جامعة مولود معمري – تيزي وزو–
كلية الحقوقوالعلوم السياسية
قسم حقوق

خصوصية الجريمة الإلكترونية في ظل القانون الجزائري

مذكرة لنيل شهادة الماستر في القانـــــــــون
تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبة:
مقاني كريمة

إشراف الأستاذة:
د/ عيلام رشيدة

لجنة المناقشة:

د/ اقلولي ولد رابح صافية (**استاذ**)، **جامعة مولود معمري، تيزي وزو .....رئيسا.**

د/ عيلام اكسوم رشيدة (أستاذ محاضر قسم أ)، جامعة مولود معمري، تيزي وزو...مشرفا ومقررا.

د/ زايدي حميد (أستاذ)، جامعة مولود معمري، تيزي وزو، .....ممتحنا.

تاريخ المناقشة: 2023/10/01

كلمة شكر

إلى الأستاذة: اكسوم/عيلام رشيدة

أتقدم بجزيل الشكر لكم أستاذتي الفاضلة على

إشرافكم على انجاز هذه المذكرة ولكم مني كل

الامتنان والتقدير لكافة مجهوداتكم، فلكم الفضل في

القيام بهذا العمل المتواضع.

إهداء

إلى كل

أفراد العائلة، الأصدقاء، الزملاء وكل من ساهم في

إنجاز هذا العمل....

كريمة

المقدمة

مقدمة

شهدت الإنسانية خلال السنوات القليلة الماضية أعظم ابتكار قدمته البشرية، نتيجة التطور المتسارع في مجال تكنولوجيا الإعلام والاتصال، فالعالم اليوم يعيش أرقى عصورها لعلمية والتكنولوجية بسبب هذا الابتكار الذي يتمثل في التكنولوجيا الرقمية والذكاء الاصطناعي، وما نتج عنه منثورة معلوماتية بالغة الأهمية، حتى بات يطلق على هذا العصر بعصر المعلومات، حيث صار العالم عبارة عن قرية صغيرة لا يعترف فيها بالحدود الجغرافية ولا السياسية، كما أحدثت تغيرا في المجتمع، حيث ساهمت في تطوره من خلال اعتماده في مختلف مجلات الحياة اليومية، إذا أصبحت مصدرا أساسيا للأشخاص والمؤسسات في كافة شؤونهم نظرا لامتيازها بالسرعة والدقة في معالجة المعلومات وتخزينها في ظرف قصير.

وعليه تتجسد تقنية المعلومات أساسا، في الانتشار الواسع لشبكة الانترنيت وأجهزة الحاسوب التي تتطور بشكل مستمر، وتستعمل برامج متقدمة وشبكات اتصال محلية وعالمية لا نكاد نستغني يوميا عن هذه التقنية في تسيير شتى مجلات حياتنا، إذا أتاح الفضاء السيبيري الاتصال المستمر بين الدول، بفضل شبكة الانترنت التي تشهد حضورا في جميع الميادين العلمية، البحثية، الاقتصادية، السياسية والاجتماعية على السواء، ومن جهة أخرى مكنت تقنية المعلومات من تطوير أنظمة المعلومات بهدف الاطلاع على المعلومات وتبادلها ومعالجتها آليا بواسطة الحاسوب الآلي وشبكة الانترنت، كما فتحت مجلات واسعة أمام الدول للمضي قدما في تجسيد متطلبات الحكومة الإلكترونية والاعتماد على التجارة الإلكترونية مثل استعمال الدفع الإلكتروني والنقود الإلكترونية والبنوك الإلكترونية ....الخ

ولكن بالمقابل أدى سوء استخدام هذا القضاء الافتراضي إلى ظهور نوع جديد من الجرائم و التي يصطلح عليها ب"الجرائم الإلكترونية "أو" الجرائم المعلوماتية" ذات طبيعة خاصة، تختلف في مفهومها

وأركانها ووسائل ارتكابها ونوعية الجناة والمجني عليهم على الجرائم التقليدية المعروفة، مما خلق صعوبات بالغة لأجهزة البحث والتحري لملاحقة المجرم الإلكتروني وتوقيع العقاب عليه فالنشاط الإجرامي لم يعد مقتصرا على الوسائل التقليدية المعروفة فقط، بل صار يعتمد بالإضافة إلى ذلك على وسائل أكثر حداثة وذلك بالاستعانة بنظم المعلومات والاتصالات، وهذا ما يجسد الجانب المظلم الذي يواجهه المشرع الجنائي خاصة في إثبات هذا النوع من الجرائم.

فالجرائم المرتكبة باستخدام وسائل التقنية عبر الانترنت تعد من الموضوعات الحديثة التي فرض تنفسها على المستوى الوطني والدولي على السواء والتي ينبغي على المشرع الجنائي مكافحتها بنصوص رادعة، وهو ما يشكل محور اهتمام المجتمع الدولي كونها من الجرائم المستحدثة التي تستدعي المواجهة، ووضع حد لانتشارها، فكان لابد من وضع قوانين ملائمة جديدة أو تعديل القوانين السارية المفعول بما يتلاءم مع هذه الظاهرة، بالإضافة إلى تحديد شروط استعمال هذه الوسائل في مختلف المعاملات من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في إطار الاتفاقيات الدولية.

والجزائر باعتبارها واحدة من الدول التي عرفت هذا النوع من التطور التكنولوجي سواء كان ايجابيا أو سلبيا؛ فهي أيضا معنية بالتصدي لهذه الظاهرة، فكان لابد من إيجاد حلول مناسبة لسد الفراغ القانوني انطلاقا من تجريم وعقاب مرتكبي الجريمة الإلكترونية، وذلك بتحديد مجموعة من الأحكام لقيام هذه الجرائم وتحديد العقاب المقرر لها، بالإضافة إلى وضع مجموعة من الإجراءات، منها ما يعتبر مشتركا بين الجرائم التقليدية والجرائم المستحدثة عن طريق تعديل قانون الإجراءات الجزائية باستحداث وسائل وإجراءات خاصة تتماشى وخصوصية وطبيعة هذه الجرائم المستحدثة كالجريمة الإلكترونية فنجد منها

إجراءات تطبق فقط على هذا النوع من الجرائم الإلكترونية حيث تم النص عليها في قانون المستقل يتضمن القواعد الخاصة للوقاية من جرائم المساس بتكنولوجيا الإعلام والاتصال ومكافحتها

القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]،إذ بدون هذه القواعد لا يمكن للمتحري أو المحقق الكشف عن مرتكبي هذه الانتهاكات وتقديمهم للمحاكمة وعرض الأدلة التي هي في شكل إلكتروني وفي عالم افتراضي إذ يوجد اختلاف جوهري في المبادئ التي تحكم إجراءات مكافحة هذه الجرائم، فخصائص هذه الأخيرة تفرض إيجاد قواعد إجرائية مختلفة سواء من حيث الأشخاص والهيئات التي تساهم في مكافحتها.

وتهدف هذه الدراسة إلى تحديد المفاهيم القانونية المتعلقة بالجريمة الإلكترونية، وإجراءات تحصيل الدليل في إثبات الجريمة في ظل النصوص القانونية الحالية في التشريع الجزائري على الرغم من الصعوبات التي واجهتها في إعداد هذه المذكرة منها المراجع التي يمكن الاعتماد عليها، بسبب حداثة الموضوع واتصاله بالتقنية والتكنولوجيا.

تم اختيار موضوع الدراسة لأسباب عديدة، منها الذاتية التي تكمن في طبيعة موضوع الجريمة الإلكترونية الذي يدخل في اختصاصي الشخصي في الحياة المهنية واهتمامي بمجال الجرائم الإلكترونية المستحدثة التي باتت ترتكب بكثرة في الوقت الراهن.

والأسباب الموضوعية تكمن في كون الجريمة الإلكترونية موضوع حديث، بالتالي إلقاء الضوء على هذه الظاهرة الجديدة التي تمس كل الميادين بسبب الاستخدام المتزايد للأنظمة المعلوماتية، مما أفرز

1 قانون رقم 09-04 مؤرخ 5 غشت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 71 صادر في 10 نوفمبر 2004

كثرة الانتهاكات وقصور الحماية القانونية، كون هذه الجريمة تحتاج إلى تنسيق وتعاون دولي لمكافحتها، حيث أصبحت من أبرز أفعال الإجرام محاولة مني إلى الإلمام ومعرفة الأساليب الحديثة والمتبعة في مواجهة الجريمة الإلكترونية والتصدي لها.

لقد زاد من أهمية الموضوع صعوبة تطبيق النصوص التقليدية على هذه الجرائم وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة الجريمة الإلكترونية حيث قامت بإعادة النظر في قوانينها لتجريم هذه الأفعال والاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، والقواعد الإجرائية الحديثة التي جاء بها تعديل قانون الإجراءات الجزائية وكذا القانون 09- 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، و غيرها من النصوص القانونية ذات الصلة بالمعاملات الالكترونية، مما يثير طرح الإشكالية التالية:

ما مدى نجاعة النصوص القانونية التي وضعها المشرع الجزائري في استيعاب خصوصية الجريمة الإلكترونية ومواجهتها؟

اعتمدت في دراسة هذا الموضوع على المنهج الاستقرائي كونه الأنسب لمثل هذه الدراسات من خلال وصف هذه الظاهرة وبيان المفاهيم القانونية الخاصة بها، بالإضافة إلى تحليل مختلف المواد القانونية التي تتضمن الجريمة الإلكترونية، وكذا إجراءات المتابعة فيها واختلافها عن النصوص الإجرائية التقليدية ومن اجل معالجة الإشكالية الرئيسية التي تم طرحها.

تم التطرق إلى خصوصية الأحكام الموضوعية الخاصة لمواجهة الجريمة الالكترونية (الفصل الأول) وإلى الأحكام الإجرائية الخاصة لمواجهة الجريمة الإلكترونية (الفصل الثاني).

[1] قانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق

الفصل الأول: خصوصية الأحكام الموضوعية الخاصة لمواجهة الجريمة الإلكترونية

الفصل الأول

خصوصية الأحكام الموضوعية الخاصة لمواجهة الجريمة الإلكترونية

أدى التقدم العلمي إلى ظهور أنماط مستحدثة من الجرائم لم تكن معروفة من قبل، ولم يتم النص على تجريمها في التشريعات الجنائية التقليدية، حيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها، والمحل الذي تقع عليه، وخصوصية المجرمين الذين يقدمون على ارتكابها.

