وزارة التعليـم العالــي والبحـث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

القسم: الحقوق
الشعبة: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي:.....
الرمـــــــــز: .....

الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة ماستر

إعداد الطالبة:
- آية بن ميسية

إشراف الأستاذ(ة):
د. محمد الصغير سليني

السنة الجامعية: 2025/2024

وزارة التعليم العالي والبحث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهد الحقوق

القسم: الحقوق
الشعبة: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي:.....
الرمـــــــــز: .....

الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة ماستر

إعداد الطالبة:
- آية بن ميسية

إشراف الأستاذ(ة):
د. محمد الصغير سليني

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة	الجامعة	الصفة
نضيرة بوعزة	أستاذ محاضر أ	المركز الجامعي ميلة	رئيسا
محمد الصغير سليني	أستاذ محاضر ب	المركز الجامعي ميلة	مشرفا ومقررا
بديار علي محمود	أستاذ محاضر ب	المركز الجامعي ميلة	عضوا مناقشا

السنة الجامعية: 2025/2024

شُكرٌ وتقدير

الحمد لله على إحسانه والشكر له على توفيقه وامتنانه ونشهد أن لا إله إلا الله وحده لا شريك له ونشهد ان محمدا عبده ورسوله.

بعد شكر الله سبحانه وتعالى على توفيقه لنا لإتمام هذا البحث المتواضع.

نتقدم بجزيل الشكر إلى من شرفنا بإشر افه على مذكرة بحثنا الأستاذ الدكتور"محمد الصغير سليني" الذي لن تكفي حروف هذه المذكرة لإفائه حقهُ بتوجيهاته العلمية التي لا تقدر بثمن.

كما نشكر كل من ساهم من قريب أو من بعيد على انجاز هذا البحث، لاسيما من عمل على كتابته وطباعته جزاهم الله خيرا.

الإهداء

الحمد لله الذي وفقني في إنجاز هذا العمل المتواضع

والذي أهديه:

❖ إلى من كلله الله بالهيبة والوقار إلى من علمني العطاء بدون انتظار إلى من أحمل اسمه بكل افتخار "**والدي العزيز مسعود**". وأبي الثاني **عمار** الذي كان سندا وكتفا لي.

❖ إلى بسمة الحياة وسر الوجود **"أمي العزيزة حليمة"** أكرمها الله وأطال في عمرها بالخير والبركات، وأمي الثانية **زكية** التي كانت سندي دائما.

❖ الى زوجي الحبيب رفيق دربي وشريك حياتي، الذي كان دعماً وسنداً لي في كل الأوقات. شكراً لك على محبتك وصبرك وتشجيعك المستمر، لقد كنت دوماً مصدر قوتي وإلهامي.

❖ إلى أخوتي وأخواتي الذين كانوا سندا لي في حياتي ولم يبخلوا بشيء من أجلي.

❖ إلى كل من ساعدني من قريب أو بعيد.

آيـــــة

مقدمـــــــــــــة

مقدمة

باعتبار الجريمة ظاهرة اجتماعية فقد عرفت العديد من التطورات بتطور العصور والمجتمعات أي خصصت كل حقبة زمنية بقانون عقابي خاص بها وصولا الى القرن العشرين متى عرف العالم قفزة نوعية حيث تطورت وتعددت القوانين ومع ظهور ما يسمى بالعولمة والتطور الهائل في مجال الإعلام والاتصال وانتشارها أدى إلى ظهور أشكال عديدة للإجرام اصطلح على تسميتها بالجريمة الإلكترونية التي كانت من المفرزات السلبية للتطور التكنولوجي حيث تعتبر شكل مستحدث من أشكال الإجرام الذي يستهدف الأفراد، المؤسسات و الدول عبر الفضاء الرقمي بتجاوز الحدود التقليدية للجريمة.

المشرع كغيره من التشريعات الدولية حاول التصدي لهذه الجريمة من خلال نص 09-04 المؤرخ في 15 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، حيث تكمن أهمية دراستنا لموضوع الجريمة الإلكترونية في أنها من مواضيع الساعة وأن هذه الجريمة من التحديات الحديثة التي تهدد أمن الأفراد و الدول على حد سواء بما تحمله من خطورة تتجاوز الأطر التقليدية للجريمة خاصة وأن مرتكبيها غالبا يستغلون ثغرات تقنية للهروب من المحاسبة وهذا لفقدان الدليل التقليدي المادي وتبرز أهميتها كذلك في تعقيد إجراءات مكافحتها والتحقيق بها، ولعل من أهم الأسباب التي دفعتنا لاختيار هذا الموضوع نتيجة لما لاحظناه من تزايد مستمر في عدد الجرائم الإلكترونية لاسيما في الجزائر ومعرفة كيفية معالجة المشرع الوطني لمختلف هذه الجرائم من خلال النصوص التشريعية العقابية وكذا التجريمية لما تم استقراءه من نصوص قانون العقوبات الجزائري وبالتالي اظهار مختلف السبل والآليات المستحدثة للحد من هذه الظاهرة.

من الأسباب الشخصية لاختيار هذا الموضوع هو اهتمامي وميولي الخاصة نحو القضايا القانونية المعاصرة وخاصة تلك المتعلقة بالتكنولوجيا والمجتمع الرقمي والرغبة في تعميق الفهم القانوني وتوسيع معارفي حول هذا الموضوع والرغبة في المساهمة العلمية في تقديم مقترحات عملية قابلة للتطوير.

من أهداف دراستنا للموضوع هو التعرف ودراسة العديد من النقاط وهي التعرف على الجريمة الإلكترونية ومدى خطورتها وتحليل مدى فعالية النصوص القانونية الجزائرية التي وضعها المشرع الجزائري في مواجهة هذا النوع المستجد من الجرائم من خلال دراسة الآليات التشريعية والإجرائية المعتمدة على مستوى الحماية الموضوعية للأنظمة والمعلومات أو من حيث التحقيق وجمع الأدلة، واقتراح مختلف السبل لمكافحة الجريمة الإلكترونية.

أما من الدراسات السابقة التي اعتمدتها:

رسالة ماجيستر: الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري جامعة د.مولاي الطاهر سعيدة، كلية الحقوق والعلوم السياسية قسم الحقوق، فليح نور الدين سنة 2019/2018.

رسالة ماجيستر: آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، جامعة محمد البشير الإبراهيمي – برج بوعريريج–، كلية الحقوق والعلوم السياسية، عقباش بريزة ومبارك حنان سنة 2022/2021.

محاضرات في الجرائم المعلوماتية المركز الجامعي أفلو معهد الحقوق والعلوم السياسية قسم الحقوق للدكتور بن دراح علي إبراهيم سنة 2021/2020.

ولكل موضوع بحث لا نجده خاليا من الصعوبات ولعل أبروها محدودية المصادر الوطنية التي تناولت موضوع الجريمة الإلكترونية ضمن الإطار القانوني الجزائري بالإضافة إلى صعوبة الوصول إلى خطة متوازنة ومعالجة فعالة لموضوع البحث بالنظر إلى طبيعة الموضوع المزدوجة القانونية والفنية.

وبعد البحث والقراءة لمختلف جوانب الدراسة تراءت لنا إشكالية عامة تتمثل في:

هل تمكن المشرع الجزائري من وضع حد للجريمة الالكترونية و ماهي الاليات القانونية التي وضعها لمكافحتها؟

وهذه الإشكالية العامة التي بدورها تتفرع منها إشكاليات فرعية نذكر منها:

- كيف عالج المشرع الجزائري ظاهرة الجريمة الإلكترونية؟
- ما هو الإطار القانوني الذي اعتمده المشرع الجزائري لمكافحة الجريمة الإلكترونية؟

وقد تم الاعتماد في دراسة موضوع البحث على ثلاثة مناهج أولهما المنهج الوصفي للجانب الفني من الدراسة مع الاستعانة بالمنهج التحليلي لدراسة مختلف القواعد والسنن القانونية والتشريعية ذات صلة للبحث بالإضافة إلى المنهج المقارن في حالات محددة لبيان موقع التشريع الجزائري بين باقي التشريعات.

ومن أجل الكشف عن مختلف خطايا الموضوع وكذلك إيجاد أجوبة لكل التساؤلات المطروحة عبر الإشكال العام تم تقسيم الدراسات إلى فصلين حيث تناولنا في الفصل الأول ماهي الجريمة الإلكترونية وبدورنا قسمناه إلى مبحثين تناولنا في المبحث الأول تعريف الجريمة الإلكترونية وخصائصها وتصنيفاتها أما في المبحث الثاني فقد تناولنا الجرائم الإلكترونية وفق ما جاء به التشريع الجزائري أما في الفصل الثاني فقد تناولنا آليات مكافحة الجريمة الإلكترونية الذي بدوره قيمناه إلى مبحثين في المبحث الأول تطرقنا إلى الحماية الموضوعية للنظام المعلوماتي والمبحث الثاني الحماية الإجرائية للنظام المعلومات.

الفصل الأول: ماهية الجريمة الالكترونية

الفصل الأول: ماهية الجريمة الالكترونية

في ظل التطور التكنولوجي المتسارع وانتشار استخدام الإنترنت في مختلف جوانب الحياة اليومية برز نوع جديد من الجرائم يعرف بـ "الجريمة الإلكترونية"، وبذلك أصبحت الجريمة الإلكترونية لا تقل خطورة عن الجريمة العادية.

تنبع خطورة الجريمة الإلكترونية من صعوبة تتبع مرتكبيها وسرعة انتشارها والآثار الكبيرة التي تخلفها، مما يجعل التصدي لها أمرا ضروريا يستوجب وعيا مجتمعيا وتشريعات قانونية رادعة، وتعد جريمة ذات طابع خاص إذ تستهدف المعنويات أكثر من الماديات المحسوسة، إلا أن آثارها قد تكون معنوية كما قد تكون مادية محسوسة أيضا.

تعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية، تختلف كثيرا عن الجريمة التقليدية، في طبيعتها، ومضمونها ونطاقها وتأثيريها وأنواعها ووسائلها وأدواتها، وحتى في خصوصية وتميز مرتكبيها، وقد ساهمت عوامل التحضر السريع والرغبة بتحقيق الثراء، وتوافر الفرص لارتكابها في انتشارها، وارتفاع نسبة ضحاياها، خاصة مع قصور وسائل الرقابة، وضعف التشريعات القانونية، وفرض العقوبات لتحجيم تأثيرات هذا النوع من الجرائم المستحدثة، التي تستهدف الأفراد والبيانات والدول وترهق كاهلها بالخسائر الفادحة سواء مادية أو معنوية في مختلف قطاعات الحياة، فهي تمثل حقيقة الاستعمار الإلكتروني في مختلف وأبشع صوره.

الجريمة الإلكترونية هي فعل ينتهك القانون، والذي يرتكب باستخدام تكنولوجيا المعلومات والاتصال لاستهداف الشبكات والأنظمة والمواقع الإلكترونية وتسهيل تسهيل ارتكاب الجريمة، تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث أنها لا تعرف حدودا مادية أو جغرافية ويمكن تنفيذها بجهد أفل وسهولة أكبر وبسرعة أكبر من الجريمة التقليدية (على الرغم من أن هذا يعتمد على نوع الجريمة الإلكترونية).

وقد يستخدم المجرمون في هذا المجال تكتيكات الكترونية مثل البرامج الضارة وتعدد الاختيارات الخبيثة في هذا المجال الذي يعتبر حديث من حيث نوع الجريمة أو أسلوبها كما أن المشرع الجزائري حاول في عدة تويعات التطرق لهذا المجال وتوعية المجتمع أكثر للوقاية منه وتجنب الوقوع فيه.

المبحث الأول: مفهوم الجريمة الالكترونية

مع التطور السريع للتكنولوجيا وازدياد الاعتماد على الوسائل الرقمية في مختلف مجالات الحياة برزت تحديات جديدة في ميدان الأمن والسلوك الاجتماعي كان من أبرزها ظاهرة الجريمة الإلكترونية، لم تعد الجرائم تقتصر على الأطر التقليدية بل اتخذت شكلا جديدا أكثر تعقيدا وسرعة مستغلة الفضاء الرقمي لتوسيع نطاقها وإخفاء آثارها، من هنا أصبح من الضروري فهم مفهوم الجريمة الإلكترونية تحديد خصائصها وأبعادها القانونية والاجتماعية، للتمكن من مواجهتها بفعالية وحماية الأفراد والمجتمعات من آثارها السلبية.

المطلب الأول: تعريف الجريمة الالكترونية

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للإختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع، وسأحاول التعرض لهذه التعاريف من خلال البندين المواليين.

الفرع الاول: تعريف الجريمة الالكترونية لغة

تتكون الجريمة الإلكترونية من كلمتين:

أولا: جريمة: أصلها من جرم بمعنى كسب وقطع والجرم بمعنى الحر، وقيل انها كلمة فارسية معربة والجرم مصدر الجارم الذي يجرم نفسه وقومه شرا، كما تعني التعدي والذنب فالجريمة والجارم بمعنى الكاسب، واجرم فلان أي اكتسب الإثم كما تعني ما يأخذه الوالي من المذنب ورجل جريم وامرأة جريمة أي ذات جرم أي ذات جسم: وجرم الصوت جهارته والجريمة تعني الجناية والذنب[1].

ثانيا: الكترونية: يوصف جزء من الحاسوب وعمله.

الفرع الثاني: تعريف الجريمة الإلكترونية اصطلاحا

هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي، أو الاقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب.[2]

[1] سامية عزيز، مازيا عيساوي، الجريمة من منظور سوسيولوجي الأسباب الآثار، مجلة دراسات في سيكولوجية الإنحراف، المجلد 6 العدد 1، 2021، ص 128.

[2] سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث، ص 04/01.

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات، أو بيانات أو برامج أو محوها، أو كتابتها، أو أي تدخل آخر في محال إنجاز البيانات أو معالجتها وتبعا لذلك تسببت في ضرر اقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب اقتصادي غير مشروع له، أو لشخص آخر.[1]

ودائما حسب أنصار هذا الاتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة.[2] أما البعض من الفقهاء يعرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسوب الآلي الرقمي وشبكة الأنترنت بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف[3] .

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الأسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا نكون أمام جريمة إلكترونية كمن يقوم بالاتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك .

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية". [4]

[1] مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية، العدد 21، 2012، ص 09.

[2] كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية حلب 21/23/ تشرين الأول، 2000، بدون صفحة .

[3] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال جامعة مولود معمري تيزي وزو 06/03/2013، ص 09، نقلا عن كحلوش علي جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني العدد 84، 2007، ص 51.

[4] القانون رقم 09-04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج والعدد 47 .

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات[1] من المادة 394 مكرر إلى 394 مكرر 07، وترك المجال واسع لاي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية،[2] ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية[3].

عـرف المشـرع الجزائـري الجريمة المعلومـاتية فـي نص المـادة 02-الفقرة – أ –من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول بأن "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية**"

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب "**المتعلقة بالجريمة هذه فنعرفها بأنها "كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية**"[4].

---

[1] القانون رقم 04-15 الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66/156، الصادر في 08 جوان 1966 المتضمن قانون العقوبات، ج والعدد 71

[2] سوير سفيان جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة ابوبكر بلقايد، تلمسان، 2010-2011، ص 14.

[3] جازية سليماني، موقع العربي الجديد، تاريخ الدخول،09/02/2017الساعة http//www.ala

[4] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص: إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة، الجزائر، 2019، ص 4.

المطلب الثاني: خصائص الجريمة الالكترونية

تشكل الجريمة الإلكترونية أحد التحديات الحديثة التي فرضها التطور التكنولوجي المتسارع في العالم الرقمي، فهي تختلف عن الجرائم التقليدية من حيث الوسائل والأساليب والمجال الذي ترتكب فيه مما يمنحها خصائص فريدة وتزداد خطورتها مع صعوبة تعقب مرتكبيها واتساع نطاق تأثيرها عبر الحدود.

الفرع الاول: السمات الخاصة بالجريمة الالكترونية

تتميز الجرائم الإلكترونية بجملة من الخصائص لا تتوافر في الجرائم العادية، وكذلك الأمر بالنسبة لمرتكبيها فإن لهم عدة خصائص تميزهم عن المجرمين العاديين، نبين ذلك في التالي:

1. صعوبة اكتشاف الجريمة الإلكترونية

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم.[1]

وبالتالي فإن هذه الجرائم وفي الغالب لا تترك اثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها.

2. الجريمة الإلكترونية عابرة للحدود الزمان والمكان

المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهكذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة. [2]

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الإلكترونية في مكان

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص 31.
[2] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص42.

الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث .[1]

3. جرائم هادئة

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر[2] .

وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[3] .

4. جرائم صعبة الإثبات:

يعد إثبات الجريمة الإلكترونية من الصعوبة بمكان، حيث يصعب تتبعها واكتشافها، فهي لا تترك أثراً يقتفى، حيث تعتبر مجرد أرقام، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً[4] .

ومن جهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الإلكترونية إلى ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبيها.

الفرع الثاني: السمات الخاصة بالمجرم الالكتروني

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005، ص 52.

[2] عبد الفتاح مراد، مرجع سبق ذكره، ص 46.

[3] مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، مقال مقدم إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-2012/09/25، ص 31.

[4] رستم هشام الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة 11 العدد 2، 1999، ص11.

يتميز مرتكب الجريمة الإلكترونية بصفات خاصة تميزه عن غيره من مرتكبي الجرائم الأخرى، وذلك من حيث الآتي:

1. المجرم الإلكتروني ذكي ومتخصص

في الغالب يتميز المجرم الإلكتروني بالذكاء، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية الإلكترونية، حيث يستطيع المجرم الإلكتروني أن يكون تصور كاملا لجريمته حتى لا يتمكن ملاحقته وتتبع أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكومبيوتر، فالمجرم الإلكتروني عادة يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به، لتجنب ما من شأنه ضبط أفعاله والكشف عنه.[1]

كما أنه يتمتع بقدرة ومهارة تقنية يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة في أجهزة الكومبيوتر ومن خلال الشبكات.[2]

2. المجرم الإلكتروني شخص سوي واجتماعي

يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه 1 ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال، أو بهدف الانتقام.

المطلب الثالث: تصنيف وانواع الجريمة الالكترونية

تتنوع الجرائم الإلكترونية بشكل كبير نتيجة لتعدد أهداف مرتكبيها وتطور الوسائل التقنية المستخدمة فيها، ويعد تصنيف هذه الجرائم أمرا ضروريا لفهم طبيعتها وتحديد سبل مواجهتها بفعالية، وتقسم عادة بحسب الدوافع أو الضحايا أو نوع النشاط الإجرامي إلى فئات مختلفة تسهل التعامل القانوني والتقني معها.

[1] طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة، القاهرة، مصر، 2009، ص 177.

[2] محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة عمان الأردن، ص 14.

الفرع الاول: تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة

خطى المشرع الجزائري خطوات كبيرة في مجال مكافحة الجريمة المعلوماتية، يعتبر القانون الجزائري سباقا في مجال مواكبة التشريعات الغربية التي سعت إلى هذا النوع من التجريم كالأمريكي والفرنسي[1]، وذلك بعد أن أقر بتجريم صور الاعتداء على شبكة الانترنت والمساس بالبيانات المعالجة آليا، في إطار أحكام التعديل الذي شمل قانون العقوبات لسنة 2004، بموجب القانون رقم 04-15 المؤرخ في 2004/11/10[2]، في إطار أحكام القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، هذه المواد هي من 394 مكرر إلى 394 مكرر 7، والمتمثلة في الجرائم التالية:

أولا: جريمة الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات (م 394 مكرر/1) أو محاولة ذلك

تنص المادة 394 مكرر على أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك"، لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي، وذلك حين عبر عنه بطريق الغش، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكلها .

وهنا سيتخلص من نص المادة ما يلي:

1. التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.
2. عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات، لكون اعتبارها جريمة وقتية.
3. مجرد المحاولة يعتبر في حد ذاته جريمة حتى وان لم يتحقق فعلا.

ثانيا: جريمة البقاء (م 394 مكرر /1)

بالرجوع إلى نفس المادة السابقة وفي نفس الفقرة 1 فان المشرع قد فرق بين فعل الدخول غير الشرعي والبقاء فيه، وذلك باعتبار كل فعل يعتبر مجرما، فالبقاء قرينة على توفر القصد الجنائي، كما تعتبر جريمة مستمرة، على عكس الجريمة الأولى، غير أن المشرع لم يفرق بين البقاء غير الشرعي أو مجرد المحاولة على غرار الجريمة الأولى .

[1] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 48.

[2] الجريدة الرسمية، عدد 71 المؤرخة في 2004/11/10، ص 8.

