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

جرائم تكنولوجيات الإعلام و الإتصال

مذكرة لنيل شهادة الماجستير في القانون

تخصص: تحولات الدولة

مذكرة لنيل شهادة الماستر في القانون

تخصص: قانون الأعمال

إعداد الطالبتين :

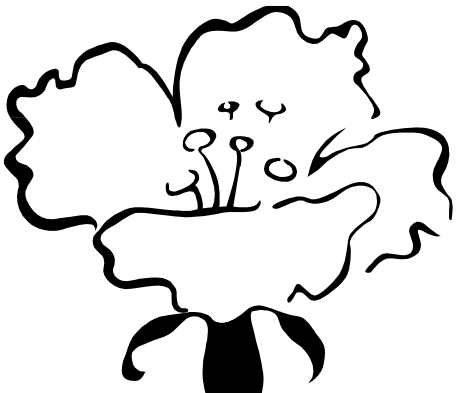
- عبد الرحماني أمينة
- مرابطين حفيظة

إشراف الأستاذ:

د/- جعفور إسلام

تاريخ المناقشة...../...../.....

بسم الله الرحمن الرحيم



إهداء

إلى من لا يمكن للكلمات أن توفي حقهما،

الوالدين الكريمين

إلى من لا أستطيع الاستغناء عنهم،

زوجي و أولادي

وإلى كل الأهل و الأقارب

و جميع الأصدقاء و الزملاء

أهدي ثمرة جهدي.

أمينة.

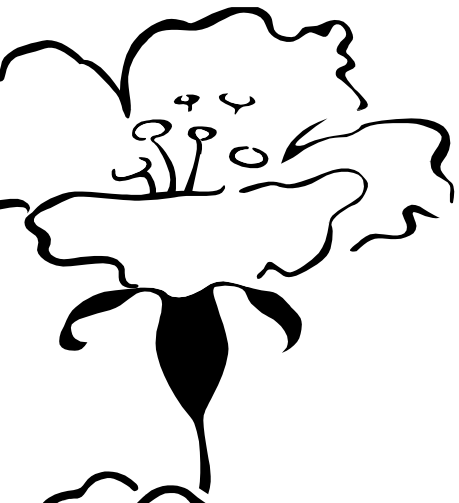
شكر و عرفان

في البداية، أحمد الله الذي أعطانا القوة والصبر لإتمام هذا العمل العلمي المتواضع.

ثم أتوجه بجزيل الشكر و الامتنان إلى الأستاذ جعفور اسلام لقبوله الإشراف على هذه المذكرة، إذ لم يبخل عليا بإرشاداته وتوجيهاته القيمة لإثراء هذا العمل رغم مشاغله الكثيرة .

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة.

ولا أنسى أن أشكر كل من قدّم لي يد العون من قريب أو بعيد في إنجاز هذا العمل.



إهداء

إلى من قال فيهما العزيز تعالى :

"و اخفض لهما جناح الذل من الرحمة و قل ربي ارحمهما كما ربياني صغيرا."

أتقدم الإهداء إلى:

والدي الحنون و أمي العزيزة

إلى من لا أستطيع العيش بدونهم :

زوجي الغالي" **بنور لياميـن** و أولادي الأعزاء" **ثيزيري- محمد - ثيللي**".

إلى كل الأهل و الأقارب و جميع الأصدقاء و الزملاء

خاصة عبد الرحمان أمينة التي شاركتني في إتمام هذه المذكرة

حفيظة

مقدمة:

لا شك أن التقدم الحضاري الذي اجتاح العالم في العصر الحديث أثرّ في كافة مناحي الحياة الإنسانية من سلوكيات وغيرها، وقد طال هذا التأثير نوعية الجريمة والمجرم وأصبح ملموساً لدى كل المختصين والمهتمين بعلم الإجرام والمجرمين.

ومن نتائج التطور الحضاري الذي اجتاح العالم الحديث تقنية المعلومات التي تعتبر العامل الأساسي الذي أحدث ثورة هائلة في مجال الاتصالات واستخدامات الحاسب الآلي و شبكة الإنترنت للأغراض المختلفة، ولا شك أن هذه الثورة المعلوماتية الهائلة قد انعكست بصورة إيجابية على كثير من جوانب الحياة المعاصرة، بسبب ما توفره من الوقت والجهد والتكلفة عن الإنسان تجعل حياته اليومية أكثر سهولة و يسر، الأمر الذي أدى إلى تضاعف الطلب على هذه التقنية المعلوماتية، وتوسع ميادين استعمالها وازداد الاعتماد عليها بشكل مفرط في كل القطاعات العامة أو الخاصة، إلى حد بدا من الصعب على هذه القطاعات أداء نشاطاتها دون الاستعانة بشكل أساسي على هذه التقنيات الحديثة.

إلا أن الاستخدام المتنامي لهذه التقنيات انطوى، في الوقت ذاته، على بعض الجوانب السلبية التي تمثل تهديدا خطير ا للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات. الشيء الذي استتبعه ظهور نمطا جديدا من الجرائم، لم يكن معهودا من قبل سمي بجرائم تقنية المعلومات أو جرائم تكنولوجيا الإعلام و الإتصال.

ولا جدال في اعتبار جرائم تكنولوجيا الإعلام و الإتصال من أخطر و أعقد الجرائم على الإطلاق، و تأتي في مقدمة الأشكال الجديدة للجريمة المنظمة، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها وخصوصية مرتكبيها و وسائل كشفها . فهي جريمة تقنية سهلة الارتكاب،

تنشأ في الخفاء وفي بيئة الكترونية افتراضية مكونة من إشارات وذبذبات مغناطيسية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصالات بصورة آلية دون أن تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات و خبرات تقنية عالية، فضلا على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأية سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي.

وقد أدت هذه الخصائص التي تميز جرائم تكنولوجيا الإعلام و الإتصال إلى صعوبة التعامل معها وتكييفها على أساس النصوص الجنائية التقليدية مع ما قد يشكله ذلك من مساس بمبدأ الشرعية الجزائية والتفسير الضيق للنص الجنائي وحضر القياس، وهو ما ألقى مسؤولية كبيرة على عاتق المشرع الجزائي في اتخاذ الخطوات التشريعية الضرورية لمواجهة هذه الظاهرة الإجرامية الناشئة عن إساءة استخدام وسائل الاتصال الحديثة و النظم المعلوماتية.

وباعتبار الجزائر واحدة من الدول التي تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان سلبي أو إيجابي فهي أيضا معنية بتنظيم هذا المجال، فكان لا بد من إيجاد إطار قانوني مناسب لسد الفراغ التشريعي الذي يعتريه خاصة ما تعلق منه بالإجرام الإلكتروني، لذلك وضعت مجموعة من التدابير و الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المستحدثة، و ذلك عن طريق تعديل النصوص العقابية و الإجرائية القائمة لتتماشى وطبيعة الجرائم المستحدثة من جهة، ، و بإستحداث نصوص جديدة خاصة بهذه الأخيرة

بناء على ما سلف يثير موضوع البحث الحالي إشكالية جوهرية حول **الطبيعة الخاصة لجرائم تكنولوجيا الإعلام و الاتصال و الأساليب الكفيلة لمواجهتها.**

و للإجابة على هذه الإشكالية ارتأينا تقسم بحثنا الى فصلين، تناولنا الإيطار المفاهمي لجرائم تكنولوجيا الإعلام و الاتصال في (الفصل الأول). ثم تدابير مواجهة لجرائم تكنولوجيا الإعلام و الاتصال في (الفصل الثاني). معتمدين في ذلك على منهج يجمع بين المقارنة و التحليل.

الفصل الأول

الإطار المفاهمي للجريمة تكنولوجيات الإعلام و الاتصال

لقد شهد العالم في الآونة الأخيرة تطورا غير مسبوقا في مجال تكنولوجيا الإعلام و الاتصال، مما نتج عنه استعمال الحاسب الآلي وشبكة الأنترنت في جميع الميادين، لكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة، الأمر الذي قد ينجر عنه ارتكاب أصناف عدة من جرائم حديثة و غير مألوفة لها علاقة بالتقنية المعلوماتية.

تعتبر الجريمة تكنولوجيا الإعلام و الإتصال من الآثار السلبية التي خلفتها التقنية العالية، حيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها، مما إنجر عنه وضع عدة مصطلحات للدلالة عليها من بينها جرائم الحاسب، جرائم التقنية العالية،جرائم الانترنيت، جرائم السبيرانية و صولا إلى الجرائم الإلكترونية. و يعد عدم الاستقرار على مصطلح واحد للدلالة على الجريمة المرتكبة عبر وسائل تكنولوجيا الإعلام و الاتصال، من الصعوبات الواردة عليها مما استوجب وضع مفهوم موحد لها.

ونظرا للخصائص الاستثنائية التي تتميز بها هذه الظاهرة الإجرامية الجديدة سواء من حيث وسيلة و تقنيات ارتكابها أو البيئة الافتراضية و اللامادية التي تقع فيها. أو من حيث طبيعة مرتكبيها (المجرم الإلكتروني) الذي يتسم بالذكاء و المعرفة الخارقة في مجال المعلوماتية مقارنة لنضيره المجرم التقليدي ، فقد أثارت صعوبات كثيرة في التعامل معها و التصدي لها، و هو دفعنا إلى محاولة إظهار جانب من هذه الصعوبات من خلال دراسة مفهوم الجريمة الإلكترونية في (المبحث الأول) ، و بيان خصائص و أهم تصنيفات هذه الجريمة في (المبحث الثاني).

المبحث الأول

مفهوم جريمة تكنولوجيات الإعلام و الاتصال

إن بيان المشكلات القانونية و العملية التي تثيرها الجريمة الإلكترونية تتطلب من الباحث أن يقوم بدراسة مسألة أولية تتعلق بالتعريف بهذه الجريمة من خلال بيان معناها ، و كذا إظهار مختلف الخصائص والمميزات التي تختص بها هذه الظاهرة الإجرامية الجديدة في (المطلب الأول). ثم يتم بعدها التطرق الى أهم أنواع و تقسيمات الجريمة (في المطلب الثاني).

المطلب الأول

مقاربة تعريف جريمة تكنولوجيات الإعلام و الاتصال

لم تهتم معظم تشريعات دول العالم بوضع تعريفا محددا جريمة تكنولوجيا الإعلام و الإتصال ، إنما تركت الأمر لاجتهادات الفقهاء، الذين انقسموا في ذلك إلى عدة اتجاهات مختلفة.

فقد اعتمد الاتجاه الأول في تعريف هذه الجريمة على الجانب التقني المحيط بها أو وسيلة ارتكابها ، فنجد الفقيه الألماني تاديمان **Tièdement** عرفها بأنها " **كل أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب باستخدام الحاسب الآلي** "[1] في حين اعتبرها آخرون من نفس الاتجاه بأنها " **نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود** "[2]. و منهم كذلك من عرفها بأنها " **كل سلوك غير مشروع يكون العلم بتكنولوجيات الحاسبات**

---

[1]– نائلة عادل محمد فريد فودة، جرائم الحاسب الاقتصادية دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ، 2004، ص25 .

[2]– محمد الأمين البشري" التحقيق في جرائم الحاسب الآلي " بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت كلية الحقوق و الشريعة جامعة الإمارات، 21 مايو 2005 ، ص 6.

لآلي بقدر كبير لازما لارتكابه من ناحية، ولملاحقته و تحقيقه من ناحية ثانية" [3] . أما البعض الأخر فاعتبرها " **كل نشاط أو سلوك إجرامي يؤدي فيه الحاسوب الألي دورا لإتمامه بشرط أن يكون هذا الدور على قدر من الأهمية**"[4].

في حين ركز الا تجاه الثاني من الفقه على الجانب الموضوعي لتعريفه جريمة تكنولوجيا الإعلام و الإتصال ، إذ يرى بأنه لا يكفي لإطلاق هذا الوصف عليها بمجرد استخدام الحاسب الآلي أو أية وسيلة أخرى من وسائل الاتصال الحديثة، بل يشترط كذلك أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة إلكترونية. و من هنا عرفها الفقيه الفرنسي ماس MASS بأنها " **كل سلوك غير مشروع يتعلق بالمعلومات المعالجة و نقلها**" و في نفس السياق عرفت جريمة تكنولوجيا الإعلام و الإتصال كذلك بأنها " **نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي ترسل عن طريقه**"[5].

وأما الاتجاه الفقهي الثالث، فقد ركز في تحديد المقصود جريمة تكنولوجيا الإعلام و الإتصال على الجانب المعرفي، لا على الوسيلة أو الموضوع، وذلك لكونها مرتبطة بالجوانب المعرفية الفنية أو المعرفة باستخدام الحاسب الآلي و مختلف وسائل الاتصال الحديثة الأخرى، فحسب أنصار هذا الاتجاه تعتبر جريمة تكنولوجيا الإعلام و الإتصال " **أية جريمة يكون متطلباً لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي** ". و من هذا المنطلق صرح الفقيه David Thimson بأن جريمة تكنولوجيا الإعلام و الإتصال هي تلك التي يتطلب لاقترافها توافر لدى فاعلها معرفة فنية بتقنية الحاسب [6]. و السياق ذاته

---

[3]– عبد الحكيم، مولاي براهيم، الجرائم الإلكترونية، مجلة الحقوق و العلوم الإنسانية، جامعة زيان بن عاشور بالجلفة، الجزائر، عدد 23، جوان 2015، ص 213.

[4]– نائلة عادل محمد فريد فودة، مرجع سابق، ص 26.

[5]– موسي مصطفي محمد" التحقيق الجنائي في الجرائم الإلكترونية" مجلة الشرطة، عدد 1، لسنة 2009، ص 120.

[6]– غانم مرضي ألشمري، الجرائم المعلوماتية،ماهيتها – خصائصها – كيفية التصدي لها قانونا، دار العلمية الدولية للنشر و التوزيع، عمان،2016، ص 25.

عرفها الأستاذ هشام فريد رستم بأنها " **أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه**"[7] .

