر 2018، ص ص165-179.

59. **محمد أبو العلا عقيدة**، «التحقيق وجمع الأدلة في الجرائم الإلكترونية»، مقال متوفر على الموقع التالي: www.osamabahar.com

60. **فروحات سعيد**، «السلطة التقديرية للقاضي الجنائي في التعامل مع الخبرة الجنائية»، مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 09، العدد 02، 2016، ص ص119-137.

61. **شرف الدين وردة**، «مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية –في التشريع الجزائري–»، مجلة المفكر العدد 15،

كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، د.س.ن، ص ص538-560.

62. **عنتر أسماء**، «مكافحة الجرائم المستحدثة في التشريع الجزائري "التسرب نموذجا"»، مجلة القانون العام الجزائري والمقارن، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 06، سنة 2017، ص ص 74-89.

63. **شيخ ناجية**، «إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة»، مجلة معارف، جامعة البويرة، العدد 25، ديسمبر 2018، ص ص 01-25.

64. **باخويا دريس، رواق عمرية**، «أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الإنسان»، مجلة الدراسات القانونية والسياسية، جامعة عمر ثليجي الأغواط، العدد 05، المجلد 01، جانفي 2017، ص ص 76-88.

65. **بولافة سامية، ساسي مبروك**، «الأساليب المستحدثة في التحريات الجزائية»، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، العدد التاسع، جوان 2016، ص ص389-405.

66. **جبار فطيمة**، «مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري»، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة الشلف، العدد الثالث، ديسمبر 2016، ص ص 09-22.

67. **بثينة حبيباتني**، «معوقات مكافحة الجريمة المعلوماتية»، مجلة العلوم الإنسانسة، جامعة الإخوة منتوري قسنطينة، العدد 50، المجلد أ، ديسمبر 2018، ص ص 85-97.

68. **فريجة محمد هشام**، «النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني»، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، العدد 24، جوان 2018، ص ص 141-163.

69. **الطيبي البركة، حاج سودي محمد**، «إشكالية الإثبات في الجرائم الإلكترونية، مجلة آفاق علمية»، جامعة تمنراست، المجلد 11، العدد 01، سنة 2019، ص ص 266-284.

70. **بعقيقي عبير، نسيغة فيصل**، «الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، المجلد 09، العدد 02، جوان 2018، ص ص34-49.

71. **عبد السلام محمد المايل، عادل محمد الشربجي، علي قابوسة**، «الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم –الأسباب- سبل المكافحة مع التعرض لحالة ليبيا»، مجلة آفاق للبحوث والدراسات، المركز الجامعي إيليزي، العدد 04، جوان 2019، ص ص 242-255.

72. **ربيعي حسين**، «المجرم المعلوماتي شخصيته وأصنافه»، مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، العدد 40، جوان 2015، ص ص 285-302.

73. **عطوي مليكة**، «الجريمة المعلوماتية»، مجلة حوليات، جامعة الجزائر، العدد 21، جوان 2012، ص ص08-23.

74. **خليل يوسف جندي**، «المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني دراسة مقارنة»، مجلة كلية العلوم القانونية والسياسية، د.ب.ن، المجلد 07، العدد 32، سنة 2018، ص ص80-125.

75. **أحمد عبد الرحمن المجالي**، «الظواهر الإجرامية الحديثة والجريمة المنظمة»، مجلة العلوم الإنسانية، جامعة بسكرة، العدد الثاني والثلاثون، نوفمبر 2013، ص ص 219-238.

76. **معاشي سميرة**، «الجريمة المعلوماتية، دراسة تحليلية لمفهوم الجريمة المعلوماتية»، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 17، جوان 2018، ص ص 398-417.

77. **فكيري أمال**، «اشكالات الإثبات والاختصاص في جرائم تكنولوجيا الاعلام والاتصال العابرة للحدود»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 17، جانفي 2018، ص ص630-651.

78. **آمال فكيري**، «إشكالات الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود»، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة وادي سوف، عدد 17، جانفي 2018، ص ص 630-651.

79. **لموسخ محمد**، «تنازع الاختصاص في الجرائم الإلكترونية»، مجلة دفاتر السياسة والقانون، العدد الثاني، كلية الحقوق والعلوم السياسية، جامعة ورقلة، جوان 2009، ص ص 151-167.

80. **يوسفات علي هاشم**، «الحق في الحياة الخاصة وآليات التعويض عن المساس به في التشريع الجزائري»، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، العدد 17، سنة 2006، ص ص_286.