ثالثا: جريمة حذف أو تغيير في معطيات المنظومة (م 394 مكرر /2) كنتيجة للدخول غير الشرعي أو البقاء واعتبارهما كجريمتين مضاعفتين

تنص المادة 394 مكرر في فقرتها الثانية على أنه " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة وعليه فان المشرع الجزائري فرق بين عملية حذف البيانات وعملية تغييرها، اللذين يعتبرهما كنتيجة لفعل الدخول غير الشرعي أو البقاء كما اعتبرهما جريمة مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما .

رابعا: جريمة تخريب نظام الاشتغال كنتيجة للدخول غير الشرعي أو البقاء (م394 مكرر/3)

نصت المادة 394 مكرر 3 على أنه "وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج وعلى أساس ذلك لم يعتبر المشرع الجزائري جريمة تخريب نظام الاشتغال جريمة مستقلة بذاتها على غرار الدخول غير الشرعي أو البقاء، بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة.

خامسا: جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش (م 394 مكرر1)

نصت المادة 394 مكرر 1 على أنه يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل " ومنه فان المشرع قد اعتبر أن إدخال معطيات مغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة ، واذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح "الحذف" لاستخدامه ضمن نفس المعنى .

وان ذهبنا إلى المعنى اللغوي فان معنى الحذف هو الإسقاط بينما يعني مصطلحا لإزالة هو الإبعاد من المكان، ومنه فان المشرع قد يكون فرق في الآثار بين الفعلين، فحذف بيانات الكترونية معينة بكون بإسقاطها من موقعها في النظام المستهدف، ولو كان بصفة مؤقتة، مما يعني ظرفيتها وبذلك تكون قابلة للاسترجاع عن طريق برامج من Logiciel de récupération de données électroniques خاصة

صعوبتها، ولكن إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل كامل، لذلك يكون المشرع قد فرق بين الفعلين الإجراميين واعتبر الفعل الأخير أشد وطأة ، لذا فرق بين عقوبة كل فعل مجرم منهما.

الفرع الثاني: تصنيف الجرائم تبعا لدور الكومبيوتر في الجريمة

إن هذا التصنيف يبين أن الكمبيوتر يكون كوسيلة أو هدفا لارتكاب الجريمة والمقصود بأن يكون هدفا هو أن يستهدف الفعل الإجرامي المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر وشبكات الاتصال، والمقصود بأن يكون وسيلة مثل جرائم الاحتيال ببطاقة الائتمان والتزوير وكذلك يكون جسرا لارتكاب جرائم أخرى كالمتاجرة بالمحذرات وغسيل الأموال مثلا، وفي هذا الصدد ينتج عن دور الكمبيوتر في الجريمة مفهومين هما الأول يتعلق بجرائم التخزين و الثاني يتعلق بجرائم المحتوى، والمقصود بجرائم التخزين هو تخزين المواد الإجرامية المستخدمة في ارتكاب الجريمة والناشئة عنها، أما جرائم المحتوى أو ما يعبر عنه بالمحتوى الغير المشروع مثل جرائم المقامرة (القمار) أو جرائم المحتوى الإباحية والغسيل للأموال الإلكتروني[1]، فكلها تنصب على المحتوى الغير المشروع و بهذين المفهومين اللذان يتصلان بدور الكمبيوتر و شبكة الاتصال كبيئة لارتكاب الجريمة المعلوماتية أو في الوقت نفسه كوسيلة لارتكابها، ومع تطور التدابير التشريعية في أوروبا و العالم قسم أغلب المشرعين هذه الجرائم إلى جرائم هدف ووسيلة ومحتوى للكمبيوتر، ومن أهمها اتفاقية بودبست لسنة 2001 [2]، وذلك في إطار خلق نوع من التعامل الدولي في مجال مكافحة الجريمة المعلوماتية، وقد جاء في هذه الاتفاقية ما يلي:[3]

1. الجرائم التي تستهدف العناصر السرية وسلامة المعطيات والنظم وتتمثل في الدخول الغير القانوني وتدمير هذه المعطيات .
2. الجرائم المرتبطة بالكمبيوتر مثل التزوير المعلوماتي .
3. الجرائم المرتبطة بالمحتوى وتضم الجرائم المتعلقة بالإباحية والأفعال الغير الاخلاقية .
4. الجرائم المرتبطة بحق المؤلف والحقوق المجاورة مثل قرصنة البرمجيات.[4]

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2019، ص 64.

[2] اتفاقية بودابست المؤرخة في 23 نوفمبر 2000.

[3] يوسف حسين يوسف، الجريمة الدولية للأنترنت، المركز القومي الإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2011، ص37.

[4] عادل عزام، سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة في وسط الالكتروني، دار الثقافة للنشر والتوزيع، طبعة الأولى، عمان، الأردن، 2011، ص 123.

المبحث الثاني: الجرائم الالكترونية وفق ما جاء به التشريع الجزائري

شهدت الجزائر على غرار باقي دول العالم تطورا ملحوظا في استخدام تكنولوجيا المعلومات، مما أدى إلى ظهور الجرائم الإلكترونية كنوع جديد من التهديدات، هذه الجرائم ترتكب عبر الوسائل الرقمية وتستهدف الأفراد والمؤسسات، وقد استجاب المشرّع الجزائري لهذه التحديات بإصدار قوانين خاصة أبرزها القانون 09-04 لمكافحة هذه الجرائم، ويهدف التشريع إلى حماية المجتمع وتعزيز الأمن السيبراني في ظل التطورات التكنولوجية المتسارعة.

المطلب الأول: جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات

تعد الأنظمة الآلية لمعالجة المعطيات مثل الحواسيب والشبكات المعلوماتية من الركائز الأساسية في تسيير شؤون الأفراد والمؤسسات في العصر الرقمي، ومع تزايد الاعتماد عليها ظهرت جرائم تستهدف هذه الأنظمة كالدخول غير المشروع أو التلاعب بالبيانات أو تعطيل الخدمات، ويولي المشرع الجزائري أهمية بالغة لهذا النوع من الجرائم، حيث أدرجها ضمن نصوص قانونية خاصة تهدف إلى حماية سلامة المعطيات الرقمية وضمان أمن واستقرار المنظومة المعلوماتية الوطنية.

الفرع الأول: جرائم الدخول والبقاء الغير المشروع لأنظمة المعالجة الآلية المعطيات

أن المشرع الجزائري بتجريمه لفعل الدخول المجرد بدون تصريح إلى نظام المعالجة الآلية يكون قد أعتبر جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها البسيطة جريمة شكلية، بحيث يعد هذا السلوك في حد ذاته جريمة ولا يتطلب حدوث أية نتيجة معينة، فمجرد الدخول إلى هذا النظام سواء كان ذلك بقصد الحصول على البيانات أو لغرض التسلية يعد انتهاكا له وإن لم بترتب على ذلك أية أضرار بهذا النظام أو بالمعلومات الموجودة بداخله، كما جرم البقاء في النظام بدون تصريح لمواجهة حالات الدخول عن طريق الخطأ أو السهو أو تجاوز التصريح، وهذا حسب ما جاء في نص المادة 394 مكرر الفقرة الأولى منها.

إلا أنه إذا نجم عن هذا الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية نتائج معينة يترتب على ذلك تشديد العقوبة، وهذا ما يعرف بجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، نص عليها المشرع الجزائري في المادة 394 مكرر الفقرة الثانية والثالثة، والتي أشار فيها إلى النتائج التي يترتب عليها تشديد العقوبة وحصرها في ثلاثة نتائج فقط وهي حذف أو تغيير في معطيات النظام وتخريب اشتغال نظام المعالجة الآلية للمعطيات، أما بالنسبة للمشرع الفرنسي فقد أشار إلى جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة في المادتين 323-

1 الفقرة الثانية و 323-2، في حين تطرقت إليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 6 الفقرة الثانية منها.

وللوقوف على ثنايا هذه الجريمة سوف نقوم بتقسيم هذا المطلب إلى ثلاثة فروع يتناول الفرع الأول الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشدة والفرع الثاني نكرسه للركن المعنوي لهذه الجريمة، أما الفرع الثالث والأخير نخصصه للعقوبات المقررة لهذه الجريمة.

أولا: الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشدة

أن المشرع الجزائري شدد العقوبة في حالة إذا ما ترتب عن الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية نتائج معينة ينجم عنها إحداث أضرارا بالنظام في حد ذاته أو بالمعطيات التي يتضمنها، وذلك طبقا للمادة 394 مكرر الفقرة الثانية والثالثة منها، والتي تنص على ما يلي تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة .

وإذا ترتب على الأفعال المذكورة تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج[1].

وذهبت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في نفس الاتجاه في المادة 6 الفقرة الثانية منها بقولها تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

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

ب- الحصول على معلومات حكومية سرية[2].

أما بالنسبة للمشرع الفرنسي نص على هذه الجريمة في المادة 323-1 الفقرة الثانية من قانون العقوبات الفرنسي، والمعدلة بموجب القانون رقم 912-2015 الصادر بتاريخ 2025/07/24، والتي نصت على ما يلي ".. وإذا نجم عن هذا السلوك محو أو تعديل المعطيات المختزنة في النظام أو إتلاف تشغيل النظام تكون العقوبة الحبس ثلاث سنوات والغرامة مقدارها 100000 يورو[3]، ونص كذلك على إفساد تشغيل نظام المعالجة

[1] المادة 394 مكرر الفقرة الثانية والثالثة من القانون رقم 04-15

[2] المادة 6/2 من الاتفاقية العربية لمكافحة تقنية المعلومات لسنة 2010

[3] Article 323-1/2: Lorsqu 'il en est résulté soit la suppression ou la modification de données contenues dans le système, sait une altération du fonctionnement de ce système, la peine est de trois ans

الآلية للبيانات كجريمة مستقلة في المادة 323-2 من قانون العقوبات الفرنسي المعدل، والتي نصت على ما يلي " تعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس لمدة خمس سنوات وبغرامة قدرها 150000 يورو"[1].

وهو ما ذهبت إليه العديد من التشريعات بإفراد هذا السلوك كجريمة مستقلة كالمشرع السعودي في المادة الخامسة[2] الفقرة الثانية والثالثة من نظام مكافحة جرائم المعلوماتية رقم 17 لسنة 2007، والمشرع الإماراتي في المادة 8[3] من مرسوم بقانون اتحادي رقم (5) لسنة 2012، السالف الذكر، وكذلك القانون العربي الإسترشادي النموذجي لمكافحة جرائم تقنية المعلومات في المادة17[4] منه، بينما البعض الآخر من التشريعات نص عليها ضمن النصوص الخاصة بالإتلاف كالمشرع الأمريكي في المادة (1030) أ من القانون الفيدرالي إتلاف المعلومات الذي يترتب عليه تعطيل أنظمة الحاسبات الآلية التابعة إلى الحكومة، واتجه كذلك القضاء

الإنجليزي إلى تطبيق نص المادة الثالثة من قانون إساءة استخدام الحاسبات الآلية لسنة 1990 والذي جاء خاليا من نص خاص يجرم تعطيل أو إفساد النظام المعلوماتي – والخاصة بإتلاف المكونات المنطقية للحاسب الآلي على تعطيل (إعاقة) النظام المعلوماتي مستندين في ذلك على ما أشارت إليه الفقرة الثانية من هذه المادة التي تقضي أن اتجاه الجاني إلى تعطيل (إعاقة) نظام الحاسب الآلي تتوافر به نية إحداث تغيير

---

d'emprisonnement et de 100 000 € d'amende, modifié par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[1] Article 323-3; Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € D'amende, modifié par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

[2] تنص المادة 5 الفقرة الثانية والثالثة من نظام مكافحة جرائم المعلوماتية السعودي رقم 17 لسنة 2007 على أنه " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: 1...2 إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها.

[3] تنص المادة 8 من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، على أنه " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلوماتي إلكتروني"، أنظر: مرسوم بقانون اتحادي رقم (5) لسنة 2012.

[4] تنص المادة 7 من القانون العربي الإسترشادي النموذجي لمكافحة جرائم تقنية المعلومات، على أنه " كل من أعاق أو شوش أو عطل عمدا أو بأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب وما في حكمها الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس... "، أنظر: قرار رقم 417 بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية، جامعة الدول العربية الدورة 21 لسنة 2004

في محتوى الحاسب الآلي مما يعد مكونا لجريمة الإتلاف[1]، والى جانب ذلك اتجه جانب آخر إلى إدراجها ضمن النصوص الخاصة بالدخول بدون تصريح إلى نظام المعالجة الآلية كما فعل المشرع الجزائري، والذي برر البعض موقفه بعدم النص على جريمة تعطيل أو إفساد النظام المعلوماتي للتشابه الكبير بينها وبين جريمة الاعتداء على المعطيات، والتي يصعب بحسب هذا الرأي التمييز بينهما، ذلك لإن الأفعال التي تتضمنها جريمة الاعتداء على المعطيات تؤدي هي الأخرى إلى تعطيل النظام أو فساده[2].

وان الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة يتكون من عناصره الثلاث، والمتمثلة في السلوك الإجرامي (الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية) والنتيجة الإجرامية (حذف أو تغيير في معطيات النظام أو تخريب نظام اشتغاله) والعلاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية المحددة أفعالها على سبيل الحصر في المادة 394 مكرر في الفقرة الثانية والثالثة من قانون العقوبات الجزائري وهي:

1. **حذف المعطيات:** وهو الفعل الذي يشير إلى إزالة المعلومات الموجودة داخل نظام المعالجة الآلية، وهو أقصى أنواع الضرر .
2. **تغيير المعطيات:** وهو الفعل الذي يشير إلى إحداث تعديلات في المعلومات فحسب دون أن يصل الأمر إلى إزالتها، بحيث تظل المعلومة موجودة ولكن بدون معنى ولا فائدة .
3. **تخريب نظام اشتغاله:** وهو الفعل الذي يتم عن طريق ممارسة بعض الأفعال على النظام من شأنها جعله غير قابل للاستخدام أو للاستعمال[3].

وان حدثت إحدى هذه النتائج نتيجة فعل آخر فلا نكون أمام هذه الصورة المشددة من الجريمة بل البسيطة لتحقق فعل الدخول أو البقاء فقط، وعليه فإذا أثبت الجاني انتفاء العلاقة السببية بين فعله والنتيجة التي تحققت لم تقم الجريمة، كتدخل عامل آخر حادث مفاجئ أو قوة قاهرة[4].

كما أن نتيجة حذف أو تغيير معطيات النظام هي النتيجة ذاتها المتطلبة في جريمة التلاعب بالمعطيات، وتتمثل في تغيير حالة المعطيات غير إن الفرق بينهما في جريمة التلاعب تقع إرادية أي يريدها

[1] دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية–دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ط 1، 2016، ص 251.

[2] دلخار صلاح بوتاني، مرجع سبق ذكره، ص 249.

[3] بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، لبنان، ط 1، 2012، ص 231.

[4] جدي نسيمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013، ص 59.

الفاعل أو يقبلها على الأقل، بينما في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة لا تقع كذلك، إذ لا يريدها الفاعل وهي تفرقة تتعلق بالركن المعنوي ولا شأن لها بالنتيجة التي هي من عناصر الركن المادي.

أما النتيجة الأخرى التي أعتد بها المشرع في تشديد عقوبة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة هي تخريب اشتغال نظام المعالجة الآلية للمعطيات، وهي النتيجة ذاتها التي تتطلبها جريمة إفساد نظام المعالجة الآلية للمعطيات المنصوص عليها في المادة 323-2 من قانون العقوبات الفرنسي، وما يفرق بين النتيجتين هو الإرادة، إرادة النتيجة في جريمة إفساد نظام المعالجة الآلية للمعطيات وعدم إرادتها في جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة، وهي أيضا تفرقة لا علاقة بالنتيجة في حد ذاتها بل تتعلق بالركن المعنوي أي بالموقف النفسي للفاعل من هذه النتيجة[1].

وفضلا عن ذلك، فإن حصر المشرع الجزائري لهذه النتائج الثلاثة لا يعني أنه لا توجد أضرار أخرى قد تترتب على فعل الدخول أو البقاء المشدد بل هناك العديد من أشكال النتائج الضارة التي قد تصيب المعلومات في بيئتها التقنية، مما قد يصعب حصرها، إلا أن المشرع الجزائري قد تناول أخطرها جسامة وأغلبها وقوعا في هذه البيئة، وتبعا لذلك فإن حدثت نتائج أخرى غير هذه النتائج لا يبقى أمام المتضرر إلا أن يطالب بالتعويض وفق ما تقتضيه قواعد المسؤولية المدنية.[2]

ثانيا: الركن المعنوي

إن النتيجة المشددة التي نصت عليها الفقرة الثانية من المادة 323-1 من قانون العقوبات الفرنسي والفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات الجزائري هي نتيجة غير عمدية، وأن أول ما يتبادر إلى الذهن من خلال نص هذه المادة الأخيرة بفقرتيها الأولى والثانية أن الظرف المشدد هو من الظروف المشددة المادية التي لا تغير من وصف الجريمة، والتي تقوم بمجرد قيام الركن المادي له وهو حدوث النتيجة المشددة وارتباطها بفعل الدخول أو البقاء برابطة سببية، أي أن المسؤولية عن هذا الظرف المشدد هي مسؤولية

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص 161.

[2] بوكر رشيدة، مرجع سابق، ص 233.

مادية موضوعية" تقوم بمجرد توافر الركن المادي، وهي لا تقوم إلا إذا حصلت النتيجة المشددة عن طريق قوة قاهرة[1].

وهو الأمر الذي وجد معه البعض من الفقه أن تلك الجريمة المنصوص عليها في المادة 323-1 الفقرة الثانية من قانون العقوبات الفرنسي، بقولها أنه".. وإذا نجم عن هذا السلوك محو أو تعديل المعطيات المختزنة في النظام أو إتلاف تشغيل النظام تكون العقوبة الحبس ثلاث سنوات والغرامة مقدارها 100000 يورو[2]، تقع بطريق الخطأ في التشريع الفرنسي ولا يتطلب المشرع فيها تطلب القصد الجرمي بحيث أن الخطأ يعد كافيا لقيام الجريمة، ومن تم فإن هذه الجريمة تعد من جرائم الإهمال، وبالتالي فمجرد ارتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذا استطاع الجاني إثبات حدوث قوة قاهرة أدت إلى حدوثها، والأمر ذاته ينطبق على المادة 394 مكرر في فقرتها الثانية والثالثة من قانون العقوبات الجزائري.

وعليه فإنه لا يمكن تطبيق الظرف المشدد إذا قصد النتيجة المشددة لإن ذلك يقع مباشرة تحت طائلة المادة 394 مكرر 1 من قانون العقوبات الجزائري والمادة 323-3 من قانون العقوبات الفرنسي والمتعلقتين بجريمة التلاعب بالمعطيات والتين تضمنتا فعلي التعديل والإزالة العمديين[3].

أما بالنسبة لظرف التشديد المتعلق بتخريب نظام اشتغال نظام المعالجة الآلية للمعطيات المنصوص عليه في الفقرة الثالثة من المادة 394 مكرر من قانون العقوبات الجزائري، فهو يتعلق بنتيجة لا تقع في القانون الجزائري إلا غير عمدية أي كظرف تشديد فقط، ولا تقع عمدية على الإطلاق، أما في القانون الفرنسي فقد تقع هذه النتيجة كظرف تشديد غير عمدي (المادة 323-1 من قانون العقوبات الفرنسي) أو كجريمة خاصة عمدية وهي جريمة إعاقة أو إفساد نظام المعالجة الآلية، والتي نصت عليها المادة 323-2 من قانون العقوبات الفرنسي[4].

وكموقف للقضاء الجزائري عن جريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية في صورتها المشددة تمكنت فرقة الجرائم المعلوماتية لأمن ولاية الجزائر من توقيف المشتبه فيه المقيم بولاية باتنة شرق البلاد المتورط في قضية الدخول عن طريق الغش لنظام المعالجة الآلية مع البقاء والتغيير وحذف

---

[1] محمد خليفة، مرجع سبق ذكره، ص 169.

[2] Article 323-1/2 Lorsqu 'il en est résulté soit la suppression ou la modification de données contenues dans le système, sait une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende, modifié par LOI N° 2015-912 du 24 JUILLET 2015-ART 4JORF N° 0171 du 26 JUILLET 2015.

[3] بوكر رشيدة، مرجع سابق، ص 241.

[4] محمد خليفة، مرجع سبق ذكره، ص 170.

معطيات مخزنة من أجل الإضرار وتعطيل منظومة الإعلام الآلي والموقع الإلكتروني المؤسسات اتصالات الجزائر، وذلك فور تقديم شكوى من قبل الممثل القانوني لذات المؤسسة، حيث أسفرت التحريات عن تحديد هوية المشتبه فيه، الذي يقيم بولاية باتنة، وتم التوصل إليه بعد إذن تمديد الاختصاص، وبالتنسيق مع فرقة مكافحة الجرائم المعلوماتية لأمن ولاية باتنة، تم تفتيش مسكنه أين حجزت دعائم رقمية استعملت في عملية القرصنة ممثلة في هاتفين نقالين وجهاز إعلام آلي محمول ووحدة مركزية بلواحقها وقرص صلب خارجي وقرصين داخليين، وقد تم تقديم المشتبه فيه إلى وكيل الجمهورية المختص إقليما الذي اتهمه وفقا للمادة 394 مكرر 1 فقرة وفقرة 3[1].