مقابل ذلك نجد الفقه الجزائري قد تأثر كثيرا بمقاربة المؤتمر العاشر للأمم المتحدة لمنع جريمة الحاسب الآلي و شبكاته، الذي عرُف جريمة تكنولوجيا الإعلام و الإتصال بكل " **جريمة يتم إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، و جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية**". [8] و هو ما انعكس على نية المشرع الجزائري في تبني معيار النظام المعلوماتي لتحديد معالم هذه الجريمة ، و ذلك حينما نص المادة الثانية (2) من قانون 04/09[9] بأن جرائم تكنولوجيا الإعلام و الإتصال هي "**الجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية**".

الملاحظ من هذا التعريف أن المشرع الجزائري لم يحدد بشكل دقيق المقصود بجريمة تكنولوجيا الإعلام و الإتصال إنما اكتفى فقط بالإحالة إلى بعض الجرائم المذكورة في قانون العقوبات في المواد من 394 مكرر الى 394 مكرر 7، و ترك المجال واسعا لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

و بمقارنة كل التعريفات السابقة نرجح الباحثة التعريف الذي أطلقته منظمة التعاون و التنمية الاقتصادية التابعة للأمم المتحدة (OCDE) على جريمة تكنولوجيا الإعلام و الإتصال أو الجريمة الإلكترونية باعتبارها " **كل فعل أو امتناع من شأنه الاعتداء على**

---

[7]– عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي الإسكندرية، 2006 ، ص 25.

[8]– زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزا ئري و الدولي ، دار الهدى ، الجزائر، 2011، ص17 .

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

حقوق مادية أو معنوية يحميها القانون يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية".

المطلب الثاني

مميزات جريمة تكنولوجيا الإعلام و الإتصال

تتسم جرائم تكنولوجيا الإعلام و الإتصال بجملة من الخصائص المميزات تجعلها تنفرد عن غيرها من الجرائم التقليدية و المألوفة أهم هذه المميزات مايلي:

الفرع الأول : الطابع العابر للحدود جريمة تكنولوجيا الإعلام و الإتصال

يعد الطابع عبر الوطني أهم السمات التي تميز هذا النوع من الإجرام عن غيرها من الجرائم التقليدية ، ويقصد به أن أثار هذه الجرائم قد تتجاوز الحدود الوطنية للدولة إلى غيرها من الدول ، لارتباطها بالشبكة العالمية للمعلومات – الانترنت– وما طرأ عليها من تطور ات هائلة في الآونة الأخيرة، تلاشت أمامها كل الحواجز و الحدود الجغرافية للدول[10].

فمعظم جرائم تكنولوجيا الإعلام و الإتصال يتجزأ ركنها المادي و يتوزع على أكثر من إقليم، ويتحقق ذلك عندما يرتكب السلوك الإجرامي في إقليم دولة معينة وتتحقق النتيجة الإجرامية في دولة أو عدة دول أخرى، كأن يرسل المتهم برنامج من برامج الفيروسات من جهاز الكتروني متواجد في دولة معينة إلى جهاز آخر يقع في دولة ثانية مرورا بجهاز ثالث ورابع في دول أخرى . كما أن الأثر الناتج عن الجريمة الإلكترونية لا يصيب المجني عليه وحده، إنما قد يمتدّ إلى متضررين آخرين في دول عدة، كما هو الحال بالنسبة لجرائم نشر معلومات ذات التهديد الديني أو الأخلاقي أو الأمني أو السياسي أو الاقتصادي. ومثل هذه الجرائم السهلة الإركاب و السريعة الانتشار عبر عدة الأقاليم.

[10]-**CHAWKI Mohamed**, combattre la cybercriminalité, Edition de saint-amans, Paris, 2008, p318.

من هنا فقد يثير الطابع الدولي و العابر للحدود للجريمة الإلكترونية عدة عقبات بخصوص مواجهتها و ملاحقة المجرمين، منها ما تعلق بتنازع الاختصاص القضائي بين الدول المتأثرة معا بنفس الجريمة الإلكترونية، وبالتنازع حول القانون الواجب التطبيق، بالإضافة الى غيرها من الصعوبات المتعلقة بإجراءات المتابعة القضائية للمجرم الإلكتروني[11].

ـ الفرع الثاني: جرائم تكنولوجيات الإعلام و الإتصال جرائم ناعمة

تتميز جريمة تكنولوجيات الإعلام و الإتصال عن الجريمة التقليدية بكونها هادئة و ناعمة، لأن ارتكابها لا يحتاج إلى استعمال العنف أو القوة ولا إلى سفك دماء أو وقوع جثث، وإنما يتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح لحدوث اختراق معلومات و سجلات مخزنة في الحاسب الآلي و هتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها دون أن تخلف أية آثار خارجية مرئية أو ملموسة[12].

فمثل هذه الجرائم لا تترك شهودا يمكن الاستدلال بأقوالهم ولا بصمات يمكن تحليلها أو أدلة مادية يمكن فحصها ، إنما تقع في بيئة الكترونية افتراضية عن طريق نقل معلومات رقمية و تداولها بواسطة ذبذبات الكترونية غير مرئية.

فجريمة تكنولوجيات الإعلام و الإتصال في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها، بحيث يمكن للمجرم الالكتروني استعمال عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة من أهمها، أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات و البرامج أو إدخال

---

[11]– موسى مسعود أرحومة "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية " مقال مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي نظمته أكادمية الدراسات العليا، طرابلس،28/29/10/2009 ،ص03.

[12]–حسين بن سعدي الغافري " التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت" ص 19. مقال متوفر في الموقع التالي: www.eastlaws.com.

بيانات مختلقة مزيفة أو محرفة في نظام معلومات الحاسب، أو تغيير مسار البيانات الصحيحة المدخلة دون أن يحس المجني عليه بذلك . أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن ارتكابها وبين حدوث النتيجة الإجرامية (كما هو الحال بالنسبة لمقاهي الانترنت) مما يفسح المجال لحدوث تغيرات أو عبث في الآثار المادية للجريمة أو زوال بعضها، وهو ما يلقي ظلالا من الغموض على الدليل[13].

كما أن الدليل في جريمة تكنولوجيات الإعلام و الإتصال يتمثل عادة في بيانات أو معطيات الالكترونية على شكل كتابة أو تسجيلات صوتية أو صورية أو فيلمية، تخزن بذاكرة الحاسب بلغة رقمية في صورة برامج أو أنظمة تشغيل تتجسد في وحدات حسابية لا يمكن لأي شخص قراءتها و فهمها إلا باستعادتها في شاشة ال حاسب، لذا يسهل محوها والتخلص منها بسرعة فائقة بمجرد الضغط على زرّ واحد في لوحة المفاتيح.[14]

ـــ الفرع الثالث: جريمة تكنولوجيات الإعلام و الاتصال ذات تقنية عالية

عرفت هذه الجريمة بذات التقنية العالية بالنظر إلى أساليب ارتكابها المبنية عادة على وسائل تقنية و علمية متطورة جدا وبالنظر كذلك إلى مرتكبها أي المجرم الإلكتروني الذي يتميّز عن المجرم التقليدي بالذكاء والمعرفة الفنية الواسعة في مجال الأنظمة الإلكترونية و المعلوماتية، فهذه الخصلة تمكنه من التخطيط جيدا لجريمته قبل أن يقدم على ارتكابها ، وإحاطتها بأساليب أمنية وتدابير الحماية الفنية التي تحول دون كشف أمره وتعيق مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل[15].

---

[13]– حسين بن سعدي الغافري" التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت"، مرجع سابق، ص 09.

[14]– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، عمان، 2008، ص 51.

[15]– موسى مسعود أرحومة، مرجع سابق، ص03.

فالمجرم الالكتروني يتمتع بالذكاء الخارق و بقدر كبير من المهارة بتقنيات الحاسوب والإنترنت بل أن بعض مرتكبي الجرائم الإلكترونية هم من المتخصصين في مجال المعالجة الآلية للمعلومات الذين يعلمون بخبايا هذا المجال و تقنون تفاصيله، فمثل هؤلاء غالبا ما يضربون سياجا أمنيا على أفعاله م غير المشروعة قبل ارتكابها ، وذلك باستخدام كلمات المرور السرية وترميز البيانات المخزنة إلكترونيا والمنقولة عبر شبكات الاتصال، وتشفيرها بشكل يستحيل على سلطات البحث والتحري تعقب آثار الجريمة واستخلاص الدليل حولها دون الحصول على هذه الرموز والشفرات[16].

كما قد يعمدون كذلك إلى حماية حاسوبهم الذي ارتكب بواسطته الجريمة الإلكترونية بكلمة السرّ لمنع الغير من الدخول إليه والإطلاع على محتواه. ففي هذه الحالة يكون القائمين على تنفيذ القانون أمام خيارين هما، إما أن يطلب من المتهم الإفصاح عن كلمة السر التي تسمح له بالولوج إلى داخل الحاسب و تفتيشه ، وهنا غالبا ما يتحفّظ المتهم عن تقديم كلمة السرّ لأن القانون لا يجيز إجبار المتهم على تقديم أدلة أو الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته؛ إذ من حقه الإعتصام بالصمت دون أن يُفسَّر ذلك ضد مصلحته. وإما أن يسعى القائم بالتفتيش بنفسه إلى الكشف عن كلمة السر و فكّ رمز الدخول إلى الحاسوب، وفي هذه الحالة أيضا تصطدم سلطات البحث بجملة من الصعوبات، لان فكّ رموز الدخول ليس بالأمر الهين إذ يحتاج في أغلب الأحيان إلى جهد و وقت كبيرين بالإضافة إلى خبرة ومعرفة عالية في الميدان وهو الأمر الذي لا يتوفر عادة لدى معظم رجال القضاء خاصة في الدول المتخلفة[17].

---

[16]- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2002، ص 115.

[17]– ممدوح عبد الحميد عبد المطلب" جرائم استخدام شبكة المعلومات العالمية" بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة ، 2000، ص.ص 24 وما بعدها.

وقد يلجأ كذلك المتهم إلى تشفير البيانات المخزنة داخل حاسوبه للحيلولة دون وصول المحقق إلى الأدلة التي تدينه، ويقصد بتشفير البيانات استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها البيانات أو المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من قبل الغير ، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات المخزنة في الحاسوب بدونها [18]. مع العلم أن عملية التشفير تتم وفق معادلات رياضية معقدة تسم ى الخوارزميات. وهنا أيضا يجد المحقق نفسه أمام خيارين لحل مشكلة التشفير وهما ، إما أن يحصل على مفاتيح الشفرات من المتهم مشغل الحاسوب، وإما أن يحاول فكّ الشفرات بنفسه. إلا أن في الخيار الثاني يجب أن يكون المحقق ملمّ بعلم تحليل الشفرات أو ما يعرف بعلم استرجاع النص الواضح بعبارة معينة بدون معرفة المفاتيح، ويرتكز هذا العلم على الرياضيات التطبيقية وفروعها المختلفة مثل نظرية الاحتمالية و نظرية الإعداد والإحصاء والجبر، وهو الأمر المفقود لدى السلطات الأمنية و القضائية.

هناك تقنية حديثة يستعين بها المجرم الالكتروني من أجل عدم كشف آثار جريمته تسمي بتقنية إخفاء المعلومات (Steganography)[19]، يقوم المتهم من خلالها بإخفاء بيانات مهمة داخل بيانات أخرى قد تكون على شكل ملفات مصورة أو صوتية أو فيلمية أو على شكل بيانات تنفيذية لبرامج الحاسب، أو يقوم بإخفاء هذه المعلومات في مساحة معينة من القرص الصلب مخصصة فقط ل تخزين ملفات أنظمة التشغيل دون غيرها تسمى بالمساحة الهادئة (Slack). وهذه التقنية من ش أنها تغليط مسار رجال التحقيق و تعيقهم من الوصول إلى أدلة مادية ضد المتهم، مع العلم أن اكتشاف البيانات المخفية و تحليلها

---

[18]– إسماعيل عبد النبي شاهين" أمن المعلومات في الانترنت" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2000، ص11.

[19]– للمزيد من التفاصيل في هذا الموضوع راجع : مراد عبد الرحمان مكاوي " الستيغانوغرافي " مجلة المعرفة، العدد 147، نيسان، 2009، ص 41. منشور على الموقع التالي:

http://www.almarefh.org/news.php?action=shawgid=6,4

في هذه الحـالة لا تتم إلا بطريقة علمية و رياضية معقدة جدا تسمـى بتقنية تحليل البيانات المخفية (Steganalysis) لا يفهمها إلا ذوي الاختصاص.

بناء على ما سبق، يرى المتخصصون في مكافحة الجرائم الإلكترونية أن الأنظمة المعلوماتية و ما يقع عليها من جرائم تعد تحديا حقيقيا لأجهزة العدالة الجنائية، ذلك لأن رجل الأمن بما يعانيه من نقص مهاراته الفنية في استخدام الوسائل الالكترونية الحديثة والانترنت، وقلة خبرته في تقنيات البحث والتحقيق بخصوص الجرائم المتصلة بهذه الوسائل، الناتج عن عدم إلمامه بأساليب ارتكاب الجرائم الالكترونية وعدم معرفته باللغة العلمية الرقمية، لن يكون قادرا على التعامل مع الجريمة الالكترونية الحديثة التي ترتكب بواسطة تقنيات عالية[20].

ـــ الفرع الرابع: جريمة تكنولوجيا الإعلام و الإتصال حديثة النشأة و سريعة التطور

تعتبر الجرائم الالكترونية من بين الجرائم المستحدثة التي ظهرت في ظل التطور التكنولوجي الهائل الذي عرفه مجال الإعلام و الاتصالات، فهي تختلف عن الجرائم التقليدية التي ترتكب في العالم المادي، وتتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يألفها العالم من قبل. [21] و متجددة لارتباطها بالتطور السريع الذي يشهده العالم يوما بعد يوم في ميدان تكنولوجيا الاتصالات، الذي انعكس بدوره على تطور مرتكب الجريمة الإلكترونية أسلوب ارتكابه من خلال ما يحمله من أفكار و تبادل المعارف و الخبرات مع المجريمين حول العالم عبر شبكة الأنترنت، و تطور التقنيات في ذلك.