لقد أثارت الجرائم الإلكترونية على مدى السنوات المنصرمة وتثير إلى حد الآن تحديات بالغة في حقل أنشطة المكافحة وأنشطة التحقيق للوصول إلى مرتكبها، كما أثارت تحديات قانونية وفنية بشأن آليات مباشرة إجراءات التفتيش والضبط والتعامل مع الأدلة الإلكترونية أي الرقمية المتعلقة بهذه الجرائم، وهو ما استدعى جهدا دوليا عريضا من قبل المؤسسات وهيئات تنفيذ القانون، بغية رصد هذه التحدي اتو توفير الحماية اللازمة على المستوى الفني والتشريعي.

وفي هذا الفصل سنحاول تحديد خصوصية الإحكام الموضوعية الخاصة لمواجهة الجريمة الإلكترونية من خلال تحديد الطبيعة القانونية الخاصة للجريمة الإلكترونية (المبحث الأول) والتعرف على القواعد الموضوعية الخاصة لمواجهة هذه الجرائم (المبحث الثاني).

المبحث الأول:

الطبيعة القانونية الخاصة للجريمة الإلكترونية

تتطلب مكافحة الجرائم الالكترونية بذل مجهودات كبيرة نظرا للصعوبات الكثيرة الناتجة عن الطبيعة الخاصة بها، والسبب في ذلك كون المعلومات هي محور ارتكاب هذا النمط من الجرائم، كما أن تحديد هذه الطبيعة تستلزم إضافة مجال معالجة الكلمات أو النصوص، إذا هي عملية وثيقة الصلة بارتكاب الجرائم، وأن القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه، وللتطور السريع في مجال المعلوماتية[1]، و كذلك من حيث تكييفها القانوني، إذ لم تكن النصوص التقليدية المخصصة والمطبقة على هذا النوع من الجرائم المستحدثة كافية مما أدى إلى ظهور سلسلة من المشكلات باعتبارها جرائم تقع على المعلومات فيعالم الافتراض فهي غير ملموسة أو مادية فمن المستحيل الاعتداء عليها، وصعوبة الحصول على الدليل المادي لإثباتها، لأن المجرم الالكتروني يقوم بمحو أدلة الإدانة في لحظات، نجد أيضا الصعوبة في حالة إجراء التفتيش الواقع على المكونات المعنوية للحاسوب، فقد تكون البيانات المبحوثة عنها مشفرة مما يثير مساءلة مدى مشروعية إجبار الجاني على فك الشفرة الخاصة به[2]إضافة إلى صعوبة ملاحقة مرتكبي الجرائم الإلكترونية المقيمين في دول أجنبية لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي، باعتبارها جرائم عابرة للحدود بسبب ما توفره شبكة الانترنت من حرية الإبحار في هذا العالم الافتراضي دون قيود أو حدود[3] .

---

[1] المرجع نفسه، ص 05 وما يليها.

[2] محمد علي سالم وحسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، كلية القانون، جامعة بابل، المجلد 14، العدد 06، 2007، ص 91.

[3] محمد علي سالم وحسون عبيد هجيج، مرجع سابق ص 91،92.

المطلب الأول:

مفهوم الجريمة الإلكترونية

يعد تحديد مفهوم الجريمة الإلكترونية الخطوة الأولى للتعرف عليها من جميع جوانبها القانونية مما أنجر عنه وضع عدة مصطلحات للدلالة عليها بسبب ذاتيتها ولتميزها عن غيرها من الجرائم التقليدية، سواء في محلها أو خصائصها، في الجريمة الإلكترونية يمكن أن تتجلي تحت عدة تسميات مختلفة من بينها جرائم الحاسب، الجرائم التقنية العالية، جرائم المعلوماتية وجرائم الانترنت.

إن عدم وجود مصطلح قانوني موحد للدلالة على هذا النوع من الجرائم أدى إلى عدم الوصول إلى تعريف مناسب يتلاءم مع طبيعة الجريمة الإلكترونية.

ومما لا شك فيه أن عدم وضع تعريف محدد للجريمة الإلكترونية يثير العديد من المشاكل لعل أهمها، صعوبة مواجهتها وتعذر إيجاد الحلول الملزمة والملائمة لمكافحتها نتيجة التطور المستمر لتكنولوجيات الاتصالات والمعلومات الذي حال دون وضع تعريف جامع وشامل للجريمة الإلكترونية سواء في التشريعات الوطنية أو الدولية.

ففي هذا المطلب سنحاول وضع تعريف للجريمة الإلكترونية (الفرع الأول) ثم التطرق إلى تحديد أهم الخصائص التي تميزها عن الجرائم التقليدية (الفرع الثاني) ثم التعرف على عناصرها، (الفرع الثالث).

الفرع الأول:

المقصود بالجريمة الإلكترونية وخصائصها

أولا: تعريف الجريمة الإلكترونية

اختلفت التعاريف بشأن الجريمة الإلكترونية باعتبارها ظاهرة جديدة ما زالت قيد البحث والدراسة من طرف القانونيين والعديد من الفقهاء، وعدم الاتفاق هذا أنجز عنه عدم وضع تعريف محدد ومتفق عليه لهذا النوع المستحدث من الجرائم[1]

وللوقوف على مفهوم الجريمة الإلكترونية يقتضي من الحال تعرضه إلى التعريف الفقهي. لهذه الجريمة(أ) ومن ثم التطرق إلى تعريفها من الناحية القانونية(ب).

أ: التعريف الفقهي للجريمة الإلكترونية

انقسم الفقه في محاولته لوضع تعريف للجانب الإلكترونية إلى عدة اتجاهات فهناك من استند في تعريفها على أساس موضوع الجريمة أو محلها، وهناك اتجاه آخر يعرفالجريمة الإلكترونية على أساس توفر المعرفة التقنية والمعلوماتية لدى مرتكب الجريمة.

1.تعريف الجريمة الإلكترونية على أساس وسيلة ارتكابها

يستند أصحاب هذا الاتجاه تعريف الجريمة الإلكترونية على أساس موضوع الجريمة، إذا يرى أن الجريمة الإلكترونية هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه[2]

[1] بالطلي غنية، الجريمة الإلكترونية، الدار الجزائرية، الجزائر 2015، ص 15، 16

[2] الملط احمد خليفة، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006، ص 85، 86.

وتعرف أيضا وفقا لهذا الاتجاه على أنها" **نشاط غير مشروع موجه لنسخ أو للوصول إلى "المعلومات المخزنة داخل الحاسب وتغييرها أو حذفه"**[1]

ويمكن تعريفها أيضا بأنها" **الجريمة الناتجة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر**[2]

مما لا شك فيه أن نماذجها عديدة وتنطلق من فكرة دور الكمبيوتر في ارتكاب الجريمة الإلكترونية أو إساءة استخدام جهاز الكمبيوتر، ومن بين التعاريف التي استندت على هذا الأساس تعريف الفقيه الألماني تاديمان Tiedeman بأنها" **كل أشكال السلوك الغير المشروع الذي يرتكب باستخدام الحاسوب**" كذلك مكتب تقييم التقنية في الولايات المتحدة الأمريكية قد عرفها أنها "**الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا**"[3].

والملاحظة أن أنصار هذا الاتجاه اقتصروا في تعريفهم للجريمة الإلكترونية على حالة واحدة تقوم فيها وهي حالة استخدام جهاز الحاسوب أو تقنية المعلومات في ارتكاب الجريمة، دون الأخذ بعين الاعتبار الحالة التي يكون فيها الحاسوب والانترنت هدفا وموضوعا لهذه الجرائم.

2. تعريف الجريمة الإلكترونية على أساس موضوعها

ذهب أصحاب هذا الاتجاه إلى التركيز على الجانب الموضوعي من الجريمة، فموضوعها هو المعالجة الآلية للبيانات فكل تعريف أو تعديل أو نقل أو نسخ غير مشروع لها يعد جريمة إلكترونية،

[1]محمود احمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2015، ص 17.

[2]عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2013، ص 03.

[3]عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 22.

وعليه فقد عرفها الفقيه Rosenblatt على أنها" **كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات**"[1] .

الملاحظة من خلال التعريفات التي تستند إلى موضوع الجريمة تعريفها أنها كل اعتداء موجه سواء إلى المكونات المادية للنظام المعلوماتي كالأجهزة Matérielأو إلى المكونات غير المادية كالبيانات و البرامج Logiciel .

إلا أن هذا المعيار لم يسلم من الانتقادات لأنه قصر مفهوم الجريمة الإلكترونية على المعلومات والبرامج ومكونات الحاسوب المادية والمعنوية ويكون بذلك قد اخرج من نطاق الجريمة الإلكترونية الجرائم التقليدية التي تستخدم الوسائل التقنية في ارتكابها كجريمة القذف أو التشهير أو غيرها من الجرائم التي ترتكب باستخدام الانترنت ووسائل التقنية والمعلوماتية.

3.تعريف الجريمة على أساس المعرفة التقنية

يرى أصحاب هذا الاتجاه أن تعريف الجريمة الإلكترونية يعتمد على المعيار الشخصي ومن هذه التعريفات تعريف الفقيه David Thomson" **بأنها أيه جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب**"[2].

وذهب مجموعة من خبراء منظمة التعاون الاقتصادي OCDE إلى تعريف الجريمة الإلكترونية بأنها" **كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها**"[3]، اعتمد هذا الاتجاه على أساس معرفة الجاني بتقنية المعلومات، فهذه التعريفات قد ضيقت من مفهوم الجريمة الإلكترونية، فلا يجب أن يكون مرتكب الجريمة الإلكترونية على قدر كبير من المعرفة التقنية التي تمكنه من ارتكابها.

من خلال ما سبق فقد اعتمد أصحاب الاتجاهات السابقة في تعريف الجريمة الإلكترونية على معيار واحد سواء كان وسيلة ارتكابها أو موضوعها، أو شخصية مرتكبها ساهم هذا الأمر في ظهور

---

[1] هدى حامد قشقوش، مرجع سابق، ص 22 .

[2] هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح آلية عربيه موحدة للتدرب التخصصي، بحوث مؤتمر القانون والكمبيوتر والانترنت، من 1 إلى 3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص 407.

[3] اقلولي ولد رابح صافية، الطبيعة القانونية للجريمة المعلوماتية، مداخله في ملتقى الدولي حول الجريمة المعلوماتية جامعة بسكر، الجزائر، يومي 16 و17 نوفمبر 2015، ص 4 .

اتجاه آخر وسع من تعريف الجريمة الإلكترونية لتشمل جميع الجرائم التي لها علاقة بالمعلوماتية والتي تستخدم نفس التقنية تقع في البيئة الإلكترونية.