الفرع الثاني: جرائم المساس بالأنظمة الآلية لمعالجة المعطيات

حاول المشرع الجزائري خلال الفترات الأخيرة من الزمن تدارك الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني، فقام بتعديل أحكام قانون العقوبات الجزائري، بموجب القانون رقم 04-15[2]، مستحدثا فيه مجموعة من النصوص التي جرم من خلالها كل الأفعال والسلوكات المرتبطة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها جزاء.

ويمكن الإشارة قبلها، إلى تعريف الجريمة المعلوماتية أو الجريمة السبيرانية أو جريمة الفضاء الالكتروني مثلما يسميها البعض، وهي جريمة يستخدم الحاسوب في ارتكابها، وهي عبارة عن مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وسواء كان ذلك بطريقة مباشرة أو غير مباشرة، والمهم في ذلك هو استخدام وسائل الاتصال الحديثة بشأنها من كمبيوتر، أو أية آلة ذكية أخرى.

وتتميز الجريمة المعلوماتية عن الجريمة التقليدية من حيث تعريفها، وخصائصها، وأركانها، وكذا القانون وجب تطبيقه عليها.

وتجدر الإشارة إلى أن جريمة الاعتداء على نظام المعالجة الآلية للمعطيات تتحقق في صورتين:

تبرز الأولى في جريمتي الدخول والبقاء غير المرخص بهما في النظام، وبينما تظهر الصورة الثانية في تلك النتائج غير المشروعة ضد معطيات النظام المترتبة عن فعل الدخول أو البقاء.

[1] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) -دراسة مقارنة-، دار الخلدونية، الجزائر، 2018، ص 143.

[2] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يتضمن قانون العقوبات، جريدة رسمية عدد 71 لسنة 2004 معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 07، المضافة بموجب القانون نفسه.

أولا: الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

تتمثل الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما .

1. الدخول غير المرخص به

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنه: "**يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 500000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك**".

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

كما يفهم من البند نفسه أن المشرع لا يعاقب على الفعل الكامل، أي على الجريمة التامة، وإنما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة الإجرامية والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألا يكون الدخول صدفة أو خطأ.

وتجدر الإشارة هنا، إلى أن المشرع الجزائري لم يشترط في البند أعلاه، طبيعة خاصة لهذا النظام، أي أن المادة 394 مكرر لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية وبدون أي استثناء.

وبذلك يكون مشرعنا قد أصاب بشكل كبير في تنظيمه لهذه المسألة، حيث وبتمييز المشرع بين تجريم الدخول غير المرخص به إلى نظام معلوماتية محاط بحماية فنية وعدم التجريم للدخول غير المرخص به إلى نظام غير محاط بحماية فنية، سيؤدي حتما إلى فتح المجال للمجرمين من التهرب من المسؤولية الجزائية عن

فعل الاعتداء، بحجة أن النظام المعتدى عليه غير محاط بحماية فنية، وبذلك، فيكون المشرع قد أحسن فعلا عندما لم يفصل بين النظام المحاط بالحماية الفنية، وذلك النظام غير المحاط بها[1].

2. البقاء غير المرخص به

يقصد بالبقاء غير المرخص به هنا الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص[2].

ولقد سوى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وذلك على غرار ما اتخذه المشرع الفرنسي في منظومته الجزائية، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة (03) أشهر إلى سنة، وغرامة مالية من 50000 دج إلى 100000 دج ويعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يحتمل صورتين مختلفتين هما:

أ. تتمثل الصورة الأولى في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى وإن كان خطأ أو صدفة، غير انه وبتفطن الفاعل للوضع وبدلا من الانسحاب أو مغادرة النظام فورا، فإنه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.

ب. بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشأن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله.

والإشكال الذي يمكن أن يثيره هذا الاجتماع والتداخل للسلوكين من دخول إلى النظام والبقاء فيه، هو تحديد النطاق الزمني لكل واحدة منها، بمعنى متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟

ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة

[1] عمار حشمان، مرجع سبق ذكره، ص 25.

[2] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص 102.

البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام[1].

ومهما يكن من أمر، فإن المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى الدخول ثم إلى البقاء، وكأن المشرع يصنف الأولى بجريمة وقتية كون فترة استمرارها قصيرا جدا والأخرى بجريمة مستمرة، مقارنة بالأولى.

ثانيا: الصور المشددة للاعتداء على نظام المعالجة الآلية للمعطيات

يشدد المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، وذلك بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات التي تنص أنه: "... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج".

تبعا لذلك، فإن المادة تحدد ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية وهما:

1. حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام.
2. ويتحقق الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته.

وتجدر الإشارة هنا إلى أن الصورة البسيطة للاعتداء على النظام المحددة في المادة 394 مكرر 01 السابقة لم تشترط البحث في النتيجة الإجرامية، بينما وباستقرار الفقرة 02 من المادة 394 مكرر يفهم أن النتيجة الإجرامية واجبة الإثبات، فيجب إثبات المحو أو التعديل أو التخريب للإقرار بالصورة المشددة للجريمة[2]، وإلا كنا بصدد الصورة الأولى والبسيطة لا أكثر.

ولقد أصاب المشروع مجددا في تشديده للعقاب هنا، والهدف طبعا هو الحد من تفاهم الإجرام المعلوماتي وما يرتبه من أضرار بالغة ووخيمة على الفرد والمجتمع والدولة ككل.

المطلب الثاني: الجرائم الالكترونية الواقعة على الأموال.

أصبحت الجرائم الإلكترونية التي تستهدف الأموال من أخطر مظاهر الجريمة الحديثة نظرا لاعتماد المعاملات المالية بشكل متزايد على الوسائط الرقمية، وتشمل هذه الجرائم أفعالا كالاحتيال الإلكتروني والاستيلاء

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 28.

[2] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى عين مليلة، الجزائر، 2010، ص 123.

على حسابات بنكية واختراق نظم الدفع عبر الإنترنت، ونظرا لخطورتها وتناميها، سعى المشرّع الجزائري إلى تجريم هذا النوع من السلوكيات من خلال إدراجها ضمن القوانين الخاصة بمكافحة الجرائم الإلكترونية، بهدف حماية الممتلكات والأموال العامة والخاصة في البيئة الرقمية.

الفرع الأول: جرائم التحويل الغير مشروع للأموال أو جرائم الاحتيال الالكتروني

إن التطور الهائل لشبكات التواصل الاجتماعي، تطور الخدمات التي تمتاز بها جعل لذوي البيئة الاجرامية يجدون طرقا جديدة من أجل الاعتداء على الأموال والممتلكات بصورة ذكية وحضارية وصعبة الاكتشاف.

أولا: النصب والاحتيال

طرق النصب والاحتيال أصبحت تتغير وتتنوع بين فترة وأخرى، وقد أصبحت العملات الرقمية الوهمية والألعاب الإلكترونية، والتجارة الإلكترونية غير المنظمة، وعروض المشاركة والمساهمة والاستثمار في مشاريع تدر أرباحا شهرية خيالية، وعروض شراء الأسهم في شركات وهمية تحت مسميات كاذبة، من أكثر وسائل النصب والاحتيال على المستخدمين والمتفاعلين على منصات التواصل الاجتماعي، ولقد بدأت الدول تشدد في وضع قوانين وتشريعات للراغبين في إطلاق مثل هذه الأعمال بشكل عام، ومع ذلك فإن هناك طرقا وأساليب جديدة كل يوم يستخدمها (الهاكرز)، وأصحاب الخبرات المالية البنكية والعاملون في الاستثمارات الوهمية[1].

عرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جريمة الإحتيال بأنه التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الإحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو الغير، عن طريق :

1. إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
2. التدخل في وظيفة أنظمة التشغيل وأنظمة الإتصالات أو محاولة تعطيلها أو تغييرها.
3. تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

من خلال تصفح شبكات التواصل الاجتماعي خصوصا الفايسبوك أو الإنستغرام مثلا نصادف العديد من الإعدادات والمتاجر الإلكترونية لعرض العديد من الخدمات وسلع مجهولة المصدر والتي تكون غالبيتها غير حقيقة للإيقاع بكثير من الأشخاص من أجل التسويق الشبكي لاستغلال الشباب بحجة الحصول على وظيفة لتحقيق الثراء السريع، وهناك تقارير تفيد بأن 3.5 مليون مستخدم تكبدوا خسائر تقدر بـ 3.2 مليار

[1] بسام الزعبي، النصب والاحتيال عبر منصات التواصل الاجتماعي، مقال منشور على الإنترنت www.alrai.com تاريخ النشر: 2022/02/19 10:29 تاريخ الإطلاع: 2025/03/10، ساعة 14:30.

دولار بسب الإعلانات الوهمية عبر البريد الإلكتروني باستغلال بوابة البنوك، وهذه المعلومات يسيء استخدامها المحتالون على شبكة الإنترنت من خلال إجراء مزاد وهمي أو عرض تأشيرات وهمية مزورة وقد يستغل الفايسبوك في التعرف إلى بيانات الأشخاص من خلال معلوماتهم وجهات الاتصال الخاصة بهم، وعناوين البريد الإلكتروني ثم يتم إرسال العديد من رسائل البريد المزعج إليهم ويسبب لهم خسائر ناجمة عن هذه الأفعال[1]، فهدف هؤلاء المجرمين هو تلقي أرباح وأموال عن كل فرد جديد يلتحق بهم، وبرغم من اختلاف التسميات إلى أن النتيجة واحدة هو النصب والاحتيال على الأشخاص لجني أموال من دون تعب أو جهد ومن دون وجه حق مستغلين ميزة التخفي أو فتح صفحات بأسماء مستعارة ووهمية أو انتحال الشخصيات، وتشير الإحصائيات المختلفة على أن غالبية الأشخاص الذين تعرضوا للنصب والإحتيال عبر شبكات التواصل الإجتماعي تتراوح أعمارهم ما بين 18-39 سنة، أي أنهم ليسوا من كبار السن مثلا الذين قد تنقصهم الخبرة في التكنولوجيا ودهاليزها بشكل عام، وخير مثال على هذا القضية التي شغلت الرأي العام في الجزائر في العام الماضي حين قام بعض الأشخاص بإنشاء شركة وهمية و بإشتراك مع أشخاص معروفين على شبكات التواصل الإجتماعي الذين يطلقون على أنفسهم تسمية (المؤثرين) باستغلال فضاء التواصل الإجتماعي للنصب والإحتيال على مجموعة من الطلبة الجامعيين بإيهامهم بأن يساعدونهم للانتقال لإكمال دراستهم في إحدى الجامعات الأوربية (جامعة أكرانيا) وهذا ما كلف هؤلاء الطلبة مبالغ مالية معتبرة دون أن ينالوا مبتغاهم.

مثل هذه التجاوزات الماسة بأموال الأفراد عاقب عليها المشرع الجزائري بموجب المادة 371 (معدلة) من قانون العقوبات الجزائري حيث نص على أن: كل من تحصل بطريق التهديد كتابة أو شفاهه أو إفشاء أو نسبة أمور شائنة على أموال أو أوراق مالية أو على توقيع على المحررات المبين في المادة 370 أو شرع في ذلك يكون قد ارتكب جريمة التهديد بالتشهير ويعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20.000 دج إلى 100.00 دج".[2]

كما نصت المادة 372 فقرة 01 من نفس القانون على ما يلي: " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إيراد من الالتزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان بالاحتيال لسلب ثروة الغير أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو الأمل بالفوز بأي شيء أو في وقوع حادث أو أي

[1] خالد حامد مصطفى، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الإجتماعي، كلية القانون، جامعة عمان، 2013، ص 12.

[2] القانون رقم 06-23 مؤرخ في 20 ديسمبر 2006، المعدل والمتمم، الجريدة الرسمية عدد 84، الصادرة في 24ديسمبر 2006، المعدل والمتمم

واقعة أخرى وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 20.000 دج إلى 100.000 دج [1].

من خلال نص المادتين المذكورتين نستنتج أن المشرع الجزائري عاقب على الإحتيال وسلب أموال الغير كما عاقب على مجرد الشروع فيه بأي وسيلة كانت، وعلى الرغم من أنه لم يذكر من خلال نص المادتين الجرائم الحديثة المرتكبة عبر شبكات التواصل الإجتماعي لكن ذكرها بشكل عام ونفهمها من سياق الكلام من خلال ذكره كلمة بأي "وسيلة كانت"، كما ندعوه إلى استحداث مواد جديدة ومواكبة الجرائم الحديثة خاصة الواقعة عبر الشبكات الاجتماعية.

الفرع الثاني: جرائم الاستخدام غير المشروع لأدوات الدفع الالكتروني

قد يقع الاستعمال غير المشروع لبطاقات الدفع من طرف الغير وذلك عن طريق سرقتها أو العثور عليها واستعمالها أو تزويرها وتقليدها وهو ما سنتناوله تبعا.

أولا: المسؤولية الجزائية للغير عن سرقة بطاقات الدفع الإلكتروني أو العثور عليها واستعمالها

من بين الجرائم الواقعة على بطاقات الدفع الإلكتروني سرقتها أو العثور عليها واستعمالها بعد الحصول على الرقم السري فما هو التكييف القانوني لهذه الجريمة؟

1. المسؤولية الجزائية للغير عن سرقة بطاقات الدفع الإلكتروني:

جريمة السرقة كما سبق وأن ذكرناها هي اختلاس شيء مملوك للغير وهو ما ينطبق على سرقة بطاقات الدفع الإلكتروني كون هذا الفعل يتوافر على جميع أركان جريمة السرقة من الركن المادي وهو اختلاس شيء مملوك للغير وركن معنوي كون السرقة من الجرائم العمدية، كما أنه قد تتم السرقة عن طريق شبكة الإنترنيت وذلك بسرقة أرقام بطاقات الدفع، وكذا عن طريق الاختراق غير المشروع لمنظومة خطوط الاتصالات العالمية أو ما يعرف بـ illegal-acces وقرصنته"[2].

غير أنه وبالرجوع إلى قانون العقوبات الجزائري يشرط لقيام جريمة السرقة وقوعها على منقول وبالرجوع إلى تعريف المنقول نجده ينطبق كذلك على المال المعنوي وهو محل خلاف فقهي فمنهم من يعتبره منقولا ومنهم من لا يعتبره كذلك[3].

[1] المادة 372 ق.ع.ج.

[2] بلعالم فريدة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقة الائتمان، مذكرة ماجستير تخصص قانون الأعمال، قسم الحقوق، جامعة محمد لمين دباغين سطيف، ص 141.

[3] بلعالم فريدة، مرجع سبق ذكره، ص 146.

2. المسؤولية الجزائية للغير عن استعمال بطاقات الدفع المسروقة أو المفقودة:

ينسب لمستعملها في هذه الحالة عدة جرائم جريمة السرقة كون الفعل يتوافر على جميع أركانها وكذا جريمة النصب لاستعمال اسم كاذب وطرق احتيالية وهو ما استقرت عليه محكمة الجنايات الفرنسية، بالإضافة إلى جريمة التزوير وذلك لتزوير التوقيع عند السحب أو الوفاء[1].

ثانيا: المسؤولية الجزائية للغير عن تزوير أو تقليد بطاقات الدفع الإلكتروني

تتعرض البطاقات الإلكترونية كغيرها من المستندات والمحررات إلى التزوير المادي بمختلف أشكاله وطرقه سواء كان التزوير جزئيا كالتغيير في إحدى بيانات البطاقة، أو كليا وهو ما يسمى بالاصطناع، من خلال اصطناع نماذج واستخدامها في الوفاء أو السحب يهدف الاستيلاء على أموال الغير[2].

1. مدى توافر صفة المحرر في بطاقات الدفع الإلكتروني:

هي محل اختلاف فقهي حيث يرى البعض أن التزوير يقع على محررات رسمية واضحة البيانات وترى بالعين المجردة، وأخرجوا بطاقات الدفع من ذلك .

أما جانب آخر فيرى أن التزوير يقع على البطاقات كذلك كون المعلومات الإلكترونية قد يطالها التحريف .

2. مدى توافر أركان جريمة التزوير في بطاقات الدفع:

بالنظر إلى أركان جريمة التزوير والتي تقوم على ركنها المادي والمتمثل في تحريف الحقيقة وكذا التزوير بالطرق المحددة قانونا إضافة إلى الركن المعنوي المتمثل في العلم والإرادة وهي أركان تتوفر في التزوير في بطاقات الدفع الإلكتروني[3].

غير أنه وفي غياب نصوص جزائية واضحة يصعب التطبيق سواء في جريمة التزوير أو النصب أو خيانة الأمانة وتبقى أراء فقهية لا يعتمد عليها تطبيقا لمبدأ الشرعية لا جريمة ولا عقوبة إلا بنص.

3. العقوبة المقررة لجريمة التزوير:

حدد المشرع الجزائري عقوبة التزوير في المحررات العرفية أو التجارية أو المصرفية بالحبس من سنة إلى خمس سنوات وبغرامة من 20.000 دج إلى 100.000 دج بالإضافة إلى العقوبات التكميلية كحرمان

[1] بلعالم فريدة، مرجع سبق ذكره، ص 155.

[2] ذبيح هشام، وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني، مجلة الاجتهاد القضائي، العدد 14، جامعة بسكرة، 2017، ص115.

[3] بلعالم فريدة، مرجع سبق ذكره، ص 158.

الجاني من حق من الحقوق الوطنية وبالمنع من الإقامة من سنة إلى خمس سنوات، كما تضاعف العقوبة إذا كان الجاني أحد موظفي المصارف أو مدير شركة.[1]

كما يعاقب كل من اعتدى على أنظمة المعالجة الآلية للمعطيات باختراقها بعقوبة تتراوح بين الحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج وتضاعف العقوبة إذا تم حذف أو تغيير للمعلومات، ومن سنة أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج إذا ترتب على الاختراق تخريب النظام[2].

وإذا ترتب عن الدخول إلى نظام المعلومات إدخال بطريق الغش معلومات أو أزالها يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500,000 دج إلى 4.000.000 دج.[3]

وإذا تم استغلال المعلومات في الاتجار أو التصميم أو النشر يعاقب الجاني بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 10.000.00 دج[4]، وتضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ويعاقب كذلك الشخص المعنوي على ارتكابه لهذه الجرائم بغرامة تعادل خمس مرات الحد الأقصى المقررة للشخص الطبيعي[5].

ونشير إلى أن النصوص الجزائية التي تعاقب على المساس بأنظمة المعلومات جاءت عامة ولم توضع طبيعة الأنظمة وما تحتويه من وسائل كبطاقات الدفع الإلكتروني مما يصعب تطبيق هذه النصوص في أرض الواقع لإمكانية عدم مطابقة النص للواقعة هو ما سيطرح الكثير من الإشكالات العملية.

الفرع الثالث: جرائم الاعتداء على الملكية الفكرية

نظر الفقه في مدة الحماية التي يعطيها القانون للمصنفات ضمن حقوق الملكية الصناعية ومنها الاختراعات عموما، فرأى فيها مددا طويلة جدا لا تتناسب مع برامج الحاسب الآلي، من حيث إخضاعها لهذه المدة، ذلك أن الفكر الإنساني والحاجة لديه لا تتناسب مع مدد الحماية الطويلة، فيما يتعلق ببرامج الحاسب الآلي خاصة، إذ لا تقبل منطقيا أن توضع برامج الحاسب الآلي ضمن مدد الحماية الطويلة، وإيقاف المد الفكري التطويري حولها، خصوصا مع ازدياد الحاجات الشبه اليومية لبرامج حاسب آلي جديدة متطورة، ضمن

[1] المادة 219 من قانون العقوبات الجزائري.

[2] المادة 394 مكرر من قانون العقوبات

[3] المادة 394 مكرر1 من قانون العقوبات

[4] المادة 394 مكرر2 من قانون العقوبات

[5] المادة 394 مكرر4 من قانون العقوبات

فئات ونواح حياتية صناعية، تجارية وثقافية متعددة، فكان أثر ذلك الانحراف بالحماية الجزائية لبرامج الحاسب الآلي من قوانين الملكية الصناعية والدخول بها حيز قوانين حق المؤلف"[1].

مع تقدم عصر الثورة الرقمية ، طفت إلى السطح تحديات تتناسب مع هذا التطور فقد برزت مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية ، وهي تلك الملكية التي تنصب على برامج الحاسوب وبيانتها والمصنفات الرقمية المنشورة على شبكة الانترنت التي بذل في إنتاجها وجمعها وإظهارها جهد فكري إبداعي جعل من الواجب حمايتها، كحق ملكية فردية وجماعية أن مسيرة التحول نحو مجتمع المعلومات تقضي السماح للأفراد بالنفاذ إلى هذه المعلومات مع كفالة حماية حقوق المؤلفين بمظاهر حماية حديثة تشمل الملكية الرقمية .