81. **محمد نور الدين**، «الحماية الجنائية للحق في خصوصية المكالمات الهاتفية دراسة تحليلية نقدية للقنونين الكويتي والإماراتي»، مجلة دراسات علوم

الشريعة والقانون، الجامعة الأردنية، المجلد 43، ملحق 04، سنة 2016، ص ص1689-1719.

82. **عيدة بلعابد،** «الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية»، مجلة آفاق علمية، جامعة تمنراست، المجلد 11، العدد 01، سنة 2019، ص ص 135-154.

83. **محمد أمين الخرشة، إبراهيم سليمان القطاوية،** «الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الإماراتي»، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 13، العدد 01، سنة 2016، ص ص 60-88.

84. **عثمان طارق،** «حماية الأطفال من الاستغلال في المواد الإباحية عبر الإنترنت في التشريع الجزائري»، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد الثالث عشر، د.س.ن، ص ص 417-448.

85. **محمد نور الدين،** «الحماية الجنائية للحق في خصوصية المكالمات الهاتفية دراسة تحليلية نقدية للقانونين الكويتي والإماراتي»، دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد 43، ملحق 4، سنة 2016، ص ص 1689-1719.

86. **منى تركي الموسوي، جان سيريل فضل الله،** «الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها»، مجلة كلية بغداد للعلوم الإقتصادية الجامعة، العدد الخاص بمؤتمر الكلية، 2013، ص ص 303-352.

87. **حاحة عبد العالي، يعيش تمام آمال،** «الترصد الإلكتروني كآلية للتحري عن جرائم الفساد بين متطلبات حماية الحقوق والحريات وضرورات الكشف عن الجريمة»، مجلة كلية القانون الكويتية العالمية، ملحق خاص

بأبحاث المؤتمر السنوي الدولي الخامس المنعقد بتاريخ 09-10 ماي 2018، العدد 03، الجزء الثاني، أكتوبر 2018، ص ص341-387.

88. **جبار فطيمة**، «مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري»، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة الشلف، العدد 03، ديسمبر 2016، ص ص09-22.

89. **بهنوس أمال**، «الدليل الرقمي في الإجراءات الجنائية، المجلة الأكاديمية للبحث القانوني»، كلية الحقوق والعلوم السياسية، جامعة بجاية، مجلد 16، عدد 02، سنة 2017، ص ص 169-189.

90. **لعوارم وهيبة**، «مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي، مجلة الفقه والقانون»، مجلة إلكترونية شهرية تعنى بنشر الدراسات الشرعية والقانونية، العدد العشرون، سنة 2014، ص ص 99-113.

91. **إلهام شهرزاد روابح**، «الدليل الرقمي بين المشروعية وانتهاك الخصوصية المعلوماتية»، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة البليدة، العدد العاشر، د س ن، ص ص 184-198.

92. **أحمد شرف الدين**، «حجية الرسائل الإلكترونية في الإثبات»، ص 03، مقال متوفر على الموقع التالي: www.eastlaw.com

93. **مزيود سليم**، «الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها»، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد 01، أفريل 2014، ص ص 94-107.

94. **منصور أحلام**، «الحلول الحديثة لأمن المعلومات لمواجهة المخاطر الإلكترونية»، مجلة دراسات في الاقتصاد والتجارة والمالية، المجلد 07، العدد

01، مخبر الصناعات التقليدية لجامعة الجزائر 3، سنة 2018، ص ص305-326.

4-المداخلات:

1. **جان فرنسوا هنروت،** «أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي»، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص ص 95-111.
2. **خالد محي الدين أحمد،** «الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر»، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص ص 38-48.
3. **كريستينا سكولمان،** «المعايير الدولية المتعلقة بجرائم الإنترنت (مجلس أوربا)»، مقال مقدم لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، بتاريخ 19-20 يونيو 2008، ص ص 61-66.
4. **مختارية بوزيدي،** «ماهية الجريمة الإلكترونية»، مقال موجه للملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص 18، ص ص 7-22.
5. **فشار عطاء الله،** «مواجهة الجريمة المعلوماتية في التشريع الجزائري»، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا بليبيا، أكتوبر ، 2009، ص ص 01-50.
6. **خالدة هناء سيدهم،** «حماية حقوق الملكية الفكرية للمصنفات الرقمية في بيئة الإنترنت»، مقال موجه للمؤتمر الدولي الرابع عشر: الجرائم

الإلكترونية، المنعقد بطرابلس، بتاريخ 24-25 مارس 2017، منشورات مركز جيل البحث العلمي، لبنان، ص ص 29-47.

