

الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر

Criminalité électronique et action législative pour y remédier en Algérie

تاريخ قبول المقال للنشر: 2018/05/09

تاريخ إرسال المقال: 2018/03/31

د. بوضياف إسمهان / جامعة محمد بوضياف - المسيلة

ملخص:

لقد تناولت في هذه المقالة الإطار المفاهيمي للجريمة الإلكترونية وإبراز مدى إهتمام المشرع الجزائري بتنظيمها والتصدي لها بإعتبار الجريمة الإلكترونية من الجرائم المستحدثة الناتجة عن الممارسة السيئة للتكنولوجيا المعلوماتية.

إذ نجد ان المشرع الجزائري قد قام بسن نصوص قانونية لقمع الجريمة المعلوماتية وذلك بسبب التزايد اللامتناهي للإعتداءات على الأنظمة المعلوماتية في الجزائر.

الكلمات المفتاحية: الجريمة الإلكترونية، إجراءات مواجهة الجريمة الإلكترونية، الجزائر.

Résumé :

Dans cet article, j'ai discuté du cadre conceptuel de la cybercriminalité et souligné l'intérêt du législateur algérien concernant son organisation afin de la combattre en tant que crime électronique suite à la pratique frauduleuse concernant les technologies de l'informatique.

Le législateur algérien a promulgué des textes légaux visant à réprimer la cybercriminalité en raison du nombre croissant d'attaques contre les systèmes informatiques en Algérie.

Mots clés : Crime électronique, Action contre la cybercriminalité, Algérie.

مقدمة :

تميز القرن العشرين باختراعات هائلة على المستوى التقني بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات ، حتى أصبح يعرف بقرن المعلوماتية أو-De Linfor le siecle matique، حيث أصبحت المعلوماتية وأدواتها وسائل ضرورية في العمليات البنكية أو سجلات الشركات وحتى علاقات الدولة مع الأفراد.

وعلى الرغم من أهمية الوسائل الإلكترونية وإيجابيات إستعمالها، إلا أن الإستخدام غير المشروع لها، قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية- les infrac- tion électronique أو الجرائم المعلوماتية les infraction informatique أو جرائم الأنترنت Cri- minalite par internet ، وهذه المصطلحات كلها تعبر عن مجموعة الجرائم المرتبطة بالأنظمة الإلكترونية والشبكة المعلوماتية وخصوصا على شبكة الأنترنت.

وبتنامي معدلات الجريمة وتطور أشكالها وتهديدها المباشر قد دق ناقوس مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة.

فهي جريمة تقنية تنشأ في الخفاء وتوجه للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الأنترنت، وتظهر مدى خطورتها في الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري.

وأصبح يواجه المؤلفون في البيئة الرقمية المتشابكة العديد من المشاكل بسبب سهولة الوصول إلى مؤلفاتهم واستنساخها، في ظل تقاعس أو مواكبة التشريعات التقليدية للسرعة التي تتطور بها التكنولوجيا الحديثة وعصر المعلوماتية، وعدم قدرتها على التكيف مع الوضع الحالي.

الأمر الذي دفع بالدول إلى العمل مليا للحد من هذه الجرائم من خلال التوعية والوسائل الوقائية الأمنية وغيرها، بحيث بات لزاما أن يواكب تطور الجريمة وأساليبها تطورا في مجال السياسة التشريعية عموما والسياسة الجنائية على وجه الخصوص، بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية.

وترتيبا على هذه المعطيات نطرح الإشكالية التالية : ما مدى معالجة المشرع الجزائري للجريمة الإلكترونية؟

للإمام بجميع عناصر الموضوع محل البحث اقترحنا الخطة التالية :

المبحث الأول: ماهية الجريمة الإلكترونية

المبحث الثاني: مكافحة التشريعية للجريمة الإلكترونية في الجزائر

المبحث الأول: ماهية الجريمة الإلكترونية

تعد الجرائم المعلوماتية من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث، والسبب يعود إلى إرتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الأنترنت والمواقع الإلكترونية، تعد الأنترنت من أكبر شبكات الكمبيوتر ذات الإرتباط الوثيق بالجرائم المعلوماتية وكلمة انترنت (Internet) وفي اللغة مشتق من اللغة الإنجليزية (Internet Network) أي شبكة التشبيك ويعني أنها شبكة تربط مجموعة من أجهزة الكمبيوتر المتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها، أما عن مفهوم الجرائم المعلوماتية فإنه لا يوجد إلى الوقت الحالي تعريف جامع مانع لهذا النوع من الجرائم، وقد اختلف الفقه القانوني في تعريفها.

أما التشريعات فنجد بعض التشريعات عرفت الجرائم المعلوماتية بطريقة غير مباشرة وبعضها لم يتعرض لتعريف الجرائم المعلوماتية فمهمة المشرع هي تجريم الأفعال ووضع الجزاء المناسب لها.

سوف نستعرض في هذا المبحث مفهوم الجرائم الإلكترونية في المطلب الأول من خلال التطرق أولاً إلى تعريف الجريمة الإلكترونية من الناحية الفقهية والقانونية في الفرع الأول مروراً بالتطرق للطبيعة القانونية للجريمة الإلكترونية.