أولا: تعريف المصنفات الرقمية

يعرف المصنف الرقمي بأنه كل: "مصنف إبداعي، عقلي، ينتمي إلى بيئة تقنية المعلومات". فبرنامج الحاسوب مصنف رقمي، وكذلك قاعدة البيانات وطوبوغرافيا الدوائر المتكاملة باعتبار لها نتائج تطور علم الحاسوب، بخلاف أسماء وعناوين الانترنت والبريد الالكتروني التي تعتبر من المصنفات التي ارتبط ظهورها بشبكة الانترنت.

وتصنف المصنفات عموما بطابع الأصالة أما من حيث الإنشاء أو التعبير أي انه نتاج ذهني بطابع معين يبرز شخصية صاحبه سواء في مضمون وجوهر الفكرة أو في مجدد طريقة عرضها.

ثانيا: صور الجرائم المعلوماتية الواقعة على المصنفات الرقمية

اهتمت غالب التشريعات بوضع نصوص تحرم المساس بالحقوق المعنوية والفكرية للغير وبالتالي تضمن للمصنفات الحماية القانونية اللازمة، ومنها المصنفات الرقمية من كافة أنواع الاعتداء وهو ما تكلفت به وعلى نحو مفصل ودقيق اتفاقية بودابست لمكافحة الجريمة المعلوماتية وهو ما دعمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة2010.[2]

وهي الجهود التي توجها المشرع الجزائري حيث أشار إلى مفهوم المصنفات الرقمية في الأمر 08/03 المؤرخ في 2013/07/19 في نصوص المواد 02-03-04-05،[3] إضافة إلى نص المادة 03 والمادة 27

[1] أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الاردن، 2014، ص 197.

[2] أسامة احمد المناعسة، جلال محمد الزعبي، مرجع سبق ذكره، ص 197.

[3] الامر 08/03، المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة بتاريخ 2003/07/23، الجريدة الرسمية رقم 36 ص 44.

من الأمر 05/03 المؤرخ في 2003/07/19[1]، أن كل هذه النصوص يجسد مفاهيم جرائم النقدي على المصنفات الرقمية.

فجرائم المعلوماتية هي أكثر الجرائم مساسا بحق المؤلف من خلال ما يعرف بجرائم التقليد (La Contrefaçon) مثل جرائم التحميل غير المشروع عبر شبكة الانترنت، فملايين المتصفحين لشبكة الانترنت اعتادوه على تحميل الأفلام والموسيقى دون شرائها من مصدرها الأساسي، مستقلين في ذلك برامج متخصصة في فك شفرات الحماية، وذلك أما بغرض استعمالها الشخصي أو بغرض إعادة نشرها، وطرحها، للغير على شبكة الانترنت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة.

المطلب الثالث: جرائم التعدي على الاشخاص

تعد الجرائم الإلكترونية الواقعة على الأشخاص من أخطر أشكال الاعتداءات في الفضاء الرقمي إذ تمس بحقوق الأفراد وكرامتهم وحرياتهم الشخصية، وتشمل هذه الأفعال السب والقذف عبر الإنترنت، وانتهاك الخصوصية، والابتزاز الإلكتروني، ونشر الصور والمعلومات دون إذن، ونظرا لتأثيرها النفسي والاجتماعي الخطير، عمل المشرع الجزائري على تجريم هذه الأفعال بنصوص قانونية صريحة لحماية الأفراد وضمان أمنهم داخل البيئة الرقمية.

الفرع الأول: الجرائم الماسة بالحريات العامة

ولعلها تعرف بالجرائم المعلوماتية الماسة بالآداب العامة تتلخص عموما هذه الجرائم في تلك السلوكيات الماسة بالأخلاق ولو أن التعرض الجرائم الأخلاق ليس بالأمر المين، بالنظر إلى تباين القيم الاجتماعية من مجتمع الأخر، بل وحتى بين طبقات المجتمع نفسه، فما بعد الحلال حاليا في مجتمع ربما يكون غير ذلك في مجتمع آخر، وجرائم الأخلاق هي تلك التي تتضمن العدوان على القيم الاجتماعية والأخلاقية التعارف عليها في النظم الاجتماعية[2].

يشترط في القانون في غالبية القول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستول جملة من الشروط الأساسية وهي أن تكون علنية أي أن تترتب نتائج يعترف بها القانون ويرتب عليها أثاره، إضافة إلى أن تكون معروضة على الجمهور.

[1] الأمر 05/03 المتعلق بحقوق المؤلف الحقوق المجاورة، بتاريخ 2003/07/23، الجريدة الرسمية رقم 44، ص 04 إلى 07.

[2] عادل عبد العال ابراهيم حزامني، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

وقد تعرض المشرع الجزائري المفهوم هذه الجرائم في بعض نصوص قانون العلويات دون أن عدد نطاقها المتصل بتقنية المعلوماتية، إلا انه يمكن لنا إعمال هذه النصوص على جرائم المعلوماتية بالنظر إلى عمومية والدولية النصوص، فتحد نص المادة 333 من قانون العلويات الجزائري، تشير إلى عقاب كل شخص ارتكب فعلا، عملا بالحياء بصفة علنية وذلك بالحبس من شهرين (12) إلى سنتين (02) وبغرامة من 500 دج إلى 2000 دج إضافة إلى نصر المادة 333 مكرر والتي تنص على نفس المقدار من الطلاب في حق كل من صنع، أو حاز أو استورد أو سعى إلى ذلك، أو وزع ا واحد أو الصق أو أقام معارض أو عرض أو شرح في ذلك أو باع أو شرع في البيع أو وزج أو شرح في ذلك، كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زينيه أو صور فوتوغرافية أو أنتج أي شيء مخل بالحياء[1].

من خلال استقراء نصوص المواد السالفة الذكر بعد أن المشرع الجزائري لم يذكر بالتخصيص الجرائم التي تقع بواسطة النظم المعلوماتية والتي تستهدف المساس بالآداب العامة، وإنما يمكن تطبيق نصوص هذه المواد على الجريمة المعلوماتية باعتبارها وفي الوقت الراهن من أبرز الوسائل الإجرامية المستعملة من قبل مجرمي المعلوماتية الذين وجدوا في هذه التقنية وسيلة ذات كفاءة عالية، لأجل نشر إعلاناتهم الإلكترونية التي تمس بالآداب العامة، والأفعال المحرمة حسب نص المادة تشمل: الصناعة أو الحيازة أو الاستيراد أو العرض الشروع في العرض للجمهور البيع أو التوزيع أو الشروع فيهما، فيمكن تصنيع وتركيب الأفلام والصور بواسطة الحاسوب وكذلك ترينها وكذلك تعديلها ونشرها إما على شبكة المعلومات أو على وسائط التخزين الخارجية، كالأفراس المضغوطة، وبالتالي إتاحتها للجمهور والتأثير على قيمهم الاجتماعية وخصوصا بالنسبة للمجتمعات العربية والإسلامية وهو الأمر الذي شددت عليه الاتفاقية العربية تجارية جرائم التقنية المعلوماتية[2].

الفرع الثاني: جرائم الاعتداء على حرمة الحياة الخاصة

تعد الحياة الخاصة قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، وإلا تحول إلى أداة صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة ولا يمكنه إن يتمتع بهذه الملامح إلا في إطار مغلق، يحفظها ويهيأ لها سبل البقاء وتقتضي حرمه هذه الحياة إن يكون للإنسان الحق في إضفاء السرية على مظاهرها. وفي إطار المعلوماتية فبرز خطورة التهديد المعلوماتي للحياة الخاصة إساءة استخدام المعلومات والبيانات المتعلقة بالإفراد.

[1] اسامة احمد المناعسة، جلال محمد الزعبي، مرجع سبق ذكره، ص 197.

[2] عكاشة مخلوف، مرجع سبق، ص 53.

وصور الاعتداء على الحياة الخاصة يصعب حصرها، لأنها متطورة نتيجة تطور تكنولوجيا المعلومات باستمرار إلا إننا يمكن إن نشير إلى أبرز الانتهاكات التي قد تطال حق الإفراد في حرمة حياتهم الخاصة نتيجة لاستخدام الأنظمة المعلوماتية[1].

أولا: جرائم القذف والتشهير عبر الانترنت:

للشخص الحق في الشرف الذي يكفل له احترام سمعته وشرفه واعتباره وكرامته من التعدي والإيذاء، ويقصد بالشرف مجموع القيم التي يضيفها الشخص على نفسه وتشكل سمعته التي ستتبع تقدير الناس له، ويتمثل الإخلال بالشرف في الحط من مكانة الإنسان وتعريضه للاحتقار والازدراء من قبل الغير عن طريق الأقوال والتشهير أو نسب الأفعال.

وتعد جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعا في نطاق شبكة الانترنت، إذا اسيء استخدامها يهدف النيل من شرف الغير وكرامته واعتباره، ففي إطار مجتمع المعلومات الالكترونية يجد العابثون الحرية في نشر وبث رسائل تحتوي عبارات الذم والقدح والتحفيز اتجاه آخرين مستهدفين بذاتهم، بصفة وجاهية أو غيابية أو بواسطة الوسائط الالكترونية السمعية أو السمعية البصرية[2].

وغالبا ما تقع هذه الجرائم بوصفها الحديث الالكتروني تحت سلطة النصوص التقليدية مما يخلق إشكالا في أمر إثباتها وهو ما ينطبق على أحكام التشريع العقابي الجزائري، بحيث يخلو من نصوص تتعلق بتحريم الاعتداءات على شرف واعتبار الأشخاص ذات الطبيعة الالكترونية، وتبقى المادة 296، 297 من قانون العقوبات الجزائري مجرد نصوص توضيح الفعل المادي المكون الجريمة القذف والسب والقدح والتحفيز، إضافة إلى العقوبات المقرر لها بدون أي ربط مباشر مع تقنية المعلوماتية بالرغم من إقرار القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم النصوص قانون العقوبات، وهو على عكس المشرع السعودي الذي تكفل في نصوص مكافحة الجرائم المعلوماتية بإيضاح هذا النوع من الجرائم بالتفصيل كما هو نص الفقرة من المادة 03 من نفس القانون وذلك تفسير لما ورد في نص المادة أربعة عشر (14) من مضمون الاتفاقية الفردية المكافحة جرائم تقنية المعلوماتية[3]، ويمكن حصر هذه الجرائم في الأنماط والسلوكيات التالية:

1. استهداف شخص معين بذاته بالذم والتحقير والتشهير:

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 174.

[2] عكاشة مخلوف، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، جامعة د طاهر مولاي، سعيدة، الجزائر، 2017/2016، ص 55.

[3] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة بمقر جامعة الدول العربية، مصر بتاريخ 21-12-2010.

يكون ذلك إما باستخدام البريد الالكتروني بحيث يعمد الجاني من خلاله، إسناد مادة معينة إلى شخص ما قد يكون معنيا بذاته بحيث ينال من شرفه أو كرامته وتعرضه إلى بغض الناس واحتقارهم، خصوصا إذا ما اعتمد الجاني في ذلك على توزيع مضمون الرسالة الالكترونية إلى عدد غير محدد من المتعاملين مع الانترنت عن طريق رسائل البريد الالكتروني وقد يجد الجاني في شبكة الويب (web) العالمية وسيلة في إسناد مادة كتابية أو صوتية أو مرئية مسيئة لشخص ما، فتنال عن شرفه وكرامته وتعرضه للاحتقار والذم من قبل الغير، كما أنها قد ترتكب عن طريق مواقع التواصل الاجتماعي (Facebook أو Twitter) أو (Chatrooms) أو (Skype)

2. استهداف مجموعة من الأفراد وحث الغير على كراهيتهم:

ويمكن أن تستهدف هذه الجرائم مجموعة من الأفراد جملة واحدة من خلال انتماءاتهم الدينية أو العقائدية أو العرقية، وهي النقطة الأساسية التي شكلت موضوع البروتوكول الإضافي لاتفاقية الجريمة الالكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية، والتي تحرض على كراهية الأجانب والتي يرتكب عن طريق أنظمة الكمبيوتر المؤرخة في 28-01-2008 بستر اسورغ بفرنسا والتي جاءت بفصلين الأول تضمن الأحكام العامة التي تبين الغرض الأساسي من هذا البروتوكول والثاني تكفل ببيان هذه الجرائم المعلوماتية وحصرها في السلوكات التالية:

أ. نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أنظمة الحاسوب.

ب. التهديد الذي تحركه دوافع التمييز العنصري وكراهية الأجانب.

ج. الاهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب.

د. الانكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية

ثانيا: جرائم التعدي على البيانات الشخصية:

إن احترام الحق في الحياة الخاصة بعد من المبادئ الدستورية الثابتة، بحيث يعد الدستور بان الحياة المواطنين الخاصة حرمة يحميها القانون فلكل شخص الحق في أن تظل أسرار حياته الخاصة محجوبة عن العلنية ومضمونة من تدخل الغير واستطلاعه وتشكل الجريمة المعلوماتية مظهرا حديثا، يهدد بخطر محدق على البيانات الشخصية للأفراد من عدة زوايا تتمثل فيما يلي:

1. تجميع البيانات وتخزينها على نحو غير مشروع:

يتمثل فعل انتهاك الحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة منهم ولكن على نحو غير مشروع، ويستمد هذه الصفة غير المشروعة من الأساليب المستخدمة الأجل الحصول على هذه البيانات أو من حيث طبيعة هذه البيانات[1].

أما من حيث الأساليب فقد يعمد الجاني على أسلوب النقاط ارتجاجات الجدران وترجمتها إلى عبارات وكلمات وذلك بواسطة معدات خاصة تغذي الحاسوب المزود ببرنامج خاص لترجمة كل ذلك، أو من خلال اعتراض الرسائل الالكترونية أو اختراق النظام المعلوماتي للضحية.

أما من حيث طبيعة البيانات فان البيانات الاسمية الخاصة يجب أن يحظر جمعها وتخزينها ومعالجتها داخل الحاسوب من قبل الغير، إضافة إلى المعلومات المتعلقة بالسجل القضائي التي لا يحق إلا للسلطة القضائية جمعها وتخزينها حفاظا على سمعة الشخص.

2. إساءة استعمال البيانات والمعلومات الاسمية انتحال الشخصية:

ترتكز جريمة انتحال الشخصية على مبدأ النقدي على البيانات الاسمية للغير من اجل التخفي والتهرب من المسؤولية، أي الإفلات من المتابعة الجزائية، أي هي استخدام بيانات شخصية للغير من اجل الوصول إلى هدف غير مشروع يتمثل في جريمة تحقق الربح المادي المفترقها، دون أن يكون هو المتابع بشأنها، وقد أشارت الإحصائيات السنوية لسنة 2009 أن حوالي 210000 شخص في فرنسا قد وقعوا ضحايا هذا النوع من الإجرام عبر الانترنت، يقدر معدل نموها على مستوى الدول الغربية بـ 40% وتشكل هذه الجريمة جزءا من جرائم الاحتيال المعلوماتي[2]، فالفرد أصبح معرضا أكثر من أي وقت مضى المخاطر انتحال هويته من قبل الغير بسبب اعتماده المطلق أو الشبه الدائم على تقنية المعلوماتية وشبكة الانترنت خصوصا، ضف إلى ذلك أن وسائل التحقق من الشخصية عبر الانترنت هي غير تلك المتبعة أمام الجهات الرسمية.

3. إفشاء الأسرار والبيانات والمعلومات الاسمية:

إن هذا النوع من السلوكات الإجرامية قد يكون نتيجة حتمية الجرائم السابق ذكرها، بان البيانات الخاصة قد انتقلت من السر إلى العلانية، بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتى بصفة مشروعة

[1] نهلا عبد القادر المومني، المرجع السابق، ص 174.

[2] أسامة احمد المناعسة، جلال محمد الزعبي، مرجع سبق ذكره، ص 260.

وبالتالي فإنها تكون عرضة للاطلاع عليها من قبل عدد غير محدد العدد من الأشخاص في حال عرضها على شبكة الانترنت أو على الأقل من قبل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية.

الفرع الثالث: جرائم الاستغلال الجنسي للأطفال عبر الأنترنت

إن الإنترنت عندما ساد كل مناحي الحياة بات جزءا لا يتجزأ من حياة واهتمامات الأطفال، فعلى الرغم مما قد يعود عليهم من فوائد متعددة في التعلم والتعليم وتطورهم الشخصي جراء استخدامهم الإنترنت، إلا أنه قد يعرضهم لمخاطر كثيرة كالوصول إلى محتويات غير لائقة والتواصل مع غيرهم من الأطفال والبالغين على نحو يضر بهم ويعرضهم لممارسات عدوانية واستغلال جنسي، وتعتبر شبكات التواصل الإجتماعي بشكل خاص من أكثر الفضاءات التي ترتكب فيها جرائم الإستغلال الجنسي ضد الأطفال وذلك عن طريق نشر وتوزيع صور أو رسائل المحتوية على كلام فاحش أو أفلام إباحية لاستدراج الضحايا القصر من خلال غرف الدردشة أو المجموعات وصفحات وحتى عن طريق البريد الإلكتروني من أجل التحريض على الفجور وممارسة الرذيلة مستغلين القصر وذلك لعدم توفر تمام العقل واكتمال نموه[1].

إن جريمة الإستغلال الجنسي للأطفال كغيرها من الجرائم وما تخلفه من ضرر على المجتمعات في العديد من النواحي سوآءا نفسية أو اجتماعية أو سياسية هي مدمرة للضحية بالنظر لخصوصيته الفيزيولوجية ولبسيكولوجيه، فتنعكس صور الإستغلال الجنسي للطفل على جسده ونفسيته لأن هذا النوع من الممارسات لا تتلاءم مع عالمه الخالي من الإرهاقات الجنسية التي تشوه براءة الطفل وتغير فطرته، كما أنها تعرقل وتأثر في نموه وتطور أفكاره حول كل ما هو جنسي حيث أن هناك إرتباطا قويا بين تعرض الأطفال للمواد الإباحية والسلوك الجنسي المنحرف، وهو ما يجعلهم فريسة للعنف الجنسي في كثير من الأحيان.

الإستغلال الجنسي للأطفال عبر الإنترنيت بشكل عام تعددت صوره وخصوصا شبكات التواصل الإجتماعي لما تحتويه من مواقع كثيرة ينصب محتواها على فيديوهات وصور وأفلام جنسية خاصة بالأطفال القصر ولا تزال هذه الظاهرة في تزايد مستمر، ومن أبرز صور الإستغلال الجنسي للأطفال نذكر ما يلي:

1. جريمة تحريض الأطفال على المواد الإباحية

تقوم هذه الجريمة عن طريق تهيج شعور الطفل ودفعه إلى ارتكاب أفعال الفسق والفجور، ويتم إستخدام فيها مختلف وسائل التواصل الإجتماعي من أجل استقطاب العديد الأطفال من بينها موقع الفيسبوك وموقع الإنستغرام مثلا عن طريق:

[1] فضيلة تراموشت، جرائم الإنترنت الماسة بالأطفال، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2014، ص 31.

أ. التحريض بالمحادثة الشفهية والمكتوبة حيث تتضمن هذه المحادثات بصورتيها الحض على إرتكاب أفعال الفسق والفجور أو باحتوائها على كل ما هو خليع من شأنه تجميل عملية ممارسة الجنس وتذليل صعوبات الوصول إليها وممارستها.

ب. التحريض عن طريق صنع مواقع إباحية مهمتها الترويج للإباحية الجنسية، كما تتوفر في الموقع أماكن بيوت الدعارة وكيفية الاتصال بهم وتوفير صور من يمارس معهم الجنس، وقد تتضمن المواقع عروضا تشغيلية في مجالي الدعارة والبغاء ولا سيما تشغيل الأطفال تمهيدا لاستغلالهم في أغراض جنسية[1].

ج. التحريض عن طريق الرموز أو الرسوم أو الصور أو الأفلام أو برامج الحاسوب الخاصة بذلك، والتي قد تكون صريحة أو ضمنية بحملها معنى التحريض على الفسق والفجور وارتكاب الرذيلة[2].

2. جريمة عرض صور وأفلام منافية للآداب العامة

من ذلك عرض الجاني وبثه صورا وموادا إباحية عبر شبكات التواصل الإجتماعي، حيث يتحقق الركن المادي للجريمة بقيام الجاني بصناعة أو تسجيل أو نقل صور أو فيديو إباحي لطفل لغرض عرضه على أقراص حاسب آلي أو شبكة الإنترنت، وتتحقق الجريمة بمجرد قيام الجاني بتصوير الأطفال في أوضاع جنسية مختلفة وعرضها على شبكة الإنترنيت أو عرض عليهم هذه الأوضاع مع أشخاص آخرين أو إرسال لهم بريدا إلكترونيا يحضهم على الانحراف أو الفساد الأخلاقي، ولا عبرة في تحقق الإنحراف فعلا في قيام مسؤولية الجاني، كما يجب أن يعلم الجاني بأنه يقوم بعمل أو تسجيل أو نقل أو عرض صور أو فيديوهات ذات صبغة جنسية للأطفال وأن تتجه إرادته لذلك[3].