---

[20]– حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 410.

[21]– عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الأنترنت دراسة مسحية على ضباط الشرطة في البحرين، مذكرة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، 1999، ص 26.

فالجرائم الالكترونية تقع في بيئة افتراضية لا مادية عبر نبضات وذبذبات إلكترونية رقمية غير محسوسة و لا يتطلب ارتكابها استعمال العنف أو بذل مجهودا كبيرا كما في الجرائم التقليدية، فكل ما تحتاجه هو القدرة على التعامل مع حاسوب مرتبط بشبكة المعلومات الدولية بمستوى تقني يوظف لارتكاب أفعال غير مشروعة، فيكفي لتحققها مجرد نقرة بسيطة على لوحة مفاتيح الحاسب ، و في وقت قياسي قد يكون جزءًا من الثانية، مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، وإنما حتى في الوسيلة التي ترتكب.

أضف إلى ذلك فهده الجرائم المستحدثة لا تعترف بالحدود الجغرافية لارتباطها بشبكة الانترنيت، ولا توجد حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسيب و شبكاتها في نقل كميات كبير من المعلومات و تبادلها بين أنظمة يفصل بينها ألاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دولة مختلفة قد تتأثر بالجريمة الالكترونية الواحدة .

نتيجة لذلك تعد جريمة تكنولوجيا الإعلام و الإتصال من الجرائم الأكثر تطورا و الأسرع انتشارا في العالم بسبب ارتباطها الوثيق بالتطور التكنولوجي الهائل و المتسارع والذي تجسده و سائل الاتصال الحديثة و شبكة المعلومات، بالإضافة إلى مختلف المؤتمرات التي يعقدها القراصنة بهدف تطوير قدراتهم التقنية و المعرفية في مجال الإجرام المعلوماتي و ابتكار تقنيات حديثة و طرق جديدة لارتكاب جرائمهم.

بمقابل ذلك نجد القوانين العقابية لا تطور بنفس السرعة والوتيرة التي تتطور بها وسائل الإعلام والتكنولوجيا و مهارات الذهن البشري في تسخير مبتكرات التكنولوجية، مما يجعلها عاجزة عن مواجهة العديد من هذه الجرائم الجديد التي ارتبطت بظهور و انتشار الوسائل والأجهزة الالكترونية، خاصة إذا علمنا أن القوانين الوضعية السائدة في اغلب دول

العالم يحكمها مبدأ الشرعية الجزائية الذي ينص على انه" **لا جريمة و لا عقوبة إلا بالنص**"، وأن نطاق التجريم بالقياس في ظل هذا المبدأ يكون ضيقا جدا[22].

فثمة أفعالا جديدة كثيرة خاصة في الدول المتخلفة، مرتبطة باستعمال الحاسب الآلي غير مجرّمة بمنظور القوانين العقابية التقليدية، ولا تمتد إليها لمكافحتها رغم تهديدها للمصالح العامة و تشكل خطورة بالغة على النظام العام، ومن الأمثلة على هذه الأفعال الاعتداء على حرمة الحياة الخاصة المعلوماتية، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما التسلل والنفاذ إلى أسرار الفرد وخصوصياته الشخصية أو المهنية من خلال الوصول إلى المعلومات المخزنة لديه في أنظمته المعلوماتية داخل الحاسب، فان هذا التصرف لا يخضع للتجريم وفقا للقواعد العامة[23].

كما أن الدخول في نظام حاسب مملوك للغير وسرقة المعلومات منه ، لا يعد جريمة بمفهوم القوانين التقليدية لان السرقة حسب هذه الأخيرة لا ترد إلا على المال المنقول، وهذه الصفة لم تثبت بعد للمعلومات كونها تعتبر سوى أفكار معنوية بحتة ، زيادة على ذلك فان فعل السرقة أو الاختلاس بالمفهوم الكلاسيكي يعني تجريد الغير من ماله في حين أن اختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها، لذا فإنها لا يحميها التجريم المقرر في جرائم الأموال [24]. والشيء نفسه قيل بعدم وقوع جريمة الإتلاف

---

[22]– سرحان حسن ألمعيني ، مرجع سابق، ص21.

[23]– غنام محمد غمام" عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر" بحث مقدم إلى مؤتمر القانون و الكمبيوتر والانترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة الممتدة من 01 إلى 03 ماي 2003، ص 625.

[24]– المرجع نفسه، ص646.

على الكيانات غير المادية للوسائل الالكترونية كالبيانات و البرامج [25]، وعدم وقوع جريمة التزوير على المعلومات المبرمجة في الحاسب أو في أية دعامة مادية كالاسطوانات أو أقراص ممغنطة أو أشرطة لعدم انطباق وصف المحرر عليها[26].

ففي مثل هذه الحالات، تثور العديد من الصعوبات أمام تطبيق نصوص التجريم التقليدية، مردها أن هذه النصوص وضعت أساسا لحماية الأشياء المادية في مواجهة صور الاعتداء المألوفة والتقليدية مما يتعذر معه أو يستحيل أن يقع تحت طائلة العقاب الاعتداء على عناصر ومكونات الأنظمة المعلوماتية المتمثلة في صور غير مادية، فضلا عن أن تطبيق مثل هذه النصوص قد يتعارض أحيانا مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها البيانات أو المعلومات بشتى أنواعها المرئية أو المصورة أو المكتوبة[27].

لذلك، دفع عدم مواكبة القوانين العقابية للتطورات السريعة والمستمرة المصاحبة للجرائم الالكترونية، معظم دول العالم، لا سيما التي لم تسن بعد قوانين خاصة لتجريم مختلف أنماط الجرائم المستحدثة إلى اتخاذ سبيل التفسير الموسع للنصوص الجنائية التقليدية ليطال تطبيقها هذه الجرائم التي أوجدتها ثورة الاتصالات عن بعد. وذلك بمنح سلطاتها القضائية حرية تفسير هذه النصوص بشكل أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة، تفاديا من إفلات الجنات من قبضة العدالة.

ولكن تطبيق النصوص التقليدية بمفهومها الموسع لتشمل الجرائم الالكترونية قد يشكل خرقا صارخا لمبدأ جوهري من مبادئ القانون الجنائي وهو مبدأ التفسير الضيق للنصوص العقابية وحضر القياس، ومن شأنه أن يمس بمبدأ الشرعية الجزائية إذا ترك الأمر بيد

---

[25]– **بكرى يوسف بكرى**، مرجع سابق، ص22.

[27]– **بكرى يوسف بكرى**، مرجع سابق، ص 23.

القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله [28]. الأمر الذي قد يؤدي إلى ارتكاب خروقات واعتداءات على الحريات والحقوق الفردية بدون مبرر أو أساس قانوني مشروع.

ونظرا للعجز الكبير الذي أثبتته القوانين العقابية التقليدية في مواجهة جرائم تكنولوجيا الإعلام و الإتصال ، حاولت بعض الدول خاصة المتقدمة منها إلى استدراك الوضع بسن تشريعات جديدة تتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة، فمنها التي اختارت تعديل قوانينها العقابية وإضافة نصوص جديدة إليها تتجاوب مع الظاهرة الإجرامية الحديثة لسدّ الفراغ التشريعي القائم في هذا المجال، ومنها التي فضلت استحداث نصوص جديدة خاصة بهذا النوع المستجد من الإجرام. غير أن الملاحظ في هذه القوانين، أنها لا تشمل كافة الأفعال غير المشروعة الناتجة عن استعمال التكنولوجيا الحديثة، بسبب عدم تطورها بالوتيرة نفسها التي تتطور بها الجرائم الالكترونية، كما أن معظم دول العالم خاصة المتخلفة منها لم تسن بعد قوانين تجرم مثل هذه الأفعال غير المشروعة، واكتفت فقط بتطبيق القواعد القانونية القائمة رغم ثبوت قصورها. ولعل السبب في ذلك هو افتقارها إلى الخبرة والتخصص والمعرفة الكافية للبيئة الالكترونية العالية التقنية والمعقدة .

[28]–عبد الفتاح بيومي حجازي، مرجع سابق، ص 115.

المبحث الثاني

أركان جريمة تكنولوجيات الإعلام و الاتصال

إذا كانت الجرائم الإلكترونية تنفرد بمميزات خاصة بها تجعلها مختلفة عن غيرها من الجرائم التقليدية، إلا أن ذلك لا يعني خروجها عن المبادئ العامة التي تحكم التجريم و العقاب، فجرائم تكنولوجيا الإعلام و الإتصال مثلها مثل غيرها من الجرائم يشترط لقيامها توفر ثلاثة أركان أساسية يحددها المشرع مسبق بنصوص قانونية واضحة طبقا لمبدأ الشرعية الجزائية.

تعتبر أركان الجريمة جزءا لا يتجزأ من طبيعتها و تركيبتها و تخلف أحدها يؤدي الى إنتفاء الجريمة بأكملها، لذا يتطلب القانون كأصل عام ركن مادي و ركن معنوي، و ركن شرعي بموجبه يتم التجريم و العقاب. و هو الأمر المعمول به في كل الجرائم تقليدية كانت أم مستحدثة مع احتفاظ هذه الأخيرة بعض الخصوصيات متعلقة بأركانها الثلاثة، كما يأتي بيانه فيما يلي.

المطلب الأول

الركن الشرعي لجريمة تكنولوجيا الإعلام و الاتصال

الأصل في تصرفات و معاملات الأشخاص الإباحة إلا ما جرمه القانون، من هنا يتمثل الركن الشرعي للجريمة في النص القانوني الذي يجرّم الفعل بشكل واضح و صريح و يحدد الجزاء الذي يقابله وقت وقوع هذا الفعل. فعملا بمبدأ الشرعية الجزائية الذي يقضي بأن " لا جريمة و لا عقوبة إلا بالنص " فإن المصدر الوحيد للتجريم و العقاب هو التشريع ، فما اعتبرته النصوص الجنائية فعل غير مشروع كان جريمة و ما لم تعتبره كذلك كان فعلا مباحا و تمنع معه المساءلة الجنائية. ومتى انتفى نص التجريم فلا يجوز اعتبار واقعة ما

على أنها مجرّمة قياسا على واقعة أخرى مشابهة لها ، كما يمنع تفسير النصوص الجنائية إلى خارج حدود نية و إرادة المشرع.

ومن هنا فإن حداثة جرائم تكنولوجيا الإعلام و الاتصال و تطوراتها السريعة و المستمرة جعل مهمة القضاء عسيرة نظرا لعدم وجود نصوص كفيلة بمواجهة هذه الجرائم، الناتج عن عدم مواكبة التشريعات الجنائية القائمة لهذه الظاهرة الإجرامية الجديدة و المتجددة. مما دفع الدول التي لم تسنّ بعد قوانين خاصة لتجريم مختلف الجرائم الناشئة عن الاستخدام غير المشروع لوسائل تكنولوجيا الإعلام و الإتصال الحديثة الى تطبيق القوانين الجنائية القائمة بموادها التقليدية على هذه الوقائع الإجرامية لتفادي إفلات الجناة من قبضة العدالة و كبح انتشارها. و ذلك بالتفسير الموسع لهذه النصوص القانونية[29].

ويكون السبيل الى التفسير الموسع للنصوص القائمة من أجل تطبيقها على الجرائم المستحدثة ، بمنح القاضي الجزائي حرية تفسير هذه النصوص تفسيرا أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة الجزائية، وذلك في حدود السلطة التقديرية التي يتمتع بها القاضي[30].

وفي هذا الصدد نجد القضاء في العديد من الدول، قام بتفسير النصوص الجنائية التي تجرّم استخدام مال الغير دون وجه حق، مثل القانون البلجيكي المادة (2/261) والدانمركي المادة (293)، بشكل يسمح بمدّ نطاقها لتجريم سرقة وقت وجهد وخدمات الأجهزة والأنظمة المعلوماتية في حالة ما استخدمت من قبل الغير بدون الحصول على

[29]– هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012، ص 72.

[30]– يوسف حسن يوسف، الجرائم الدولية للانترنت، مرجع سابق، ص 126 و ما يليها.

موافقة حائزها أو مالكها. وذلك نظرا لعدم توفر قوانينها الجنائية لنص صريح يجرّم هذه الأفعال[31].

كما نجد القضاء الفرنسي قد وسّع من تفسير نص المادة (145) من قانون العقوبات المتعلقة بجريمة تزوير المحررات التقليدية قبل تعديلها بالمادة(462) من قانون الغش المعلوماتي لعام 1988، لتشمل كل أشكال التلاعب في البيانات و الأنظمة المعلوماتية. وكذلك فعل القضاء الياباني، إذ لجأ في ملاحقة جرائم التزوير المعلوماتي، إلى تبني المفهوم الموسع لجريمة التزوير، واعتبر تغيير الحقيقة في الجزء الممغنط من بطاقات البيانات يقع تحت طائلة العقاب على التزوير في المحررات التقليدية[32].

كذلك الشأن بالنسبة لجريمة الاحتيال فقد أكد الفقه الكندي بأنه في ظل عدم وجود نصوص جديدة تجرّم الاحتيال عبر وسائل تكنولوجيا الإعلام و الإتصال ، فلا مانع من مد نطاق المادتين(387 و 388) من قانون العقوبات الكندي إلى جرائم الاحتيال الالكتروني[33].

وينبغي ألا يقتصر التفسير على تمديد سلطان النصوص الجنائية التقليدية الموضوعية حتى تسري على جرائم تكنولوجيا الإعلام و الاتصال فقط، بل لابد أن يشمل كذلك النصوص الإجرائية، لا سيما المتعلقة بالتحقيق والإثبات، وهو ما أوصت به اللجنة الأوروبية الخاصة بمشكلات الإجرائية الجزائية المرتبطة بتكنولوجيات الإعلام الدول الأعضاء في المجلس الأوروبي من خلال توصيتها رقم (ر 89) 9 الصادرة في عام 1990 وأكدته في توصيتها رقم (ر 95) 13 المؤرخة في 11 سبتمبر 1995 بتصريحها أنه " إلى حين وضع

---

[31]–غازي عبد الرحمن هيان الرشيد، الحماية القانـــونية من جرائم المعلوماتية، رســـالة لنيل درجة دكتــوراه في القانون، كلية الحقوق، الجامعة الإسلامية ، بيروت، 2004، ص 222.