ب: التعريف التشريعي للجريمة الإلكترونية

معظم التشريعات لم تتعرض إلى تعريف الجريمة الإلكترونية، إلا أن هناك البعض من التشريعات من أشار إلى تعريفها كما هو الحال بالنسبة للمشرع الجزائري، من خلال المادة الثانية الفقرة الأولى من الفانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنها" **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتكب أو يسهل لارتكابها عن طريق منظومة معلوماتية أو النظام للاتصالات الإلكترونية**"[1].

تجدر الإشارة إلى أن المشرع الجزائري لم يعرف الجريمة الإلكترونية في القانون رقم 04- 15 المعدل لقانون العقوبات؛ بل عدد الجرائم مثل بأنظمة المعالجة الآلية للمعطيات والتي تعتبر جزء من ظاهرة إجرامية حديثة وخطيرة تسمى الجريمة المعلوماتية.

واكتفى بالعقاب عليها في الكتاب الثالث الخاص بالجنايات والجنح وعقوبتها في الفصل الثالث المعنون بالجنايات والجنح ضد الأموال في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى غاية المادة 394 مكرر7[2]

أما على المستوى الدولي تم إبرام أول اتفاقية حول الإجرام المعلوماتي بتاريخ 8 نوفمبر 2001، لمكافحه مختلف أشكال الإجرام المعلوماتي[3].

[1] أنظر المادة 2 الفقرة 1 من القانون رقم 09 04 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام والاتصال ومكافحتها المؤرخ في 05 عشت 2009،الجريدة الرسمية للجمهورية الجزائرية، العدد 47.

[2] هروال هيبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة لنيل شهادة الدكتورة، كلية الحقوق، والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان, 2014،ص 18.

[3] الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/8 من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ http://www.asj.cerist.DZ2001/11/23

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة 2000 تعريف الجريمة الإلكترونية بأنها" **أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية**"[1].

ثانيا: خصائص الجريمة الإلكترونية

لما كانت الجريمة الإلكترونية هي نتائج التطور العلمي والتكنولوجي، وبالتالي ارتباطها بجهاز الحاسوب وشبكة الانترنت فهي تختلف عن نظيرتها التقليدية التي ترتكب في الواقع المادي الملموس، لذا نجدها تتميز بمجموعة من الخصائص أو السمات تجعلها منفردة عن غيرها من الجرائم سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة وهذا ما يتم بيانه من خلال هذا الفرع.

أولا: خفاء الجريمة وسرعة التطور في ارتكابها

حيث تتسم بأنها خفية لا يلاحظها الضحية رغم أنها قد تقع أثناء وجوده على شبكة الاتصالات، لأن الجاني ذكي يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة البيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم[2]، ويمكن تنفيذها خلال جزء من الثانية في بعض الجرائم.

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان،2011، ص 30.

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو 2013، ص 14 ،15.

ثانيا: ترتكب الجريمة الالكترونية في بيئة خاصة

يتم ارتكاب الجريمة الالكترونية في بيئة رقمية معلوماتية؛ قوامها النظم المعلوماتية، وتجهيزات الحاسب الآلي المتمثلة في المكونات المادية للحاسوب ومكوناته البرمجية.

ثالثا: خصوصية الجاني في الجريمة الالكترونية

مرتكب الجرائم الالكترونية غالبا ما يكون شخصا يمتز بالذكاء والدهاء، وذو مهارة تقنية عالية ودراية بأنظمة الحاسوب، وهذا عكس الحال في الجريمة التقليدية التي تحتاج من مرتكبها إلى قوة عضلية لتنفيذها.

رابعا: خصوصية الدليل الجنائي في الجريمة الالكترونية

صعوبة الحصول على دليل مادي في مثل هذه الجرائم حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر ولعل صعوبة كشف الدليل يزداد بصورة خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثار تدل عليهم[1].

خامسا: خصوصية الإثبات في الجرائم الالكترونية

الجريمة الإلكترونية تستلزم طرق خاصة ومستحدثة للإثبات قوامها التعليم والتدريب المتخصص لعلوم الحاسب الآلي مما يتطلب الاستعانة بالخبراء المتخصصين في مجال الحاسب الآلي والانترنت مما يساعدهم على كشف الأدلة والحفاظ عليها.

[1] موسي مسعود. دار حومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا، طرابلس، أكتوبر 2007، ص 10.

سادسا: صعوبة تحديد إقليم الجريمة الالكترونية

تتسم الجريمة الإلكترونية بالطابع الدولي، ذلك لأن الطابع العالمي لشبكة الانترنت التي جعلت من العالم يعيش في قرية صغيرة يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة الإلكترونية لا تعترف بالحدود بين الدول والقارات فهي جريمة عابرة للقارات، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل: جريمة غسل الأموال، القرصنة والاحتيال المعلوماتي.

الفرع الثاني:

عناصر الجريمة الإلكترونية

إن الجرائم الإلكترونية كغيرها من الجرائم تحتاج إلى طرفين فاعل أوجاني ومجني عليه، غير أن أطراف الجريمة الإلكترونية يختلفون نوعا ما عن أطراف باقي الجرائم، مما لا شك فيه أن الشخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية، ولكن الأمر يختلف بعض الشيء فالمؤسسات العامة والبنوك وغيرها، التي تحمل صفة الشخص المعنوي معرضة للاعتداءات عن طريق هذه الشبكة من المعلومات، فعل الرغم من وسائل الحماية المتعددة إلا أنه تثبت عدم فعاليتها أمام قرصنة شبكة المعلومات[1].

أولا: أطراف الجريمة الإلكترونية

إن الجرائم الإلكترونية رغم أنها جرائم ذات خصائص أوسيمات منفردة بها لا تتوافر في أيمن الجرائم التقليدية في أسلوبها وطريقة ارتكابها بسبب ارتباطها بالحاسب الآلي ومكوناته المادية منها

[1]David Johnson, Electronic privacy, stoddar. Canada, 1997. PP 66

والمعنوية فهي جرائم تقع في مسرح افتراضي ولكن رغم ذلك فهي كغيرها من الجرائم تحتاج إلى طرفين جاني ومجني عليه.

أ- المجني عليه في الجريمة الإلكترونية (الضحية)

يمكن أن يرتكب الجرائم الإلكترونية شخص طبيعي أو معنوي، فأن المجني عليه فيتلك الجرائم قد يكون كذلك شخصا طبيعيا أو معنويا، مع أن الغالبية العظمى من هذه الجرائم تقع على شخص معنوي يتمثل في مؤسسات وقطاعات المالية وشركات ضخمة[1]، فيبد وأن المعلومات المجردة تعد في الوقت الحاضر من أهم المصالح المستهدفة بعد الأموال وخصوصا إذا كانت ذات أهمية عالية، فهدف المجرم الالكتروني هو الحصول على مقابل وعوض، عن طريق المقايضة غير المشروعة لهذه المعلومات أو بيعها لغير أصحاب الشرعيين ويظهر ذلك من المعلومات الآتية

المعلومات المالية المرتبطة بالمركز المالي الحسابي والإداري وانتقال الأموال والاستثمارات[2]

و المعلومات التجارية المتعلقة بالتجارة الإلكترونية عمليات التجسس والقرصنة الحاصلة عليها[3].

المعلومات الشخصية المرتبطة بخصوصيات الأشخاص الطبيعية أو المعنوية، إذ يتم تشويهها وإظهارها على غير حقيقتها[4].

---

[1]المناعسة أسامة أحمد وآخرون، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، 2001، ص 88، وهامش رقم اثنين.

[2]توفيق شمبور وآخرون، السرية المصرفية، أبحاث ومناقشات الندوة التي نظمها اتحاد المصارف العربية، بيروت، 1993 ص 82 وما يليها.

[3]هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة, 2000 ص 6_ 18، و مدحت عبد الحليم رمضان الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص 10 وما يليها و ص 119.

[4]طوني ميشال عيسي، التنظيم القانوني لشبكه الانترنت، دار صادر للمنشورات الحقوقية، بيروت، 2001 ص 150 وما يليها، كذلك يونس خالد عرب، جرائم الحاسوب، رسالة ماجستير مقدمة إلى كلية الحقوق في الجامعة الأردنية، 1994 ص 203 وما يليها.

مما تجدر الإشارة إليه هو دور المجني عليه في كبح الجريمة الإلكترونية أي التكتم والإبقاء على ما لحقهم من أضرار ناتجة عن الجريمة الإلكترونية سرا وذلك للحفاظ على مكانتهم الاجتماعية أو سمعتهم التجارية وكذلك حماية لمركزهم المالي وثيقة العملاء بهم[1].

ب- الجاني في الجريمة المعلوماتية (المجرم المعلوماتي)

المجرم المعلوماتي فكرة جديدة في الفقه الجنائي، ففي الجرائم المعلوماتية لن نكون بصدد مجرم عادي، بل نكون أمام مجرم ذات مهارات تقنية وذي علم بالتكنيك المستخدم في نظام الحاسوب الآلي فشخصية المجرم المعلوماتي سواء كان طبيعيا أو معنويا والية ارتكابه الجريمة تجعل منه شخصا يتسم بسمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي[2]، والشرط الأساسي الذي يتوافر لدى الشخص الجاني هو درايته بالمسائل المعلوماتية و التقنية و كيفية تشغيلها باعتبار أن الإجرام المعلوماتي ينشأ من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية[3] فالإجرام المعلوماتي يعد إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، ولذا يمكن القول أن الإجرام المعلوماتي، بوصفه ظاهرة اجتماعية قد أسفر عن عوامل مستحدثة في أذهان مرتكبيه، إذ يلجأ العديد من مرتكبي هذه الجرائم إلى ارتكابها بدافع اللهو أو لمجرد إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتية، دون الحصول على منفعة مالية، بل الاكتفاء بالتفاخر بأنفسهم وأن يظهروا لضحاياهم ضعف أنظمتهم، مما يبدو معه انعدام أي خطر اجتماعي للإجرام المعلوماتي، وليس السبب في ذلك عدم وجود

[1] المناعسة أسامة أحمد وآخرون، مرجع سابق، ص 61.

[2] هدى حامد قشقوش، مرجع سابق، ص 32.

[3] إياد احمد البطانية، النظام القانوني لعقود برامج الحاسوب، دراسة مقارنة، أطروحة الدكتورة مقدمة إلى كلية القانون في جامعة بغداد، 2002، ص 6.

نوايا آثمة، ولكن للسلوك الغير الواعي الذي يمكن أن يتسبب في أضرار جسيمة، حتى لو لم يكشف عن أي عداء للمجتمع[1].