ثم نستعرض في الفرع الثاني أركان وخصائص الجريمة الإلكترونية وصولاً في الأخير إلى أنواع الجرائم الإلكترونية والمدرجة في المطلب الثاني.

المطلب الأول: مفهوم الجريمة الإلكترونية

الفرع الأول: تعريف الجريمة الإلكترونية وطبيعتها القانونية

أ- تعريف الجريمة الإلكترونية.

1- التعريف الفقهي للجريمة الإلكترونية:

إن مسألة وضع تعريف للجريمة الإلكترونية كانت محلاً لإجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة الإلكترونية مذاهب شتى ووضعوا تعريفات مختلفة، ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي

نوع من المعدات الرقمية، وتعرف الجرائم الإلكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن تم ابتزاز الأشخاص باستخدام تلك المعلومات¹.

فقد انقسم أنصار تعريف الجريمة من الجانب التقني والفني فالبعض استند إلى موضوع الجريمة والبعض الأخر إلى وسيلة الجريمة².

✓ - أهم التعريفات التي استندت على موضوع الجريمة:

ويذهب أصحاب هذا الإتجاه الفقهي إلى التركيز على الجانب الموضوعي في تعريف الجريمة المعلوماتية باعتبار أن هذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها حسب بل تقع على الحاسب الآلي او في داخل نظامه.

فعرفت الجريمة المعلوماتية من قبل أنصار هذا الإتجاه بأنها (نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه) وعرفت كذلك بأنها (غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها)³.

✓ - أهم التعريفات التي استندت على وسيلة الجريمة:

- إن أنصار هذا الإتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لإرتكاب الجريمة، وبالتالي تعرف على أنها «فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية» كما تعرف بأنها «كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب» وكذلك تعرف بأنها «الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا» وإنما كل فعل أو إمتناع من شأنه الإعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية» يعتبر هذا التعريف الأخير الرأي الراجح لتبنيه من قبل العديد من الباحثين والدارسين نظرا لشمولية بحيث يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية⁴.

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: «الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا» ، وقد اتجه جانب كبير من الفقهاء إلى إعتقاد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية (OCDE) للجريمة

المعلوماتية في اجتماع باريس عام 1983، من أنها: «كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها»، وهو تعريف تبنى أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أو نقلها⁵.

كما يعرفها خبراء منظمة التعاون الاقتصادي والتنمية OECD بأنها «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها». ويعرفها الفقيه الفرنسي Vivant بأنها «مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب»⁶⁶.

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقة المجرمين المنعقد في فيينا سنة 2000 تعريف الجريمة الإلكترونية بأنها «أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

أما التعريف الدولي للجريمة الإلكترونية فهو يعتمد في الغالب على الغرض من استخدام المصطلح: فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر وأنظمة تمثل جوهر الجريمة الإلكترونية، كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر⁷.

2- التعريف القانوني للجريمة الإلكترونية:

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة بتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية»، وبهذا فقد وُفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية، ولولا هذه النظم المعلوماتية وشبكات الاتصالات ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم⁸.

على خلاف المشرع الفرنسي الذي لم يعطي تعريفا للجريمة الإلكترونية فإن المشرع الجزائري قد إصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة الثانية من القانون 04-09 على أنها «جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

ويلاحظ على هذا التعريف ما يلي:

أولاً: أن المشرع الجزائري قد إعتد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكترونية، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانياً: كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري⁹.

ب- الطبيعة القانونية للجريمة الإلكترونية:

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى إرتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال معالجة النصوص، وصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة.

بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات، ومتابعة مرتكبيها وعلى ضوء الإعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة¹⁰.

الفرع الثاني: أركان الجريمة الإلكترونية وخصائصها

أ- أركان الجريمة الإلكترونية.

1- الركن المادي للجريمة الإلكترونية:

تمهض الجريمة على ركنين رئيسيين هما الركن المادي والركن المعنوي، فلا بد للجريمة المعلوماتية إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها، ولا بد أيضاً من ركن معنوي يعبر عن إرادة المجرم المعلوماتي.

1- الركن المادي:

لابد من فعل أو إمتناع يمكن إثباته إذ لا عبارة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل

وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها، وهذا ما يدعو للتدخل التشريعي¹¹.

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتائجها، (مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل).

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب (مثلا: جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية¹²).

2- الركن المعنوي للجريمة الإلكترونية:

تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم، والإرادة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة¹³.

يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما العلم والإرادة.

- العلم: هو إدراك الفاعل للأمر.

- أما الإرادة: فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخصوصا، القصد الجنائي العام: هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود ارتكاب الفعل.

أما القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكفي الفاعل بإرتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة (مثلا: في جريمة القتل لا يكفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه) وعليه ما هو القصد الجنائي الذي

يجب توافره في الجريمة الإلكترونية؟

الأصل إن الفاعل في الجريمة الإلكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصداً ذلك ومهما يكن لا يستطيع إنتفاء علمه كركن للقصد الجنائي العام.

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي إستثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص (مثلاً: جرائم تشويه السمعة عبر الأنترنت، وجرائم نشر الفيروسات عبر الشبكة). وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي¹⁴.