7. **الأزرق بن عبد الله، أحمد عمراني،** «نظام المعلوماتية في القانون الجزائري واقع وآفاق»، مداخلة ضمن المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة، المفاهيم والتشريعات والتطبيقات، المنعقد بالرياض خلال الفترة 06-07 أفريل 2010.

8. **عمرو حسين عباس،** «أدلة الإثبات الجنائي والجرائم الإلكترونية (المعلوماتية)»، بحث مقدم إلى المؤتمر الإقليمي حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد خلال الفترة 26-2008/04/27، بمقر جامعة الدول العربية، القاهرة، ص ص01-26.

9. **أمجدي بوزينة أمنة،** «إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)»، مقال موجه للملتقى الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص ص 57-82.

10. **داود سليمان الصبحي،** «أساليب البحث والتحري»، بحث مقدم إلى الدورة التدريبية إجراءات التحري والمراقبة والبحث الجنائي، المنعقدة بكلية التدريب قسم البرامج التدريبية بجامعة نايف العربية للعلوم الأمنية، الرياض، خلال الفترة 25-29/أفريل/2009، ص ص01-43.

11. **عمر عبد العزيز موسى الدبور،** «آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية (إنشاء ضبطية خاصة بالجرائم الإلكترونية)»، مقال موجه للمؤتمر الدولي: الجرائم الإلكترونية، المنعقد بطرابلس، بتاريخ

24-25 مارس 2017، منشورات مركز جيل البحث العلمي، لبنان، ص ص 215-230.

12. **هشام محمد فريد رستم**، «أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي»، مقال مقدم لمؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص ص 401-506.

13. **ذياب موسى البداينة**، «الجرائم الإلكترونية: المفهوم والأسباب»، ورقة علمية مقدمة للملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المنعقد بكلية العلوم الإستراتيجية، عمان، بتاريخ 2-2014/09/4، ص ص 1-28.

14. **مفتاح بو بكر المطري**، «الجريمة الإلكترونية والتغلب على تحدياتها»، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا، المنعقد بجمهورية السودان، في 23-2012/09/25، ص ص 1-57.

15. **موسى مسعود أرحومة**، «الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية»، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، أكاديمية الدراسات العليا، خلال الفترة 28-2009/10/29، طرابلس، ليبيا، ص ص 1-24.

16. **محمد زيدان، محمد حمو**، «متطلبات أمن المعلومات المصرفية في بيئة الإنترنت»، مداخلة مقدمة في المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية، البيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد بالرياض خلال الفترة 06-07 أفريل 2010.

17. **خبازي فاطمة الزهرة**، «جرائم الدفع الإلكتروني وسبل مكافحتها»، مقال موجه للملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بالجزائر العاصمة، بتاريخ 29 مارس 2017، ص ص 23-42.

5-النصوص القانونية:

أ- الاتفاقيات الدولية:

1. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصادق عليها من قبل الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر سنة 2014، ج.ر عدد 57، صادر في 28 سبتمبر سنة 2014.
2. العهد الخاص بالحقوق الاقتصادية والاجتماعية والثقافية والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية الموافق عليها من طرف الجمعية العامة للأمم المتحدة يوم 16 ديسمبر سنة 1966، المصادق عليه من قبل الجزائر بموجب المرسوم الرئاسي رقم 89-67 مؤرخ في 16 مايو سنة 1989، ج ر عدد 20، صادر بتاريخ 17 مايو سنة 1989.

ب- الدساتير:

1. مرسوم رئاسي رقم 96-438 مؤرخ في 7 ديسمبر سنة 1996، يتعلق بنص تعديل الدستور المصادق عليه في استفتاء 28 نوفمبر سنة 1996، ج ر، عدد 76، صادر في 28 ديسمبر سنة 1996.
2. مرسوم رئاسي رقم 20-442، مؤرخ في 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر، عدد 82، صادر في 30 ديسمبر 2020.