وعليه فأن مرتكبي الجرائم المعلوماتية ليسوا على درجة واحدة من الخطورة أو الكفاءة، وعلى هذا الأساس يمكن تصنيفهم حسب إمكانياتهم ومقاصدهم من ارتكاب الجريمة إلى صنفين هما:

1. مجرمين مستعملي الانترنت

من تتوافر لديهم معرفة كافية أو خبرة لبأس بها في مجال المعلوماتية أو عمل الحاسب الآلي ومكوناته ووظائفه الأساسية، ومعرفة بعض البرامج التي يجري العمل بها كبرامج المحاسبية، ومع الإقرار بأن المعلوماتية تكنولوجيا حديثة، ودخولها واقع الحياة اليومية حديث نسبيا، ونظرا إلى قلة المعرفة بهذه التكنولوجيا، ولما كان هؤلاء يمارسون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسة هوية اللهو، وهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي بأفعالهم الغير المشروعة إلى نشاط معين[2]، فان هذه الطائفة من المجرمين تعد أقل خطورة مقارنة بغيرها، ولكن مع ملاحظ ازدياد الأعداد المستعملة لهذه التكنولوجيا (الانترنت)، وما سيتبعه بلا شك من ازدياد نسبة الجرائم في هذا المجال، فليس من المستبعد احتمال انزلاق هذه الفئة من مجرد هواة صغار للأفعال الغير المشروعة إلى محترفين[3]، وخصوصا إذا تم احتضانهم من قبل منظمات إجرامية لتحقيق أغراض خطيرة تؤثر بصورة أو بأخرى على معطيات التطور العلمي.

[1] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص37.

[2] المناعسة أسامة أحمد وآخرون، مرجع سابق، ص 82.

[3] إسماعيل رضا، الوقاية من الجرائم الناشئة عن استخدام الحاسب الآلي. مقال منشور في مجلة الاقتصاد الإسلامي، عدد 219، 1999 ص 34.

2. مجرمين مبرمجين

نظرا إلى المستوى المهارى الذي يتمتع به المجرمون، من دخول واقتحام للأنظمة الحاسوبية بكل سهولة واقتدار، رغم احتياطات الأمن المتعددة ورغم قلة العناصر الخبيرة على كشفها، مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، فغالبا ما تكون جرائم النسخ والإضافة والتحويل للمعلومات على البرامج أو تغيير محتواها من هذه الفئة ضخمة[1]فاستخدام هذه الفئة للأساليب المعلوماتية ليس فقط في ارتكاب الجريمة بل حتى على إعاقة ملاحقتهم من خلال تضييع الأدلة الموجودة المؤدية إلى إدانتهم[2]، ومن خلال ما تقدم يتضح أن مرتكب الفعل الجرمي الالكتروني قد يكون فاعلا أصليا أو شريكا في ارتكابه للجريمة، فصفة الفاعل الأصلي في الجريمة الإلكترونية غالبا ما تكون من أحد العاملين في منشأة تسير بالنظام المعلوماتي، ولما كان هذا النوع من الإجرام يستلزم الدقة والتنفيذ للعمليات الغير المشروعة، فانه يستلزم مشاركة أشخاص آخرين، سواء كانوا فنيين أم مجرد وسطاء، وقد يكون هذا الاشتراك سلبيا، يترجم بالصمت أو السكوت ويتمثل بالمساعدة الفنية والمالية[3]، بقي أن نشير في هذا المقام إلى أن هناك بواعث رئيسية تدفع بهؤلاء المجرمين نحو الإقدام على ارتكاب الجرائم الإلكترونية، منها الشغف بالإلكترونيات، ودوافع شخصية متعلقة بالعظمة واثبات القدرة والسعي إلى تحقيق الربح، ومؤثرات خارجية تمثل بدافع الإكراه والحقد، أو قد تتعلق بأسباب خاصة بالمنشاة[4].

---

[1] عبد الرحمن الشنيقي، المواجهة الأمنية لجرائم الحاسبات الآلية، مجلة الأمن والحياة، السنة 11 العدد 129, 1993 ص 46، وكذلك المناعسة اسامة احمد وآخرون، مرجع سابق ص 84.

[2] سعد الحاج بكري، شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، السنة 06 العدد 11، 1990، ص 210.

[3] محمد سامي الشوا، مرجع سابق، ص45 وما يليها.

[4] محمد سامي الشوا، ص 48 وما يليها، كذلك أسامة أحمد المناعسة وآخرون، مرجع سابق، ص 88.

ثانيا: الأجهزة المستعملة في الجريمة الإلكترونية

توفر التقنية المعلوماتية إمكانات هائلة في مجال استعمال شبكة الانترنت يستغلها المجرم الالكتروني في تنفيذ جرائمه المختلفة التي يغلب عليها الطابع التقني والفني، وهذا ما يميزها عن باقي الجرائم التقليدية، في الوسائل المستعملة لارتكاب الجرائم الإلكترونية التي لاحصر لها نتيجة التقدم الهائل الحاصل في مجال تقنية الحاسوب والاتصال، فهي من جهة توفر للمستعمل أدوات كثيرة تسهل عليه معالجة المعلومات وتخزينها واسترجاعها وإرسالها كأجهزة الحاسوب وملحقاته وبرامجه، إضافة إلى الأهمية التي تكتسبها تقنية البريد الالكتروني الذي يمكننا من استقبال وإرسال ملفات على اختلاف أنواعها، ومن جهة أخرى تعتبر تقنية الاتصالات الحديثة والشبكات المحلية والعالمية كالهواتف النقالة والشبكة العنكبوتية وسائل فعالة تمكن المجرم المعلوماتي من ارتكاب الجرائم الإلكترونية على اختلاف أنواعها، سنتطرق إلى بعضها فيما يلي:

أ- الوسائل الالكترونية

حققت التقنيات الحديثة قفزة عملاقة في مجال الحاسوب وملحقاته و برامجه، إلى جانب التطورات الهائلة في مجال الاتصال وعلى رأسها شبكة الانترنت التي لم يعد من الممكن استغناء الإنسان عنها في نظرا لما توفره هذه التقنية من خدمات سريعة وغير مكلفة ولكن للأسف وككل تكنولوجيا حديثة لها سلبياتها وسوء استخدامها أدى إلى اعتبار الحاسوب الأداة الأولى لارتكاب الجرائم الإلكترونية[1]، ويتم ذلك بتحاور مع البرامج أو النظم المبرمجة في الحاسوب بصفة غير مشروعة، كما في حالة استغلال الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف

[1] فايز الظفيري، الأحكام العامة للجريمة الالكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عيش الشمس، 2002 من 492.

والتزوير، و الاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها للحصول على الأموال1،حتى أن الكمبيوتر قد يستخدم كوسيلة في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية و العلاجية و تدويرها، أو تحوير عمل الأجهزة الطبية عبر التلاعب ببرمجياتها أو قرصنة برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها[2]

وقد يكون أيضا الكمبيوتر بيئة الجريمة وذلك في حالة استخدامه لنشر المواد غير القانونية أو أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية وشبكات الاتجار بالبشر، إلا أن للحاسب دور مهم في اكتشاف الجريمة، حيث تعتمد الجهات القضائية المختصة بالتحقيق في الجرائم الإلكترونية على أحدث النظم والبرامج المعلوماتية في إدارة مهامها.

و من الوسائل ذات أهمية بالغة بخصوص الاستعمال الشخصي نجد البريد الالكتروني، فهو عبارة عن رسالة إلكترونية تكتب من خلال استخدام لوحة المفاتيح عوضا عن الورقة والقلم وتكتب على جهاز الكتروني، و هي طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[3].

فهو يستخدم كمستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم، بشرط تأمينه باستعمال كلمة السر[4].

أصبحت هذه الأداة من أسرع الوسائل التي وفرتها التقنية المعلوماتية بالمجان قصد توفير خدمات الاتصال، لأنه أداة اتصال ناجزة للمصالح خاصة في المعاملات التجارية[5].

---

[1]حسن إبراهيم الحاسب الآلي وتحديات القرن الحادي والعشرون، مجلة مركز بحوث الشرطة، أكاديمية الشرطة، ، العدد 14، 1998، ص91.

[2]يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، دمشق، 2010، ص 34.

[3]محمود محمد لطفي صالح، المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية دراسة مقارنة، دار الكتب القانونية، دار النشر والبرمجيات، القاهرة– دبي 2014 ص 185.

[4]عباد الفتاح بيومي حجازي، التزوير الكمبيوتر والانترنت دراسة مقارنة، منشأة المعارف، القاهرة، 2010 ص 66.

[5]myriamquemener et Joe ferry.OP.cit.p.36

لكنه بالمقابل يستخدمه المجرم المعلوماتي في إرسال الفيروسات على اختلاف أنواعها وأهدافها كنسخ البيانات الشخصية أو تدميرها أو تعديلها أو إرسال روابط لمواقع مشبوهة وترويج الشائعات والأكاذيب وغيرها.

نجد أيضا الهاتف النقال أو الخلوي وهو عبارة عن أداة لاسلكية تعمل من خلال شبكة من أبراج البث موزعة لتغطي مساحة معينة، ثم تترابط عبر خطوط ثابتة أو أقمار صناعية، أصبح أكثر من مجرد وسيلة اتصال صوتي فهي حاسوب محمول حجمه بكف اليد، له وظائف كثيرة كالاتصال المرئي وتنظيم المواعيد واستقبال البريد الصوتي وإرسال واستقبال ملفات الفيديو والبريد الالكتروني، وتصفح شبكة الانترنت والتصوير واستعمال البلوتوث، فقد تزايد عدد مستخدمي هذه الأجهزة باستمرار ليحل محل أجهزة الاتصال الثابتة.

ب- شبكة المعلومات المحلية والعالمية

تعرف شبكة الحاسوب على أنها نظام لربط جهازين أو أكثر باستعمال إحدى تقنيات نظم الاتصالات من اجل تبادل المعلومات، كما تسمح بالتواصل المباشر بين المستخدمين[1].

إذ يمكن أن تكون أجهزة الحاسوب في الشبكة قريبة جدا من بعضها كأن تكون في غرفة واحدة وتسمى في هذه الحالة بالشبكة المحلية (LAN) كما يمكن أن تكون مكونة من مجموعة أجهزة في أماكن بعيدة مثل الشبكات بين المدن أو الدول وحتى القارات وتسمى بالشبكات الإقليمية(MAN)ويتم وصل هذه الشبكات بالأنترنت أو بالساتلSatellite،و تسمى حينئذ شبكة عريضة) (WAN)، كما نجد أيضا ما يعرف بالشبكة الشخصية(PAN)، والتي تربط مجموعة أجهزة قريبة من المستخدم، ومن جهة أخرى تعتبر شبكة الانترنت (Internet) من أهم الشبكات، تضم كافة أنواع الشبكات السابقة، فهي عبارة عن

[1] فايز الظفيري، مرجع سابق ص 494-495.