[32]– المرجع نفسه، ص.ص 252– 258.

[33]- **BRIAT Martin**. La Fraude Informatique: Une approche de droit compare, Revue D.P.C, N04 Paris, Avril 1985, p 191.

نصوص إجرائية جديدة تخص التفتيش و الضبط واعتراض المراسلات في البيئة الالكترونية، يمكن للسلطات القضائية المختصة في الدول الأعضاء الاستعانة بالنصوص الإجرائية القائمة في هذا الخصوص، حتى لا تبقى الجرائم المتصلة بتكنولوجيات الإعلام بلا متابعة أو عقاب"[34].

وتجدر التنبه إلى أن تطبيق النصوص الجنائية التقليدية على الجرائم التي تقع في البيئة الالكترونية، وإن كان يشكل ضرورة ملحة في الدول التي لم تسنّ بعد تشريعات حديثة مواكب لهذا النوع من الجرائم، إلا أنه لابد من توخي الحذر في ذلك. إذ أن الآلية الوحيدة لإعمال هذا الخيار هو توسع القضاء في تفسير النصوص الجناية التقليدية بما يضمن سريانها على الجرائم الحديثة ، وهو ما قد يشكل إنتهاكا خطيرا لمبدأ الشرعية الجزائية الذي طالما كان درعا حاميا للحقوق والحريات الفردية من تعسف القضاء [35].

المطلب الثاني

الركن المادي لجريمة تكنولوجيات الإعلام و الاتصال

لا تختلف جريمة تكنولوجيا الإعلام و الاتصال عن غيرها من الجرائم من حيث ضرورة توافرها على الركن المادي حتى يكتمل بنيانها و من ثم محاسبة و معاقبة مقترفيها وفقا للقانون. فلا جريمة دون ركن مادي، الذي يتكون من عناصر ثلاثة على التوالي، سلوك إيجابي أو سلبي الذي يأتيه الجاني قصد المساس بمصلحة أو حق يحميه القانون. ونتيجة إجرامية ممثلا في الأثر الحسي الملموس الذي يحدث في العالم الخارجي نتيجة للسلوك

[34] - voir : la recommandation n R (89) 9 sur la criminalité informatique, comité européen pour les problèmes de droit procédural liés a la criminalité informatique, conseil de l'Europe, Strasbourg, 1990, p 80. Et sa recommandation n R (95) 13, conseil de l'Europe, Strasbourg, 1995, p19.

[35] -**CHAWKI Mohamed**, combattre la cybercriminalité, op.cit. , p 399.

الإجرامي. بالإضافة الى العلاقة السببية المتمثلة في الصلة التي تربط بين الفعل و النتيجة و تثبت أن ارتكاب السلوك الإجرامي هو الذي أدى الى حدوث النتيجة الإجرامية[36].

إلا أن الركن المادي في جرائم تكنولوجيا الإعلام و الاتصال يختلف عن مثيله في الجرائم الأخرى، وذلك راجع إلى طبيعة الوسط الذي تتم فيه هذه الجرائم المتمثلة في الجانب التقني، و الذي يشترط أن يتم السلوك الإجرامي باستخدام جهاز الحاسب الآلي أو إحدى وسائل الاتصال الحديثة الأخرى عبر الشبكة العالمية الانترنت. مما يثير عدة نقاط إستفهام حول بداية تنفيذ النشاط التقني أو الشروع فيه، و إتمام عناصر الركن المادي، أجزاء السلوك الإجرامي في الوسط المادي أو الافتراضي[37].

أما بالنسبة للنتيجة الإجرامية في جرائم تكنولوجيا الإعلام و الاتصال، فهي أيضا تطرح عدة إشكالات حول ما إذا كانت تقتصر على العالم الإفتراضي، أم لها جزء في العالم المادي. و هل تقتصر النتيجة على مكان واحد في إقليم دولة ما أم تمتد لتشمل أماكن عدة في أكثر من دولة . فإذا قام أحد المجرمين في الجزائر باختراق جهاز خادم أحد البنوك في كندا، و هذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت جهاز الخادم في الصين[38].

كما أن تحديد العلاقة السببية بين السلوك الإجرامي و النتيجة في جرائم تكنولوجيا الإعلام و الاتصال ليس بالأمر الهين، بالنظر الى تعقيدات تقنية الوسائل المستعملة لارتكاب هذه الجرائم و تطورها، إضافة الى تنوع و تعدد أساليب الإتصال بين الأجهزة الإلكترونية و تعدد المراحل التي تمر بها الأوامر المدخلة حتى تنفذ و تتحقق النتيجة المراد

---

[36]– منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر و التوزيع، عنابة، 2006، ص 94.

1 – [37]– صغير يوسف، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجستير في القان ون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود، معمري بتيزي وزو، 2013، ص 66.

[38]– عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، بهجات للطباعة و التجليد، القاهرة، 2009، ص. ص 113–114.

الحصول عليها، كل ذلك يحول حتما دون تحديد السبب أو الأسباب الحقيقية المساهمة في حدوث الأضرار أو الآثار غير المشروعة[39].

المطلب الثالث

الركن المعنوي لجريمة تكنولوجيا الإعلام و الاتصال

يتمثل الركن المعنوي للجريمة في العلاقة التي تربط بين ماديات الجريمة و شخصية مرتكبها، فهو بذلك يتجسد في القصد الجنائي أو النية الإجرامية عند الجاني التي تتجه إلى ارتكاب سلوك أو فعل يعلم مسبقا بأنه غير مشروع و يعاقب عليه القانون[40].

و لا يتحقق الركن المعنوي أو القصد الجنائي إلاّ إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء ما تعلق بسلوكه الإجرامي أم بموضوع الاعتداء أو المصلحة المعتدى عليها. أما إذا كان الجاني يجهل بأحد هذه العناصر إنتفى معه القصد الجنائي و من ثم إنتفاء الجريمة برمتها. ففي جريمة السرقة مثلا لا يتحقق القصد الجنائي إلا إذا كان الجاني يعرف أن المال محل السرقة ملك للغير. و أن اختلاسه كان بقصد التملك. فالذي يأخذ مال معتقد أنه ماله، أو قصد إرجاعه لصاحبه، فلا يعد سارقا بحكم عدم تحقق القصد الجنائي لديه[41].

كما لا يكتمل الركن المعنوي لجريمة ما إلا إذا توافر على عنصر الإرادة، و التي تتمثل في النشاط النفسي الذي يهدف الى تحقيق غرض معين، فإذا كان غرض الجاني تحقيق نتيجة إجرامية ، كانت الإرادة المتجهة الى الفعل المنطوي على إحداث النتيجة هي "

---

[39]– صغير يوسف، مرجع سابق، ص 68.

[40]– حسني محمود نجيب، النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، 1971، ص 90.

[41]– عبد الله دغش العجمي، المشكلات العلمية و القانونية للجرائم الإلكترونية ـ دراسة مقارنة، مذكرة ماجستير في القانون العام، بكلية الحقوق بجامعة الشرق الأوسط، الكويت، 2014، ص 29.

القصد الجنائي". و الغرض هو الهدف القريب الذي تتطلع إليه الإرادة، أما الباعث فهو عبارة عن الدافع الى إشبتع حاجة معينة، و هذا الدافع له طبيعة نفسية، بخلاف الغاية التي لها طبيعة موضوعية. فإذا أراد الجاني سرقة المجني عليه لضائقة مالية مر بها، كانت الغاية التي يسعى لها أخذ المال، أما الغرض فهو التعدي على الضحية لسرقته، في حين أن الباعث هو التخلص من الديون التي أثقلت كاهله[42].

من هنا فإن تحديد الركن المعنوي في جرائم تكنولوجيات الإعلام و الاتصال، أمرا ضروريا جدا لاكتمال بنيانها، لأن القول بقيام مسؤولية مرتكب الفعل الإجرامي من عدمه يتوقف أساسا على مدى توفر القصد الجنائي بعنصريه العلم و الارادة لديه . فالحالة النفسية للجاني بصفة عامة و القصد بصفة خاصة هو الذي يحدد لنا مسؤولية الفاعل من عدها، إذ لا يعقل أن نحاسب شخص مسلوب الإرادة الذي أكره على فعل شئ غير مشروع في نظر القانون.

غير أنه رغم هذا المساواة بين جميع الجرائم في وجوب توافر الركن المعنوي فيها، إلا أن هناء استثناءات فيما يخص جرائم تكنولوجات الإعلام و الإتصال، و ذلك بالنظر الى طبيعتها اللامادية والسرعة الفائقة في إرتكابها مع تعقيد أساليب وقوعها، حيث لا تدع المجال لتحديد الفعل من عدمه فما بلك بتحديد القصد الجنائي فيها، بالإضافة إلى اختلاف عنصر الباعث أو الدافع النفسي لدى مرتكبي هذه الجرائم عن نظرائهم في الجريمة التقليدية. فغموض الباعث في الجرائم المرتكبة عبر وسائل تكنولوجيا الإعلام و الإتصال الحديثة يعد من الصعوبات التي تحول دون الوصول الى تحديد العقوبة لمقترف الفعل المجرم، و ذلك لانعدام القصد الجنائي[43]. فمثلا إذا إخترق أحد القراصنة الهواة لقاعدة بيانات شركة معينة قصد التعلم أو التسلية دون علمه أن هذا الفعل مجرم فهنا ينتفي القصد الجنائي. مما يحول

---

[42]– عبد الله دغش العجمي، مرجع سابق، ص 30.

[43]– عبد الله ذيب عبد الله محمود، حماية المستهلك في التعاقد الإلكتروتي ـ دراسة مقارنة، مذكرة ماجستير في القانون الخاص، كلية الدراسات العاليا، جامعة النجاح الوطنية، القدس، 2009، ص 96.

دون مسائلة الفاعل. لذا فمن المستحسن اعتبار جرائم تكنولوجيات الإعلام و الاتصال ضمن جرائم الضرر التي تكتفي لقيامها توفر الركن المادي و الشرعي فقط .

الفصل الثاني

تدابير مواجهة جرائم تكنولوجيات الإعلام والاتصال

تعد جرائم تكنولوجيات الإعلام والاتصال من الجرائم المستحدثة، والتي تناولها المشرع الجزائري بنصوص قانونية خاصة وعامة، وذلك للحد من إنتشارها ومكافحتها بكل الوسائل المتاحة، وقد حددها التشريع الجزائري بدقة من خلال تجريم كل الأفعال المتعلقة باستعمال تكنولوجيات الإعلام والإتصال المستعملة في الإجرام، ولقد تم وضع آليات قانونية لمكافحة هذا النوع من الجرائم، بوضع تدابير لمواجهة جرائم تكنولوجيات الإعلام والاتصال، باتخاذ واتباع نوعين من التدابير وهي التدابير الردعية لجرائم تكنولوجيات الإعلام والاتصال (المبحث **الأول**)، أما النوع الثاني من التدابير فهي تدابير الوقاية من جرائم تكنولوجيات الإعلام والاتصال (المبحث الثاني).

المبحث الأول

التدابير الردعية لجرائم تكنولوجيات الإعلام والاتصال

حاول المشرع الجزائري الحد من جرائم تكنولوجيات الإعلام والاتصال باتخاذ التدابير الردعية لهذا النوع من الجرائم، لذا صدرت عدة نصوص قانونية تتعلق بمكافحة هذه الجرائم، وهذه النصوص ترتكز على نوعين من التدابير الردعية وهي سن نصوص موضوعية زجرية لجرائم تكنولوجيات الإعلام والإتصال (المطلب الأول)، وكذلك وضع نصوص إجرائية خاصة لمتابعة جرائم تكنولوجيات الإعلام والإتصال (المطلب الثاني).

المطلب الأول

سن نصوص موضوعية زجرية لجرائم تكنولوجيات الإعلام والإتصال

تعتبر التدابير الردعية نوع من الحلول التي يصفها المشرع الجزائري لمكافحة الجرائم، والآليات المناسبة للحد من جرائم تكنولوجيات الإعلام والإتصال هي سن نصوص موضوعية زجرية وهذا بإدراج نصوص تجريمة و عقابية لهذه الأفعال غير المشروعة في القواعد العامة أي قانون العقوبات (الفرع الأول)، ثم تدعيمها كذلك بنصوص موضوعية في القوانين الخاصة (الفرع الثاني).

ـ الفرع الأول: سن نصوص موضوعية زجرية في القواعد العامة (قانون العقوبات)

لقد تطرق المشرع الجزائري إلى تجريم الأعمال الإلكترونية وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15[44] المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-165 المتضمن قانون العقوبات تحت عنوان "المساس بأنهم المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة (394 مكرر إلى 394 مكرر 7).

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23[45] المؤرخ في 20 ديسمبر 2006، حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعاملة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون رقم 04-15، وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتباكه، ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف فقط من الطبقة المثقفة بل من قبل

[44] ـ قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يتضمن تعديل قانون العقوبات، الجريدة الرسمية عدد (71) لسنة 2004.

[45] ـ قانون رقم 06-23 مؤرخ في 20 ديسمبر، يتضمن تعديل قانون العقوبات، الجريدة الرسمية عدد (84) لسنة 2006.

الجميع بمختلف الأعمار والمستويات نتيجة بتبسيط وسائل التكنولوجيا وانتشار الانترنت كوسيلة لنقل المعلومات[46].

نجد أن المشرع الجزائري قد تبنى المبدأ المقرر في الاتفاقية الدولية للإجرام المعلوماتي بموجبها أن تكون العقوبات المقررة نتيجة إرتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية، كما أضافت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ مساءلة الشخص المعنوي، لذا سن عقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي.

أولا: العقوبات المطبقة على الشخص الطبيعي: نجد عقوبات أصلية وعقوبات تكميلية على الشخص الطبيعي:

1- العقوبات الأصلية المطبقة على الشخص الطبيعي:

نجد عقوبات أصلية وعقوبات تكميلية على الشخص الطبيعي.