إن ظاهرة الإستغلال الجنسي للأطفال وما ينتج عنها من تأثير سلبي على الطفل لخطورة آثارها التي تمتد إلى كبره، فيكون فردا سلبيا في المجتمع يحمل معه معاناته إلى كبره فهذه الجرائم تترك تشوهات في جسد ونفسية الطفل الأمر الذي قد يؤثر سلبا على حياته في المجتمع وعلى غيره أيضا، هذه الجريمة صارت تتزايد يوما بعد يوم وذلك لسهولة وسرعة تنفيذها وسهولة إخفاء الأدلة من قبل المجرم ومحو كل آثارها، ولازالت النصوص القانونية والمواثيق الدولية بمختلف هياكلها التي تعنى بحماية الطفل تسعى لبث الوعي الأسري والاجتماعي بضرورة توفير بيئة مناسبة لرعاية الأطفال والتصدي لكافة أشكال التعدي من خلال تقرير عقوبات رادعة ومشددة على منتهكي الحرمة الجسدية والنفسية للطفل.

[1] أسامة محمد المناعسة، جلال محمد الزغبي، مرجع سبق ذكره، ص141.

[2] سحر فؤاد مجيد، جريمة التحرش الجنسي بالأطفال عبر الإنترنيت، المجلة الأكاديمية للبحث القانوني، عدد خاص 2017، جامعة بغداد العراق، ص 309.

[3] سحر فؤاد مجيد، نفس المرجع، ص 307.

المشرع الجزائري جرم كل الأفعال والتصرفات التي ترتكب من أجل إفساد أخلاق الطفل أو تشجيعه على الفسق والفجور مهما كانت الوسيلة المستعملة وذلك بهدف حماية الطفل وصيانة حقه، وذلك من خلال المادة 333 مكرر 1 من قانون العقوبات والمادة 342 من نفس القانون التي نصت على ما يلي: " كل من حرض قاصرا لم يكمل 18 سنة كاملة ذكرا أو أنثى على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له وكل من ارتكب ذلك بصف عرضية يعاقب بالحبس من خمس سنوات إلى عشرة سنوات وبغرامة من 20.000 إلى 100.000 دج[1].

باستقرائنا لنص المادة السالفة الذكر نجد أنها جرمت فعل تحريض القصر على الفسق بصورتيه، أي يمكن تطبيقه على الأفعال التي تتم باستعمال شبكات التواصل الإجتماعي والتي يكون موضوعها التحريض على فساد الأخلاق[2].

كما قام المشرع الجزائري بسن قانون جديد لمحاربة ظاهرة الإستغلال الجنسي للأطفال بشتى صوره وذلك لحمايته من خلال القانون رقم 15-12 المتعلق بحماية الطفل حيث جاء فيه العديد من النصوص منها:[3]

نصت المادة 140 منه على أنه:" يعاقب بالحبس من سنة إلى 03 سنوات وبغرامة من 150.000 إلى 300.000 دج من ينال أو يحاول النيل من الحياة الخاصة للطفل بنشر أو ببث نصوص أو صور بأية وسيلة يكون من شأنها الإضرار بالطفل".

وكذلك نصت المادة 141 على "دون الإخلال بالعقوبات الأشد يعاقب بالحبس من سنة إلى 03 سنوات وبغرامة من 150.000 دج إلى 300.000 دج كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب والنظام العام".

ونصت المادة 143 بقولها: "يعاقب على الجرائم الأخرى الواقعة على الطفل لاسيما الإستغلال الجنسي للطفل واستعماله في البغاء وفي الأعمال الإباحية والإتجار به والتسول به أو تعريضه للتسول واختطاف الطفل طبقا لتشريع ولا سيما قانون العقوبات".

[1] المادة 342 من ق.ع.ج.

[2] سارة مقراني، جريمة الإستغلال الجنسي للأطفال عبر الإنترنت، مذكرة تكميلية لنيل شهادة الماستر، جامعة العربي بن مهيدي، كلية الحقوق والعلوم السياسية، أم البواقي، الجزائر، 2016/2015، ص 72.

[3] قانون رقم 15-12 المؤرخ في 28 رمضان 1436، الموافق لـ 15 يوليو 2015، المتعلق بحماية الطفل، الصادر بالجريدة الرسمية يوم 09 يوليو 2015، العدد 39.

خلاصة الفصل:

تعد الجريمة الإلكترونية من أخطر التحديات التي تواجه المجتمعات الحديثة نتيجة للتطور السريع في تكنولوجيا المعلومات والاتصال، وتشمل هذه الجرائم مجموعة واسعة من الأفعال غير المشروعة التي ترتكب عبر الوسائل الإلكترونية مثل القرصنة، الاحتيال الإلكتروني، الابتزاز الرقمي، ونشر المحتوى غير القانوني، وقد أدرك المشرع الجزائري خطورة هذه الظاهرة، فسعى إلى مواجهتها من خلال إدراج نصوص قانونية صريحة ضمن المنظومة التشريعية الوطنية.

تمثلت أهم خطوات الجزائر في مكافحة الجريمة الإلكترونية في سن قانون 09-04 الصادر سنة 2009، والذي يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقد تضمن هذا القانون تعريفات دقيقة للجرائم الإلكترونية، والعقوبات المقررة لها، بالإضافة إلى آليات المراقبة والتحقيق والمتابعة، مع احترام خصوصية الأفراد وحرياتهم.

كما نص القانون على التعاون الدولي لمكافحة هذا النوع من الجرائم نظرا لطبيعتها العابرة للحدود، وأكد على أهمية تعزيز قدرات الضبطية القضائية وتكوين الكوادر المتخصصة في المجال الرقمي، ورغم هذه المجهودات، لا تزال الحاجة قائمة لتحديث التشريعات بشكل مستمر ، ومواكبة المستجدات التكنولوجية من خلال تبني سياسة وطنية شاملة في مجال الأمن السيبراني.

الفصل الثاني: آليات مكافحة الجريمة الالكترونية في التشريع الجزائري

الفصل الثاني: آليات مكافحة الجريمة الالكترونية في التشريع الجزائري

شهد العالم في العقود الأخيرة تطورا هائلا في مجال تكنولوجيا المعلومات والاتصالات مما أفرز تحولات جذرية في مختلف مجالات الحياة، وأدى إلى بروز نوع جديد من الجرائم يعرف بـ"الجريمة الإلكترونية"، هذه الجرائم التي ترتكب عبر الشبكات الرقمية ووسائل الاتصال الحديثة لم تعد تقتصر على حدود جغرافية معينة، بل أصبحت عابرة للحدود، سريعة الانتشار، وصعبة الاكتشاف أحيانا، وهو ما شكل تحديا كبيرا أمام المنظومات القانونية والأمنية في مختلف دول العالم بما في ذلك الجزائر.

وفي ظل هذا الواقع المتغير كان لزاما على المشرع الجزائري أن يتفاعل مع هذه المستجدات بوضع إطار قانوني ملائم لمواجهة هذا النوع المستحدث من الجرائم، من خلال سن نصوص قانونية جديدة وتعديل بعض النصوص التقليدية واستحداث آليات قانونية وتقنية ومؤسساتية تمكن من رصد الجريمة الإلكترونية والتصدي لها بكفاءة وفعالية، مع ضمان احترام حقوق الأفراد وحرياتهم الأساسية.

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال وظهور شبكة الأنترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام لأنه بقدر ما أحدث أثار جانبية وغير نمط حياة المجتمعات وجب على المشرع الجزائري مواكبة هذه التطورات من خلال تطوير أنظمة التحقيق والحماية ونص قوانين تجرم هذه الأفعال وفرض عقوبات صارمة على مرتكبيها وعدم التساهل في أي تجاوزات تمس الفرد أو المجتمع وتكريس كل الوسائل الرقمية والبشرية لمكافحة مختلف الجرائم الإلكترونية.

وهذا ما أوجب ضرورة تفعيل التعاون التشريعي والقضائي والأمني داخليا أو خارجيا مع مختلف الدول العربية أو مع مختلف الدول الغربية الأكثر دراية بالجرائم الالكترونية وآليات مكافحتها ومواكبة كل التطورات الواجب اتخاذها لمكافحة وصد هذه الجرائم وهذا يعتبر تحديا للمشرع الجزائري من جهة وللمجتمع من جهة أخرى.

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى استوجب ذلك توفير حماية جنائية خاصة بها، فالمعلومة أصبحت تقوم ماليا، وبالتالي تدخل في عتاد الأموال الاقتصادية، وقد تكون المعلومة شخصية وإفشائها يهدد الحياة الخاصة من جوانب متعددة. ونظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات (شبكة الأنترنت) أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها عبر الشبكات وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة المواجهة هذه الجرائم المستحدثة[1].

المطلب الأول: الحماية في نصوص الملكية الفكرية

يقصد بالحقوق الذهنية أو الفكرية، بأنها حقوق ملكية معنوية ترد على أشياء غير مادية وتقسم إلى ثلاثة أنواع:

1. حق الملكية الصناعية، ويرد على ابتكارات جديدة تمكن صاحبها من احتكار استغلال ابتكاره قبل الكافة، وهي أنواع حقوق تتعلق بابتكار جديد من حيث الشكل والمظهر الخارجي للمنتجات (الرسوم أو التصميمات أو النماذج الصناعية)، حقوق تتعلق بابتكار جديد من حيث الموضوع كالاختراعات حقوق ترد على شارات مميزة تمكن صاحبها من احتكار استغلال علامة تستخدم لتمييز المنشآت كالاسم التجاري.
2. حقوق الملكية التجارية وهي تتضمن ما للتاجر من حق على محله التجاري، باعتباره مال منقول.
3. حقوق الملكية الأدبية والفنية، وتعني ما للمؤلف من حق على إنتاجه الذهني في الآداب والفنون والعلوم.[2]

وقد اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة، تتمثل في وجود المصنف أولا ثم عدم مخالفته للنظام العام ثانيا، وأخرى خاصة وهي وجود ابتكار جديد في المصنف أولا ثم القيام بإيداعه القانوني ثانيا[3].

---

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص 88.

[2] محمد عبد الرحيم الناغي، الحماية الجنائية للرسوم والنماذج الصناعية، (دراسة مقارنة) دار النهضة العربية، القاهرة، مصر، 2009، ص 12.

[3] بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، ط01، الجزائر، 2007، ص37.

الفرع الأول: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية

ترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالاختراعات، ومعنى الاختراع إيجاد شيء لم يكن موجودا من قبل، أو اكتشاف شيء كان موجودا ولكنه كان مجهولا وغير ملحوظا ثم أبرزه في المجال الصناعي، فالاختراع الذي لا يؤدي إلى تقدم ملموس في الفن الصناعي لا يستحق براءة عنه[1]. ولما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب الآلي، فهي من هذه الزاوية تصبح قابلة للبراءة.[2] وقد نص عليها الأمر رقم 03-07 الصادر في 2003، حيث نصت المادة الثالثة منه على الشروط الواجب توافرها حتى يحظى الاختراع بالحماية بقولها: "يمكن أن تحمى بواسطة براءة الاختراع الاختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصناعي...".[3] وعليه يمكن القول أنه حتى يحظى أي اختراع ما بالحماية ضمن نطاق براءات الإختراع، وجب توافر شرطي الابتكار والجدة والقابلية للتطبيق الصناعي.[4]

وتجدر الإشارة إلى أنه يمكن الحصول على براءة الإختراع بخصوص برامج الإعلام الآلي في حالتين:

1. أن يكون البرنامج جزءا من ذاكرة الحاسوب نفسه ومثاله البرنامج المبني.
2. أن يكون البرنامج جزءا، أي أن طلب البراءة ينصب على وسيلة صناعية جديدة، يستخدم البرنامج في تحقيق إحدى مراحلها، فالحماية تبقى رهينة توفر الشرطان المذكوران، مما يصعب توفرها، فالمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الإختراع طبقا[5] للمادة 07 من الأمر رقم 03-07 التي تنص على: "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"[6].

الفرع الثاني: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية والفنية

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط02، 2000، ص 51.

[2] بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس 2013، العدد 01، ص 68.

[3] الأمر رقم 03-07 الصادر في 19 يوليو 2003 المتعلق ببراءات الإختراع، ج.ر عدد 44.

[4] ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، 2010، ص69.

[5] بوعناد فاطمة زهرة، مرجع سبق ذكره، ص66

[6] الأمر رقم 03-07، القانون السابق الذكر.

تظهر الملكية الأدبية والفنية من خلال حق المؤلف، وهو حق استئثاري يمنحه القانون المؤلف أي مصنف للكشف عنه، كابتكار له أو استنساخه أو توزيعه أو نشره على الجمهور، والإذن للغير باستعماله على وجه محدد.[1] وقد انقسم الفقه إلى اتجاهين، اتجاه يرى أن برامج الحاسب الآلي مصنفة ضمن قانون حق المؤلف وأنه لا حاجة لتعديل النصوص التقليدية في قانون حق المؤلف، باعتبار برامج الحاسب الآلي ما هي إلا طرق مختلفة للتعبير عن الأفكار الإنسانية وهو مثل سائر المصنفات، أما الاتجاه الآخر أقر لبرامج الحاسب الآلي الصفة المميزة عن سائر المصنفات الأخرى المحمية بموجب قانون حماية حق المؤلف، وتبنى هذا التوجه العديد من الدول التي عدلت قوانينها بما ينسجم والصفة المميزة لبرامج الحاسب الآلي[2]، ومنهم الجزائر حيث جاء الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة باستخلاص ما يلي:

1. أن المشرع وسع قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي.
2. تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لاسيما المصنفات المعلوماتية،[3] حيث تنص المادة 05 من القانون رقم 03-05 [4]على أنه: " تعتبر أيضا مصنفات محمية الأعمال الآتية .... مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواءا كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى... تكفل الحماية لمؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية. والمادة رقم 04 من نفس القانون نصت على أنه " تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل ... وبرامج الحاسوب ..... كما أن مدة الحماية تحدد ب 50 سنة بعد وفاة المبدع وفقا للمادة 58 فقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي لمؤلف برنامج فعلا من أفعال التقليد، حيث نص المشرع في المادة 151 من الأمر رقم 05/03، على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء فني أو في حالة المساس بسلامة مصنف أو أداء فني، أو في حالة استنساخ مصنف أو أداء فني بأي أسلوب في شكل نسخ مقلدة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول.

---

[1] عفيفي كامل عفيفي، مرجع سبق ذكره، ص 75.

[2] حلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان لأردن، 2010، ط 01، ص 189.

[3] بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 66.

[4] الأمر رقم 03-05، الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المحاورة، ج.ر عدد 44.

وقد قرر المشرع جزاءات الجرائم التقليد، حيث ربط المشرع الجزائري حماية المصنف بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة، كما حول المشرع لصاحب المصنف المعتدى عليه القيام بإجراء تحفظي يتمثل في حجز التقليد، وبواسطته يتم حجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من 156/153 إلى 159 من نفس القانون السابق الذكر، حيث قدرت العقوبة الأصلية بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 1.000.000 دج سواء تمت عملية النشر داخل الجزائر أو خارجها، ومنح المشرع للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الإستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة وإتلاف كل عتاد أنشأ خصيصا المباشرة النشاط غير المشروع، وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبية، كما للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.[1]

المطلب الثاني: الحماية في قانون العقوبات

الفرع الأول: العقوبات الأصلية:

تتمثل العقوبات الأصلية المطبقة على الشخص الطبيعي في إطار الجريمة الإلكترونية المؤشر الصريح الخطورة هذه الجريمة والتي أقرها المشرع على الأفعال التي يجرمها قانون العقوبات والمتمثلة فيمايلي:[2]

1. العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي:

تعتبر هذه الجريمة من أهم الجرائم الإلكترونية وأخطارها على المؤسسات والأفراد لكونها تشكل انتهاكا صارحا ومباشرا للحقوق والحريات ويختلف الفقه في طبيعة هذه الجريمة بين من يعتبرها جريمة واحدة تؤدي نفس النتيجة وبين من يقسمها الى جريمتين بحيث يفصل رواد هذا المذهب بين الدخول إلى النظام المعلوماتي كجريمة أولى والبقاء غير المشروع في النظام كجريمة ثانية[3].

2. العقوبات المقررة لجريمة إفساد أو تعطيل سير النظام:

وتسمى أيضا جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات" حيث أغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على جريمة سير نظام المعالجة الآلية للمعطيات، إلا أنه يمكن

[1] سوير سفيان، مرجع سبق ذكره، ص 75.

[2] عماد دمان ذبيح، سمية بهلول، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 13، جامعة عباس لغرور خنشلة، الجزائر، 2020 ص 145.

[3] عماد دمان ذبيح، سمية بهلول، مرجع سبق ذكره، ص 146.

استخلاص التجريم من خلال النصوص القانونية المستحدثة في إطار تحريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات الأنظمة الداخلية والخارجية.

3. العقوبات المقررة الجريمة الاعتداء العمدي على المعطيات:

تنص المادة 394 مكرر 1 من ق ع أنه "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 الى 2.000.000 كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

فيقصد بالاعتداء على المعطيات التجاوز الذي يهدف الى الأضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسلامة محتوياتها وتكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم"[1].

الفرع الثاني: العقوبات المقررة للشخص المعنوي

لقد أقر المشرع الجزائري للمسؤولية الجنائية للأشخاص المعنوية بنص عام وهو نص المادة 18 مكرر من ق ع ج، مبينا الجرائم التي يعاقب عنها الشخص المعنوي، وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقد شدد في عقوبة هذه الجرائم إذا ارتكبها شخص معنوي، او كانت موجهة ضد الجهات العامة أي إذا كانت هذه المعطيات تابعة للدولة.[2]

1. شروط تقرير المسؤولية الجزائية للشخص المعنوي

نصت المادة 394 مكرر 4 من ق ع ج "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ونصت المادة 6/323 من ق ج ف" يمكن للأشخاص المعنوية أن يسألوا جنائيا عن الجرائم المرتكبة في هذا القسم طبقا للمادة 2/121، وكذا المادة 7/121 تنص على أنهم يسألوا في الحالات التي نص عليها القانون أو اللائحة عن الجرائم التي ارتكبوها لحسابهم أو من طرف أعضائهم أو ممثليهم.

المسؤولية الجنائية للأشخاص المعنوية لا تستبعد الأشخاص الطبيعية فاعلين أو مساهمين الذين ارتكبوا نفس الوقائع[3]. والمادة 51 مكرر من ق ع ج باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة

[1] عماد دمان ذبيح، سمية بهلول، مرجع سبق ذكره، ص 7.14

[2] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، (د.ط)، 2016، ص .218

[3] غنة باطلي، مرجع سبق ذكره، ص 219.

للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال"[1].

يتضح من هذه المادة أن المشرع الجزائري أراد أن يشارك الأشخاص الطبيعية في المسؤولية مع الأشخاص المعنوية حتى لا يتحملوا وحدهم نتائج فعل مترتب عن الإرادة الجماعية، وهذه المسؤولية مقتصرة على الحالات التي نص عليها القانون أو اللوائح وهي مسؤولية مرتبطة بتوافر شروط:

أ. أن ترتكب الجريمة من أحد أعضاء الشخص المعنوي أو ممثليه

ب. يجب أن ترتكب الجريمة الحساب الشخص المعنوي

ج. ويسأل الشخص المعنوي بصفته فاعلا أصليا أو مساهما.[2]

2. العقوبات المقررة في حالة الاعتداء على الجهات العامة:

قد يشترط القانون بالنسبة لبعض الجرائم أن يكون موضوع النتيجة الإجرامية شيئا أو شخصا معينا تتوافر فيه صفات معينة حتى يقوم بتشديد العقوبة. في هذه الجرائم الإلكترونية أو الاعتداء على المعطيات نجد أن هذه المعطيات أو المعلومات قد تخص الأفراد أو شركات أو جهات معينة. ويأخذ المشرع في الاعتبار الجهة التي تتبعها هذه المعطيات، ويولي اهتمام أكبر للمعطيات التي تتبع للدولة والجهات العامة.

الاعتداء على المصلحة العامة أشد وأخطر من الاعتداء على المصالح الخاصة نجد أن المشرعين يقدرون ذلك لا سيما إذا كانت هذه الجهة المعتدى عليها حساسة كالدفاع والأمن الوطنيين. وقد خطى المشرع الجزائري نفس المسلك حيث بسط حمايته على المعطيات بمختلف أنواعها والجهات التابعة لها. إلا انه شدد العقوبة في حالة ما إذا كان الاعتداء على المعطيات تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.[3]

[1] المادة 51 مكرر من ق. ع. ج.