ويرى الباحث أن القصد العام والخاص في جرائم المعلوماتية هو أساسي لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفائها من مكونات كل جريمة على حدا وبشكل مستقل، وبالتالي فإن الجرائم المعلوماتية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة ولا يتصور قيام أي نوع من أنواع الجرائم المعلوماتية دون وجود الركن المعنوي.

أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا، والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات وتمحيصها بما لها من صلاحية بإعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها¹⁵.

ب - خصائص الجريمة الإلكترونية.

للجريمة الإلكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن أهم هذه الخصائص أن الجرائم الإلكترونية تتطلب وجود جهاز إلكتروني ومعرفة كيفية إستخدامه وإن الهدف من هذه الجرائم الكيانات المعنوية لهذا الجهاز، كما أن الجريمة الإلكترونية لا حدود لها، وهذه الجرائم صعبة الإثبات والإكتشاف، ولذلك فهي مغرية للمجرمين، وعلى ضوء ما سبق سنتناول هذه الخصائص بالتفصيل عبر ما هو تال¹⁶:

1- انها جريمة عابرة للحدود الدولية:

الجريمة الإلكترونية ذات بعد دولي، أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية¹⁷.

2- الجريمة الإلكترونية صعوبة الإكتشاف والإثبات:

تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعوبة الإثبات، وهذا راجع إلى إفتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة¹⁸.

لا تحتاج جرائم الإعتداء على برامج ومعلومات الحاسب الإلكتروني إلى أي عنف أو جثث أو سفك للدماء أو أثار إقتحام لسرقة الأموال، وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحى كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الإلكتروني، لذا يكون من الصعب إكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبيها¹⁹.

3- يتطلب لإرتكابها وجود جهاز إلكتروني ومعرفة بتقنية إستخدامه.

إن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم، أنها تتطلب وجود علم كافي بالجوانب الفنية كالتقنية لإستخدام الحاسوب والإنترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد إحتمال إستخدام خبرتهم بشكل غير مشروع.

وأثبت الواقع العلمي، أن الجرائم الإلكترونية قد ترتكب من خلال الهواتف المحمولة، خاصة بعد ظهور أجهزة الهاتف الذكية كالتالي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الإتصال بشبكة الإنترنت، ويسهل تخزين ونقل المعلومات من خلالها، وليس كما ذكر بعض الباحثين بأن الحاسب الآلي هو الأداة الوحيدة في إرتكاب الجريمة الإلكترونية، ففي أيامنا هذه نرى أنه يمكن تصنف الهواتف المحمولة الذكية ضمن أجهزة الكمبيوتر، كذلك لأنه لا يختلف عن الحاسوب سوى في الحجم- بل أن الهواتف الذكية يمكن من خلالها الإتصال المباشر بخلاف - الحاسب الآلي أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسب الآلي من خلال الهاتف الذكي.

ويتمثل علاج المشكلة السابقة من خلال وجود برامج حماية على كل أجهزة الحاسوب سواء المنزلية أو المتوافرة في أماكن العمل، وذلك لضمان الحفاظ على الأسرار الشخصية والمهنية، وعدم جعل الجهاز متصل بالإنترنت والتيار الكهربائي خارج وقت الإستخدام له²⁰.

4- الجرائم الإلكترونية جرائم الأذكاء:

إن مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء، والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وكيفية تشغيله، وكيفية تخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي

بسيط متوسط التعليم²¹²¹.

المطلب الثاني: أنواع الجرائم الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة، والتي اختلف الفقه في تصنيفها إلى عدة مسميات، ولم تراع أغلب التقسيمات خصائص الجرائم الإلكترونية وموضوعها، وإن أهم ما يميز الجرائم الإلكترونية عن غيرها هو أن هذه الجرائم تستهدف الكيانات المعنوية للحاسب الآلي، وترتكب بواسطة جهاز إلكتروني، أما ما يستهدف الكيانات المادية للحاسب الآلي فيندرج تحت صور الجرائم التقليدية.

وإختلاف الفقه في تقسيم الجرائم الإلكترونية هو نتيجة ظهور جرائم جديدة من حين لآخر، حيث أن الجرائم الإلكترونية لا حصر لها، ولا يمكننا أن نجملها بكل أصنافها وأشكالها، فهي متغيرة ومتجددة، فكلما ظهرت وسيلة جديدة لإستخدام الحاسب الآلي والأنترنت ظهرت معه جريمة جديدة²².

إذ لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الإلكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو على أساس محل الجريمة، وعلى هذا الأساس يمكن تقسيمها إلى²³:

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة، وتنقسم هذه الجرائم بدورها إلى²⁴:

أ- الجرائم الواقعة على الأشخاص:

ان للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال ذلك الإعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الإطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته.

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالأداب العامة، ويقوم بنشرها عبر الأنترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة على ذلك²⁵.

ب- الجرائم الواقعة على الأموال:

لقد صاحب ظهور شبكة الأنترنت تطورات كثيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الأنترنت انتهب بعض المجرمين الفرصة من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقه، والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة²⁶.