من خلال إستقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذ نجد سلم خطورة يتضمن ثلاث درجات: جريمة الدخول أو البقاء بالغش في الدرجة الأولى، وبعدها الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات[47].

أ- جريمة الدخول والبقاء بالغش:

---

[46] بن لغوم خالد أمين: إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص قانون خاص، كلية الحقوق، جامعة مستغانم، 2019، ص37-40.

[47] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2008، ص127.

- الدخول والبقاء بالغش (الجريمة البسيطة) العقوبة المقررة هي 03 أشهر إلى سنة حبس و(50.000) دج إلى (100.000 دج) غرامة، ما تضمنته الفقرة الأولى من المادة 394 مكرر من قانون العقوبات.
- الدخول والبقاء بالغش(الجريمة المشددة) تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات، والعقوبة المقررة من 06 أشهر إلى سنتين وغرامة من (50.000 دج) إلى (150.0000) إذا ترتب عن الدخول أو البقاء غير المشروع لنظام إشتغال المنظومة وهذا حسب الفقرة (2) و(3) من المادة (394 مكرر)[48].

ب- **جريمة التلاعب بالمعطيات:** نصت عليها المادة (394 مكرر 1) من قانون العقوبات الجزائري، وذلك بالحبس من (06) أشهر إلى (03) سنوات وعقوبة الغرامة التي تتراوح من (500.000 دج) إلى (2.000.000دج)[49].

والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدى إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي، بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة[50].

---

[48] – المادة (394 مكرر) من قانون العقوبات.

[49] – المادة(394 مكرر 1) من قانون العقوبات.

[50] – نائلة قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الأردن، 2005، ص228.

ت- **جريمة التعامل في معطيات غير مشروعة:** تعاقب المادة (394 مكرر 2) من قانون العقوبات الجزائري على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى (03) سنوات وبالغرامة المالية من (1.000.000دج) إلى (5.000.000دج)[51].

بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمة الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة والمشددة وبين جريمة التلاعب بالمعطيات(غير أن حدها الأدنى يقل عن كلتا الجريمتين) ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتيهما(سنة أو سنتين) وستساوي مع الحد الأقصى لجريمة التلاعب بالمعطيات (03 سنوات)، غير أن حدها الأدنى يقل عن الجريمتين معا، لأنه في جريمة الدخول أو البقاء البسيطة (03 أشهر)، وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب هو (6 أشهر)[52].

2- العقوبات التجميلية المطبقة:

نصت المادة (394 مكرر 6) من قانون العقوبات الجزائري على العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية، وجاء فيها مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها في هذا القسم، علاوة على إغلاق المحل او

---

[51] – المادة(394 مكرر 2) من قانون العقوبات.

[52] – محمد خليفة، الحماية الجزائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2008، ص219.

مكان الاستعمال إذا كانت الجريمة قد إرتكتب بعلم مالكها، ويستخلص من نص هذه المادة العقوبات التكميلية كالتالي:

-مصادرة الأجهزة والوسائل والبرامج المستخدمة.

-إغلاق المواقع التي تكون محلا للجريمة من جرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

-إغلاق المحل او مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها [53].

3- الظروف المشددة للشخص الطبيعي:

نصت المادة 394 مكرر الفقرة الثانية والثالثة على ظرف التشديد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام إشتغال المنظومة[54].

تفي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة الحبس (06) أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج، هذا الظرف المشدد هو طرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول او البقاء غير المشروع علاقة السببية، كما نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية، وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[55].

ثانيا: العقوبات المقررة على الشخص المعنوي

---

[53] .448، ص 2008ـ أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، دار هومة، ، الجزائر،

[54] من قانون العقوبات.394ـ المادة

[55] من قانون العقوبات.3 مكرر 394 ـ المادة

أقر المشرع الجزائري المسؤولية الجزائية للشخص المعنوي من إرتكاب أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك في المادة 394 مكرر 4 من قانون العقوبات الجزائري[56]، وتنقسم العقوبات المقررة للشخص المعنوي إلى عقوبات أصلية وأخرى تكميلية، فالعقوبات الأصلية للشخص المعنوي نصت عليها المادة 18 مكرر والمادة 18 مكرر 1 من قانون العقوبات الجزائري سواء كانت جنايات او جنح أو مخالفات[57].

كما وسع المشرع الجزائري من دائرة الإجرام فنص على العقوبات المطبقة في حالة الإشتراك والشروع، فقد نصت المادة 394 مكرر 5 على حالة الإشتراك بنصها: "**كل من شارك في مجموعة أو في إتفاق تألف بفرض الإعداد لجريمة او أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل او عدة أفعال مادية، يعاقب بعقوبات المقررة للجريمة ذاتها**"[58]، أما حالة الشروع فقد تضمنتها المادة 394 مكرر 7 بنصها: "**يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها**"[59].

ـ الفرع الثاني: سن نصوص موضوعية زجرية في القوانين الخاصة

لو يكتف المشرع الجزائري بسن نصوص قانونية على جرائم تكنولوجيات الإعلام والاتصال في قانون العقوبات الجزائري، بل شدد على ضرورة زجر هذه الجرائم باستحداث نصوص قانونية خاصة بها، وهذا ما كرسه في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها **(أولا)**،

---

[56] من قانون العقوبات كما يلي: "**يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم** 4 مكرر 394 ــ تنص المادة **المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي**"

[57] ــ بن عطية الحبيب: المعالجة الآلية للمعطيات في القانون الجزائري، مذكرة ماستر في القانون، كلية الحقوق، جامعة مستغانم، 2020 ص 65.

[58] ، المتضمن قانون العقوبات، المعدل والمتمم، السالف الذكر.66-156 من الأمر رقم 5 مكرر 394 ـــ المادة

[59] من قانون العقوبات 7 مكرر 394 ــ المادة

وكذلك في القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية[60] **(ثانيا)**.

أولا: سن نصوص موضوعية في القانون رقم (09-04)

من أجل المحاصرة الجيدة و المواجهة الفعالة للظاهرة الإجرامية الجديدة المتعلقة بتكنولوجيات الإعلام و الاتصال، فقد عمد المشرع الجزائري إلى تدعيم نصوص التجريم التي تضمنتها القواعد العامة في هذا المجال، بقواعد قانونية خاصة و هي التي إستحدثها بموجب القانون رقم(09-04) المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها،[61] حيث يعتبر هذا القانون إطارا تشريعيا شاملا لمكافحة الجرائم الإلكترونية و الوقاية منها.[62] من خلال وضع إطار قانون أكثر ملائمة مع خصوصية هذه الجرائم الإفتراضية، كما أنه أجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للإعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها[63].

ولقد تبنى المشرع الجزائري بموجب هذا القانون تعريفا موسعا للجرائم الإلكترونية بعد ما كان النظام العقابي يقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أصبحت تشمل بالإضافة إلى هذه الأفعال أي جريمة أخرى أو يسهل إرتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية، وبذلك لم يعد مفهوم

---

[60] ، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة 2018 ماي 10 مؤرخ في 18-04 ـــ قانون رقم 2018، لسنة 27الرسمية، عدد.

[61] ـــ نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، ص 2017، 171.

[62] ـــ رزيق ليلة، رمضاني حميدة: الجريمة الإلكترونية واقع وتحدي، مذكرة ماستر في القانون، تخصص قانون جنائي وعلوم إجرامية، كلية الحقوق، جامعة تيزي وزو، ص 2018، 41.

[63] ـــ نعمان عبد الكريم، مرجع سابق، ص.ص 171-172.

الجريمة الإلكترونية في الجزائر يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتي محلا للاعتداء بل توسع نطاقها إضافة لتلك الأفعال التي تكون المعلومة[64].

فقد نصت المادة 11 من القانون رقم 09-04 على مسؤولية مقدمو الخدمات في حالة مخالفة إلتزام حفظ المعطيات والتي جاءت كما يلي: "... **دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الإلتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمسة (5) سنوات وبغرامة من 50.000دج إلى 500.000دج، يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات...**"[65]

ثانيا: سن نصوص موضوعية زجرية في القانون رقم (18-04)

تضمن القانون رقم 18-04 المؤرخ في 10 ماي سنة 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية[66] عقوبات جزائية لكل من يستخدم تكنولوجيات الإعلام والاتصال بطريقة غير مشروعة، فقد جاء في الباب الرابع بعنوان الأحكام الجزائية، حيث نصت المادة 164 من القانون رقم 18-04 على جريمة انتهاك سرية المراسلات عن طريق البريد أو الاتصالات الإلكترونية وجاءت كما يلي: "**يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500.000دج إلى 1.000.000دج كل شخص ينتهك**

---

[64] رزيق ليلة، رمضاني حميدة، مرجع سابق، ص 41.

[65] المادة 11 من القانون رقم 09-04 المؤرخ في 5 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، السالف الذكر.

[66] قانون رقم 18-04 المؤرخ في 10 ماي سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، عدد 27، لسنة 2018.

سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها"[67].

كما أضافت المادة 165 الفقرة الثانية من نفس القانون ما يلي: "**تسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في إرتكاب هذه الأفعال**"[68]، كما يعاقب الشخص المستخدم لدى متعامل للإتصالات الإلكترونية الذي يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة، أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أ و ساعد في إرتكاب هذه الأفعال[69].

ويعاقب أيضا الشخص الذي يحول خطوط الاتصالات الإلكترونية او يشغلها وهذا ما نصت عليه المادة 175 من القانون رقم 18-04 عما يلي: "**يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 200.000دج إلى 500.000دج أو بإحدى هاتين العقوباتين، كل شخص حول خطوط الاتصالات الإلكترونية أو يشتغل خطوط الاتصالات الإلكترونية المحولة**"[70].

المطلب الثاني

وضع نصوص إجرائية خاصة لمتابعة جرائم تكنولوجيات الإعلام والاتصال

[67] ، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، مرجع سابق.18-40 من قانون رقم 164ــ المادة

[68] ، مرجع سابق.18-40 من القانون 165 المادة

[69] ، المرجع نفسه18-40 من القانون 166 أنظر المادة

[70] ، المرجع نفسه18-40 من القانون 175 المادة

نظرا لخطورة الجزائم المتعلقة بتكنولوجيات الإعلام والاتصال، فقد شدد المشرع الجزائري الإجراءات المتعلقة بالبحث والتحري، حيث كرس نصوص قانونية إجرائية للحد من هذه الجرائم، تتمثل في نصوص إجرائية بالنسبة لإجراءات البحث والتحقيق في جرائم تكنولوجيا الإعلام والاتصال **(الفرع الأول)**، كما وضع المشرع الجزائري مجموعة من النصوص المتعلقة بإجراءات المحاكمة **(الفرع الثاني)**.

ـ الفرع الأول: بالنسبة لإجراءات البحث والتحقيق في جرائم تكنولوجيات الإعلام والاتصال

تبنى المشرع الجزائري سياسة مزدوجة قصد تحقيق الفعالية في المواجهة الإجرائية للجرائم الحديثة، و ذلك من خلال مدّ وصال إجراءات المتابعة الجزائية التقليدية حتى تسري على هذه الجرائم هذا من جهة (أ). و من جهة أخرى قام بسن إجراءات تحقيق خاصة تتناسب مع طبيعة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال (ب) .

أــ إعمال إجراءات التحقيق التقليدية على جرائم تكنولوجيا الإعلام والاتصال:

نجد أن المشرع الجزائري إعتمد على تقنيات تقليدية في التحقيق على جرائم تكنولوجيات الإعلام والاتصال، وعمل على تطويرها باستخدام نفس التكنولوجيا وتتمثل فيما يلي:

1- التفتيش: يعد التفتيش إجراء من إجراءات التحقيق، يباشره موظف مختص لهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا[71]، كما عرف التفتيش أيضا على أنه البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة ونسبتها إليه

[71] ـ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، الاسكندرية، 2006، ص 192.

أو الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه ويستوي في ذلك ان يكون المحل مسكنا أو ما في حكمه أو أن يكون شخصا[72].

كما هناك التفتيش الإلكتروني أو التفتيش عن الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، فيعرف بأنه إجراء من إجراءات التحقيق يهدف إلى الوصول على الأدلة المنبثقة من جناية أو جنحة تحقق وقوعها فعلا داخل نظام المعالجة الآلية للمعطيات لإثبات ارتكابها ونسبتها لمتهم معين وينبغي التعامل مع الأدلة المعلوماتية بحيطة وحذر لتفادي تلفها وضياعها[73].

أما مصطلح التفتيش في البيئة الإلكترونية، فقد استخدم المشرع الجزائري في المادة الخامسة من قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصطلح الدخول إلى منظومة معلوماتية أو منظومة تخزين معلوماتية بغرض التفتيش في إطار قانون الإجراءات الجزائية بمعنى أن الدخول هو التفتيش طبقا لأحكام قانون الإجراءات الجزائية، ولكنه يكون على نظام المعالجة الآلية للمعطيات أو مستخرجاتها والمحمولة على وسائط إلكترونية[74].

أما محل التفتيش الإلكتروني فتتمثل في تفتيش المكونات المادية للحاسوب، فليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها يخضع لإجراءات التفتيش المألوفة، لأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد فيه ما إذا

---

[72] ، 1ـــ طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر . 115ص 2012

[73] ، جامعة 05 ـــ رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد .164، ص 2012الوادي، جوان

[74] ـ إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي بجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة .31، ص 2020، جامعة الوادي، ماي 01، عدد 04الدولية للبحوث القانونية والسياسية، المجلد

كان عاما أو خاصا، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاته وبالإجراءات والضمانات المقررة قانونا في التشريعات المختلفة لذلك[75].

كما أجاز المشرع الجزائري صراحة تفتيش المنظومات المعلوماتية، وذلك بموجب المادة 5 من قانون رقم 09-04 السالف الذكر التي نصت كما يلي: "**يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى:**

أ- **منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنةفيها.**

ب- **منظومة تخزين معلوماتية...**"[76].