[2] غنية باطلي، مرجع سبق ذكره، ص 219.

[3] غنية باطلي، مرجع سبق ذكره، ص 223.

وهذا ما جاء في نص المادة 394 مكرر 3 من ق ع ج "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد"[1].

لقد خصت هذه المادة مؤسسة الدفاع الوطني نظرا لأهميتها في الحفظ على سلامة التراب الوطني والأمن العام، وبالتالي خطورة الاعتداء على المعطيات التابعة لها، والحكمة من التشديد هو ما يتطلب الأمر من وجوب العمل على سلامة وامن القوة العسكرية والتي في حفظها وسلامتها حفظ وسلامة الدولة بأكملها. وشملت المادة كذلك الهيئات والمؤسسات التابعة للقانون العام[2].

الفرع الثالث: عقوبة الاشتراك والشروع في الجريمة

1. عقوبة الاشتراك: نصت عليها المادة 394 مكرر 05 من القانون رقم 04/15 بقولها: " كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد الجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير بجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها."
2. عقوبة الشروع نصت عليها المادة 394 مكرر 07 من نفس القانون بقولها: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

الفرع الرابع: العقوبات التكميلية

نص المشرع الجزائري في المادة 394 مكرر 06 من ق ع على العقوبات التكميلية للجرائم السالفة الذكر وتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة مع الحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها[3].

المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

نتناول في هذا المطلب اجراءات الوقاية والمكافحة من الجريمة المعلوماتية في ظل القانون الجزائري الفرع الأول، وآليات الوقائية في الفرع الثاني وفصلنا فيه كالاتي:

[1] المادة 394 مكرر 3 من قي. ع. ج.

[2] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة المرجع نفسه، ص 224.

[3] فاروق خلف، الآليات القانونية لمكافحة الجريمة الإلكترونية، مجلة الحقوق والحريات، قسم الحقوق، كلية الحقوق، جامعة حمة لخضر الوادي، العدد 02، الجزائر، 2015، ص 17.

الفرع الأول: اجراءات الوقاية والمكافحة من الجريمة الإلكترونية في ظل القانون الجزائري 09-04

لقد خص المشرع الجزائري الجانب الإجرائي من أجل الوقاية والمكافحة من الجريمة الإلكترونية بالاهتمام بدليل أنه أفرد له نصوص قانونية خاصة به والذي تبنى بموجبها صراحة إجراءات خاصة واستثنائية كالمراقبة الإلكترونية.

اولا: الترتيبات التقنية لمراقبة الاتصالات الإلكترونية.

أما فقها فقد اختلفت التعريفات التي تم وضعها لتعريف المراقبة الإلكترونية فقد ذهب اتجاه للقول بأنها: "اجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض"[1].

وهنالك من عرفها بأنها: "تعمد الإنصات والتسجيل ومحلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة"[2].

فالاتصالات الإلكترونية التي تتم من خلال أجهزة ووسائل مختلفة يمكن ضبطها بشكل عام في ثلاثة صور:[3]

1. التنصت
2. اجهزة التسجيل المرئية
3. المراقبة الالكترونية على شبكة الانترنت.

ثانيا: خصائص مراقبة الاتصالات الإلكترونية

من خلال التعاريف التي قيلت فإننا يمكن أن نستنبط من المراقبة الإلكترونية أربعة خصائص والتي تم الاتفاق عليها فقها والتي تميزها عن غيرها من اجراءات التحقيق والمتمثلة في النقاط التالية:[4]

1. اجراء المراقبة الاتصالات الإلكترونية بصورة سرية:

[1] بن موسى خديجة، الحماية الجنائية للمعطيات في المجال المعلوماتي، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2022، ص 54.

[2] أحمد فتحي سرور، الوسيط في قانون الإجرءات الجنائية، دار النهضة العربية، الطبعة 07، القاهرة، مصر، 1993.

[3] العربي شحط عبد القادر، نبيل صفر، الإثبات في المواد الجزائية، دار الهدى عين مليلة، الجزائر، ص 15.

[4] عفيفي كامل عفيفي، مرجع سبق ذكره، ص 273.

يعني أن هذا الاجراء استثنائي يباشر خلسة أي في الخفاء دون رضا أو علم صاحب الشأن وعلة ذلك المحافظة على خصوصية الأحاديث وسريتها وبالتالي يمكن معه تطبيق كل الضوابط وضمانات المراقبة والحماية المقررة قانونا لحماية حق الفرد في سرية مراسلاته واتصالاته.

2. مساس اجراء مراقبة الاتصالات الإلكترونية بحق الشخص في سرية مراسلاته واتصالاته الإلكترونية

من شأن هذه الخاصية أن تكشف عن خطورة المراقبة، فالتنصت على الأحاديث الخاصة للإنسان يتيح للمسترق اختراق ذاته واقتحام عقله والتلصص بأفكاره ونواياه والوقوف على مشاعره وأحاسيسه وعليه فلا تعد من قبيل المراقبة ضبط الرسائل والكتابات وشهادة الشهود والاستجواب إلى غير ذلك من الإجرءات والمشرع الجزائري على غرار نظيره المصري وكذلك الفرنسي قرن الحق في الحياة الخاصة للفرد بالحق في سرية مراسلاته واتصالاته الإلكترونية منها.

3. هدف المراقبة الإلكترونية الحصول على دليل غير مادي إلكتروني:

إن الغاية من اللجوء إلى مراقبة الاتصالات الإلكترونية هو الحصول على دليل من شأنه أن يساهم في كشف الحقيقة وتأكيد أدلة الاتهام لأن إسناد الجريمة لشخص معين يقتضي معه إقامة الدليل على صلته بها.

4. الاعتماد في مراقبة الاتصالات الالكترونية على الأجهزة المخصصة لذلك:

أما المشرع الجزائري وبالرجوع لنص قانون 09/04 المتعلق بالقواعد الخاصة بمكافحة جرائم الإعلام والاتصال والوقاية منها وباستقراء المادة 04 المتعلقة بمراقبة الاتصالات الإلكترونية فإنه لم يشترط استخدام أي جهاز لتحقق المراقبة.

ثالثا: موقف المشرع الجزائري من مسألة مشروعية إجراء مراقبة الاتصالات الإلكترونية.

1. فيما يخص إجراءات المتابعة: فقد تم إنشاء الأقطاب القضائية المتخصصة في هذا النوع من الجرائم بالإضافة إلى توسيع دائرة الإختصاص المحلي بالنسبة الضباط الشرطة القضائية عبر كامل التراب الوطني فيما يخص جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهذا ما أوردته بالذكر المادة 16 مكرر من قانون الإجرءات الجزائية، وذلك من أجل تسهيل عمل الضبطية القضائية في إطار البحث والتحقيق عن هذه الجرائم.
2. فيما يخص توسيع الإختصاص المحلي لوكلاء الجمهورية وقضاة التحقيق: إن مسألة توسيع الإختصاص المحلي لوكلا الجمهورية وقضاة التحقيق إلى دائرة اختصاص محاكمة أخرى في الجرائم

الماسة بأنظمة المعالجة الآلية للمعطيات يكون طبقا لنص المادتين 37/2 40 ومن قانون الإجرءات الجزائية والذي أتبعه صدور المرسوم التنفيذي رقم 06/348 المؤرخ في 05/10/2006 المتضمن تمديد الاختصاص لبعض المحاكم ووكلا الجمهورية وقضاة التحقيق.

3. فيما يخص إجراءات التوقيف للنظر: فقد مدد المشرع الجزائري مدة التوقيف للنظر بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مرة واحدة لمدة 48 ساعة بمعنى أنه يمكن توقيف الشخص المشتبه فيه لمدة 96 ساعة فقط وهذا ما تقضي به المادة 51/05 المعدلة من قانون الإجرءات الجزائية، غير أن الطبيعة المعقدة للجرائم المعلوماتية العابرة للحدود لارتباطها بالتقنية المتطورة يجعل من مهمة البحث والتحري فيها والبحث عن مرتكبيها يستوجب وقتا أكبر وبالتالي فمدة التوقيف في مثل هذا النوع من الجرائم يجب أن تكون كذلك وهو الأمر الذي ينبغي على المشرع الجزائري تداركه.
4. اللجوء إلى إجراءات التحري الخاصة: فقد أوردها المشرع الجزائري بالذكر ضمن الفصل الربع من الباب الثاني من قانون الإجرءات الجزائية بنص المواد 65 مكرر 5 إلى 65 مكرر 18 منه والتي يمكن اللجوء إلى هذه الإجرءات فيما يتعلق بالتحري في الجريمة المتلبس بها والتحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ونوردها كما يلي:

اعتراض المراسلات التسجيل الصوتي، التقاط الصور[1] .

الفرع الثاني: آليات الوقاية والمكافحة من الجرائم الماسة بالمعطيات في المجال المعلوماتي

تتشكل الآليات الوقائية والمكافحة من الجرائم الماسة بالمعطيات في المجال المعلوماتي الى الية التعاون على مستوى الضبطية القضائية المنصوص عليها في قانون الاجراءات الجزائية الجزائري.

اولا: آلية التعاون الأمني في مجال الوقاية من جرائم الماسة بالمعطيات في المجال المعلوماتي:

الجزائر على غرار الكثير من الدول سعت لتفعيل الجهات الأمنية كالية فعالة يتم الاعتماد عليها من أجل الوقاية والمكافحة من الجريمة المعلوماتية، فجهاز الشرطة عموما هو المكلف بالتحري عن الجرائم وضبطها وتلقي البلاغات وإجراء التحقيقات الأولية بشأنها وتقديمها للجهات القضائية المختصة لمباشرة الدعوى الجزائية إذا صحت هذه البلاغات أو توافرت الأدلة الكافية للسير في إجراءاتها[2] .

ثانيا: على مستوى جهاز الدرك الوطني الجزائري

[1] بوخبرة عائشة الحماية الجزائية من الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، تخصص قانون جنائي، جامعة وهران، 2013.

[2] بوخبرة عائشة، مرجع سبق ذكره

في سبيل سعي جهاز الدرك الوطني الجزائري للوقاية والتصدي لظاهرة الجريمة المعلوماتية عموما وظاهرة الإرهاب على شبكة الأنترنت خصوصا وذلك بوضع إستراتيجية من خلال إعادة تنظيم هياكلها وتقسيمها حسب الاختصاصات المستجدة بسبب أن الفضاء المعلوماتي أو بيئة الأنترنت باتت تشكل الملاذ الآمن للمجرمين عموما والإرهابيين على وجه الخصوص[1] .

الفرع الثالث: الهيئة الوطنية للوقاية من جرائم الماسة بالمعطيات في المجال المعلوماتي

من بين الآليات التي أوجدها المشرع الجزائري في مجال الوقاية والمكافحة من الجريمة المعلوماتية إنشاء هيئة وطنية للوقاية والمكافحة من جرائم الإعلام والاتصال ومكافحتها ويكمن دورها الأساسي في تنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الافتراضية ومدها بالمساعدة والاستشارة اللازمة.

وقد تم استحداثها بموجب القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في نص مادته 15 منه التي تنص:[2]

1. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.
2. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
3. تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الرابع: التعاون والمساعدة القضائية الدولية المقررة للوقاية من جرائم المساس بالمعطيات في المجال المعلوماتي.

ومما لا شك فيه ان التعاون والمساعدة القضائية الدولية المقررة للوقاية من جرائم المساس بالمعطيات في المجال المعلوماتي المتضمنة العناصر التالية:[3]

1. الإنابة القضائية الدولية.
2. نقل الإجراءات.
3. تبادل المعلومات
4. تبادل الخبرات.

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2007.

[3] بوخبزة عائشة، مرجع سبق ذكره

5. تسليم المجرمين.

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي

المطلب الأول: التحقيق في الجريمة الإلكترونية

الفرع الأول: الأجهزة المكلفة بالبحث والتحري

ان التزايد المستمر للجرائم المعلوماتية قد طرح عدة تحديات لأجهزة الضبط القضائي، مما ترك أثرا بالغا لضرورة تطوير هذه الأجهزة لمواكبة التطور الحاصل في مجال الجريمة، ونتيجة لذلك قامت معظم الدول بإحداث أجهزة متخصصة لمكافحة الجريمة المعلوماتية، والتي تتولى مهمة التحري عن جرائم العالم الافتراضي وإزالة الغموض عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها شرطة الأنترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

إلا ان دور هذه الأجهزة لا يقتصر على المستوى الوطني، بل هناك أجهزة خصصت للمستوى الدولي بدورها، سنحاول في هذا المطلب ذكر بعض الأجهزة سواء كان ذلك على المستوى الوطني او الدولي كالتالي:

أولا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي (الوطني):

ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة إلى أن تحيل مسألة البحث والتحري في هذا النوع من الجرائم لأجهزة متخصصة، تكون لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام، بالنظر إلى الطبيعة التقنية التي يتميز بها وسوف نحاول أن نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول وفي بلادنا.

1. **الأجهزة المختصة في الدول الأجنبية:** كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة ونذكر على سبيل المثال في هذا الصدد الدول التالية:

أ. **الولايات المتحدة الأمريكية:** قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها:[1]

- **شرطة الواب Web police:** وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[2] .

[1] بوبقرة خيرة، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم، 2020/2019، ص 45، 46

[2] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2002، ص 77

- **مركز تلقي شكاوى الأنترنت IC3:** والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي FBI في سنة 2000، ثم في عام 2003 تم دمج مركز شكاوى الاحتيال عبر الأنترنت المعروف بـ IFCC مع هذا المركز، ويعمل مركز 3ic بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء NWC، ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الأنترنت أين يقوم الشاكي بماء استمارة الكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل.
- **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفردية الفكرية:** ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.
- **نيابة جرائم الحاسوب والاتصالات CTC:** وتتألف من مجموعة من قضاة النيابة العامة ممن تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات وتم منحهم صلاحيات واسعة في مجال الجرائم المعلوماتية والعدوان على حقوق الملكية الفردية.
- **المركز الوطني لحماية البنية التحتية:** التابع للمباحث الفدرالية الأمريكية وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الأنترنت وعلى رأسها شبكات الاتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتحدة الأمريكية وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والأنترنت ومن مستشارين قانونيين.[1]

ب. **بريطانيا:** قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001 [2].

ج. **فرنسا:** قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكر[3] هذه الأجهزة:

- القسم الوطني لقمع جرائم المساس بالأموال والأشخاص ويتكون هذا القسم من مختصين في التحقيق بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997.

[1] نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 108.

[2] بوبقرة خيرة، مرجع سابق، ص 46.

[3] المرجع نفسه.

- المكتب المركزي لمكافحة الإجرام المرتكب بتكنولوجيات المعلومات والاتصالات: ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في: 2000/05/15:

د. **الصين:** قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم القوة المضادة للهكرة وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الأنترنت[1].

هـ. **مصر:** قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرضها على النحو التالي:

- إدارة مكافحة جرائم الحسابات وشبكات المعلومات: أنشئت هذه الإدارة بموجب قرار وزاري[2]، وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثالث أقسام رئيسية هي: قسم العمليات قسم التأمين وقسم البحوث والمساعدات الفنية، وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية، فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الأنترنت على مختلف أنواعها[3].
- قسم مكافحة جرائم الحاسبات وشبكات المعلومات: وقد أنشأ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جريمة عليها باستخدام الأساليب والتقنيات العملية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات[4] .

2. الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني:

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى دار النهضة العربية، القاهرة 2004، ص 812.

[2] قرار وزير الداخلية المصري رقم 13507 لسنة 2002 الصادر بتاريخ: 2002/07/17.

[3] نبيلة هبة محمد هروال، مرجع سابق، ص 141.

[4] بوبقرة خيرة، مرجع سابق، ص 46، 47.

أما الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

فعلى مستوى جهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاموناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر. [1]

أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الإنشاء[2] .

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها[3].

ثانيا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي:

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لا بد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام، ومن أساليب التعاون

[1] بوبقرة خيرة المرجع السابق، ص 48.

[2] المرجع نفسه.

[3] عثماني عزالدين، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله تيبازة، المجلد الثاني، العدد 04، 2018، ص 52.

الدولي الأمني الذي يمكن أن يحقق أهدافه لا قبل للشرطة الإقليمية من تحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر ما يلي:[1]

1. **على الصعيد الدولي:** تعد المنظمة الدولية للشرطة الجنائية (الإنتربول)، من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

أ. **الأولى:** تجمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

ب. **الثانية:** التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم. وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة اسمية الضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية بوضع قائمة اسمية لضباط مختصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين[2]، ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

2. **الأجهزة على المستوى الإقليمي**

أ. **الشرطة الأوروبية أو الأوروبول:** هو جهاز على مستوى الاتحاد الأوروبي تم إنشاؤه في لوكسمبورغ عام 1992 ومقره في مدينة لاهاي بهولندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرام المعلوماتي، ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة المختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية. وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز

[1] عثماني عزالدين، مرجع سبق ذكره، ص 49.

[2] Myriam QUEMENER Cybercriminalité–droit pénal appliqué economica, Septembre 2010, p208.

على مستوى الأوروبول أطلق عليه اسم (Internet Crime Reporting online System) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

ب. **الأوروجست Eurojust :** وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي، ويعد الأوروجست وحدة للتعاون القضائي مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية.

الفرع الثاني: خصائص التحقيق والمحقق

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإحباط والإعجاب معا[1] .

أولا: خصائص التحقيق في الجريمة المعلوماتية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة. وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزائها شيئا سوى الخضوع والامتثال أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير[2].

1. منهج أو أسلوب التحقيق الابتدائي في الجريمة المعلوماتية والهدف من التحقيق

الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في

[1] الخن محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، 2010، ص 230.

[2] خالد ممدوح إبراهيم، مرجع سبق ذكره، ص56.

ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي عن غيره بالنسبة للجرائم الأخرى[1] .

أ. **وضع خطة عمل التحقيق:** يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي: [2]

- وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.
- التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.
- عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.
- تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة[3] .

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية يتم الارتكاز عليها أثناء تنفيذ الخطة، وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب استيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق[4]، بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أن من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل[5] ومنها:

- مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة.

---

[1] بوبقرة خيرة، مرجع سابق، ص 52.

[2] المرجع نفسه، ص 52، 53.

[3] محمد نصير السرحاني، مهارات التحقيق الفني في الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 72.

[4] هشام رستم الحواسب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة أسيوط، 2000، ص 59.

[5] بوقرة خيرة، مرجع سابق، ص 53.

- مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.
- مستوى الاختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش وذلك من خلال تحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.

ب. تشكيل فريق التحقيق: يجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنت، يمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة[1] .

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تطلبه من مهارات فنية وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

- المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.
- خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي.[2]

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك.[3]

ثانيا: العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة المعلوماتية

[1] عبد الله حسين، محمود إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص 612.

[2] عبد الله حسين محمود المرجع السابق، ص 612.

[3] انظر المادة 05 الفقرة الأخيرة من القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي[1] .

1. الإجراءات التي يجب على الضبطية القضائية مراعاتها قبل البدء في التحقيق:

ويمكن أن نسرد الأهم منها[2] كما يأتي:

أ. تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

ب. وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل واحد منهم.

ج. إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها المعرفة الطريقة التي تمت بها عملية الاختراق من عدمه، وهل هناك حواسيب آلية خارج هذه الشبكة ولها إمكانية الاتصال بها أم لا؟

د. مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

هـ. مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

و. يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

ز. فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها الطمس البيانات.

ح. التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

ط. إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر وكذا الشفرات في حالة وجودها.

ي. تصوير الأجهزة المستهدفة التي وقعت بها أو عليها الجريمة من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2. الإجراءات التي يجب مراعاتها أثناء التحقيق:

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1، ص 84.

[2] بوبقرة خيرة، مرجع سابق، ص 55 56.

عند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم بمراعاة[1] ما يلي:

أ. عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر (disque comp).

ب. نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

ج. أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضغط على أزرار معينة مثل Shift delete في وقت واحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.

د. العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.

هـ. العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

و. حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

ثالثا: خصائص المحقق المعلوماتي:

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية فإن المختصين بالتحقيق في هذا النوع من الإجرام المستحدث يختلفون عن أولئك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين.

ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

وإذا كان قد سبق وأن طرحنا خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي فإنه في اعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفر عليها من يتصدى لمهمة البحث والتحري عن هذا النوع من الجرائم والمجرمين.

1. الخصائص الفنية للمحقق في الجريمة المعلوماتية:

[1] بوبقرة خيرة، المرجع السابق، ص 56، 57.

والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصص الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دواع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة معلوماتية ما، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم.

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلازمه عند مباشرته التحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجه ونذكر منه:[1]

أ. معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل على اعتبار أن جهله بارتكاب أساليب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات[2].