في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجز عنه من تطور وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الأنترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

- ✓ السطو على أرقام بطاقات الإئتمان والتحويل الإلكتروني الغير مشروع.
- ✓ القمار وغسيل الأموال عبر الأنترنت.
- ✓ جريمة السرقه والسطو على أموال البنوك.
- ✓ تجارة المخدرات عبر الأنترنت²⁷.

ج- الجرائم الواقعة على أمن الدولة:

إستغلت الكثير من الجماعات المتطرفة الطبعة الإتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذتا معنى آخر في إستعمال الأنترنت، التي سمحت لهم في ارتكاب جرائم غاية الشك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت، الأنترنت لكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على مختلف الأسرار العسكرية الإقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الأنترنت، حيث تعطي الأنترنت فرصا للتأثير على معتقدات وتقاليده مجتمعات بأكملها مما يسهل خلق الفوضى²⁸.

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع بإستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي.

أ- الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل لسرقة وخيانة الأمانة أو الإلتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى إلى إلتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقدرت الخسائر بـ 5 ملايين فرنك فرنسي²⁹.

ب- الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

نعتقد أن هذه الصورة تعتبر بدون شك أكثر الصور إنتشارا وخطورة حيث يتم بواسطة الإحتيال إدخال معطيات في نظم المعالجة الآلية للمعطيات أو إلتلافها أو حذفها أو تغيير المعطيات المدرجة³⁰.

وقد عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات والتي تنص على أنه «يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 5000.00 دج إلى 20.000.00 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، من خلال هذا النص ومن أجل معالجة عناصر هذه الجريمة يتوجب تحديد معنى الإلتلاف ثم الوسائل التي يتحقق بها الإلتلاف.

يعرف البعض الإلتلاف بأنه هو ذلك الفعل الذي يجعل الشيء غير الصالح للإستعمال أو بإعدام صلاحيته أو تعطيله (وقف عمله) سواء بصفة كلية أو جزئية.

ويقصد كذلك بالإلتلاف إفناء مادة الشيء أو هلاكه كليا وبالتالى توقف الشيء تماما على أن يؤدي منفعته ولو لم تفتى مادته سواء كان هذا التوقف كليا أو جزئيا ويكون الشيء غير صالح للإستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل.

كما يقصد أيضا بإتلاف برامج الحاسوب الآلي ومعلوماته إلتلاف أو محو تعليمات البرامج والبيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات وعادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه بل لمجرد إعاقة نظام المعلومات.

وعلى ضوء هذه التعريفات يمكن القول بأن الإلتلاف لا يتحقق فقط في التأثير على مادة الشيء بل يتحقق كذلك حتى في حالة الإنتقاص من قيمة الشيء الإقتصادية مما يعني أن الحكمة من الإلتلاف هي ليس التعرض لمادة الشيء وإنما العبرة بمدى مساس الفعل بقيمته المالية ذلك أن الفعل الذي يترتب عنه فقدان الشيء لقيمته المالية أو الإنتقاص منها هو الذي

يحقق الإعتداء الذي يعاقب عليه القانون على إعتبار أنه قد ذهب بأهمية الشيء بالنسبة لمالكه.

ومن اجل الإشارة إلى مدلول الإلتلاف إستخدم المشرع الجزائري عدة تعابير حيث إستخدم (أدخل .أزال ، عدّل) وإن كان لهذه التعابير مدلولات خاصة إلا أنها تندرج تحت مدلول الإلتلاف وهو ما ذهب إليه بعض التشريعات المقارنة خاصة التشريع الفرنسي، وبالتالي يمكن القول كذلك أن المشرع الجزائري قد أورد هذه الصور التي يتحقق بها الإلتلاف على سبيل المثال لا الحصر، وبمعنى آخر يمكن أن يتحقق الإلتلاف بصور أخرى غير تلك التي أوردتها المشرع الجزائري في قانون العقوبات.

إن المقصود بالإلتلاف في هذا الإطار ذلك الذي يوجه إلى الجانب المنطقي والمعنوي في الحاسب الآلي، والذي بات يشكل قيمة إقتصادية عالية، فإلتلاف برامج ومعلومات الحاسب الآلي فيه إفتقاد لمنفعة هذه البرامج والمعلومات³¹.

ج- الجرائم الواقعة على البرامج الإلكترونية:

وتنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أو لآثم التلاعب به أو تعديله، ومن أمثلتها قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم zzwick.

وكذلك تضم هذه الجرائم. الجرائم الواقعة على برنامج التشغيل وهي البرامج المسؤولة عن عمل النظام المعلوماتي، ومن حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثالها: جريمة تصميم برنامج وهمي من خلاله يتم تنفيذ الجريمة، ومثاله ما قامت به إحدى الشركات التأمين الأمريكية في مدينة لوس أنجلوس بواسطة مبرمجها، إذ قامت بتصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بهدف تقاضي هذه الشركة لعمولات من اتحاد شركات التأمين³².

المبحث الثاني: المكافحة التشريعية للجريمة الإلكترونية في الجزائر

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه للتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية الى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات

الإجرامية في مجال تكنولوجيا الإعلام و الإتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية، ومع هذا فيبقى السؤال مطروح حول مدى فعالية وفعالية هذه القوانين في مواجهة الجرائم الإلكترونية.