مجموعة من الحواسب المتصلة فيما بينها عن طريق أسلاك (Câbles) أو دون أسلاك (Wifi)، بحيث يمكن لأي منها الوصول إلى محتوى الأخر واستخدام موارده من تطبيق اتو معطيات وغيرها من المعلومات[1].

فقط تكون شبكة الانترنت هدفا للجريمة كما في حالة الدخول غير المشروع به إلى الأنظمة المعلوماتية بقصد الاستيلاء أو تدمير بياناتها وإجراء تحويلات غير مشروعة لذا تعد هذه الشبكات مجالا خصبا لارتكاب جميع أنواع الجرائم الإلكترونية.

المطلب الثاني:

الوصف القانوني للجريمة الإلكترونية وأركانها

وبعدها يتم التطرق في هذا المطلب إلى الوصف القانوني للجريمة الالكترونية (الفرع الأول) وأركانها (الفرع الثاني)

الفرع الأول:

الوصف القانوني للجريمة الإلكترونية

حاول المشرع الجزائري إعطاء تعريف للجريمة الإلكترونية، فعرفها على أنها جرائم المساس بأنظمة المعالجة الآلية المعطيات المحددة في قانون العقوبات، وعليه فهي تختلف في طبيعتها على الجرائم التقليدية المعروفة لذا يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات وعليه يثار التساؤل الآتي: هل المعلومة قابلة للاستثمار، ومن ثم تكون محلا للاعتداء عليها؟ في هذا الصدد برز اتجاهان فقهيان، الأول اتجاه تقليدي يرى بأن المعلومة لا تعد قيمة

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت، 2007، ص 20.

في حد ذاتها بل لها طبيعة من نوع خاص، أما الثاني اتجاه حديث يرى بأن المعلومة عبارة عن مجموعة مستحدثة من القيم[1].

أولا: المعلومة لها طبيعة من نوع خاص يرى أنصار هذا الاتجاه التقليدي أن للمعلومة طبيعة خاصة بموجبها تضفي وصف القيمة على الأشياء المادية، فهي قابلة للاستحواذ، وبالتالي فمن غير المقبول أن تكون المعلومات قابلة للاستئثار وفق هذا الاتجاه إلا عن طريق حق الملكية الأدبية أو الفكرية أو الصناعية[2].

وعليه فإن المعلومات المختزنة التي لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، لا تندرج حتما في مجموعة القيم المحمية، ثم لا يعني ذلك استبعاد الحماية القانونية لها إذ نجد الفقه والقضاء، يعترفان بوجود اعتداء يعاقب عليه عند الاستيلاء على مال الغير[3].

إذا فوصف القيمة لا ينطبق إلا على الأشياء المادية القابلة للاستحواذ والمعلومات ذات الطبيعة معنوية فإنها غير قابلة للاستئثار وبالتالي لا تندرج في مجموعة القيم[4].

ثانيا: المعلومات مجموعة مستحدثة من القيم القابلة للاستئثار، ويمكن الاعتداء عليها بأي طريقة كانت، حيث يرى الأستاذ كاتالا catala أن المعلومة المستقلة عن دعامتها المادية تكون لها قيمة قابلة للاستحواذ، تلك أن المعلومات لها قيمة اقتصادية قابلة لان تحاز حيازة غير مشروعة، وأنها تربط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة الملك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[5].

---

[1] محمد سامي الشوا، مرجع سابق، ص 178.

[2] الملط أحمد خليفة، مرجع سابق، ص 104.

[3] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، القاهرة، 2011، ص 44، 45.

[4] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية،2009، ص 263.

[5] السلامة محمد عبد الله، موسوعة الجرائم المعلوماتية جرائم الكمبيوتر والانترنت، المكتب العربي الحديث، الإسكندرية، 2007، صفحه 43، 44.

الفرع الثاني:

أركان الجريمة الإلكترونية

لا تقوم الجريمة إلا بتوافر الركنين المادي والمعنوي، فلابد أن تتبلور ماديا وتتخذ شكلا معينا وهو الركن المادي، أو المظهر الخارجي لنشاط الجاني، إلا أنه لا يكفي وحده لإسناد المسؤولية إلى شخص معين بل يجب أن تتوفر لديه النية الجرمية التي تشكل الركن المعنوي للجريمة، الذي قد يأخذ أيضا صورة الخطأ وبالإضافة إلى هذين الركنين لابد من نص قانوني يجرم الفعل إذ لا جريمة بغير قانون تتخذ الجريمة الإلكترونية من الفضاء الافتراضي مسرحا لها، يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم المادي، فهي تشترك بوجود الفعل الغير المشروع والمجرم الذي يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرق إلى الأركان التي تقوم عليها هذه الجريمة[1].

أولا: الركن الشرعي

نص المشرع الجزائري على أنه لا جريمة ولا عقوبة إلا بنص، فقد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات[2]

وهوما نصت عليه المادة 01 من قانون العقوبات الجزائري "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"[3]

[1] صغير يوسف، مرجع سابق، 2013، ص 59

[2] أمر رقم: 20 – 01 المؤرخ في 30 يونيو 2020، المعدل والمتمم لأمر رقم: 66 –156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية العدد 44، المؤرخ في 20 يونيو 2020.

[3] حسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للنشر، الجزائر، الطبعة 10، 2011، ص27.

ويقصد بالركن الشرعي للجريمة وجود النص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل، ويتجسد هذا النص القانوني من خلال مبدأ شرعية الجرائم والعقوبات فالركن الشرعي للجريمة له ركنان أساسيان وهما:

- تطابق الفعل مع نص التجريم.
- عدم خضوع الفعل المرتكب لسبب من أسباب الإباحة.

ثانيا: الركن المادي

يقصد به كل فعل أو سلوك إجرامي صادر من شخص بهدف المساس بحق من الحقوق التي يحميها القانون، ويعتمد على ثلاث عناصر أساسية هي: السلوك والنتيجة والعلاقة السببية.

مع العلم أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها مثل إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الشخص أو الفاعل[1]، ويتخذ الركن المادي للجريمة الإلكترونية عدة صور بحسب الجريمة، وهو ما سنوضحه بداية بالسلوك الإجرامي (أ)، النتيجة (ب)، ثم العلاقة السببية (ج)

أ-السلوك الإجرامي (الفعل):

عبارة عن نشاط أو سلوك إجرامي يتم عبر الأنترنت أو باستخدام المعالجة الآلية للبيانات فهو نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت، حيث يتخذ السلوك الإجرامي في الجرائم الإلكترونية صورتين:

[1] مرابط حياة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، مستغانم، 2019، ص 13.

الصورة الأولى: تتمثل في السلوك الايجابي الذي يتمثل في الإقدام على فعل ينهي القانون عن ارتكابه[1] بهدف إحداث نتيجة مثلا كفعل الدخول أو البقاء عن طريق الغش في كل جزء من النظام المعالجة الآلية للمعطيات.

الصورة الثانية: وهي السلوك السلبي، وهو الامتناع عن القيام بعمل يوجبه القانون مثلا امتناع موظف عن حماية بيانات ومعلومات الشركة التي يعمل بها

ب: النتيجة الإجرامية

يقصد بالنتيجة الإجرامية، الأثر المادي أو ما يترتب من ضرر من الأفعال الإجرامية أو خطر يصيب أو يهدد مصلحة محمية قانونا، ومفهوم النتيجة كعنصر في الركن المادي للجريمة يقوم على أساس ما يعتد به المشرع وما يترتب عنه من نتائج، بغض النظر عما يحدثه السلوك الإجرامي من نتائج أخرى[2].

ج: العلاقة السببية

تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجع إلى إسناد النتيجة إلى الفعل، و هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحدد العلاقة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت

[1] أحسن بوسقيعة، مرجع سابق، ص 116.

[2] بالعاليات إبراهيم، أركان الجريمة الالكترونية وطرق إثباتها في قانون العقوبات الجزائري، الجزائر، 2007، ص 18.

الجريمة غير عمدية فإن نفي العلاقة السببية يؤدي إلى انتفاء المسؤولية كليتا، ذلك أنه لا شروع في الجرائم الغير العمدية[1] .

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب، مثلا جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات أو المحررات الإلكترونية[2].

ثالثا: الركن المعنوي

يتخذ الركن المعنوي في اغلب الجرائم صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه[3].

ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكاب جريمته، حيث لا تقوم الجريمة قانونا بدونه، فلابد من توفر الإرادة الآثمة لدى الجاني عند إقدامه على السلوك الإجرامي، أي تكون الأفعال إرادية وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال متجهة نحو مخالفة القواعد القانونية، ليترتب على مخالفتها الجزاء الجنائي المناسب، للجريمة الإلكترونية غالبا ما تقع بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق الشبكة، والأصل أن الجرائم الإلكترونية عمدية إلا ما استثنى بنص[4].

يتخذ الركن المعنوي في هذا النوع المستحدث من الجرائم صورة القصد الجنائي العام بعنصريه العلم والإرادة فالعلم هو علم الفاعل بأن نشاطه الإجرامي يؤدي إلى ارتكاب سلوك يعاقب عليه القانون،

---

[1] أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، 2009، ص 82.

[2] أسامة أحمد بلال محمد، جرائم تقنية نظم المعلومات الالكترونية، الطبعة3، عمان، 2014 ص، 58،59.

[3] بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الالكترونية دراسة مقارنة، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص وعلوم جنائية، كليه الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية, 2018, ص 35 ، 36.

[4] بالطي غنية، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر, 2015 ص 48.

أما الإرادة هي اتجاه إرادة الجاني إلى فعل الاعتداء وبالتالي تحقيق النتيجة، وطبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما أو خاصا.

1. القصد الجنائي العام

يهدف الجاني عند ارتكابه للواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، بتحقيقه قد تتم الجريمة ويتوفر لها القصد الجنائي العام[1].

بالتالي نجد معظم الجرائم الإلكترونية اشترط فيها المشرع القصد الجنائي العام، حيث اكتفى بالضرورة إلى توافر القصد الجنائي العام لوحده لقيام الركن المعنوي لهذا النوع من الجرائم المستحدثة على غرار التشريعات الأخرى التي دعت إلى توافر القصد الجنائي الخاص إلى جانب القصد الجنائي العام في بعض الجرائم الإلكترونية.