كما توسعت المادة 5 الفقرة الثالثة في إجراء التفتيش بنصها: "... **إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل**"، والملاحظ في هذه المادة أن المشرع الجزائري لم يسمح للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الإلكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الإتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام المعلوماتي[77].

2- المراقبة الإلكترونية:

---

[75] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 195.

[76] ـ المادة 05 من القانون رقم 09-04، مرجع سابق.

[77] ـ براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018، ص 28.

يمكن تعريف المراقبة الإلكترونية على أنها عمل امني أساسي له نظام معلومات إلكتروني، يقوم به المراقب (بكسر القاف) بمراقبة المراقب (بفتح القاف) بواسطة الأجهزة الإلكترونية وعبر شبكة الأنترنت لتحقيق غرض محدد وإفراغ النتيجة في ملف إلكتروني وتحرير تقارير بالنتيجة[78] حدد المشرع الجزائري مكانة المراقبة الإلكترونية ضمن الإجراءات الخاصة في البحث والتحقيق عن الجرائم، فيمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه[79]، بحيث يقوم بها مراقب إلكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية، وباستخدام تقنيات وبرامج الإلكترونية فيها، لذا وبالرجوع إلى القانون رقم 09-04 نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الجنائي الرقمي فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية[80].

و قد حددت الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية في المادة 04 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من بينها حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ولا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة[81].

---

[78] ــ مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب القانونية، القاهرة، 2005 ص 192 .

[79] ــ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، مصر، 2007 ص 199.

[80] ــ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في القانون، كلية الحقوق، جامعة باتنة، 2013 ص.ص 23-24.

[81] ــ المادة 04 من القانون رقم 09-04. مرجع سابق ،

ب- استحداث إجراءات تحقيق خاصة بجرائم تكنولوجيات الإعلام والاتصال:

أورد المشرع الجزائري ضمن إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والاتصال إجراءين مستحدثين وهما التسرب الإلكتروني **(أولا)** والحجز الإلكتروني **(ثانيا)**.

1ـ التسرب الإلكتروني

يعد التسرب الإلكتروني من الإجراءات الحديثة في المنظومة الإجرائية الجزائرية، فنجد أن المشرع الجزائري عند تعديله لقانون الإجراءات الجزائية الجزائري في القانون رقم 06-22[82]، قد استحدث آليات جديدة للبحث والتحري عن الجرائم الخاصة، منها أسلوب التسرب المنصوص عليه في المواد 65 مكرر 11 إلى غاية 65 مكرر 18.

وقد ورد تعريف التسرب في المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري في الفقرة الأولى منها كالآتي: "**يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإتهامهم بانه فاعل معهم أو شريك لهم أو خاف**"[83].

من خلال التعريف يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية، وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين، وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم[84]، ويمكن تصور عملية التسرب في الجرائم الإلكترونية في ولوج ضابط أو عون

---

[82] .2006، لسنة 84، يتضمن قانون الإجراءات الجزائية، ج.ر، عدد 2006 ديسمبر 20، المؤرخ في 06-22ـ قانون رقم

[83] من قانون الإجراءات الجزائية.12 مكرر 65ـ المادة

[84] ـ نجيمي جمال، إثبات الجريمة على ضوء الإجتهاد القضائي، دراسة مقارنة، دار هومة للطباعة والنشر والتوزيع، .451، ص 2011الجزائر،

الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات إختراق شبكات الإتصال أو بث الفيروسات او انخراطه في مجموعات أو نوادي الماكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها بمظهر طبيعي، كما لو كان واحد مثلهم قصد استدراجهم والكشف عنهم وعن أعمالهم الإجرامية[85].

ثانيا: الحجز الإلكتروني

تناول المشرع الجزائري الحجز الالكتروني من خلال المادة 06 من القانون قم -04 09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بعنوان حجز المعطيات المعلوماتية، وقد نصت على ما يلي: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزونة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها أو أنه ليس من الضروري حجز كل المنظومة.

يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية..."[86]

وعليه نجد أن الحجز الإلكتروني في التشريع الجزائري مؤطرا بنص المادة السادسة بعبارة "حجز" التي يراد بها حمل وأخذ الدعامة المادية المتواجد عليها المعطيات المخزنة، أو

---

[85] ــ بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص قانون خاص، كلية الحقوق، جامعة مستغانم، 2019، ص 94 .

[86] ــ المادة 06 من القانون رقم 09-04. مرجع سابق ،

القيام بإنشاء أو حفظ نسخة من هذه المعطيات، وأن الإجراء القانوني للحجز يشمل في مفهومه استخدام أو حجز البرامج الضرورية للدخول إلى المعطيات المراد حجزها، ونظرا لكون الضبط محله في مجال الجرائم المعلوماتية، المعطيات المعالجة إلكترونيا، فقد أثيرت إشكالية مدى قابلية هذا النوع من المعطيات لأن يكون محلا للضبط الذي يعني وضع اليد على شيء مادي ملموس، وهذا التساؤل كان في بداياته خلال نهاية التسعينات فأثار جدلا فقهيا عويصا لكن أضحى حاليا باستعمال والأهمية الاقتصادية في المجتمع من المسلمات[87].

ـ الفرع الثاني: نصوص إجرائية بالنسبة لإجراءات المحاكمة

تعامل المشرع الجزائري مع خصوصية الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال بنوع من التشديده وذلك لخطورتها وإتساع نطاقها، لذا قام بتوسع الاختصاص القضائي في هذه الجرائم **(أولا)**، ثم تم الاعتراف بحجية وسائل الإثبات الإلكترونية أمام القضاء الجزائي **(ثانيا)**، ثم تم انشاء جهات قضائية متخصصة بالفصل في جرائم تكنولوجيات الإعلام والاتصال **(ثالثا)**.

أولا: توسيع الاختصاص القضائي في جرائم تكنولوجيات الإعلام والاتصال

الأصل العام أنه يتحدد الاختصاص القضائي بالنظر في الدعوى العمومية التي ترمي لتوقيع العقاب على الجاني بناء على أحد المعايير التالية:

ـ مكان وقوع الجريمة

ـ محل إقامة أحد المتهمين

ـ مكان إلقاء القبض على أحد المتهمين ولو كان القبض لسبب آخر.

[87] ـ مناصرة يوسف، الإثبات الإلكتروني في القانون الجنائي المقارن، أطروحة دكتوراه في الحقوق، تخصص قانون عام، 339.، ص 2017، 1كلية الحقوق، جامعة الجزائر

ويشمل هذا الاختصاص الإقليمي كل من سلطة الاتهام ،و سلطة التحقيق، وسلطة من قانون الإجراءات الجزائية (بخصوص 37الحكم، وهذا ما نصت عليه المواد من قانون الإجراءات الجزائية (بالنسبة 40الاختصاص الإقليمي لوكيل الجمهورية)، المادة من قانون الإجراءات الجزائية (بالنسبة لجهة الحكم)، وهذا 329لقاضي التحقيق)، المادة الاختصاص هو من النظام العام.

إلا أن المشرع وعند تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 04-14 [88] المؤرخ في 10 نوفمبر 2004 قام بتمديد الإختصاص الإقليمي لوكلاء الجمهورية وقضاة التحقيق وقضاة الحكم لجهات قضائية معنية لتشمل دوائر إختصاص جهات قضائية أخرى في جرائم محددة ومن بينها الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال وترك المجال للتنظيم لتحديد هذه الجهات القضائية ذات الإختصاص الموسع، وفعلا بعد هذا التعديل صدر المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 المتضمن عديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[89]، وبالتالي تم إنشاء ما يعرف بالجهات القضائية ذات الإختصاص الموسع او ما يعرف القضائي بالأقطاب الجزائية المتخصصة التي بدأت عملها فعليا انطلاقا من سنة 2008 وهي أربع جهات تشمل وسط، شرق، غرب، جنوب، هذه الأقطاب مسيرة من طرف 37 قاض بمختلف وظائفهم يختارون من ضمن القضاة الأكفاء الذين تلقوا تكوينيا متخصصا في الجرائم التي خولها القانون سلطة النظر فيها منها الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال[90].

---

[88] ، المتضمن قانون الإجراءات 66-155، يعدل ويتمم الأمر رقم 2004 نوفمبر 10 المؤرخ في 04-14ــقانون رقم 2004، صادر في سنة 71الجزائية، ج.ر، عدد.

[89] ، يتضمن تمديد الاختصاص المحلي لبعض المحاكم 2006 أكتوبر 05 المؤرخ في 06-348ــ مرسوم تنفيذي رقم 2006، لسنة 63ووكلاء الجمهورية وقضاة التحقيق، ج.ر، عدد.

[90] ــ بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة ماجستير في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، صص 2012/2011، 102-103.

ثانيا: الاعتراف بحجية وسائل الإثبات الإلكترونية أمام القضاء الجزائي

الواقع أن موقف القوانين المقارنة فيما يتعلق بسلطة القاضي الجنائي في قبول الدليل الإلكتروني تخضع إلى طبيعة نظام الإثبات السائد في الدولة[91].

وقبل بيان موقف المشرع الجزائري من الأدلة الجنائية الرقمية، يمكن القول بعد استقراء نصوص قانون الإجراءات الجزائية أن المشرع الجزائري قد أخذ بنظام الإثبات الحر شأنه كشأن المشرع الفرنسي، وذلك من خلال تكرسي مبدأ الاقتناع الشخصي للقاضي[92].

وخلاصة الأمر أن موقف المشرع الجزائري من الإثبات بالأدلة الإلكترونية هو على العموم موقف التشريعات التي أخذت بنظام الإثبات الحر، إذ أجازت الإثبات في المسائل الجزائية بكافة وسائل الإثبات، أيا كان نوعها أو طبيعتها، على نحو تكون فيه جميع الأدلة متساوية ومتساندة في قيمتها التدليلية، ومقبولة أمام القضاء الجزائي من حيث المبدأ[93]

المبحث الثاني

تدابير الوقاية من جرائم تكنولوجيات الإعلام والاتصال

تعتبر جرائم تكنولوجيات الإعلام والإتصال من اخطر الجرائم التي لا يمكن حصرها والقضاء عليها بالوسائل التقليدية، فهي تتميز بتطور وتغير أركانها وصورها، لذا يجب تشديد إجراءات الوقاية من هذه الجرائم للحد من أضرار جرائم تكنولوجيات الإعلام والاتصال فالمشرع الجزائري حاول التضييق والتشديد في مكافحة هذه الجريمة عن طريق تعزيز دور الأجهزة الأمنية (الضبطية القضائية) في منع وقوع هذه الجرائم، كما دعم في إطار مكافحة

---

[91] – عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، مذكرة ماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، 2009 ص 116.

[92] بوزيد أغيلس، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي، دار الهدى، الجزائر، 2010 ص 110.

[93] براهمي جمال، مرجع سابق، ص 180.

جرائم تكنولوجيات الإعلام والاتصال هيئة خاصة تسمى الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال (المطلب الأول)، كما قام المشرع بتفعيل وسائل الرقابة والحماية الفنية للحد من وقوع جرائم تكنولوجيات الإعلام والاتصال (المطلب الثاني).

المطلب الأول

إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال

تم تسخير هيئة متخصصة لمكافحة جرائم تكنولوجيات الإعلام والإتصال، تكون كجهاز مساعد للهيئات القضائية، وحدد دورها الأساسي في مواكبة التطور الحامل في مجال الجريمة المعلوماتية، والعمل على الحد من انتشار جرائم تكنولوجيات الإعلام والاتصال، لذا سنتناول نشأة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومهامها (الفرع الأول)، ثم تحديد كيفيات سير الهيئة (الفرع الثاني).

ـ الفرع الأول: نشأة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال

أنشأت الهيئة في الجزائر بموجب المادة 13 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وقد نصت ما يلي: "**تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم**"[94].

وعليه أعيد تنظيم الهيئة بموجب المرسوم الرئاسي رقم 20-183 المؤرخ في 13 جويلية 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[95]، وقد نصت المادة 02 منه على الطبيعة القانونية لهذه الهيئة

---

[94] ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام 09-04 من القانون رقم 13ــ المادة والإتصال ومكافحتها، مرجع سابق.

[95] يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم، 2020 جويلية 13 المؤرخ في 20-183ــ مرسوم رئاسي رقم 2020.، لسنة 40المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر، عدد

كما يلي: "**الهيئة المالية، توضع تحت سلطة رئيس الجمهورية**"، وأضافت المادة الثالثة من نفس المرسوم أن مقرها بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني، بموجب مرسوم رئاسي.

وتتمثل مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فيما يلي:

في إطار المهام المنوطة بها والمنصوص عليها في المادة 14 من القانون رقم 04-09 وتحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول، تكلف الهيئة على الخصوص بما يأتي:

- اقتراح المتصلة بتكنولوجيات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، لاسيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.
- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

-تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

-المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

-المساهمة في تحسين المعايير القانونية في مجال اختصاصها[96].

وتتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان له عرضا عن نشاطاتها[97].

ـ الفرع الثاني: كيفيات سير الهيئة

تعتبر الهيئة مؤهلة لكي تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها، وما عدا الحالات المبينة في قانون الإجراءات الجزائية وقصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، وفي إطار التنسيق مع المصالح الأمنية المعنية، تكلف الهيئة حصريا في مجال اختصاصها بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حيتها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية وفقا للأحكام المنصوص عليها في المادة 04 من القانون رقم 09-04.

كما تسجل الهيئة الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية[98].

---

[96] ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة 20-183 من المرسوم التنفيذي رقم 04ـ المادة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[97] ، مرجع سابق.20-183 من المرسوم التنفيذي رقم 05ـ المادة

[98] ، مرجع سابق.20-183 من المرسوم التنفيذي رقم 21-22-25ـ أنظر المواد

وأخيرا يجب تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول، ألا تستخدم المعلومات والمعطيات التي تستلمها أو تجمعها الهيئة لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما يمنع منعا باتا تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول، قيام أي شخص أو هيئة مهما كانت طبيعتها بعمليات الاعتراض الإلكترونية أو التدخل على المعطيات الخاصة التي تعتبر من اختصاصات الهيئة دون سواها[99].