نتناول في هذا المبحث مظاهر مكافحة المشرع الجزائري للجريمة الإلكترونية من خلال التطرق إلى دور القوانين العامة الجزائرية في مكافحة الجريمة الإلكترونية وذلك في المطلب الأول، وصولاً في الأخير إلى دراسة القوانين والهياكل الخاصة في مكافحة الجريمة الإلكترونية بالجزائر وذلك في المطلب الثاني.

المطلب الأول : مكافحة الجريمة الإلكترونية بموجب القوانين العامة

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قرصنة الأنترنت وإحالتهم قانوناً على المحاكم، متأثراً بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الإلكترونية، ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام.

الفرع الأول : مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني

أ- مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري: لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية حقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم إنتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردتها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

المادة 44: حرية الإبتكار الفكري والفني والعلمي مضمونة للمواطن ، حقوق المؤلف يحميها القانون.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.

تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

إذ لا يجوز إنتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، كما أن القانون يحيي

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي³³.

ب- مكافحة الجريمة الإلكترونية بموجب القانون المدني الجزائري: ترتباً على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الإعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري «كل عمل أيا كان يرتكبه المرء يسبب ضرراً للغير يلزم من كان سبباً في حدوثه بالتعويض» وقد جاء هذا النص عاماً وشاملاً لأي إعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهماً هو حق من وقع إعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض «فالفعل الضار هو أساس المسؤولية» وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الإعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الأنترنت، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدى، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل إعتداء قابل للإثبات وإن وقع على الشبكة³⁴.

الفرع الثاني: مكافحة الجريمة الإلكترونية بموجب قانون العقوبات

الجزائري وقانون الإجراءات الجزائية الجزائري

أ- مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري: لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الألي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 المادة مكرر³⁵.

وبغرض تدارك الفراغ القانوني، فقد قام المشرع الجزائري بموجب القانون رقم 04-15³⁶ بإستحداث جملة من النصوص والتي جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع الجزائري بسن «جملة من

القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة³⁷، وإلى جانب ذلك فقد قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22³⁸.

إذ نصت المادة 394 مكرر منها يلي: «يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك»، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إستغلال المنظومة «تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج»، وذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الإعتداءات تلك التي تمس ببعض صور الحياة الخاصة، ونصت المادة 394 مكرر 2 على أنه: «يعاقب... كل من يقوم عمدا وعن طريق الغش بما يأتي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم».

وتضيف المادة 394 مكرر 6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية: «يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو المكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها»³⁹

ب- مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية الجزائرية: بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة وإستجواب المتهم والضبط والتسرب والشهادة والخبرة⁴⁰.

نجد أن المشرع نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية، ونص على التفتيش في المادة 45 الفقرة 7⁴¹ من نفس القانون المعدلة حيث إعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي

لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على «إعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5⁴².

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الإتصالات الإلكترونية تسجيلها والتسرب.

يقصد بإعتراض المراسلات إعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الإستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الإتصال السلوكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو: «إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الإبتدائي في... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن:

- باعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلوكية واللاسلكي.

- وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط و تثبيت و بث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص».

فموجب هذه المادة فإن المشرع الجزائري يسمح لسلطات التحقيق والإستدلال إذا إستدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء إعتراض المراسلات السلوكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، والإستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملبسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة.

ومع هذا فإن المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الإستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد⁴³

المطلب الثاني : مكافحة الجريمة الإلكترونية بموجب القوانين والهيكل الخاصة

الفرع الأول : مكافحة الجرائم الإلكترونية بموجب القوانين الخاصة

أ- القانون الخاص بحماية حق المؤلف والحقوق المجاورة: يرى معظم الفقه أن «الموقع الإلكتروني مصنف متعدد الأغراض»، يتم إستخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الأنترنت، أو كإسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو... وغيره، وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة، وبمجرد تسجيل إسم الموقع يحضى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه، أي بتحديد القانون الواجب التطبيق حسب الطبيعة القانونية للمواقع فعند تسجيل الموقع كمصنف أدبي أو فني «لا يجوز أن يعتدى على أي جانب من جوانب الحياة الخاصة للأفراد» كإستعمال إسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها أو إستغلال صورة أي شخص في الموقع دون الموافقة منه، والمصنف من حيث المفهوم لا ينصرف فقط إلى المادة الملموسة في الخطوط والتمثيل أو اللوحات الزيتية وإنما هي الفكرة المدرجة في المحل الملموس وهي جوهر الإبداع الأدبي أو الفني لأنها الأساس الذي يقوم عليه المصنف، أما المادة التي نفذت عليها المادة ما هي إلا وسيلة لنقله إلى الجمهور وقياسا لذلك على موضوعنا تصبح مواقع الأنترنت الوسيلة المستخدمة لعرض المصنفات على الجمهور، وبهذه الصورة فإن حماية مواقع الأنترنت التي تستغل مصنفات أدبية أو فنية على شبكة الأنترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الأدبي والمالي للموقع المسجل كمصنف، وحماية قانونية لأي حق آخر يتم الإعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الإسم والصورة والمعلومات الخاصة... وفي كل الأحوال لا يمكن الفصل بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف والحقوق المجاورة في الوقت نفسه، لأن حماية الموقع تؤدي بالضرورة إلى عدم محتوياته بما في ذلك المصنف⁴⁴.