2. القصد الجنائي الخاص

إن اغلب الجرائم ترتكب بصورة قصدية، وبالتالي يعد القصد الجنائي من بين أكثر عناصر الركن المعنوي تصورا.

لقد اختلفت بعض التشريعات حول مدى ضرورة التوافر القصد الجنائي الخاص في بعض الجرائم الإلكترونية، فنجد القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الانترنت من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما أو خاص[2]حيث يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى فجريمة الاحتيال الالكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية، الجزائر 1995 ص 261 .

[2] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، 2004، ص 294.

بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير المشروع[1].

وبالتالي نجد المشرع الجزائري لم يشترط توافر القصد الجنائي الخاص في هذا النوع من الجرائم المستحدثة بل اكتفى بالضرورة توافر القصد الجنائي العام لقيام الركن المعنوي فيهذا النوع من الجرائم[2]

إذا فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الانترنت، وجرائم النشر الفيروسات عبر الشبكة ويرجع الأمر للسلطة التقديرية للقاضي[3].

المبحث الثاني:

القواعد الموضوعية الخاصة لمحاربة الجريمة الإلكترونية

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد في الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام والاتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية، ومع هذا يبقى السؤال مطروح حول مدى فعالية هذه القوانين في مواجهة الجرائم الإلكترونية.

---

[1] المرجع نفسه، ص 294.

[2] خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص 213 – 215.

[3] محمود نجيب حسن، شرح قانون العقوبات_ القسم الخاص، دار النهضة العربية، القاهرة، 1992، ص 13.

المطلب الأول:

الأحكام الخاصة لمحاربة الجريمة الالكترونية في القانون الجزائري

استقر الفكر القانوني على ضرورة وجود نصوص قانونية على حماية المال المعلومات؛ وقد استجابت عدة دول ومنها الجزائر، فبالنسبة للتشريع الجزائري تدارك المشرع الجزائري مؤخرا الفراغ القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية ضمن نصوص قانون العقوبات، قانون الملكية الفكرية والصناعية، وعليه سنتطرق في هذا الجزء إلى بعض القوانين التي سنتها الجزائر لمواجهة الجريمة الإلكترونية والهيئات المكلفة بمحاربة هذه الجريمة.

الفرع الأول:

محاربة الجريمة الإلكترونية في ظل قانون العقوبات

تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04 – 15 المتضمن تعديل قانون العقوبات المتمم لأمر رقم 15 – 02 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ضمن المواد من 394 إلى 394 مكرر 7، بموجبها ستحدث المشرع الجزائري جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة وإلى جانب ذلك قام بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06 – 22.

الفرع الثاني:

محاربة الجريمة الإلكترونية في ظل القوانين الخاصة وأحكام الاتفاقيات الدولية

قامت الجزائر بسن قوانين خاصة بالجريمة الإلكترونية وهي تعتبر متأخرة مقارنة ببعض الدول العربية، بالرغم من احتلالها المراتب الأولى عربيا وإفريقيا، ومن بين التشريعات نذكر منها.

أولا: في ظل القوانين الخاصة

أ –قانون رقم 09 –04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

صدر هذا القانون في الجريدة الرسمية رقم 47 الصادرة بتاريخ 2009/8/16، وهو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ، يحتوي على 06 فصول تناولت التعريف بالجريمة، مراقبة الاتصالات الإلكترونية، القواعد الإجرائية، الهيئة الوطنية للوقاية من الجرائم المعلوماتية والاختصاص القضائي وهذا في 19مادة[1].

ب–قانون رقم 18–05المتعلق بالتجارة الالكترونية:

نص المشرع الجزائري على استغلال شبكة الانترنت في 1998، و اعترف بالكتابة الالكترونية، و التوقيع الالكتروني في تعديل القانون المدني لسنة 2005 لتتولى بعدها صدور مجموعة من النصوص القانونية الخاصة بالمعاملات الالكترونية و أهمها القانون 18–05 المتعلق بالتجارة الالكترونية، أين حدد أطراف المعاملات الالكترونية بين المورد الالكتروني و المستهلك الالكتروني أي حصر المشرع الجزائري التجارة

[1] الانترنت _ موقع aupres.dz/ar/pub/19d1a8

الالكترونية في الجزائر على الاستهلاك الالكتروني، و استبعد بذالك باقي أنواع التجارة الالكترونية التي تتم من محترف إلى محترف أو من مستهلك إلى مستهلك[1].

ج -قانون رقم 18-07المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

بالإضافة إلى انضمام الجزائر للعهد الدولي المتعلق بالحقوق المدنية و السياسية المصادق عليها من طرف الجمعية العامة للأمم المتحدة في 16 ديسمبر 1966 القاضي باحترام الحريات وخصوصيات الأفراد و أسرهم و مراسلاتهم و سمعتهم و شرفهم، و بالنص عليها من خلال دستور 2016، أصدرت الجزائر القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من اجل تأطير الحماية القانونية للحياة الخاصة للإفراد، و الحفاظ على سمعتهم و شرفهم وكرامة عائلاتهم بحماية معطياتهم الشخصية، و الذي يشترط الموافقة الصريحة للشخص المعني من اجل معالجة معطياته الشخصية.[2]

ثانيا: في ظل أحكام المعاهدات والاتفاقيات الدولية

تنوعت الجهود الدولية في مكافحة الجريمة الإلكترونية حيث تم اتخاذ العديد من الآليات والإجراءات للحد والتقليل منها، إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى المعلوماتية والاستعمال اللامتناهي للكمبيوتر والانترنت.

[1] مرسوم تنفيذي رقم 98-257 المؤرخ في 25 غشت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "**انترنت** " واستغلالها

العهد الدولي المتعلق الخاص بالحقوق المدنية والسياسية المصادق عليها من طرف الجمعية العامة للأمم المتحدة المؤرخ في 16 ديسمبر 1966، دخل حيز التنفيذ في 23 مارس 1976

أ –المعاهدات الدولية والإقليمية

يعتمد التعاون الدولي على قوانين الجرائم الإلكترونية الوطنية المنسقة التي تجرم الجريمة الإلكترونية، والقوانين الإجرائية للجرائم الإلكترونية التي تحدد قواعد الإثبات والإجراءات الجنائية، كما يظهر أيضا التعاون الدولي من خلال تنسيق الصكوك الثنائية والإقليمية والمتعددة الأطراف بشأن الجريمة الإلكترونية فأصبح الأمر في غاية الأهمية لعقد اتفاقيات دولية بين الدول للتعاون بهذا الشأن للحد من هذه الجرائم ومكافحتها ومن أهم هذه الاتفاقيات نجد:

– الاتفاقية العربية لجامعة الدول العربية لمكافحة جرائم تقنية المعلومات المنعقدة بمقر الأمانة العامة بالقاهرة لسنة 2010التي تتضمن المادتان 32 و34 من الاتفاقية أحكاما بشأن المساعدة المتبادلة وإجراءات التعاون وطلبات المساعدة المتبادلة[1].

اتفاقية بودابست المنعقدة في سنة 2001 تحت إشراف المجلس الأوروبي التي تهدف إلى توحيد السياسة التشريعية من اجل مكافحة الجرائم الإلكترونية المرتكبة في الفضاء الافتراضي وإلى تنسيق

– التعاون بين التشريعات لتسهيل مكافحة الإجرام المعلوماتي وتطبيق إجراءات تتلاءم لتحقيق وملاحقة الفضاء الافتراضي ووضع نظام تعاون دولي[2].

– لتزايد هذه الجرائم عملت أيضا منظمة الأمم المتحدة بدورها إلى عقد اتفاقيات خاصة بمكافحة استعمال التكنولوجيا لسنة 2000 إذ أكدت على الحاجة إلى تعزيز التعاون والتنسيق بين الدول في مكافحة استعمال تكنولوجيا المعلومات[3].

---

[1] http://www.lasportal.org/wps

[2] قجاج يوسف، الإطار الاجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والتعاون، عدد 196/28، 2015، ص 182،186.

[3] مزغيش سمية/ جرائم المساس بالأنظمة المعلوماتية، بحث منشور، جامعة محمد خيضر، بسكرة، الجزائر ،2014، ص 54،55.

نجد أيضا اتفاقية الاتحاد الأمريكي بشأن الأمن الالكتروني وحماية البيانات الشخصية لسنة 2014 وهو اتفاق بشأن التعاون على مكافحة الجرائم في مجال المعلومات الحاسوبية الذي يتمثل في تبادل المعلومات وتقديم المساعدة القانونية وفقا للصكوك الدولية ومنع الجرائم الإلكترونية واكتشافها وقمعها.

ب: معاهدات تسليم المجرمين

ومن الآليات الأخرى التي تسهل التعاون الدولي في التحقيق مع مجرمي الانترنت ومقاضاتهم، معاهدات المساعدة القانونية المتبادلة وتسليم المجرمين وهي اتفاقيات بين البلدان التي تنطبق على قائمة الجرائم وتحدد نوع المساعدة المقدمة منكل بلد ومن معاهدات تسليم المجرمين نجد

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقدة في فينا سنة 2000. حيث بين المؤتمر فهرس الأمثلة المتعلقة بتسليم المجرمين وتحقيق سبل التعاون وتبادل المساعدة القانونية[1].

[1]انظر المادة 18 من القانون الجزائري رقم 09_04 المتضمن قواعد محددة للوقاية من جرائم تكنولوجيا المعلومات والاتصالات ومكافحتها.
المادة 25 الفقرة الرابعة من اتفاقيه مجلس أوروبا بشأن الجرائم الإلكترونية المرجع السابق.

المطلب الثاني:

الجزاءات المترتبة عن ارتكاب الجريمة الإلكترونية والهيئات المكلفة بالوقاية منها ومحاربتها

يترتب عن ارتكاب الجريمة الالكترونية مجموعة من الجزاءات المنصوص عليها في قانون العقوبات و بعض القوانين الخاصة (الفرع الأول)، إضافة إلى إنشاء هيئات خاصة مكلفة بالوقاية و محاربة الجرائم الالكترونية (الفرع الثاني).

الفرع الأول:

الجزاءات المقررة للجريمة الالكترونية

نظرا للتطور التكنولوجي في المجلات تسيرها أنظمة المعالجة الآلية للمعطيات مما ساهم في جعل الخطر يتزايد أكثر ما أدى بالمشرع الجزائري إلى تقرير مجموعة من العقوبات للجرائم الالكترونية، حيث نص على عقوبات تطبق على الشخص الطبيعي، وعقوبات تطبق على الشخص المعنوي، تتمثل في عقوبات أصبية، وأخرى تكميلية.