ج- النصوص التشريعية:

1. أمر رقم 66-57 المؤرخ في 19 مارس 1966، يتضمن علامات المصنع والعلامات التجارية، ج. ر عدد 23، صادر في 22 مارس 1966.
2. أمر رقم 96-16 يتضمن الإيداع القانوني، ج ر، عدد 14، صادر في 1996.
3. قانون رقم 2000-03 مؤرخ في 5 غشت 2000، يتضمن تحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر عدد 48، صادر في 6 غشت 2000 (ملغى).
4. أمر رقم 03-06 مؤرخ في 19 يوليو 2003، المتعلق بالعلامات، ج . ر عدد 44، صادر في 23 يوليو 2003.
5. أمر رقم 03-07 المؤرخ في 2003/07/19، يتضمن براءات الإختراع، ج.ر عدد 44، صادر في سنة 2003.
6. قانون رقم 04-15 المؤرخ في 2004/11/10 يتضمن تعديل قانون العقوبات، ج ر عدد 71، صادر في 2004/11/10.
7. قانون رقم 05-10، المؤرخ في 20 جوان 2005، يعدل ويتمم القانون المدني، ج.ر عدد 44، صادر بـ 26 جوان 2005.
8. قانون رقم 06-22 مؤرخ في 2006/12/20 يعدل ويتمم الأمر رقم 66-155 يتضمن قانون الإجراءات الجزائية، ج ر عدد 84، صادر بتاريخ 2006/12/24.
9. قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47، صادر بتاريخ 16 أوت 2009.
10. قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يتضمن القواعد العامة للتوقيع والتصديق الإلكترونيين، ج.ر عدد 06، صادر في 10 فبراير 2015.

11. قانون رقم 18-04 مؤرخ في 10 مايو 2018، يتضمن تحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر عدد 27، صادر في 13 مايو 2018.
12. قانون رقم 18-07 مؤرخ في 10 جوان 2018، يتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، صادر في 10 جوان 2018.
13. أمر رقم 21-11 المؤرخ في 25 غشت 2021، يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج ر عدد 65، صادر بتاريخ 26 غشت 2021.

د- النصوص التنظيمية:

1. مرسوم رئاسي رقم 15-261، مؤرخ في 08 أكتوبر 2015، يتضمن التشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،، ج.ر عدد 53، صادر بتاريخ 08 أكتوبر 2015.
2. مرسوم تنفيذي رقم 07-162، مؤرخ في 30 ماي 2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 ماي 2001، يتضمن نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37، صادر في 07 يونيو 2007.

6- الوثائق

1. مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، البند الخامس من جدول الأعمال المؤقت، النهج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدة للجريمة العابرة للحدود الوطنية والتصدي

لها على نحو ملائم، المنعقد بالدوحة من 12 إلى 19 أفريل 2015، A/CONF.222/8.

2. مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين المنعقد بالقاهرة، مصر بتاريخ 28 أبريل-05 مايو 1995، مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC
3. مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12-19 أفريل 2010، رقم A/conf.213/9.
4. الأمم المتحدة، المكتب المعني بالمخدرات والجريمة، خلاصة وافية لمعايير الأمم المتحدة وقواعدها في مجال منع الجريمة والعدالة الجنائية، نيو يورك، 2007
5. قرار الجمعية العامة لمنظمة الأمم المتحدة رقم 63/55، الدورة الخامسة والخمسون، البند 105 من جدول الأعمال، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بتاريخ 22 جانفي 2001، A/RES/55/63.
6. قرار الجمعية العامة لمنظمة الأمم المتحدة رقم 121/56، الدورة السادسة والخمسون، البند 110 من جدول الأعمال، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بتاريخ 23 جانفي 2002، A/RES/56/121.
7. لتقرير التفسيري لاتفاقية الجريمة الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، المؤرخ في 23 نوفمبر 2001، بودابست، ص 04.

8. الاتفاقية المتعلقة بالجريمة الإلكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية –رقم 185، المنعقة ببودابست بتاريخ 2001/11/23.
9. مشروع استراتيجية التحول الرقمي لإفريقيا (2020–2030)، ص 53، متوفر على موقع الاتحاد الإفريقي، www.au.int.
10. الإعلان العالمي لحقوق الإنسان بموجب قرار الجمعية العامة(217 ألف) د–3) المؤرخ في 10 ديسمبر 1948.
11. العهد الدولي الخاص بالحقوق المدنية والسياسية وعرض للتوقيع والتصديق والانظمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف(د–21) المؤرخ في 16 ديسمبر 1966.
12. قرار الجمعية العامة للأمم المتحدة رقم 162/51 المتضمن القانون النموذجي بشأن التجارة الإلكترونية الذي اعتمدته لجنة الأمم المتحدة للقانون التجاري الدولي في الدورة الحادية والخمسون، البند 148 من جدول الأعمال، رقم A/RES/51/162
13. الأمر التوجيهي رقم EC/2000/31 للبرلمان والمجلس الأوروبي المؤرخ في 2000/06/08 بشأن بعض الجوانب القانونية لخدمات مجتمع المعلومات لاسيما في مجال التجارة الإلكترونية في السوق الداخلية (أمر توجيهي في مجال التجارة الإلكترونية).
14. قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الشتراع 2001، المنعقد بفيينا من 25يونيو–13 يوليو 2001 للدورة الرابعة والثلاثون، من طرف لجنة الأمم المتحدة للقانون التجاري الدولي رقم A/CN.9/493
15. قرار الجمعية العامة للأمم المتحدة رقم 80/56 بناء على تقرير اللجنة السادسة (A/56/588)، المتضمن القانون النموذجي بشأن التوقيعات

الإلكترونية الذي وضعته لجنة الأمم المتحدة للقانون النجاري الدولي، رقم A/RES/56/80.