ب- قانون البريد والاتصالات اللاسلكية: بإستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات، لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الإلكتروني، ذلك ما نصت عليه المادة 87 منه، كما نصت المادة 2/84 منه على إستعمال حوالات دفع عادية أو إلكترونية أو برقية، كما نص في المادة 105 منه على إحترام المراسلات، بينما أتت المادة 127 منه بجراء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو

يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات⁴⁵.

ج- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: لقد جاء في القانون 04-09 مجموعة من التدابير الوقائية التي يتم إتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن تركيبها في وقت مبكر، وهي كالتالي:

1- مراقبة الاتصالات الإلكترونية: لقد نصت المادة 04 من القانون 04-09 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الإلكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

- للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب و جرائم ضد أمن الدولة.

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

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

- في أطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

2- إقحام مزودي خدمات الاتصالات الإلكترونية في مسار الوقاية من الجرائم المعلوماتية: وذلك من خلال فرض عليهم مجموعة من الإلتزامات المذكورة في المواد 10، 11، 12 بالشكل التالي:

- الإلتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات و المراسلات و وضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيق.

- الإلتزام بحفظ المعطيات المتعلقة بحركة السيروكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم و تركيبها، وهذين الإلتزامين موجبهين لكل مقدمي خدمات الاتصالات الإلكترونية (Fournisseurs de services) دون إستثناء.

- الإلتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.

- الإلتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها.
ونشير إلى أن هذين الإلتزامين يخصان فقط مقدمي الدخول إلى الأنترنت (Fournis- seurs D'accès a l'internet).

إضافة الى التدابير الوقائية السالفة الذكر تبني المشرع في القانون رقم 04-09 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجيا الإعلام والاتصال تلخص فيما يلي:

- السماح للجهات القضائية المختصة و ضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وإستدساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.
- إمكانية الإستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للإتفاقيات الدولية ومبدأ المعاملة بالمثل.

- توسيع دائرة إختصاص الهيئات القضائية الجزائرية لتشمل النظري في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.
- السماح للسلطات الجزائرية المختصة للجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق و جمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو إتخاذ تدابير احترازية في إطار الإتفاقيات الدولية ومبدأ المعاملة بالمثل⁴⁶.

د- قانون التأمينات : قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر⁴⁷.

الفرع الثاني : مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة

أ- الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها « تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته. تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم »، أما مهامها فقد أوردتها المادة 14 من نفس القانون.

- تنظيم الهيئة : بالرغم من الأهمية المرجوة من هذه الهيئة إلا أنه لم يتم إلى حد الساعة إنشاءها، ولم يصدر تنظيم تشكيلتها ستحوي مجموعة من فإن خاص بها يحدد تشكيلتها وتنظيمها وسيرها. وباستقراء نصوص القانون 04/09 فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة، وهو نفس الأمر لما هو في فرنسا إذ أنشأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال

Office central de lutte contre la criminalité liée aux technologie l'information et de la communication وهي هيئة للمديرية تابعة ، العامة للشرطة الوطنية الفرنسية وخاضعة للمديرية المركزية للشرطة القضائية، نشأت سنة 2000.

- مهام الهيئة : من خلال إسمها فإن للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها:

1/ الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيا الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الإتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية.. الخ.

2/ مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة ب من القانون 04/09، وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا، فإن لها مهام أدرجها المرسوم رقم

2000- 405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة تتمثل في⁴⁸:

✓ تنشيط وتنسيق على المستوى الوطني عمليات مكافحة ضد الفاعلين والمشاركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

✓ لقيام بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس بإختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون.

✓ تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.

✓ التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون 04/09 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.

✓ من أجل القيام بمهامها فلها تركيز، تحليل، إستقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة)، وكذلك كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها.

✓ يجب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الأجل إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما تسمح به القوانين- وخاصة منها ما يتعلق بالسرايمني- بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والاتصال.

3/ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) لمماثلة لها على مستوى الدول، بدون المساس بتطبيق الإتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم⁴⁹.

ب- المعهد الوطني للأدلة الجنائية على الإجرام: يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الألي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات⁵⁰.

ج- الهيئات القضائية الجزائرية المتخصصة: إنَّ السلطة القضائية ستتعامل تأكيداً في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

ومنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليوكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم إجراء أولاً: دمج مادة « الجريمة المعلوماتية » في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء، العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة وإطارات وزارة العدل في إطار التعاون الثنائي، ومنها: التعاون الجزائري الفرنسي، الجزائري البلجيكي، والجزائري الأمريكي الذي تناول خاصة التكوين المتخصص في الملكية الفكرية المتمحورة حول التزوير المتصل بالبيئة الرقمية ولا شك أنَّ تخصيص جهات القضاء وتخصص القضاة هما من السمات الحديثة البارزة لتنظيم القضائي الجزائري، وقد جاء في إتفاقية التمويل الجزائرية الأوروبية لمشروع دعم إصلاح العدالة في الجزائر أنَّ: هذا المشروع يهدف إلى دعم التخصص وتكوين القضاة داخل وخارج الوطن للإستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها، ونظراً لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها: مؤتمر روما سنة 1958، مؤتمر نيس سنة 1972، مؤتمر يودي جانيرو لسنة 1978، وقد أكدت هذه المؤتمرات أن التخصص في مجال القضاء له أهمية كبيرة ودور فعّال في رفع مستوى العمل القضائي، ولنظام التخصص جانبيين هما: تخصص القضاة، وتخصص جهات القضاء.