المطلب الثاني:

تفعيل دور وسائل الرقابة والحماية الفنية في الحد من وقوع جرائم تكنولوجيات الإعلام والاتصال

عزز المشرع الجزائري المنظومة الجنائية فيما يتعلق بالحد من وقوع جرائم تكنولوجيات الإعلام والاتصال بتفصيل وسائل الرقابة والحماية الفنية من هذه الجرائم عن طريق الحماية الفنية عن طريق البرامج (الفرع الأول)، والحماية الفنية عن طريق أنظمة الرقابة الإلكترونية (الفرع الثاني)، وكذا تدعيم حملات التحسيس والتوعية عن جرائم تكنولوجيات الإعلام والاتصال (الفرع الثالث).

ـ الفرع الأول: الحماية الفنية عن طريق البرامج الأمنية

وهي الحماية التي يتم توفيرها اعتمادا على البرامج الأمنية التالية:

1- برامج التعريف بالشخصية المستخدم وموثوقية الاستخدام ومشروعيته:

تهدف هذه البرامج إلى ضمان استخدام الجهاز او النظام أو الشبكة من قبل الشخص المرخص له بهذا الاستخدام فقط، وتضمّ هذه الطائفة كلمات السر بأشكالها المختلفة، رموز

[99] ، مرجع سابق.20-183 من المرسوم التنفيذي رقم 26ـ المادة

المرور، بطاقات التعريف الذكية، ووسائل التعريف البيومترية التي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه المرفولوجية، كبصمة اليد أو الأصبع، أو بصمة العين أو الوجه، بصمة الصوت، البصمة الوراثية، أو متصلة بتصرفاته مثل طريقة التوقيع، طريقة استخدام لوحة المفاتيح، طريقة التنفس. كما تضم أيضا مفاتيح التشفير، وما يعرف بالأقفال الإلكترونية التي تحدد دخولها لأشخاص بذاتهم.

2- برامج التحكم في النفاذ إلى الشبكة:

تهتم هذه البرامج أساسا بالحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، وكذا التأكد من أن الشبكة قد استخدمت بطريقة مشروعة[100]، ومن أهمها ما يعرف بالجدران النارية (Fire wall) الذي يثبت داخل نظام الحساب بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الأنترنت، فيبدأ بإجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها، على المرور من خلال هذا الجدار الناري، ثم يقوم بصدّ المستخدمين غير المرغوب فيهم عن الوصول إلى الشبكة، عن طريق مراقبة الحزم التي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم، وتنبيه هذا الأخير بذلك[101].

ومن مزايا هذه البرامج أنها تقوم بتسجيل وتخزين جميع العمليات والمعلومات والبيانات والتي تمرّ عبرها، وهو ما يسمح لسلطات البحث والتحقق استخدام بعض الوسائل المساعدة لتحليل هذه العمليات وتتبع محاولات الدخول إلى النظام ورصد المعلومات الكاملة عن هذا الاختراق، من حيث الزمان والمكان، من ثم معرفة المجرم.

---

100 أشرف السعيد أحمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة، القاهرة، 2013ـ ص 69.

101 ياسر محمد الكومي محمود أبو حطب، مرجع سابق، ص 402ـ.

3- برامج الحفاظ على سرية المعلومات:

الغرض منها ضمان عدم إفشاء المعلومات للجهات غير المصرح لها بذلك، وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، ومختلف برامج التمحيص والغربلة (Filtration).

4- برامج حماية التكاملية وسلامة المحتوى:

يكمن دور هذه البرامج في حماية محتوى المعطيات أو البيانات الإلكترونية من مخاطر العبث بالتعديل او الإتلاف أو الإلغاء من قبل جهة غير مخول لها بذلك، بعد الإطلاع عليها أو أثناء عملية إدخالها أو نقلها، ومن بين أهم هذه البرامج تقنيات (PDF)، ومختلف برامج مضادات الفيروسات (Antivirus)[102].

5- برامج منع إنكار التصرف:

مهمة هذه البرامج هو تأكيد انتساب تصرف ما على الوسائل الإلكترونية إلى مصدره الحقيقي، وضمان عدم قدرة شخص المستخدم من إنكار التصرف الذي صدر عنه، او إنكار بأنه هو مصدر هذا التصرف، وتكمن هذه البرامج في تقنيات التوقيع الإلكتروني، وشهادات التوثيق الصادرة عن الطرف الثالث[103].

6- برامج مراقبه الاستخدام وتتبع سجلات النفاذ والأداء:

[102] أمين عبد الحفيظ، الاتجاهات الفنية و الامنية لمواجهة الجرائم المعلوماتية، بدون دار النشر، القاهرة، 2005، ص. 147-149.

[103] المرجع نفسه، ص. ص 151-152.

وتتمثل في مختلف التقنيات التي تستخدم لمراقبة العمليات الالكترونية الجارية على نظام حاسب معين، وتحديد مصدرها والوقت والمدة التي استغرقتها، وتسجيل كل ذلك في ملفات خاصة يطلق عليها (Logs)، ومن ضمن هذه البرامج نذكر:

أ- **برنامج (tracer)**: وهو برنامج يتولى تقديم تقارير مفصلة حول المسار الذي سلكه مستخدم شبكة الأنترنت من خلال تحديد موقع الولوج وعنوانه الشخصي (IP)، المواقع والصفحات التي أطلع عليها، الوقت والفترة التي قضاها في كل صفحة أو موقع، ومختلف العمليات التي أجراها وتحديد نوعها.

ب- **برنامج (net stat)**: وهو برنامج مناط به عرض جميع الاتصالات التي أجراها المستخدم، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية، وتقديم تقرير كامل لجدول التوجه[104].

ت- **برنامج كشف الاختراق (IDS)**: يتولى مراقبة العمليات التي يجرى حدوثها على أجهزة الحاسب او شبكة الانترنت وتحليلها بحثا عن أية إشارة قد تنبئ بوجود خطر قد يهدد امن الحاسب او الشبكة، وفي حالة اكتشاف النظام وجود هذا التهديد يقوم برصد كل البيانات المتعلقة به، مصدره، طبيعته، ودرجة خطورته، من ثم إنذار صاحب النظام فورا بهذا التهديد[105].

والملاحظ في هذه التدابير هو أنه بالإضافة إلى كونها إجراءات وقائية فعالة لمنع وقوع الجرائم الإلكترونية أو الإنذار عنها فور وقوعها، فهي أيضا مفيدة جدا لعملية التحقيق والإثبات في هذه الجرائم، إذ تقدم معلومات قيّمة وموثوقة لفريق التحقيق تساعده على فهم لغز الجريمة، وتحديد معالمها وإبعادها، وإظهار أسلوب ارتكابها، مما قد يضفي إلى الكشف عن مرتكبها.

---

104 حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، مرجع سابق، ص.ص 17-18.

105 أشرف السعيد أحمد، مرجع سابق، ص 78.

واعتبارا لهذه الأهمية، فقد أجاز المشرع الجزائري الاستعانة بهذه التدابير لغرض التحقيق في الجرائم الإلكترونية، وذلك حينما ألزم في نص المادة 10 من الفصل الرابع من القانون رقم 09-04 مقدمي الخدمات بالعمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، من خلال تحديد مصدر الاتصال، ومكانه، تاريخ ووقت ومدة كل اتصال، بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال، وكذا عناوين المواقع المطلع عليها[106]

ـ الفرع الثاني: الحماية الفنية عن طريق أنظمة الرقابة الإلكترونية الوقائية

يعد نظام الرقابة الإلكترونية أهم آليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الحديثة، إذ تسمح بالرصد المبكّر للاعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، من ثم القبض عليهم ومحاكمتهم، فهي بذلك تختلف تماما عن وسائل الرقابة الالكترونية التي تتخذ بعد وقوع الجريمة الالكتروني أو بمناسبة البحث والتحقيق فيها كاعتراض المراسلات والتقاط الصور، الجمع الحفظ والكشف العاجل لمعطيات المرور أو المحتوى.

ويقصد بالرقابة الإلكترونية للاتصالات، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه، سواء تعلق الامر بمراقبة شخص أو مكان او شيء حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني[107].

وتتم هذه العملية بواسطة أجهزة الكترونية ذات تكنولوجية عالية تضمن الرقابة بصفة مستمرة دون انقطاع حسب الغرض، وغالبا ما يتم ربط هذه الأجهزة بأنظمة الإنذار أو الإشارة التي تتولى الإخبار أو التبليغ عن الخطر، أو عن وقوع جريمة الكترونية كلما

---

[106] ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام 09-04 من القانون رقم 10 أنظر: المادة والإتصال ومكافحتها، مرجع سابق.

[107] بوكر رشيدة، مرجع سابق، ص 370ـ.

اكتشفت أجهزة المراقبة ذلك، مع العلم أن هناك من أنظمة إنذار ما هو متصل مباشرة بمراكز الأمن فتقوم بإرسال الإشارات من دائرة المراقبة إلى وحدة الشرطة[108]، وهو ما يجعلها تؤدي دور المبلّغ عن الجريمة، وبالتالي تشكل مخرجا لعقبة الإحجام عن التبليغ بالجريمة.

ولقد أدرج المشرع الجزائري هذه الآليات ضمن الوسائل المفيدة للوقاية من الإجرام الإلكتروني ومكافحتها التي استحدثها في القانون رقم 09-04، حينما نص في المادة 03 منه على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها، كلما تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وذلك مع مراعاة الاحكام القانونية التي تتضمن سرية المراسلات والاتصالات.

ليس هذا فحسب، بل أنشأ المشرع الجزائري بموجب المادة 13 من القانون رقم 04-09 هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وجعل من مهامها الأساسية ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم الالكترونية منها المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة[109]. وإرسال المعلومات المتحصل عليها من هذه العملية إلى سلطات الأمن والقضاء المختصة[110].

ـ الفرع الثالث: التوعية والتحسيس

لقد سبق البيان أنه من ضمن العقبات التي تعتري عملية البحث والتحقيق في الجرائم الإلكترونية، تقاعس المجني عليه عن الإبلاغ بوقوع الجريمة، ما قد يستغرق اكتشافها من قبل سلطات الضبط القضائي وقتا كبير، قد يحول دون الوصول إلى الأدلة والقرائن في

---

108 أيمن عبد الحفيظ، مرجع سابق، ص. ص .118-119ـ

109 ، ، مرجع سابق.15-216 من المرسوم الرئاسي رقم 06 فقرة 04ـ أنظر المادة

110 ، المرجع نفسه.15-216 من المرسوم الرئاسي رقم 03 فقرة 11ـ أنظر المادة

الوقت المناسب أو عدم الوصول إليها إطلاقا، بسبب إمكانية محوها أو التخلص منها بسهولة في الفترة بين حدوث الجريمة واكتشافها.

ومن أجل التصدي لهذه العقبة اتخذت عدة مبادرات جريئة منها، إقرار قاعدة تجريم عدم الإبلاغ عن الجريمة، وذلك من خلال وضع نصوص عقابية تعتبر الشخص الذي يعمل بوقوع جريمة الكترونية ويتماطل في تبليغ سلطات الأمن عنها، شريكا فيها يستوجب معاقبته، ولكن رغم استقاق هذا الحل من المنطق ذاته الذي تقوم عليه جريمة "**عدم مساعدة الشخص في حالة خطر**"، إلا أنّه لم يفعل، وسرعان ما استبدل بقاعدة أخرى تعرف بالالتزام برفع شكوى (L'obligation de porter plainte)، وهذه القاعدة وإن تمّ فعلا العمل بها في بعض الولايات الأمريكية كجيورجيا وآوتاه، إلاّ أنّها لقيت رفضا كبير من غالبية دول العالم بحجة تناقضها مع منطق التجريم والعقاب، إذ لا يعقل معاقبة الضحية فقط لمجرد عدم انصياعه للقانون الذي يقضي بواجب التبليغ، في حين يترك المجرم الحقيقي حرا طليق.

أمام هذا الوضع، لم تجد الدول حلا آخر لمشكلة الإعراض عن التبليغ بالجريمة الالكترونية إلا اللّجوء إلى سياسة التحريض على التبليغ (l'incitation dénonciation)، وذلك عن طريق وضع تحت تصرف مستخدمين الأنترنت آليات سهلة ومجانية تشجع المتضررين من جريمة على التبليغ عنها إلى سلطات الأمن، كإنشاء ما يسمى بخطوط اتصال خضراء أو الأرقام الساخنة، [111] وهي قنوات مرتبطة مباشرة بمصالح الأمن، تسمح لأي شخص الاتصال من أي مكان وفي كل وقت وحين وبدون أن يكشف عن هويته، للإبلاغ عن وقوع جريمة إلكترونية ما. أو ما خلق لدى مراكز الأمن بوابات أو أنظمة إلكترونية تعمل (24سا/24سا) مخصص لاستقبال شكاوى أولية عبر الأنترنت (Pré-

[111] ــ نذكر منها الرقم الساخن في مصر وهو (108)، الرقم (1909) في المملكة السعودية، الرقم الأخضر للشرطة (1548) في الجزائر.

plainte)،[112] كما فعلت المملكة السعودية بإنشائها نظام استقبال الشكاوي الإلكترونية "أبشر"، والجزائر باستحداثها مؤخرا موقع للشكاوي الأولية لدى مصالح الدرك الوطني يسمي (PPGN.MDN.DZ). ومن أجل تفعيل وتعزيز هذه الآلية قامت بعض شركات التأمين في بعض الدول بإدراج شرط رفع شكوى ضمن بنود عقد التأمين الالكتروني الذي يؤدي تخلفه إلى فقدان الحق في التعويض.[113]

ومع ذلك، فقد كشفت الدراسة الاستقصائية التي أجرها مؤخرا فريق خبراء حول الجريمة السبيرانية والتدابير التي تتخذها الدول والمجتمع الدولي والقطاع الخاص للتصدي لها،[114] بأنّ احسن وسيلة للقضاء على مشكلة العزوف عن التبليغ بالجريمة الالكترونية بل لمنع وتفادي وقوعها هي التوعية والتحسيس، وذلك من خلال تنظيم حملات زيادة الوعي العام تشمل كل شرائح المجتمع، والمؤسسات والإدارات العمومية، بما فيها حملات التوعية بالتهديدات والمخاطر الناشئة عن هذا النمط الإجرامي، وعن سياسات وممارسات تدبّر هذه المخاطر والوقاية منها، وكذا تحسيسهم بأنّ مهمة الإفصاح عن الجريمة الإلكترونية ومكافحتها هي مسؤولية مشتركة وتستلزم تضافر جهود الجميع دون استثناء.[115]

وفي هذا الإطار، تؤدي المؤسسات الأكاديمية مجموعة متنوعة من الأدوار، منها تثقيف المهنيين وتدريبهم، اقتراح القوانين والسياسات، والعمل على تطوير المعايير والحلول التقنية لظاهرة الإجرام الإلكتروني. كما تقوم الجامعات بنشاطات وتظاهرات علمية (ندوات، ملتقيات وأيام دراسية) في هذا الشأن تشرك فيها خبراء في مجال الجرائم الإلكترونية

---

[112] ــ سميت بشكاوى أولية لأنها عبارة عن بلاغ يقدمه الشخص عبر الأنترنت، لا يتم بموجبه مباشرة إجراءات المتابعة الجزائية إلا بعد انتقال المبلغ أو الشاكي شخصيا إلى مركز الأمن لتأكيد وتدعيم بلاغه.