ب. إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقع الجريمة، وتخزينها في الأقراص المعدة لذلك ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكروويف حتى لا تتلف محتوياتها.

ج. كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والأنترنت وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك.[3]

[1] بوبقرة خيرة، مرجع سابق، ص 59 60

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002، ص 115.

[3] حسين سعيد بن سيف الغافري، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007، ص 02.

د. يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب وأن يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات كل نظام على حدي لأنه ملزم بالتعامل معها.

هـ. كذلك أنظمة الملفات التي يعتمدها كل نظام حتى يتمكن من إجراء التحقيق في الجرائم المعلوماتية وفي كشف المجرمين ومعاينة مسرح الجريمة وإذا كان التعامل المباشر مع هذه الأنظمة والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها يعتبر مهمة الخبير «إلا أن معرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية.

و. كما يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات[1]، والتي تعد أمرا في غاية الأهمية، لأنها تعتبر الوعاء الحقيقي لأدلة الإدانة في كثير من القضايا ذات الصلة بالحاسوب والأنترنت بما تحتويه من معلومات.

ز. ومن الأمور الفنية التي يتوجب على المحقق معرفتها أيضا أن يكون ملما بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتية وتقنيات الأمن المعلوماتي، ذلك أن معرفة رجال التحقيق لهذه الأساليب يعد من الأمور المهمة التي تساعدهم في معرفة الجناة ومواقع ارتكاب الجريمة ومن أي طرفية الكترونية صدر السلوك الإجرامي وكذلك في مناقشة الشهود وسماع المشتبه فيهم ومحاصر تهم بالأسئلة التي تتعلق بكيفية ارتكاب الجريمة وطرق تنفيذها.

2. **تأهيل وتدريب المحقق المعلوماتي:**

في مكافحة الجرائم المعلوماتية بصفة عامة لا بد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التأهيل والتدريب إلى العاملين بأجهزة الضبطية القضائية.

وقد تنبهت الدول إلى هذا الأمر وظهر هذا الاهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، ومنها ما جاء في القاعدة 22/1 من قواعد بيكين التي أكدت على الحاجة إلى التخصص المهني والتدريب.

[1] يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى الملفات ويتميز كل ملف ببنية وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصواتا أو مستندا خطيا منسق أو غير منسق.

ولهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق دقيقة وذكية، ويتأتى ذلك من خلال الإسراع في أن يطور رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب والنظم المعلوماتية ولكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة و التدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة عملية وسليمة[1].

وإذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب، فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في الجرائم المعلوماتية، فالتقدم المتواصل في تكنولوجيا الحاسب الآلي والأنترنت يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة مجرمي المعلوماتية.

ويرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعات عناصر أساسية تتمثل في شخص المتدرب ومنهج الدورة التدريبية وصفة وأسلوب التدريب[2] .

ويجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة والأساليب التي تتعلق بالكشف عنها وكيفية إثباتها ومعاينتها والتحفظ عليها وكيفية فحصها فنيا.

وقد كان هناك من يرى أن صعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن يعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال، لكن هذا الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد والمجتمع ويضعها تحت رحمة هذه الشركات التي يكون همها تحقيق الربح المادي على حساب إظهار الحقيقة، فضلا عن الإخلال بمبدأ سرية التحقيق سيما لو تعلق التحقيق بجرائم عرض الأشخاص وأسرارهم الشخصية أو تعلق الأمر بأمن الدولة.[3]

الفرع الثالث: الدليل المناسب لإثبات الجريمة الالكترونية

أولا: تعريف الدليل التقني

[1] البشري محمد الأمين التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من 01 إلى 03 ماي 2000.

[2] رستم هشام محمد فريد، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، ص.115

[3] البشري محمد الأمين، مرجع سابق، ص25.

تعددت التعريف التي قبلت بشأن الدليل التقني وتباينت لذا سنعرض أهم هذه التعريفات فيما يلي:

هناك من يعرفه بأنه: "معلومات يقبلها المنطق والعقل ويعتمد العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة الإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة او جاني او مجني عليه"، أو أنه يشمل "جميع البيانات الرقمية التي يمكن أن تثبت إن هناك جريمة قد ارتكبت".

والدليل الرقمي أو الإليكتروني أو الرقمي هو عبارة عن: كل البيانات التي يمكن أن إعدادها أو تخزينها في شكل رقمي في الحاسوب، ويمكن تعريف البيانات الرقمية بأنها مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات الخرائط الصوت والصورة، أو أنه الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل نبضات كهرومغناطيسية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال من أجل تقديمه أمام أجهزة تطبيق القانون.[1]

وما هو جدير بالذكر أن هناك فرق بين الدليل التقني وبرامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في القيام بمختلف العمليات التي يحتويها النظام المعلوماتي عند إعطاء الأوامر بالقيام بذلك، أما الدليل التقني فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبيها. [2]

ثانيا: تقدير القاضي الجزائي للدليل التقني

إذا توافرت في الدليل التقني الشروط العامة لما يمكن أن يتمثل أساسا لانبعاث الثقة فيه، فإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل وذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، وبالتالي فلا حرية للقاضي في مناقشة الحقائق العلمية الثابتة.

رغم أن هنالك إمكانية التشكيك في سلامة الدليل التقني بسبب قابلية للعبث إلا أن تلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم خاصة إذا توافرت في الدليل التقني الشروط الخاصة بسلامته

[1] رشيدة بوكر، مرجع سابق، ص ص 382، 383.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص 31.

من العبث والخطأ، ورغم ذلك تبقى مسألة الأدلة العلمية والفنية في الإثبات راجعة الى السلطة التقديرية للقاضي لأنه يبقى المسيطر حقيقة وباستطاعته تفسير الشك لصالح المتهم.[1]

ثالثا: حجية الدليل الإليكتروني في الإثبات

إن الخصوصية الجريمة المعلوماتية والتي تتميز بالطابع الفني دفع المشرع الجزائري بأن يبادر في مواكبة التطور القانوني على المستوى الدولي وتماشيا مع التطور التكنولوجي، بتمهيد للطريق أمام استخلاص الدليل الإليكتروني في القانون رقم 04/09 في المادة 06 منه[2]، مراعيا بذلك الإعمال بالقواعد العامة التي من الضروري توافرها في الدليل الإليكتروني وهي مبدأ المشروعية، بمعنى أنه لا يكون مستخلصا بطريقة مخالفة لأحكام القانون ولا مبادئ دستورية خاصة ما تعلق منها بحماية الحريات الأساسية ومما هو مستقر عليه فإن القاضي الجزائري ملزم بفحص الدليل الإليكتروني لكي يتواصل إلى تشكيل قناعة انطلاقا من عرض هذا الدليل على مناقشة الأطراف، وهو ما نصت عليه المواد 212 و 234 من قانون إ . ج. ج. [3]

وبذلك يتضح لنا الدليل التقني له حجية في الإثبات وذلك بما يتميز به من موضوعية وكفاءة، ومحكم وفق قواعد علمية عملية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته ويساعد القاضي من التقليل من الأخطاء القضائية والاقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة. [4]

والاستدلال على ذلك نلاحظ إن الفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشئة عن الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل: الرادارات الأجهزة السنيمائية، أجهزة التصوير، أشرطة التسجيل، أجهزة التنصت. [5]

وبظهور الدليل التقني فقد زاد من دور الإثبات العلمي واستتبعه تعاظم دور الخبراء في القيام بدور فعال في إبداء خبرتهم الفنية، كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في وضع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة عملية قد يصعب إثبات عكسها، مما يدفع هذا الأمر بالاعتقاد بأنه بمقدار اتساع مساحة الأدلة العلمية بمقدار ما يكون انكماش وتضاؤل دور القاضي الجزائي في

---

[1] رشيدة بوكر، مرجع سابق، 507.

[2] المادة 06 من القانون رقم 09/04 والتي تنص: على حجز المعطيات المعلوماتية وذلك بإفراغها أو نسخها على دعامة تخزين إليكترونية قابلة للحجز الوضع في أحراز".

[3] زيبجة، زيدان، مرجع سابق، ص 173.

[4] بوكر رشيدة، مرجع سابق، ص 497.

[5] هلالي عبد الإله أحمد حجية المخرجات الكمبيوترية في المواد الجزائية، الطبيعة الثانية، دار النهضة العربية، القاهرة، سنة 2008، ص ص،42.43.

التقدير خاصة أمام غياب الثقافة المعلوماتية للقاضي[1] ، ولكن هذا لا ينفي حقيقة الضرورة الماسة للدليل لتقني لأنه يتماشى مع طبيعة الجريمة المعلوماتية ومع التطور التكنولوجي الحاصل مما يستدعي الأمر عدم التوقف عند مضمون الدليل الإليكتروني فقط بل يجب التركيز والاهتمام بتطوير الإجراءات التي يترتب عليها الحصول على هذا الدليل مع اشتراط ضرورة مشروعيتها وخلوها من العبث والخطأ باعتبار أن الدليل الإليكتروني أو التقني له حجية في الإثبات خاصة في التشريعات التي تأخذ بمبدأ حرية الإثبات وسلطة القاضي التقديرية كما في التشريع الجزائري.

المطلب الثاني: إجراءات جمع الأدلة التقليدية

تعد عملية جمع الأدلة من أهم مراحل التحقيق الجنائي إذ تشكل الأساس الذي يبنى عليه مسار العدالة، وتعتمد الإجراءات التقليدية لجمع الأدلة على قواعد قانونية وإجراءات ميدانية دقيقة تهدف إلى ضمان صحتها ومشروعيتها.

الفرع الأول: الإجراءات المادية

عند التكلم عن إجراءات التحري كلاسيكية للكشف عن الجريمة المعلوماتية، أول ما يجب دراسته هو معاينة مسرح الجريمة المعلوماتية ويقصد بهذه الأخيرة رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[2] أو هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل ضابط الشرطة القضائية إلى عين مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء".

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات بما فيها التشريع الجزائري في المادة 61 من قانون الإجراءات الجزائية الجزائري، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراء وجوبيا في الجنايات وجوازيا في الجنح، وهي قد تتم في مكان عام أو مكان خاص.

فإذا كانت في مكان عام ضابط الشرطة القضائية لا يحتاج إلى إذن من النيابة العامة بإجرائها، أما إذا كانت بمكان خاص فلابد لصحتها ولمعاينة مسرح الجرائم المعلوماتية يجب التفرقة بين حالتين:[3]

أولا: معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware)

[1] رشيدة بوكر، مرجع سابق، ص 498.

[2] محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008، ص 123.

[3] عمار حشمان، مرجع سبق ذكره، ص 47.

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

ثانيا: معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software)

كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

1. قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.
2. الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة.

ولنجاح المعاينة في الجرائم المعلوماتية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

1. القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.
2. يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.
3. عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.
4. وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.
5. ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

6. التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.
7. القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها [1].

ثالثا: تفتيش الأنظمة المعالجة الآلية للمعطيات وضبطها

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه الضابط الشرطة القضائية بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول على دليل المصلحة التحقيق عن طريق إثبات واقعة معينة،[2]وهو ما سنبرزه فيما يلي:

1. تفتيش نظم المعلوماتية:

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات هي:

أ. **الحالة الأولى:** في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.
ب. **الحالة الثانية:** إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة،

[1] طرشي نورة مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق، جامعة الجزائر 1، 2011-2012 ص131.

[2] يمثل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المادية وهي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة وحدة الحاسوب والمنطق الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة، أنظر: طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الشر الجديدة الاسكندرية، سنة 2009، ص 441

لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن.[1]

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

ج. **الحالة الثالثة:** إذا وجدت مكونات الحاسوب المادية في حالة الحاسبات الآلية المحمولة في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة .... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات[2].

2. تفتيش نظم الحاسوب المنطقية أو المعنوية

يعرف الكيان المنطقي للحاسوب بأنه مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات[3].

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك."

الفرع الثاني: الإجراءات الشخصية (الشهادة، الخبرة)

أولا: الشهادة في الجريمة الإلكترونية

[1] طرشي نورة، المرجع السابق، ص 115.

[2] طارق إبراهيم الدسوقي عطية، مرجع سبق ذكره، ص 385.

[3] عفيفي كامل عفيفي، مرجع سبق ذكره.

الشهادة هي إخبار شخص شفويا للسلطة المختصة عما شاهده بنفسه أو عاينه بحاسة من حواسه"[1]

تعد الشهادة من أقدم وسائل الإثبات وأبرزها، فقد نص عليها القرآن الكريم في العديد من آياته، كما نصت عليها مختلف التشريعات الجنائية، لأن الجريمة ليست تصرفا قانونيا، ولكنها عمل غير مشروع، يجتهد الجاني في التكتم عند ارتكابه، ويحرص على إخفائه عن أعين الناس.

ولا تقل أهمية الشهادة في الجريمة الماسة بالمعطيات، حيث يقوم الشاهد الإلكتروني بتقديم معلومات حصلها بالملاحظة الحسية.

1. تعريف الشاهد في الجريمة الإلكترونية:

هو الشخص الفني صاحب الخبرة، والمتخصص في تقنية وعلوم الحاسب الآلي والاتصالات، بحيث تكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للمعطيات[2]، ولذلك يطلق عليه اسم الشاهد الإلكتروني تمييزا له عن الشاهد التقليدي[3].

ينحصر الشاهد الإلكتروني في عدة فئات هي:

أ. **مشغلو الحاسب الآلي:** عامل تشغيل الحاسب الآلي هو ذلك الشخص المسؤول عن تشغيل النظام والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.[4]

ب. **خبراء البرمجة:** وهم الأشخاص المختصين في كتابة أوامر البرامج وهم فئتين مخططو برامج التطبيقات، مخططو برامج النظم[5].

ج. **محللون:** المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع البيانات لنظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات.

---

[1] محمد نجم صبحي، الوجيز في قانون أصول المحاكمات الجزائية، ط2، (الأردن: دار الثقافة (2012)، ص 301، إحمود فاتح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائية (دراسة مقارنة)، ط2، (الأردن: دار الثقافة (2010)، ص 33 عبد الحميد عمارة ضمانات الخصوم أثناء مرحلة المحاكمة الجزائية في التشريعين الوضعي والإسلامي، د. ط (الجزائر، دار الخلدونية (2010)، ص 455.

[2] حكيم سياب الإعلام الآلي والقانون، ص: 149.

[3] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، ط1، (مصر: دار الفكر الجامعي، 2006)، ص 339.

[4] على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، ص: 62

[5] علي عدنان الفيل، مرجع سابق، ص 62.

د. **مهندسو الصيانة والاتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة بها.

هـ. **مديرو النظم:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.[1]

2. التزامات الشاهد في الجريمة الإلكترونية:

متى كان الشاهد المعلوماتي حائزا لمعلومات جوهرية تفيد سير التحقيق، فإنه يكون ملزما بأن يعلم بها جهات التحقيق وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة – ذلك في غير الأحوال التي يجيز له القانون فيها ذلك – والمعلومات الجوهرية التي يجب على الشاهد إفادة سلطات التحقيق بها تتركز على العناصر التالية:

أ. طبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو الدعامات الأخرى، على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق؛

ب. لإفصاح عن كلمات المرور؛

ج. الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.[2] "

ثانيا: الخبرة التقنية

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاة أو سلطات الاستدلال على حد سواء، فكلما استعصى عليهم فهم موضوع معين يتميز بتقنية ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد جرائم الواقعة على المعطيات، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الحاسوب.

1. تعريف الخبرة:

[1] على عدنان الفيل، مرجع سابق، ص،62.

[2] حكيم سياب، الإعلام الآلي والقانون، ص 152

هي إعطاء الرأي الفني أو العلمي من أهل الصنعة والفن والاختصاص، ينتدبهم القاضي بخصوص واقعة تتعلق بالإثبات في الدعوى الجزائية، ويتوقف عليها الفصل في تلك الدعوى، والرأي الذي يعطيه الخبير يعد دليلا يخضع للسلطة التقديرية للقاضي وقناعته الوجدانية.[1]

فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو تحديد مدلولها بالاستعانة بالمعلومات العلمية، والتي لا تتوافر سواء لدى المحقق أو القاضي وإذا كان للخبرة تلك الأهمية في الجرائم التقليدية، فإن أهميتها تزداد في الجريمة الإلكترونية، لذا وجب معرفة القواعد التي تحكم الخبرة التقنية.

2. القواعد التي تحكم الخبرة التقنية:

إن للخبرة التقنية قواعد تحكمها منها القانونية وأخرى فنية.

أ. **القواعد القانونية:** هي تلك الأحكام المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء[2] وواجبات الخبير منها حلف اليمين[3] وخضوعه للرقابة القضائية[4] وقيامه بأداء مهامه بنفسه[5]، واستجابته لطلبات الخصوم[6] وإيداع التقرير خلال المدة المحددة[7].

ب. **القواعد الفنية:** وتشمل خطوات الاشتقاق لدليل الإلكتروني والتي تتمثل في خطوات ما قبل التشغيل والفحص وخطوات التشغيل والفحص، وتحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني، ومرحلة تدوين النتائج وإعداد التقرير، أما بالنسبة لأدوات جمع الدليل الإلكتروني وتشمل كل من برنامج إذن التفتيش وقرص بدء تشغيل الكمبيوتر وبرنامج معالجة الملفات وبرامج الاتصالات"[8].

لكن مهما بلغت القوة التكنولوجية للدولة فلا تستطيع مواجهة الإجرام الإلكتروني لوحدها، بل لا بد من التعاون الدولي في مجال الخبرة التقنية[9].

---

[1] محمد سعيد نمور أصول الإجراءات الجزائية شرح لقانون أصول المحاكمات الجزائية، ص: 240، فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، ط3، (الأردن دار الثقافة (2010) ص 11.

[2] المادة 144 ق إ ج.

[3] المادة 145 ق إ ج

[4] المادة 148 ق إ ج.

[5] المادة 143 من الفقرة 5 ق إ ج.

[6] المادة 153 من الفقرة 3 ق إ ج.

[7] المادة 153 من الفقرة الأخيرة ق إ ج.

[8] لتفصيل أكثر أنظر عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، ص، ص: 147-151.

[9] عائشة بن قارة مصطفى، مرجع سابق، ص 152.

المطلب الثالث: اجراءات جمع الأدلة الحديثة

مع تطور التكنولوجيا وظهور أنماط جديدة من الجريمة برزت الحاجة إلى تطوير أساليب جمع الأدلة بما يواكب هذا التحول، وقد أصبحت الإجراءات الحديثة لجمع الأدلة تعتمد على وسائل رقمية وتقنية متقدمة تمكن من تتبع الجريمة وتوثيقها بدقة وفعالية.

الفرع الأول: حفظ المعطيات

ألزم المشرع الجزائري مقدي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين، في حين اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير) معطيات المرور)، وهي كما عرفتها المادة الثانية من قانون رقم 09-04 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة، باعتبارها جزءا في حلقة الاتصالات توضح مصدر الإتصال، الوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة، وقد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من القانون رقم 09-04 وتتضمن:[1]

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها المعطيات التي تسمح بالتعرف على المرسل إليه، الإتصال وكذا عناوين المواقع المطلع عليها وبما أن حفظ المعطيات إجراء وقتي، واحتراما للحق في الخصوصية، فإن المشرع الجزائري فرض على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل، إن مزودي الخدمات يعتبرون مصدرا لجهات التحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها.

[1] سعيداني نعيم، ليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 139.

الفرع الثاني: التسرب واعتراض المراسلات الالكترونية

استحدث المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات، وتتمثل هذه الإجراءات في التسرب الشهادة والخبرة التقنية.

أولا: التسرب

أدرج المشرع الجزائري عملية التسرب بموجب قانون 06-22 المتضمن قانون الإجراءات الجزائية، والذي أفرد الفصل الخامس منه تحت عنوان" في التسرب"، والذي تضمن 8 مواد من المادة 65 مكرر 11 حتى المادة 65 مكرر 18 ، وتناول من خلالها تحديد مفهوم هذه العملية وشروط إجرائها، العمليات المبررة وأخيرا الحماية الجنائية للقائم بعملية التسرب، والتي تعني قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية الكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك[1].

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة مثلا، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم وتصح عملية التسرب إذا توفرت الشروط التالية:

1. صدور أذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
2. أن يكون الإذن مكتوبا ومسيبا
3. يحدد مدة التسرب التي لا يمكن أن تتجاوز 4 أشهر غير أنه يمكن أن تحدد.[2]

ثانيا: الشهادة

تعرف الشهادة بصفة عامة أنها: "الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها[3].