أ –عقوبات المجرم الالكتروني كشخص الطبيعي:

تتباين عقوبات المجرم الالكتروني كشخص الطبيعي باختلاف أنواع الجرائم المرتكبة، وجسامة الضرر الذي أحدثته، فعقوبة الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات في صورتها البسيطة لم تؤدي إلي فساد نظام المعالجة الآلية للمعطيات إزالتها، أو تعديلها فان العقوبة الأصلية تكون الحبس من ثلاثة (03) أشهر إلى سنة، و الغرامة من خمسين ألف دينار جزائري (50000) دج إلى مائة ألف دينار جزائري (100000) دج طبقا للمادة 394 مكرر من قانون العقوبات.

أما في صورتها المشددة من خلال نص المادة 394 مكرر الفقرة الثانية و الثالثة من قانون العقوبات على مضاعفة العقوبة إذا ترتب عن هذه الأفعال تغيير، أو حذف البيانات، أما إذا ترتب عن الدخول و البقاء غير المشروع تخريب لنظام عمل المنظومة العقوبة تكون بالحبس من ستة (06) أشهر إلى سنتين و غرامة من خمسين ألف دينار جزائري (50000) دج إلى مائة وخمسين ألف دينار جزائري (150000) دج[1].

أما عقوبة الاعتداء العمدي على المعطيات طبقا لنص المادة 394 مكرر 1 فالمشرع الجزائري حدد عقوبة الاعتداء على المعطيات الموجودة داخل النظام بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من خمس مائة ألف دينار جزائري (500000) دج إلى مائتين ألف دينار جزائري (200000) دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وكذا إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية طبقا لنص المادة 394 مكرر 2من قانون العقوبات بالحبس من شهرين إلى ثلاث سنوات و بغرامة من مائة ألف دينار جزائري (100000) دج، أو إلى خمس ملايين دينار جزائر(5000000) دج[2]،كما منح المشرع الجزائري للقاضي سلطة تقرير عقوبات تكميلية حيث تنص المادة 394 مكرر 6 من قانون العقوبات على انه " **مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب الجرائم الماسة لأنظمة المعالجة الآلية للمعطيات، مع وإغلاق المواقع (les sites)التي تكون محلا للجريمة من الجرائم المعاقب عليها، علاوة على إغلاق المحل أي المقهى الالكتروني إذا ارتكبت الجريمة بعلم مالكها** ".[3]

[1]انظر المادة 394 مكرر الفقرة الثانية والثالثة من قانون العقوبات.
[2]انظر المادة 394 مكرر 1 من نفس القانون.
[3]نظر المادة 394 مكرر6 من نفس القانون

ومن الملاحظة أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة.

نظرا لخصوصية الجريمة الالكترونية التي تتسم بسرعة التطور مما دفع بالمشرع الجزائري إلى وضع قوانين خاصة لردعها، إضافة إلى ما نص عليه في قانون العقوبات تتمثل:

– العقوبات المنصوص عليها في قانون 09–04 المتعلق بالقواعد الخاصة المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحاته، حيث نصت المادة 11 من هذا القانون على أن"... **دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50000 دج إلى 500000 دج**" .[1]

– إضافة إلى ما سبق نصت المادة 43 من القانون 18–05 المتعلق بالتجارة الالكترونية على إن عند ارتكاب المورد الالكتروني أثناء ممارسة نشاطه بمخالفة تكون تحت طائلة عقوبة غلق المحل المتعلق بممارسة الأنشطة التجارية يتم تعليق تسجيل أسماء نطاق المورد الالكتروني بشكل تحفظي من طرف الهيئة المكلفة لمنح أسماء النطاق في الجزائر بناءا على مقرر من وزارة التجارة و ذلك لمدة لا تتجاوز 30 يوم.[2]

– نص المشرع الجزائري في القانون 18–07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث نصت المادة 59 منه" **يعاقب بالحبس من سنة الى ثلاث**

[1]انظر المادة 11 من القانون 09-04 المتعلق بالقواعد الخاصة المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
[2]انظر المادة 43 من القانون 18-05 المتعلق بالتجارة الالكترونية.

سنوات و بغرامة من 100000 دج إلى 300000 دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو نزيهة أو غير مشروعة".[1]

كما نصت المادة 67 من نفس القانون على انه" **يعاقب الشخص بالحبس من سنة إلى خمس سنوات وبغرامة من 500000 دج إلى 1000000 دج كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من هذا القانون** ".

كما أضافت المادة 68 من نفس القانون" **يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 60000 دج إلى 300000دج كل من قام في غير الحالات المنصوص بها قانونا بوضع او حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانة أو تدابير امن** ".

– عاقبت **المادة** 69 بالحبس من سنة إلى خمس سنوات و بغرامة من 100000 دج إلى 500000 دج كل مسؤول عن معالجة وكل معالج من الباطن وكل مكلف بالنظر إلى هذه بمعالجة معطيات ذات الطابع الشخصي يتسبب أو يسهل و لو عن إهمال الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستعملة أو يوصلها إلى غير المؤهلين بذلك.[2]

ب –عقوبات المجرم الالكتروني كشخص المعنوي

يعد إقرار مبدأ المسؤولية الجزائية للشخص المعنوي من أهم القواعد الجنائية التي تضمنها قانون العقوبات، و ذلك بموجب نص المادة 51 مكرر من قانون العقوبات التي تنص على انه " **باستثناء الدولة و الجماعات المحلية و الأشخاص المعنوية الخاضعة للقانون العام ، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين** ".[3]

[1]انظر المادة 59 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.
[2]انظر المادة 67 و68 و69 من القانون 18- 07المرجع السابق.
[2] انظر المادة 51 مكرر من قانون العقوبات.

وعلى هذا الأساس فان المشرع الجزائري وضع مجموعة من العقوبات للشخص المعنوي نصت عليها المادة 18 مكرر من قانون العقوبات، تتمثل في الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[1]

وضعت نفس العقوبات المنصوص عليها في قانون العقوبات بالنسبة للجرائم المرتكبة من طرف الشخص المعنوي في ظل قانون 09-04.

أحالتنا المادة 70 من قانون 18-07 المرجع السابق فيما يخص عقوبات الشخص المعنوي بالأخذ وفقا للقواعد المنصوص عليها في القانون العقوبات. ومن العقوبات التكميلية نجد: حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات، الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات، نشر وتعليق حكم الإدانة، الوضع تحت الرقابة القضائية لمدة لا تتجاوز 5 سنوات، م مصادرة الشيء الذي استعمل في ارتكاب الجريمة.

كما نصت المادة71 من القانون 18 – 07 على انه " **كل من يخالف أحكام هذا القانون يتعرض لعقوبات تكميلية المنصوص عليها في قانون العقوبات كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة و التي نتج عنها ارتكاب الجريمة**".[2]

[1] انظر المادة 18 مكرر من قانون العقوبات.
[2] انظر المواد 70 و71 من القانون 18-07 المرجع السابق.

الفرع الثاني:

الهيئات المكلفة بالوقاية من الجريمة الإلكترونية ومحاربتها

قامت الجزائر بوضع عدة أجهزة وهيئات من اجل مواجهة الجريمة الإلكترونية نذكر منها التالي:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال

تم إنشاء هذه الهيئة بموجب القانون رقم 09 – 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، والذي حددت المادة 14 منه مهام الهيئة والمتمثلة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال في ذلك وإنجاز الخبرات القضائية تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

ثانيا: الهيئات القضائية الجزائية المتخصصة

تم إنشاؤها بموجب القانون رقم 04 –14المعدل لقانون الإجراءات الجزائية، واختصاصها إقليمي موسع طبقا للمرسوم التنفيذ رقم 06 –348 لسنة2006،المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.[1]

[1]انظر المادة 14 من القانون الجزائري رقم09 –04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها المرجع السابق.

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب مرسوم رئاسي رقم 04 _ 183 لسنة 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام و الاتصال، وهو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزير الدفاع الوطني[1] .

يتكون المعهد من 11 دائرة متخصصة في مجلات مختلفة من بينها دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة كما تقدم مساعدة تقنية للمحققين في المعاينات.

[1] انظر المادة 02 من المرسوم الرئاسي رقم 19 / 172 مؤرخ في يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و كيفيات سيرها، الجريدة الرسمية، عدد 37 صادر في 9 يونيو 2019 .

خلاصة الفصل الأول

لقد تطرقنا في هذا الفصل إلى خصوصية الجريمة الإلكترونية من الناحية الموضوعية، واتضح لنا أن هذا النوع من الجرائم يعد من أكثر الجرائم خطورة، حيث اتسمت بطبيعة خاصة على خلاف الجرائم التقليدية، لذا وجدنا صعوبة في وضع تعريف عام جامع وموحد لها، فقط اختلفت المفاهيم حولها باختلاف الزاوية التي ينظر منها إليها. أين بينا مختلف التعاريف الفقهية والقانونية للجريمة الإلكترونية، وانتهينا إلى تعريفها " كل اعتداء على النظام المعلوماتي أو يتم باستخدام النظام المعلوماتي حيث أن له دور رئيسي في سلوك المجرم، وبهذا المفهوم نجدها تتميز بعدة خصائص تميزها عن باقي الجرائم الأخرى، ومن أهم هذه السيمات طبيعتها العابرة للحدود، لأنها جرائم خفية ومستترة، وطابعها التقني الذي يعقد من مسألة اكتشافها وإثباتها الشيء الذي يميز مرتكبيها ويجعل دوافع ارتكابهم للجرائم الإلكترونية بشتى أنواعها تختلف عن المجرمين العاديين.

تناولنا أيضا عناصر الجريمة الإلكترونية المتمثلة في الأطراف وهم الجاني والمجني عليه والوسائل المستعملة لارتكاب هذه الجرائم، إضافة إلى تحديد أركان الجريمة الإلكترونية فهي تقوم بقيامها وتزول بزوال أحدهما كأي جريمة أخرى، المتمثلة في الركن الشرعي والركن المادي والركن المعنوي وبالنسبة للمشرع الجزائري عرفها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

وما يعاب عليه أنه اهتم بالنص على بعض الجرائم الإلكترونية وليس كلها، كما أهمل المجرم الالكتروني، إذ لم يتعرض له في أي نص قانوني سواء في قانون العقوبات أو القانون 09-04 كما أن التطرق للجريمة الإلكترونية من الناحية الموضوعية والتعرف عليها بعمق يفيدنا في إيجاد الحلول لمواجهتها.