ويتجه النظام القضائي الجزائري إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائرية (ق.إ.ج) على أنَّه يجوز تمديد دائرة الإختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، كما نصت المادة 40 مكرر من ق إ ج على أنَّه « تُطبق قواعد

هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع إختصاصها المحلي طبقا للمواد 37، 40، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه».

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنه جعل المشرع الجزائري لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية⁵¹، فيتجنب إنشاء هيئات قضائية جديدة لكنه يوسع من دائرة الإختصاص الإقليمي للمحاكم لتشكّل أقطاب قضائية ويمنحها إختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن إختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أنّ التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية.

هذه الأقطاب الجزائرية المتخصصة طبقا لنصوص المرسوم التنفيذي رقم 06 / 348 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم وكلاء الجمهورية وقضاة التحقيق (جريدة رسمية رقم: 63) (في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم ريع الخاص بالصرف، ولأنّ الجريمة المنظمة تشمل جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالنش متنوعة تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وتُرتكب من طرف عدة أفراد يتصرفون بطريقة منظمة، تعدّ الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائرية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الإختصاص القضائي في إطار الإهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة⁵².

الخاتمة:

أهم النتائج التي توصلت لها الدراسة:

- لم يتفق الفقهاء على تعريف جامعا مانعا للجريمة الإلكترونية.
- تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.
- قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.
- رغم إجتهد المشرع الجزائري للتصدي لهذه الجريمة، إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.

- إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في بيئة الرقمية.
- أن النصوص الوضعية لحماية حقوق المؤلف والحقوق المجاورة تعتبر غير كافية لمواجهة الإعتداءات الواقعة عليها عبر الأنترنت.
- ضرورة مراجعة التشريعات الوطنية من خلال تشديد الوصف الجنائي والعقوبات المقررة للأنماط الإجرامية للجريمة المعلوماتية، بغية تحقيق الردع والقضاء على الإجرام المعلوماتي.
- ضرورة تعديل بعض التشريعات الجزائرية الحالية وخاصة في مجال الملكية الفكرية بما يتلائم مع طبيعة جرائم الأنترنت، والتقنية، وتهيئة العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل واضح.
- الإسراع في إصدار القوانين التنظيمية، من خلال وضع مدونة قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.
- ضرورة إبرام إتفاقات عربية ودولية في مجال مكافحة الجرائم المعلوماتية، وذلك لتحديد إطار الإختصاص القضائي الدولي والتعاون في كشف وإثبات الجريمة المعلوماتية.
- ضرورة إيجاد الوسائل المناسبة للتعاون الدولي للمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى لضمان الحماية العالمية الفعالة لبرامج المعطيات الألية والكمبيوتر وشبكة الأنترنت ككل.
- مساعدة شركات التقنية والأنترنت في اتخاذ إجراءات أمنية مناسبة، سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.
- التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم.
- الإستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن صورة.
- عقد دورات مكثفة للكوادر البشرية العاملين في حق التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الألية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن

جرائم الأنترنت.

- ضرورة خلق ثقافة إجتماعية جديدة تندد بجرائم الأنترنت مع تفعيل أسلوب التوعية والتهديب لدى مستخدمي شبكة الإتصالات العالمية وحثهم على الإستخدام الأمثل لهذه التقنيات.

- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصد لهم في حالة عدم إتخاذ الإحتياطات الوقائية اللازمة.

- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية والحد من أثارها.

الهوامش :

¹ مختارية بوزيدي، ماهية الجريمة الالكترونية، الملتقى الوطني "أليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر العاصمة، بتاريخ 29 مارس 2017، ص 09.

أنظر ايضا: مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016، ص 20.

² فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية»، طرابلس، بتاريخ 24-25 مارس 2017، ص 118.

³ عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، جامعة الكوفة «كلية القانون»، العدد السابع، 2008، ص 113.

⁴ فضيلة عاقلي، مرجع سابق، ص 118.

⁵ ياسمينه بونعارة، الجريمة الإلكترونية، مجلة المعيار لكلية أصول الدين، جامعة الأمير عبد القادر، 19/06/2015، العدد 39، ص 4.

⁶ محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، الجزء الثاني، وزارة الداخلية " الأكاديمية الملكية للشرطة"، البحرين، مارس 2010، ص 02.

⁷ مختارية بوزيدي، مرجع سابق، ص 10.

⁸ أنهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 52.

⁹ نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، بتاريخ 24-25 مارس 2017، ص 100.

¹⁰ محمد زكي أبو عامر وعلي عبد القادر القهوجي، قانون العقوبات " القسم الخاص"، دار النهضة العربية، القاهرة، 1993، ص 09.

¹¹ بن غدفة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها، أعمال الملتقى الوطني، "أليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017، ص 48.