ثانيًا – باللغة الفرنسيّة:

1- OUVRAGES

1. **RACICOT Michel, S.HAYES Mark, R.SZIBBO Alec, TREUDEL Pierre**, Etude des questions relatives à la responsabilité à l'égard du contenu circulant sur internet, industrie canada, 1997.
2. **GAUTRAIS Vincent**, Neutralité technologiques rédaction et interprétation des lois face aux changements technologique, les éditions thémis, canada, 2001.
3. **CASILE Jean-François**, Le code pénale à l'épreuve de la délinquance informatique, presses universitaires d'aix-marseille, France, 2002.
4. **ADJAYI KODJO Ndukuma**, Cyberdroit télécoms, internet, contrats de e-commerce, presses universitaires du Congo, Kinshasa, 2009.
5. **PRZYSWA Eric**, Cybercriminalité et contrefaçon, fyp éditions, France, 2010.
6. **RAUFER Xavier**, Cyber-criminologie, cnrs éditions, paris, 2015.
7. **DESFORGES Alix**, La coopération internationale et bilatérale en matière de cybersécurité: enjeux et rivalités, laboratoire de IRSEM, Paris, 2013.
8. **METILLE Sylvain**, Le Droit au respect de la vie privée les défis digitaux une perspective de droit comparé, union européenne, Bruxelles, 2018.

9. **MATTATIA Fabrice**, Internet et les réseaux sociaux : que dit la loi ? 2e édition, éditions eyrolles, Paris, 2015.

10. ——————————, Le droit des données personnelles, 2e édition, éditons eyrolles, Paris, 2016.

11. **GHERAOUTI Solange**, Cybersécurité sécurité informatique et réseaux, 5e édition, dunod, Paris, 2016.

2- <u>THESES ET MEMOIRES</u>

A-<u>THESES</u>

1. **ABDELSADOK kheira**, L'impact de nouvelle technologie de l'information sur les services bancaires en droit algérien, thèse présentée pour l'obtention du diplôme de doctorat de sciences en sciences juridique, option droit privé, faculté de droit et sciences politique, département de droit, université de Batna 01, 2017/2018.

2. **JAMMET Adrien**, La prise en compte de la vie privée dans l'innovation technologique, thèse pour obtenir le grade de docteur en droit, université Lille 2-droit et santé, 2018.

3. **BELABED Amine**, la protection de la vie privée sur internet, thèse pour l'obtention du diplôme de doctorat en sciences, spécialité: informatique, département d'informatique, faculté des sciences, université de tlemcen, 2018.

4. **JEAN-MEIRE Caroline**, Les nouvelles technologies et la lutte contre la délinquance: regards croisés France/Royaume-Uni, thèse pour le doctorat en droit, école de droit de la Sorbonne, université de paris 01 panthéon-Sorbonne, 2016.

5. **FRIEDRICH Cyrielle**, Les sciences et les techniques comme moyens de preuve dans la procédure pénale aspects techniques et juridiques de ces moyens de preuves, thèse de doctorat, faculté de droit, université de Genève, 2016.

6. **KAMENI Guy marcel**, La vie privée en droit camerounais, thèse en vue de l'obtention du doctorat, université de Toulouse 1 capitole, 2013.

7. **HUMBERT Jean-Philippe**, Les mondes de la cyberdélinquance et images sociales du pirate informatique, thèse pour le doctorat en sciences de l'information et de la communication, université Paul Verlaine, metz, 2007.

8. **HARIVEL Jean** Libertés publiques, libertés individuelles risques et enjeux de la société numérique, thèse de droit public, école doctorale de droit de la sorbonne, université paris 01 panthéon sorbonne, 2018.

9. **BOUTROS Mickael**, Le droit du commerce électronique: une approche de la protection du cyber consommateur, thèse pour obtenir le grade de docteur en droit privé, université de Grenoble, 2014.