[113] VERGUCHT Pascal, op.cit, p328.

[114] GROUPE D'EXPERTS, Etude approfondie sur le cybercriminalité et les mesures prises par les Etat Membres, la communauté internationale et le secteur privé pour y faire face, UNODDC, Vienne,25-28 février 2013, p17.

[115] –BRETANT Thierry, chantir sur la lutte contre la cybercriminalité, op.cit, p11.

ومختصين في مواجهة الطوارئ الحاسوبية، للاستفادة من مهاراتهم وخبرتهم وما يضطلعون به من أعمال.

بالإضافة إلى ذلك، فقد أشادت بعض الدراسات بأهمية إشراك القطاع الخاص بشكل عام (مؤسسات اقتصادية، مزودي الخدمات، جمعيات، مجتمع مدني) في مهمة التصدي ومنع الجرائم السبيرانية، وذلك من خلال توقيع اتفاقات وشراكات غير رسمية بين القطاع العام والخاص يلتزم فيه الطرفين معنويا على تيسير تبادل المعلومات عن التهديدات التي تثيرها هذه الجرائم، والعمل ندالند على تنفيذ السياسة الوقاية التي ترسمها الدولة.[116]

[116] –CISSE Abdoullah, Exploration sur la cybercriminalité et la sécurité en Afrique : Etat des lieux et priorités de recherche – Synthèse des rapports nationaux, Centre de recherche pour le développement international (CRDI), 2021, pp47, 49-50. Voir aussi. Groupe d'experts, op.cit., p18.

الخاتمة

في الختام فقد اتضح لنا أن جرائم ا تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، و التي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، وأنها من المستجدات التي لم تكن معروفة في القانون الجزائي بشقيه الموضوعي والإجرائي، من ثمة فأي محاولة للتعامل مع هذا النمط الإجرامي الجديد سوف يخلق إشكالات عملية أمام السلطات المكلفة بهذه العملية.

وتتجلى أولى هذه الإشكالات في القصور الذي يعتري النصوص الجزائية القائمة في مواجهة مثل هذه الجرائم، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

وقد بينا أنه من أجل تغطية و تلافي هذا القصور من جهة، وتفادي إفلات المجرم الالكتروني من المتابعة الجزائية و العقاب، بادر المشرع في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش و الضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الالكترونية. فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم، كالمراقبة الالكترونية واعتراض المراسلات والتسرب الالكتروني، وهو ما أقدم عليه المشرع الجزائري من خلال تعديل قانون الإجراءات الجزائية في عام 2006، وإصداره القانون رقم (04/09) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و لغرض التضييق أكثر على هذه الجرائم ، نقدم بعض الاقتراحات التي نعتقد انها فعالة وممكنة التجسيد، وهي مستوحاة من الاتفاقية الأوروبية حول الجريمة الالكترونية المبرمة في بودابست عام 2001، و التي نعرضها في شكل على النحو التالي :

-يتعين على الدول التي لم تسن بعد قوانين جزائية موضوعية وإجرائية خاصة بالجرائم الالكترونية، كما هو الحال بالنسبة لغالبية الدول العربية، الإسراع إلى تعديل وترشيد قوانينها القائمة بما يجعلها تسرى وتطبق على مثل هذه الجرائم، وذلك لتفادي القصور التشريعي وتخطي الثغرات القانونية الحاصلة في هذا المجال، التي قد يستفيد منها المجرم الالكتروني للإفلات من المتابعة الجزائية و العقاب.

-لا يكفي الاعتماد على التشريعات القائمة ل تجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم الالكترونية، بل لا بد من تدعيمها بنصوص خاصة حديثة تتضمن إجراءات تحقيق ملائمة مع طبيعة هذا الشكل الجديد من الإجرام، ومسايرة للمتغيرات والتطورات الحاصلة في تقنيات وأساليب ارتكابها. كما فعل المشرع الجزائري من خلال القانون رقم (09-04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حينما استحدث تقنيات ومعالم جديدة توضح القواعد الإجرائية في مجال تحريك و مباشرة الدعوى الجزائية وإتباع آثار المجرم الالكتروني من خلال تحديد الترتيبات التقنية للمراقبة الالكترونية، وكيفية تفتيش المنظومة المعلوماتية عن بعد، ثم إجراءات حجز المعطيات الالكترونية، ورسم معالم الاختصاص القضائي تحسبا للطابع الدولي الذي تكتسيه الجرائم الالكترونية .

-ضرورة إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة جرائم تكنولوجيات الإعلام و الإتصال، يكون لديهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، مع إخضاعهم لبرامج تدريبية خاصة دورية ، تساعدهم على تحيين و تحديث معارفهم و خبراتهم و اطلاعهم بآخر المستجدات الحاصلة مجال التقنية المعلوماتية.

-إتاحة الفرصة للمواطنين للمشاركة في مكافحة جرائم تكنولوجيات الإعلام و الإتصال ؛ من خلال إنشاء خطوط ومواقع اتصال ساخنة أو خضراء تعمل على مدار الساعة، و تسمح لأي كان بالإبلاغ عن بعد بوقوع جريمة الكترونية دون قيد أو شرط.

-ضرورة نشر الوعي في أوساط المجتمع بالمخاطر الاقتصادية والاجتماعية و النفسية وغيرها الناجمة عن الاستخدامات غير المشروعة وغير الآمنة للانترنت ، وبما يترتب عنها من انعكاسات سلبية على حياة الفرد والمجتمع.

-تفعيل دور المجتمع المدني و الحراك الجمعوي المؤهل في التحسيس والوقاية من الوقوع في الممارسات الخاطئة والسلوكيات الإجرامية عبر شبكة الانترنت..

ضرورة اهتمام الباحثين و رجال القانون الجزائريين بالدراسات القانونية التي تعنى جرائم تكنولوجيات الإعلام و الاتصال والعمل على إثراء محتواها، لأنها لم تنل بعد حظها من البحث والتشريح، و لا تزال لحد اليوم في منطقة الظل في بلادنا رغم ما يثيره الزحف الهائل للإجرام الالكتروني من مخاطر.

قائمة المراجع

أولا- الكتب:

ــ أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، الجزء الأول، ط9، دار هومة، الجزائر، 2008.

ــ أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للنشر والتوزيع، الجزائر، 2008.

ــ جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2002.

ــ حسني محمود نجيب، النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، 1971.

ــ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

ــ زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزا ئري و الدولي ، دار الهدى ، الجزائر، 2011

ـ عبد الحكيم، مولاي براهيم، الجرائم الإلكترونية، مجلة الحقوق و العلوم الإنسانية، جامعة زيان بن عاشور بالجلفة، الجزائر، عدد 23، جوان 2015.

ــ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي الإسكندرية، 2006 .

ـــــــــــــــــ ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، بهجات للطباعة و التجليد، القاهرة، 2009.

. ـــ غانم مرضي ألشمري، الجرائم المعلوماتية،ماهيتها – خصائصها – كيفية التصدي لها قانونا، دار العلمية الدولية للنشر و التوزيع، عمان،2016.

ـ محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت كلية الحقوق و الشريعة جامعة الإمارات، 21 مايو 2005 .

ـ محمد خليفة: الحماية الجزائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2008.

ـــ منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر و التوزيع، عنابة، 2006.

ـ نائلة عادل محمد فريد فودة، جرائم الحاسب الاقتصادية دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ،2004.

ـ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، عمان، 2008.

ـ هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012.

ثانيا ـــ الرسائل و المذكرات

أ ـ رسائل الدكتوراه

ـــ براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018.

ــ غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية، رســـالة دكتــوراه في القانون، كلية الحقوق، الجامعة الإسلامية ، بيروت، 2004.

ــ مناصرة يوسف، الإثبات الإلكتروني في القانون الجنائي المقارن، أطروحة دكتوراه في الحقوق، تخصص قانون عام، كلية الحقوق، جامعة الجزائر 1، 2017.

ب ـ مذكرات الماجستير

ـ بوذراع عبد العزيز، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مذكرة ماجستير في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2011.

ــ سعيداني نعيم، أليات البحث والتحري عن الريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في القانون، كلية الحقوق، جامعة باتنة، 2013.

ـ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مول ود، معمري بتيزي وزو، 2013.

ــ طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2012.

ــ عبد الله دغش العجمي، المشكلات العلمية و القانونية للجرائم الإلكترونية ـ دراسة مقارنة، مذكرة ماجستير في القانون العام، بكلية الحقوق بجامعة الشرق الأوسط، الكويت، 2014.

ـ عبد الله ذيب عبد الله محمود، حماية المستهلك في التعاقد الإلكتروتي ـ دراسة مقارنة، مذكرة ماجستير في القانون الخاص، كلية الدراسات العاليا، جامعة النجاح الوطنية، القدس، 2009،

ـــ عبد الرحمان محمد بحر، معوقات التحقيق في جرائم الأنترنت دراسة مسحية على ضباط الشرطة في البحرين، مذكرة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، 1999.

ج ـــ مذكرات الماستر

ـ .بن لغوم خالد أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في الحقوق، تخصص قانون خاص، كلية الحقوق، جامعة مستغانم، 2019

12ـ بن عطية الحبيب ، المعالجة الآلية للمعطيات في القانون الجزائري، مذكرة ماستر في القانون، كلية الحقوق، جامعة مستغانم، 2020.

13ـ رزيق ليلة، رمضاني حميدة: الجريمة الإلكترونية واقع وتحدي، مذكرة ماستر في القانون، تخصص قانون جنائي وعلوم إجرامية، كلية الحقوق، جامعة تيزي وزو، 2017 .

14ـ نعمان عبد الكريم: الجرائم الإلكترونية وموقف المشرع الجزائري منها، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2017.

ثالثا ـ المقالات

ـ إسماعيل عبد النبي شاهين" أمن المعلومات في الانترنت" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2000، ص11.

ـ إلهام بن خليفة، التفتيش كإجراء تحقيق تقليدي بجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 04، عدد 01، جامعة الوادي، ماي 2020، ص 31.

ـــ حسين بن سعدي الغافري " التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت" ص 19. مقال متوفر في الموقع التالي:.www.eastlaws.com

ـــ رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد 05، جامعة الوادي، جوان 2012.

ـ غنام محمد غنام" عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر" بحث مقدم إلى مؤتمر القانون و الكمبيوتر والانترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة الممتدة من 01 إلى 03 ماي 2003.

ـ ممدوح عبد الحميد عبد المطلب" جرائم استخدام شبكة المعلومات العالمية" بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة ، 2000، ص.ص 24 وما بعدها.

ـــ مراد عبد الرحمان مكاوي " الستيغانوغرافي " مجلة المعرفة، العدد 147، نيسان، 2009، ص 41. منشور على الموقع التالي:
http://www.almarefh.org/news.php?action-shawgid-6,4

ـــ موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقال مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي نظمته أكادمية الدراسات العليا، طرابلس، 2009/10/29/28 ،ص03.

ـ موسي مصطفي محمد، التحقيق الجنائي في الجرائم الإلكترونية، مجلة الشرطة، عدد 1، لسنة 2009.

رابعاـ النصوص القانونية

ـ قانون رقم 06-22، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الامر رقم 66-155، المتضمن قانون الإجراءات الجزائية، ج.ر، عدد 84، لسنة 2006

ـ قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية عدد (71) لسنة 2004.

ـ قانون رقم 06-23 المؤرخ في 20 ديسمبر، المعدل والمتمم للأمر رقم 66-156 المتعلق والمتضمن قانون العقوبات، الجريدة الرسمية عدد (84) لسنة 2006.

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

ـ قانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، عدد 27، لسنة 2018.

الفهرس

الفصل الثاني

ملخص

اتضح لنا إن جرائم التكنولوجيات الإعلام والاتصال تعد من الأصناف الجديدة التي عرفت تطورا ملحوظا في الآونة الأخيرة و التي تعتبر حديثة و تتميز بخصائص مختلفة تماما عن الجرائم التقليدية التي لم تكن معروفة في القانون الجزائي (الموضوعي و الإجرائي) و ذلك من خلال الإشكالات التي تعتري النصوص الجزائية القائمة في مواجهة مثل هذه الجرائم و من خلال ذلك يجب أو ضرورة إنشاء وحدات امن و أجهزة قضائية متخصصة في مكافحة جرائم تكنولوجيات الإعلام والاتصال باستخدام أخر التطورات و المستجدات في مجال التقنية المعلوماتية و الهدف من ذلك مواجهة و التصدي لكل أنواع و أشكال هذه الجرائم.