¹² فضيلة عاقلي، مرجع سابق، ص 119-120.

¹³ لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها" دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشعرية، الأردن، 13/08/2016، ص 24.

¹⁴ فضيلة عاقلي، مرجع سابق، ص 120.

- ¹⁵ لورنس سعيد الحوامدة، مرجع سابق، ص 25-26.
- ¹⁶ يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة"، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون "الجامعة الإسلامية"، غزة، 2013، ص 13.
- ¹⁷ ابراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مجلة كلية الشريعة والقانون بطنطا، الجزء الثاني، العدد 30، ص 374.
- أنظر أيضا: عبد الله دغش العجبي، المشكلات العلمية والقانونية للجرائم الإلكترونية "دراسة مقارنة"، رسالة استكمال للحصول على درجة الماجستير في القانون العام، الأردن، 2014، ص 20.
- ¹⁸ ذياب موسى البدانية، الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولت الإقليمية والدولية خلال الفترة من 2-3/09/2014"، ورقة علمية بعنوان الجرائم الإلكترونية: المفهوم والأسباب، كلية العلوم الإستراتيجية، عمان، 2014، ص 20.
- ¹⁹ عادل يوسف عبد النبي الشكري، مرجع سابق، ص 116.
- ²⁰ يوسف خليل يوسف العفيفي، مرجع سابق، ص 14.
- ²¹ ابراهيم رمضان إبراهيم عطايا، مرجع سابق، ص 373.
- ²² يوسف خليل يوسف العفيفي، مرجع سابق، ص 20.
- ²³ حفوطة الأمير عبد القادر و غرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 93.
- ²⁴ نمديلي رحيمة، مرجع سابق، ص 102.
- ²⁵ يوسف خليل يوسف العفيفي، مرجع سابق، ص 26.
- أضاً أيضا: مركز هردو لدعم التعبير الرقمي، التنظيم القانوني والجرائم الإلكترونية ما بين المعلومات وتقييد الحريات، القاهرة، 2018، ص 8.
- ²⁶ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون "تخصص القانون الدولي للأعمال"، جامعة مولود معمري - تيزي وزو - كلية الحقوق والعلوم السياسية، 2013، ص 44.
- ²⁷ الباحث حفوطة الأمير عبد القادر و غرداين حسام، مرجع سابق، ص 93.
- ²⁸ ناصر محمد البقبي، اثر التحويل مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن لفكري بجامعة الملك سعود، المملكة السعودية، 22-25 جمادى الأولى 1430 هـ، ص 18.
- ²⁹ نمديلي رحيمة، مرجع سابق، ص 103-104.
- ³⁰ سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والأمني، الملتقى العلمي "حول الجرائم المستحدثة في ظل المتغيرات والتحولت الإقليمية والدولية"، كلية العلوم الإستراتيجية، الأردن، 02-04/09/2014، ص 12.
- ³¹ احمد بن مسعود، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد العاشر، العدد الأول، ص 486-487.
- ³² نمديلي رحيمة، مرجع سابق، ص 104.
- ³³ فضيلة عاقل، مرجع سابق، ص 127.
- ³⁴ حسين نواره، آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017، ص 121-122.
- ³⁵ فضيلة عاقل، مرجع سابق، ص 127.
- ³⁶ قانون رقم 04-15 مؤرخ في 10/11/2004 يعدل ويتمم الامر رقم 66-156، يتضمن قانون العقوبات، جريدة رسمية عدد 71، صادر بتاريخ 10/11/2004، معدل ومتمم.

- ³⁷ قانون رقم 06-22 مؤرخ في 20/12/2006 يعدل ويتمم الأمر رقم 66-155، يتضمن قانون الاجراءات الجزائية، جريدة رسمية، عدد 84، صادر بتاريخ 24/12/2006.
- ³⁸ براهيمي جمال، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد 2، الصادرة في 15/11/2016، ص 124-125.
- ³⁹ حسين نواردة، مرجع سابق، ص 118-119.
- ⁴⁰ فضيلة عاقل، مرجع سابق، ص 130.
- ⁴¹ مولود ديدان، قانون الإجراءات الجزائية، الأمر 11-02، دار بلقيس، الجزائر، ص 33.
- ⁴² فضيلة عاقل، مرجع سابق، ص 130.
- ⁴³ براهيمي جمال، مرجع سابق، ص 138-139-140.
- ⁴⁴ حسين نواردة، مرجع سابق، ص 120-121.
- ⁴⁵ فضيلة عاقل، مرجع سابق، ص 131.
- ⁴⁶ براهيمي جمال، مرجع سابق، ص 151-154.
- ⁴⁷ فضيلة عاقل، مرجع سابق، ص 132.
- ⁴⁸ لمعرفة مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المستقبلية. أنظر www.legifrance.gouv.fr/affich_texte.de
- ⁴⁹ عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، مصر، 2007، ص 232-233.
- ⁵⁰ فضيلة عاقل، مرجع سابق، ص 133.
- ⁵¹ عمار بوضياف، النظام القضائي الجزائري، دار ربحانة، الجزائر، 2003، ص 229، 230.
- ⁵² أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي، جامعة قاصدي مرباح "كلية الحقوق"، ورقلة، 2012-2013، ص 49-50.