ويقصد بالشاهد في الجريمة الإلكترونية هو الشخص الفني صاحب الخبرة والتخصص في تقنية المعلومات، والذي يمكنه الدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب ذلك، لذلك يطلق عليه بالشاهد المعلوماتي تمييزا له عن الشاهد التقليدي وينحصر في مشغلي الحاسب الآلي، المحللون، خبراء البرمجة، مهندسو الصيانة والاتصال ومديرو النظم، أما الشهادة الإلكترونية فتفترض هذه

[1] فاطمة الزهرة بوعناد، المرجع السابق، ص 70.

[2] فاطمة الزهرة بوعناد، المرجع السابق، ص 70.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص 77.

النوعية من الشهادة حصولها أمام قاضي الموضوع حيث يكون الشاهد غير حاضر جسديا في جلسة المحاكمة إلا أنه يظهر بشكل سمعي ومرئي.[1]

ثالثا: الخبرة التقنية

تكتسي عملية ندب الخبير خلال التحقيق في الجرائم الإلكترونية أهمية بالغة، نظرا لطبيعتها الفنية والتقنية التي تتميز بها، وكذلك التنوع الأجهزة في هذا المجال وسرعة 4 تطورها، وندب الخبير من سلطات المحقق[2] وليس هناك في القانون ما يلزم بذلك، ويحدد المحقق للخبير المهمة التي كلف بها وميعاد تسليمه لتقريره كما يجب عليه أن يؤدي اليمين القانونية بهذا الخصوص.

وتخضع الخبرة التقنية في أغلب التشريعات المقارنة إلى نفس أحكام الخبرة القضائية من حيث القواعد التي تحكم عمل الخبير وإجراءاته، فبالنسبة للمشرع الجزائري تناول أحكام الخبرة في المواد من 143 إلى 155 من قانون الإجراءات الجزائية. وتكمن أهمية الخبرة التقنية أن جهات التحري والتحقيق كثيرا ما تفشل في جمع الأدلة الرقمية، بل إن المحقق في كثير من الأحيان ما يتسبب في تدمير الدليل الرقمي إما نتيجة خطأ أو إهمال أو جهل في التعامل معه، وعموما يراعي في الخبير أن تتوافر لديه القدرات الفنية والإمكانيات العلمية في مسألة موضوع الخبرة.[3]

رابعا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يقصد بها أن تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين الاستقبال والعرض التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.[4]

وقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو في الجرائم المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية

[1] محمد بن فردية، المرجع السابق، ص 152–159

[2] المادة 143 من قانون رقم 06–22 المعدل والمتمم لقانون الإجراءات الجزائية، المرجع السابق.

[3] محمد بن فردية، المرجع السابق، ص 164 165.

[4] جمال براهيمي، المرجع السابق، ص 139.

وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة او عمومية، أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

المطلب الرابع: صعوبة مكافحة الجريمة الالكترونية

يعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية وذلك للأسباب التالية:

1. يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.
2. صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام اسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.
3. تنازع القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج –فأي من القوانين سوف يخضع لها الجاني؟
4. صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الاتصال، أم مورد المنافذ، أم مورد المعلومات، أو غيرهم من العاملين في مجال الأنترنت.
5. افتراض العلم بقانون جميع الدول، ففي حالة ارتكاب الجريمة في بلد ما، وتحقق النتيجة في بلد آخر يجد الجاني نفسه يخضع لقانون هذه الدولة، وقد يكون هذا الفعل المرتكب مباح في بلده.
6. صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص.
7. جهل الناس بثقافة الأنترنت يجعلهم يقومون بأفعال لا يعرفون بأنها تشكل جريمة يعاقب عليها القانون.[1]
8. عدم ظهور الدليل المادي للجريمة الإلكترونية أو آثار مادية ملموسة.
9. عجز الوسائل التقليدية عن ضبط آثار الجريمة الإلكترونية.[2]

[1] جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات** رؤية جديدة للجريمة الحديثة، دار البلدية، عمان الأردن، 2007، ط 01، ص من 220 إلى223.

[2] عبد الفتاح بيومي حجازي، **الإثبات الجنائي في جرائم الكمبيوتر والأنترنت** دار الكتب القانونية، مصر، 2007، ص 105.

10. عولمة هذه الجريمة تؤدي إلى تشتيت جهود التحري والتنسيق الدولي، لتعقب مثل هذه الجرائم، وهي بمثابة صورة صادقة من صور العولمة.[1]
11. صعوبة تقدير حجم الجريمة الإلكترونية، فالإحصائيات الجنائية لا تعبر عن الإجرام الحقيقي
12. إذ منها ما يصل إلى علم السلطات المختصة بصورة دائمة، ومنها ما لا يصل إلى علمها إلا نادرا، كالجرائم الماسة بالعرض، وهنا يظهر الفارق بين الحجم الحقيقي للجريمة الإلكترونية، وبين ما هو مسجل بالإحصائيات.[2]

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت 2007، ط01، ص33.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت 2005، ط01، ص68.

خلاصة الفصل:

تشهد الجريمة الإلكترونية تطورا متسارعا في ظل الثورة الرقمية وتوسع استخدام تكنولوجيا المعلومات، مما فرض على المشرع الجزائري ضرورة مواكبة هذه التحديات بوضع إطار قانوني فعال للوقاية منها ومكافحتها، وقد تمثلت أبرز آليات مكافحة الجريمة الإلكترونية في الجزائر في سن قوانين خاصة أهمها الأمر رقم 09-01 المعدل والمتمم لقانون العقوبات، والذي أدرج نصوصا تجرم أفعالا إلكترونية كاختراق الأنظمة المعلوماتية، التزوير الإلكتروني، والاحتيال عبر الإنترنت.

كما عزز المشرع هذه الآليات بوسائل إجرائية خاصة، كإتاحة وسائل الإثبات الرقمية وتوسيع صلاحيات الضبطية القضائية في التعامل مع الجرائم الإلكترونية، إضافة إلى التعاون الدولي في هذا المجال، ورغم هذه الجهود لا تزال الحاجة قائمة لتحديث المنظومة التشريعية وتدعيم القدرات التقنية والبشرية لمواجهة التطورات المتسارعة لهذا النوع من الجرائم.

خاتمـــــــــــــــة

وفي الأخير فإنني حاولت معالجة هذا الموضوع من خلال التطرق إلى فصلين أساسين حيث تناولت في الأول الى ماهية الجريمة الإلكترونية الظي قسمته بدوره إلى مبحثين تطرقنا في المبحث الأول إلى تعريف الجريمة الإلكترونية وأصنافها وخصائصها التي جعلها تتفرد عن نظيرتها التقليدية سواء تعلق الأمر الجريمة أو المجرم بحد ذاته أما المبحث الثاني فقد تطرقنا إلى الجرائم الإلكترونية وفق ما جاء به التشريع الجزائري لمعالجتها في الفصل الآخر ولخطورة هذه الجريمة وتهديد أمن المجتمع جعلت المسنن الجزائري يتصدى لها بشتى الطرق و مكافحتها و هذا ما تناولناه في الفصل الثاني الذي تطرقنا فيه إلى آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري الذي عالجنا في المبحث الأول الحماية الموضوعية في النظام المعلوماتي أما المبحث الثاني فقد تناولنا فيه الحماية الإجرامية للنظام المعلوماتي ، إذ أن المشرع قام بتعديل قانون العقوبات رقم 04-15 و إصدار قانون رقم 09-04 لما يتناسب بالظاهرة المستجدة.

ومن خلال هذه الدراسة توصلنا إلى النتائج التالية: الجريمة الإلكترونية تعد من أبرز التحديات التي فرضتها التطورات الإلكترونية الحديثة، خاصة وأنها تختلف عن الجرائم التقليدية من حيث الوسائل والأساليب وحتى الأهداف. أما التشريع الجزائري ورغم محاولاته لمواكبة هذا النوع من الجرائم لايزال يعاني من بعض النقص سواء من الناحية القانونية أو الوسائل المتوفرة للتحقيق والردع، وتبين أيضا ان الجرائم الالكترونية تمس عدة مجالات، مثل المساس بالأنظمة المعلوماتية، التعدي على الملكية الفكرية، والاعتداء على الأشخاص والأموال، وهو ما يفرض تدخل تشريعي وتنظيمي أكثر دقة وفعالية. كما أن اليات الحماية والتحقيق كما ورد في الفصل الثاني، تحتاج إلى تطوير تقني وتنسيق بين مختلف الجهات المختصة مع ضرورة تعزيز التعاون الدولي بالنظر للطابع العابر للحدود لهذه الجريمة.

وعلى هذا فإننا يمكن الخروج بتوصيات منها العمل على تطوير الإطار القانوني باستمرار لمواكبة تطورات الجريمة الإلكترونية، دعم التكوين والتأهيل المستمر للقضاة وأعوان الضبطية في هذا المجال، إنشاء وحدات أمنية وقضائية متخصصة في محاربة الجريمة الإلكترونية، تعزيز التعاون الدولي نظرا للطبيعة العابرة لحدود هذه الجرائم، تشجيع البحث العلمي والدراسات الجامعية المتخصصة في هذا المجال تكثيف حمالات توعية وتحسيس حول مخاطر الجريمة الإلكترونية.

قائمـــــــة المحتويـــــات

قائمة المحتويات

قائمـــة المصـــادر والمراجـــع

قائمـة المصـــادر والمراجـع

أولا: المصادر

I. النصوص القانونية:

1. الأمر رقم 03-05، الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المحاورة، ج.ر عدد 44.
2. الأمر رقم 03-07 الصادر في 19 يوليو 2003 المتعلق ببراءات الإختراع، ج.ر عدد 44.
3. الامر رقم 03-08، المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة بتاريخ 2003/07/23، الجريدة الرسمية رقم 36.
4. قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يتضمن قانون العقوبات، جريدة رسمية عدد 71، 2004 معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 07، المضافة بموجب القانون نفسه.
5. القانون رقم 06-23 مؤرخ في 20 ديسمبر 2006، المعدل والمتمم، الجريدة الرسمية عدد 84، الصادرة في 24 ديسمبر 2006، المعدل والمتمم
6. القانون رقم 09-04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج والعدد 47 .
7. القانون رقم 15-12 المؤرخ في 28 رمضان 1436، الموافق لـ 15 يوليو 2015، المتعلق بحماية الطفل، الصادر بالجريدة الرسمية يوم 09 يوليو 2015، العدد 39.
8. القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
9. قرار وزير الداخلية المصري رقم 13507 لسنة 2002 الصادر بتاريخ: 2002/07/17.

ثانيا: المراجع

I. الكتب:

1. أحمد فتحي سرور، الوسيط في قانون الإجرءات الجنائية، دار النهضة العربية، الطبعة 07، القاهرة، مصر، 1993.
2. أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الاردن، 2014.

3. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الطبعة الثانية، الجزائر، 2007.
4. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.
5. بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، ط01، الجزائر، 2007.
6. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، لبنان، ط 1، 2012.
7. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البلدية، عمان الأردن، 2007، ط 01.
8. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002.
9. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2002.
10. حلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان لأردن، 2010، ط 01.
11. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.
12. ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، عين مليلة، الجزائر، 2010.
13. الخن محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، 2010.
14. دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية–دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ط 1، 2016.
15. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.
16. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني لحماية المعلوماتي، دار الجامعة الجديدة، القاهرة، مصر، 2009.
17. عادل عبد العال ابراهيم حزامني، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

18. عادل عزام، سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة في وسط الالكتروني، دار الثقافة للنشر والتوزيع، طبعة الأولى، عمان، الأردن، 2011.
19. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007.
20. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1.
21. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، ط1، دار الفكر الجامعي، مصر، 2006.
22. عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية.
23. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ط 01.
24. العربي شحط عبد القادر، نبيل صفر، الإثبات في المواد الجزائية، دار الهدى عين مليلة، الجزائر.
25. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط 02، 2000.
26. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى دار النهضة العربية، القاهرة 2004.
27. غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، (د.ط)، 2016.
28. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007.
29. محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008.
30. محمد عبد الرحيم الناغي، الحماية الجنائية للرسوم والنماذج الصناعية، (دراسة مقارنة) دار النهضة العربية، القاهرة، مصر، 2009.
31. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009.
32. مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) –دراسة مقارنة–، دار الخلدونية، الجزائر، 2018.
33. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت 2005، ط01.

34. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005.
35. نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
36. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 174.
37. هلالي عبد الإله أحمد حجية المخرجات الكمبيوترية في المواد الجزائية، الطبيعة الثانية، دار النهضة العربية، القاهرة، سنة 2008.
38. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2019.
39. يوسف حسين يوسف، الجريمة الدولية للأنترنت، المركز القومي الإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2011.

ثالثا: المذكرات

1. بلعالم فريدة، المسؤولية القانونية عن الاستخدام غير المشروع لبطاقة الائتمان، مذكرة ماجستير تخصص قانون الأعمال، قسم الحقوق، جامعة محمد لمين دباغين سطيف.
2. بن موسى خديجة، الحماية الجنائية للمعطيات في المجال المعلوماتي، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2022.
3. بوبقرة خيرة، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم، 2020/2019.
4. بوخبرة عائشة الحماية الجزائية من الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، تخصص قانون جنائي، جامعة وهران، 2013.
5. جدي نسيمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2014/2013.
6. خالد حامد مصطفى، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الإجتماعي، كلية القانون، جامعة عمان، 2013.
7. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2011-2012.

8. سارة مقراني، جريمة الإستغلال الجنسي للأطفال عبر الإنترنت، مذكرة تكميلية لنيل شهادة الماستر، جامعة العربي بن مهيدي، كلية الحقوق والعلوم السياسية، أم البواقي، الجزائر، 2016/2015.
9. سعيداني نعيم، ليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013.
10. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة ابوبكر بلقايد، تلمسان، 2010-2011.
11. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال جامعة مولود معمري تيزي وزو 06/03/2013، ص 09، نقلا عن كحلوش علي جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني العدد 84، 2007.
12. طرشي نورة مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق، جامعة الجزائر 1،2011-2012.
13. عكاشة مخلوف، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، جامعة د طاهر مولاي، سعيدة، الجزائر، 2017/2016.
14. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، تخصص: إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح، ورقلة، الجزائر، 2019.
15. فاروق خلف، الآليات القانونية لمكافحة الجريمة الإلكترونية، مجلة الحقوق والحريات، قسم الحقوق، كلية الحقوق، جامعة حمة لخضر الوادي، العدد 02، الجزائر، 2015.
16. فضيلة تراموشت، جرائم الإنترنت الماسة بالأطفال، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2014.
17. محمد نصير السرحاني، مهارات التحقيق الفني في الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

رابعا: المقالات

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة بمقر جامعة الدول العربية، مصر بتاريخ 21-12-2010.
2. بسام الزعبي، النصب والاحتيال عبر منصات التواصل الاجتماعي، مقال منشور على الإنترنت www.alrai.com تاريخ النشر: 2022/02/19 10:29 تاريخ الإطلاع: 2025/03/10، ساعة 14:30.
3. البشري محمد الأمين التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من 01 إلى 03 ماي 2000.
4. بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس 2013، العدد 01.
5. جازية سليماني، موقع العربي الجديد، تاريخ الدخول،09/02/2017الساعة http//www.ala
6. حسين سعيد بن سيف الغافري، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007.
7. ذبيح هشام، وسائل الدفع ما بين الحماية التقنية والقانونية للمستهلك الإلكتروني، مجلة الاجتهاد القضائي، العدد 14، جامعة بسكرة، 2017.
8. رستم هشام الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة 11 العدد 2، 1999.
9. رستم هشام محمد فريد، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت.
10. سامية عزيز، مازيا عيساوي، الجريمة من منظور سوسيولوجي الأسباب الآثار، مجلة دراسات في سيكولوجية الإنحراف، المجلد 6 العدد 1، 2021.
11. سحر فؤاد مجيد، جريمة التحرش الجنسي بالأطفال عبر الإنترنيت، المجلة الأكاديمية للبحث القانوني، عدد خاص 2017، جامعة بغداد العراق.
12. سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث.
13. عبد الله حسين، محمود إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003.
14. عثماني عزالدين، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله تيبازة، المجلد الثاني، العدد 04، 2018.

15. على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية.
16. عماد دمان ذبيح، سمية بهلول، الآليات العقابية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 13، جامعة عباس لغرور خنشلة، الجزائر، 2020.
17. كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية حلب 21/23/ تشرين الأول، 2000، بدون صفحة.
18. محمد سعيد نمور أصول الإجراءات الجزائية شرح لقانون أصول المحاكمات الجزائية، ص: 240، فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، ط3، دار الثقافة الأردن، 2010.
19. محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة عمان الأردن.
20. محمد نجم صبحي، الوجيز في قانون أصول المحاكمات الجزائية، ط2، (الأردن: دار الثقافة (2012)، ص 301، إحمود فاتح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائية (دراسة مقارنة)، ط2، (الأردن: دار الثقافة (2010)، ص 33 عبد الحميد عمارة ضمانات الخصوم أثناء مرحلة المحاكمة الجزائية في التشريعين الوضعي والإسلامي، د. ط (الجزائر، دار الخلدونية (2010).
21. مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، مقال مقدم إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-2012/09/25.
22. مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية، العدد 21، 2012.
23. هشام رستم الحواسب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة أسيوط، 2000.

المراجع باللغة الأجنبية

1. Article 323-1/2 Lorsqu 'il en est résulté soit la suppression ou la modification de données contenues dans le système, sait une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende, modifié par LOI Nº 2015-912 du 24 JUILLET 2015-ART 4JORF N° 0171 du 26 JUILLET 2015.
2. Article 323-1/2: Lorsqu 'il en est résulté soit la suppression ou la modification de données contenues dans le système, sait une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende, modifié par LOI Nº 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.
3. Article 323-3; Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de

transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € D'amende, modifié par LOI N° 2015-912 du 24 JUILLET 2015-ART 4 JORF N° 0171 du 26 JUILLET 2015.

4. Myriam QUEMENER Cybercriminalité-droit pénal appliqué economica, Septembre 2010, p208.

الملخص:

يتناول هذا البحث موضوع الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، نظرا لكون هذا النوع من الجرائم أصبح يشكل خطرا متزايدا على الأفراد والمؤسسات، في ظل الاستخدام الواسع لتكنولوجيا الإعلام والاتصال، كما يهدف البحث إلى تعريف دقيق للجريمة الإلكتروني، وبيان خصائصها التي تميزها عن الجرائم التقليدية، بالإضافة إلى تصنيف أهم أنواعها، مثل اختراق الأنظمة، الاحتيال الإلكتروني، وانتهاك الخصوصي. كما تطرقنا على دراسة كيفية تعامل المشرع الجزائري مع هذه الجرائم من خلال استغلال النصوص والقوانين التي تهدف إلى الوقاية منها ومعاقبة مرتكبيها.

تم اعتماد المنهج التحليلي في معالجة موضوع البحث، من خلال تحليل القوانين الجزائرية ذات الصلة كقانون العقوبات والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إضافة إلى الرجوع لدراسات سابقة ومراجع، كما أن المشرع الجزائري قام بمجهودات معتبرة في هذا المجال، حيث تم إدراج نصوص قانونية تهدف إلى حماية المعطيات الشخصية والأنظمة المعلوماتية، وتوفير أدوات قانونية للتحقيق في الجرائم الرقمية. ومع ذلك ما تزال صعوبات وتحديات مثل تطور الوسائل التقنية للجريم، وضعف التكوين في المجال الرقمي، مما يجعل من الضروري تعزيز التشريعات، وتحديثات بصفة مستمرة، وتكوين مختصين في التحقيقات الإلكترونية، إضافة إلى دعم التعاون الدولي لمواجهة هذا النوع من الجرائم بشكل فعال وشامل.

الكلمات المفتاحية:

الجريمة الإلكترونية، المعالجة الآلية للمعطيات، الحماية الجنائية، المسؤولية الجزائية، قانون العقوبات.

Abstract:

This research addresses the topic of cybercrime and the mechanisms for combating it in Algerian legislation, given that this type of crime has become an increasing threat to individuals and institutions, in light of the widespread use of information and communication technology. The research also aims to provide a precise definition of cybercrime, highlight its characteristics that distinguish it from traditional crimes, and classify its most important types, such as system hacking, electronic fraud, and privacy violations. We also examine how Algerian lawmakers deal with these crimes by utilizing texts and laws aimed at preventing them and punishing their perpetrators.

An analytical approach was adopted to address the research topic, through analyzing relevant Algerian laws, such as the Penal Code and Law No. 09-04 on the

Prevention of Crimes Related to Information and Communication Technology, in addition to consulting previous studies and references. Algerian lawmakers have also made significant efforts in this area, including legal texts aimed at protecting personal data and information systems and providing legal tools for investigating digital crimes. However, difficulties and challenges remain, such as the development of technical means of crime and the lack of training in the digital field. This makes it necessary to strengthen legislation, provide ongoing updates, and train specialists in electronic investigations, in addition to supporting international cooperation to effectively and comprehensively combat this type of crime.

Keywords:

Cybercrime, automated data processing, criminal protection, criminal liability, penal code.