10. **BOLZE Pierre**, Le droit à la preuve contraire en procédure pénale, thèse en vue de l'obtention du grade de docteur en droit, faculté de droit, sciences économique et gestion, université Nancy 2, 2010.

11. **Sylvain Métille**, Mesures techniques de surveillance et respect des droits fondamentaux en particulier dans le cadre de l'istruction pénale et de renseignement, thèse de doctorat, faculté

de droit, université de Neuchâtel, bale, 2010.

12. **BERSET-BIRCHER Valerie**, Les systèmes d'information et la vie privée du salarié: analyse en droit européen, en droit suisse et en droit français, thèse en vue de l'obtention du grade de docteur en droit privé, faculté de droit, de sciences politiques et gestion, université de Strasbourg, 2013.

B- MEMOIRES

1. **GODEBERGE Céline**, La coopération judiciaire en matière pénale après le traité de Lisbonne, mémoire master de droit pénal et sciences pénales, université panthéon-Assas, paris 2, 2013.
2. **MATIGNON Emmanuelle**, La cybercriminalité un focus dans le monde des télécoms, mémoire master droit du numérique administrations-entreprises de l'école de droit de la Sorbonne, université paris 1 panthéon-Sorbonne, 2011/2012.
3. **TYRODE Jean-François**, Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen, mémoire master droit de l'internet public-administration-entreprises, université paris 01 panthéon-Sorbonne, 2006/2007.
4. **MAALAOUI Ibtissem**, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit

L L M, option droit des affaires, université de Montréal, 2011.

5. **CHEVALIER Michael**, Les enjeux juridiques concernant les nouveaux modèles d'affaires basés sur la commercialisation des données, mémoire présenté en vue de l'obtention du grade de L L M en droit des technologies de l'information, université de Montréal, 2015.
6. **DIMITRIOU Philippe**, L'application du droit de la cryptologie en matière de sécurité des réseaux informatiques, mémoire pour l'obtention du déplome de D E A défense nationale, option sécurité européenne et internationale, faculté des sciences juridiques, politiques et sociales, université de Lille 2-droit et santé, 2002.
7. **ETIENNE Virginie**, Le développement de la signature électronique, mémoire master 2 recherche droit des affaires, université paris 13, 2010/2011.

3- ARTICLES

1. **MAITROT DE LA MOTTE Alexandre**, Le droit au respect de la vie privée, groupe d'études société d'information et vie privée, Disponible sur le site: http://asmp.fr
2. **DUPONT Benoit**, La gouvernance polycentrique du cybercrime: les réseaux fragmentés de la coopération international, cultures et conflits, n° 102, centre d'études sur les conflits, été 2016, disponible sur le site, http://conflits.revues.org/19292

3. ——————, La coévolution du « vol d'identité » et des systèmes de paiment, criminologie, volume 43, numéro 2, les presses de l'université de montréal, automne 2010, P p 247-268.

4. **VALLET Caroline**, Le dévoilement de la vie privée sur les sites de réseaux social. Des changements significatifs, revue droit et société, n° 80, vol 01, 2012, P p 163-188, disponible en ligne à l'adresse: https://www.cairn.info/revue-droit-et-societe1-2012-1-page-163.htm

5. **FENERON Claire, KLEIN Laurent, LE CLAINCH Julien, BATTISTI Michèle, BERGUIG Matthieu**, Droit de l'information, documentaliste-sciences de l'information, vol 49, n° 4, 2012, Disponible en ligne à l'adresse: https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2012-4-page-16.htm

6. **CHILSTEIN David,** Législation sur la cybercriminalité en France, revue internationale de droit comparé, vol 62, n° 2, 2010, p p 553-606, disponible en ligne à l'adresse: https://www.persee.fr/doc/ridc_0035-3337_2010_num_62_2_19954

7. **FREYSSINET Eric**, Botnets: illustration de nouvelles formes de criminalité organisée, revue du groupe de recherches actions sur la criminalité organisée (crasco), 2013, article disponible sur le site: https://hal.archives-ouvertes.fr/hal-01077117

8. **OK Eric**, La preuve numérique un défi pour l'enquete criminelle du 21e siècle, revue les cahiers du

numérique, n° 3, vol 4, 2003, p p 205-217, disponible en ligne à l'adresse: https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

9. **DEHOUSSE Franklin, ZGAJEWSKI Tania**, La convention Europol: un tournant pour la coopération policière européenne, courrier hebdomadaire du centre de recherche et d'information socio-politiques (crisp), n° 1577-1578, 1997, Disponible sur le site: https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-1997-32-page-1.htm

10. **DOUZET Frédérick, SAMAAN Jean-loup, DESFORGES Alix**, Les pirates du cyberespace, revue Hérodote, vol 03, n° 134, p p 176-193, disponible en ligne à l'adresse: https://www.cairn.info/revue-herodote-2009-3-page-176.htm

11. **HANS-PETER Gassmann**, Ver un cadre juridique international pour l'informatique et autres technique nouvelles de l'information, annuaire de droit international, volume 31, 1985, P p 747-761.

12. **PAYE Jean-Claude**, Lutte antiterroriste et contrôle de la vie privée, revue-multitudes, n° 11, vol 1, 2003, p p 91-105, disponible en ligne à l'adresse, https://www.cairn.info/revue-multitudes-2003-1-page-91.htm

13. **FRAYSSINET Jean**, Interpol et ses fichiers, article disponible en ligne à l'adresse: https://hal.archives-ouvertes.fr/hal-01427564

14. **VERGNE Jean-Philippe, DURAND Rodolphe**, Cyberespace et organisations « virtuelles »: l'état souverain a-t-il encore un avenir, revue-regards-croises-sur-l-économie, n° 14, vol 1, 2014, p p 126-139, disponible en ligne à l'adresse: https://www.cairn.info/revue-regards-croises-sur-l-economie-2014-1-page-126.htm

15. **PRADEL Jean**, Les infractions relatives à l'informatique, revue internationale de droit comparé, vol 42, n° 2, avril-juin 1990, p p 815-828, disponible en ligne à l'adresse: https://www.persee.fr/doc/ridc_0035-3337_1990_num_42_2_1994

16. **BOSSAN Jerome**, Le droit pénal confronté à la diversité des intermédiaires de l'internet, revue de science criminelle et droit pénal comparé, n° 2, vol 2, 2013, p p 295-319, disponible en ligne à l'adresse: https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2013-2-page-295.htm

17. **KELLO Lucas**, Traduit de l'anglais par **RICHARD Thomas**, Les cyberarmes: dilemmes et futurs possibles, revue-politique-étrangère, n° 4, institut français des relations internationales, 2014, p p 139-150, disponible en ligne à l'adresse: https://www.cairn.info/revue-politique-etrangere-2014-4-page-139.htm

18. **VOISSET Michèle**, Droit au respect de la vie privée et société de l'information, groupe d'études société d'information et vie privée,

chapitre 16, disponible sur le site: http://asmp.fr

19. **CHAWKI Mohamed**, Essai sur la notion de la cybercriminalité, voir le site : www.iehei.org
20. **DIOUF Ndiaw**, Infractions en relation avec les nouvelles technologies de l'information et procédure pénale: l'inadaptation des réponses nationales face à un phénomène de dimension internationale, afrilex n° 4, p p 251-292, http://www.afrilex.u-bordeaux4.fr
21. **BRAULT Nicolas**, Le droit applicable à internet de l'abime aux sommets, revue-legicom, n° 12, vol 2, 1996, p p 1-15, disponible en ligne à l'adresse: https://www.cairn.info/revue-legicom-1996-2-page-1.htm
22. **BARAT-GINIES Oriane**, Existe-t-il un droit international du cyberespace?, revue Hérodote, vol 01, n° 152-153, p p 201-220, disponible en ligne à l'adresse: https://www.cairn.info/revue-herodote-2014-1-page-201.htm
23. **OUDER Hadjira**, Les dispositifs légaux de lutte contre la cybercriminalité, ceristnews, bulletin d'information trimestriel, treizième numéro, juin 2013, Alger, P p 12-26.
24. **TITOYCHE Radia**, Territorialité du droit pénale et la cybercriminalité, cahiers de politique et de droit, faculté de droit et des sciences politique, université de ouargla, onzième année, volume 11, n° 01, janvier 2019, P p 26-39.

25. **DE MUNAGORRI Rafael Encinas**, Les problèmes de preuve posés par l'évolution des sciences et des technologies, article disponible en ligne à l'adresse: https://halshs.archives-ouvertes.fr/halshs-01652004

26. **HALIM Rami**, La protection pénale du consommateur dans le cadre du commerce électronique, revue de recherches et études juridique et politique, faculté de droit et des sciences politique, université de Blida, numéro 2, janvier 2012, P p 387-393.

27. **FEVRIER Rémy**, Les collectivités territoriales face aux menaces numériques, revue gestion et management public, volume 01, n° 03, 2013, p p 24-39. Disponible en ligne à l'adresse: https://www.cairn.info/revue-gestion-et-management-public-2013-1-page-24.htm

28. **BERTHELET Pierre**, La lutte contre la cybercriminalité à l'échelle de l'union: analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels, revue québécoise de droit international, hors-série, novembre 2018, P P 25-39.

29. **AKMOUCHE Walter, HEMERY Henri**, La propagande jihadiste sur internet diagnostic et perspectives, cahiers de la sécurité, n° 6, INHES, paris, octobre-décembre 2008, p p 53-58.

30. **PHILIPPE Xavier**, Vie privée et nouvelles technologies, annuaire international de justice constitutionnelle, cours international de

justice constitutionnelle, 18-2002,2003, P p 433-466.

31. **Y.Akdeniz, J.Bell**, La vie privée et l'internet perspectives du Royaume-Uni, groupe d'études société d'information et vie privée, chapitre 8, disponible sur le site: http://asmp.fr

4- DOCUMENTS

1. Dixième congrès des nations unies pour la prévention du crime et le traitement des délinquants, document de base pour l'atelier consacré au thème « Délits liés à l'utilisation du réseau informatique », Vienne, 10-17 avril 2000, A/CONF.187/10.
2. Recommandation du conseil relative aux lignes directrices régissant la politique de cryptographie adoptée par le conseil lors de la 895 éme session, le 27 mars 1997, C/M (97) 6/prov.
3. La recommandation du conseil concernant les lignes directrices régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité C(2002) 131/final.
4. La recommandation du conseil sur les principes pour l'élaboration des politiques de l'internet C(2011) 154.
5. **Département fédérale de justice et police,** approbation et mise en œuvre de la convention du conseil de l'Europe sur la cybercriminalité, avant-projet et rapport explicatif, office fédéral de la justice, berne, 2009.
6. Nations unies, commission économique pour l'Afrique, note d'orientation, relever les défis de la

cybersécurité en Afrique, NTIS/002/2014.

7. Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

فهرس الموضوعات

فهرس الموضوعات

ملخص

ترتب عن الثورة التي يعرفها العالم في مجال تكنولوجيات الإعلام والاتصال خاصة شبكة الإنترنت تسهيل العديد من الخدمات العامة التي كانت تتطلب من قبل مجهودا كبيرا، غير أن رواج هذه المعاملات واكبها ظهور ممارسات سلبية تجسدت في العديد من الجرائم خاصة المرتكبة منها عبر الإنترنت.

تكاتفت الجهود سواء على المستوى الدولي والداخلي من أجل وضع إطار قانوني موضوعي وإجرائي يكفل مكافحة تتسم بالفعالية وذلك تماشيا مع الخطورة التي تتسم بها هذه الجريمة من جهة ونظرا للخصوصية التي تتميز بها الجريمة المرتكبة عبر الإنترنت من جهة أخرى.

أثار هذا النوع الجديد من الإجرام عدة إشكالات قانونية موضوعية وإجرائية نظرا لتميزه بطبيعة خاصة تختلف كل الاختلاف عن الجرائم التقليدية، فالجريمة المرتكبة عبر الإنترنت تتميز بطابعها اللامادي بالإضافة إلى تعديها للحدود الوطنية، الأمر الذي جعل الآليات القانونية الخاصة بمكافحتها تتسم بنسبية الفعلية والفعالية وذلك بالنظر إلى قصور وعدم مواكبة هذه النصوص لسرعة تطور هذه الجريمة.

Résumé ;

La grande révolution que connait le monde actuellement dans le domaine des technologies de l'information et de la communication grâce à internet a un impact positif considérable sur la qualité des services publics qui exigeaient auparavant de grands efforts humains, néanmoins la propagation et l'expansion et la popularité de ces technologies entraiment des pratique négatives et immorales au sein des sociétés et qui sont incarnés dans le nombre des infractions, des délits et des crimes perpétrés via internet.

En effet, tout à l'échelle mondial que nationale, les actions se sont intensifiées pour mettre œuvre et en place un cadre juridique, objectif et procédurale garantissant une lutte efficiente et efficace contre la cybercriminalité, qui soit conforme la dangerosité caractérisant ce fléau d'une part et distinguant la spécificité des crimes perpétrés par l'intermédiaire d'internet d'autre part.

De nos jours, la cybercriminalité soulève des problématiques juridiques, légales, objectifs et procédurales étant donné sa dimension immatériel par opposition aux crimes traditionnels, force est constater qu'en voilant les frontières des états, les mécanismes juridiques préconisant la lutte contre la cybercriminalité demeurent inefficaces car les textes de lois les régissant ne sont pas souvent opérationnelles par rapport à la vitesse et à l'évolution des crimes perpétrés via internet.