الفصل الثاني: الأحكام الإجرائية الخاصة لمواجهة الجريمة الإلكترونية

الفصل الثاني:

الأحكام الإجرائية الخاصة لمواجهة الجريمة الإلكترونية

إن الانتشار الواسع في مجال الجرائم الإلكترونية الذي يشهده العالم اليوم بسبب التطور التكنولوجي، أدى بالفقهاء إلى اكتشاف قواعد إجرائية جديدة تضمنتها التعديلات المختلفة التي تطرأت على قانون الإجراءات الجزائية الجزائري لإثبات الجرائم الإلكترونية ومكافحتها إلى جانب القواعد التقليدية المنصوص عليها في قانون العقوبات الجزائري، هذاما سنحاول التطرق إلى: كشف الجريمة الإلكترونية (المبحث الأول)، التحقيق والمحاكمة (المبحث الثاني).

المبحث الأول:

كشف الجريمة الإلكترونية

تقتضي متطلبات تطبيق مبدأ الشرعية إرساء قواعد إجرائية تخضع لها السلطة القضائية وأعوانها، حتى تتمكن من ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن البحث والتحري فيها بالأساليب التقليدية فقط[1] .

إن أهمية الجهاز الضبطية القضائية في الكشف عن الجريمة الإلكترونية والتعرف على المجرم الالكتروني، تبعه استعداد المشرع الجزائري لأساليب التحري الخاصة المستعملة بما تناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والضبطية أن يتكيف دورها في مهامها مع الإجرام الحديث مستمدة شرعيتها من المواثيق الدولية التي صادقت، عليها الجزائري[2] .

ونظرا لأهمية التحقيق في هذا النوع من الجرائم وكشفها تطرقنا إلى: كشف الجريمة الإلكترونية وفقا للإحكام التقليدية (المطلب الأول)، كشف الجريمة الإلكترونية وفقا للأحكام المستحدثة (المطلب الثاني).

[1] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09 –04، مذكره مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ،ورقلة، 2013، ص60.

[2] هروال هيبة نبيلة، الجوانب الإجرائية لجرائم الانترنيت، الطبعة 2، دار الفكر الجامعي، القاهرة، 2011، ص76.

المطلب الأول:

كشف الجريمة الإلكترونية وفقا للأحكام التقليدية

تحتوي الأنظمة الإجرائية لمختلف الدول على مجموعة من الأساليب والوسائل التقليدية التي تلجا إليها سلطات البحث والتحري للكشف عن مختلف الجرائم حتى المعلوماتية منها، والاستعانة بتلك الوسائل رغم تقليديتها من اجل التحقيق[1].

لكن اختلاف الطبيعة الإجرامية والجاني والمجني عليه عن نظيرهما في الجرائم التقليدية، بالإضافة إلى الوسائل المرتكبة بواسطتها الجريمة المعلوماتية، أصبح من الضروري إعادة تحيين تلك الوسائل التقليدية بما يتوافق مع الطبيعة الخاصة للجريمة المعلوماتية[2].

تناولنا في هذا المطلب، التحري (الفرع الأول)، تلقي البلاغات والشكاوى (الفرع الثاني)، الإقرار بالجريمة (الفرع الثالث)، الشهادة في الجريمة الإلكترونية (الفرع الرابع).

الفرع الأول:

التحري في الجريمة الالكترونية

يقصد به البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها[3].

[1] بن بادا عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد الثاني، العاب 23، 2015، ص 78.

[2] المرجع نفسه، ص 78.

[3] محمدي بوزينة آمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية جامعة حسيبة بن بوعلي- الشلف، أعمال الملتقى الوطني، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 2017، ص 67.

وضع المشرع الجزائري قواعد وأحكام خاصة لسلطة التحري والمتابعة، الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في تعديل قانون الإجراءات الجزائية لسنة 2006 بموجب القانون رقم 19-10لسنة 2019.

فقد نصت المادة 329 من قانون الإجراءات الجزائية في الفقرة الأخيرة منها جواز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم المنظمة عبر الحدود الوطنية، والجرائم الماسة بالمعالجة الآلية للمعطيات وفق قواعد وأحكام خاصة[1].

وبموجب المادة 37 من قانون الإجراءات الجزائية فقد تم توسيع مجال اختصاص النيابة العامة، إلى اختصاصات محاكم أخرى، في الجرائم الإلكترونية[2].

الفرع الثاني:

تلقي البلاغات والشكاوى

يقصد بالتبليغ عن الجريمة مجرد الإخبار عنها، ويمكن أن يكون التبليغ من مصدر معلوم أو مجهول، ويعقب تلقي التبليغات جمع الاستدلالات مباشرة، والواقع أن التبليغ يقصد به إخبار الجهات المختصة بالتحقيق عن جريمة معينة وقعت أو على وشك الوقوع قيد التحضير أو وجود اتفاق أو عزم على ارتكابها[3].

[1] انظر المادة 329 قانون رقم 19-10 المؤرخ في 11ديسمبر 2019، يعدل الأمر رقم 66-155، المؤرخ في 08 يونيو 1966، والمتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية، عدد 78، المؤرخ في ديسمبر 2019.

[2] انظر المادة 37 قانون رقم 19-10، مرجع نفسه.

[3] فضل سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الأنترنت، دار النهضة العربية، القاهرة، 2013، ص 276.

فالأصل أنه على رجال الضبطية القضائية قبول البلاغات أو الشكاوى التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند إلحاقها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري إخطار رئاسته في حالة الجرائم الإلكترونية، والجهات المختصة في ذلك كما يتم أيضا الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، ويكون عن طريق رسالة إلكترونية إلى عنوان البريد الالكتروني للجهات المختصة. مثلا: إبلاغها عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال[1].

الفرع الثالث:

الإقرار بالجريمة الالكترونية

الإقرار هو اعتراف الشخص المتهم من نفسه بارتكابه للجريمة، وعن ثبوت حق الغير على الاعتراف به، وهو يعتبر من أقوى البيانات والحجج شرط ألا تكذبه قرائن أخرى.

فقد اشترط الفقهاء حتى يؤخذ كدليل أمام القضاء وأن يكون هذا مختارا. والإقرار حجة تقتصر على المقر ولا تتعدى غير، فإذا تضمن الإقرار أن له شريك فلا يكون حجة على الشريك، ويكون مرة واحدة هما في جرائم القصاص والتعزيز والحدود[2].

[1] بوعمرة محمد، بن ينال سيدي على، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكره تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة اكلي محند أو لحاج، البويرة، 2020، ص 42.

[2] محمد سليم العوا، في أصول النظام الجنائي الإسلامي، دار المعارف، ص 291.

الفرع الرابع:

الشهادة في الجريمة الإلكترونية

سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، حيث يقوم على استدعاء أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن الجرائم والقبض على مرتكبها، يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية[1].

المطلب الثاني:

كشف الجريمة الإلكترونية وفقا للأحكام المستحدثة

إن تطور مجال الجرائم الإلكترونية أصبح أمرا واقعا في ظل الثورة المعلوماتية والتطور الهائل في وسائل الاتصال الحديث، وهو ما أدى إلى تباين صورها الإجرامية وتنوعها. وتزايد خطرها على المستوى الوطني والدولي الأمر الذي بات يهدد الأفراد واستقرار الدولة خاصة عند ترويج معلومات كاذبة التي من شأنها أن تمس بالأمن العمومي، مما دفع بالمشرع الجزائري للتصدي لهذه الجرائم وذلك ضمن استحداث آليات جديد, تعمل على الحد منها والكشف عنها، منها إجراءات منصوص عليها في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال و مكافحتها واستحداث القطب الجزائي ضمن تعديل قانون الإجراءات الجزائية 21 – 11 لسنة 2021المعدل و المتمم لأمر 66 – 155 متخصص في المتابعة في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[2].

[1] بوعمرة محمد، بن ينال سيدي علي، مرجع سابق، ص 42.

[2] أمر رقم 21 – 11 المؤرخ في 25 أغسطس 2021، يتمم الأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 65 الصادرة في 26 غشت 2021.

الفرع الأول:

أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

تضمنت أحكام المواد 65 مكرر من قانون رقم 06- 22المتضمن قانون الإجراءات الجزائية، هذه الوسائل يقصد بها كل من اعتراض أو تسجيل عن طريق وسائل الاتصال السلكية واللاسلكية، تسجيل الأصوات والتقاط الصور اذ عرفت المادة 65 مكرر 5 من ضمن الفقرة الثانية كلا الوسيلتين:" **وضع الترتيبات التقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص**".

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص إذ اقتضت ضروريات التحري والتحقيق في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الثاني:

التسريب

إن الجريمة الإلكترونية من بين الجرائم التي يمكن فيها الاستعانة بإجراء التسرب تضمنت أحكام المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية، فالتسرب يقصد به قيام ضابط الشرطة القضائية بالتوغل داخل المجموعات الإجرامية وإيهامهم بأنه شريك معهم أو خاف وذلك من أجل الإيقاع بهم.

يمكن تصور عملية التسرب في نطاق مكافحة الجريمة الإلكترونية دخول ضابط أو عون الشرطة القضائية بالدخول إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو

اشتراكه في محادثات عرض الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر ذلك الفاعل معهم المشارك مستخدما في ذلك هوية مستعارة ووهمية من أجل الإيقاع بهم[1].

الفرع الثالث:

المراقبة الإلكترونية

إجراء تم استحداثه بموجب المادة 03 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، تم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيل وتجميع محتواها ونجد المشرع الجزائري قد تبنى هذا الإجراء رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها بنص المادة 39 من الدستور الجزائري نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا كالتالي: تسجيل الاتصالات الإلكترونية في حينها، القيام بإجراءات التفتيش والحجز للمنظومة المعلوماتية، إجراء مراقبة الاتصالات الإلكترونية، هو إجراء يدخل كذلك في إطار التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية[2].

إلى جانب إمكانية القيام بإجراء مراقبة الكترونية في إطار التحريات والتحقيقات القضائية للوصول إلى أدلة، يمكن أيضا استغلال هذه التقنية للعمل في بيئة الرقابة من اجل الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة[3] ،والأفعال الموصوفة بجرائم الإرهاب والتخريب،

[1] بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد الثاني، العدد 23، 2015، ص 78.

[2] بن بادة عبد الحليم، مرجع نفسه، ص 86.

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، السنة الجامعية 2013، ص 184.

والتي تهدد النظام العام والدفاع الوطني، حسب القانون09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال و مكافحتها في مادته الرابعة

قام المشرع الجزائري بخطوة جريئة من خلال نصه على إجراء الرقابة الإلكترونية للاتصالات، باعتبارها من أخطر الإجراءات في النظام الإجرائي عبر العالم الافتراضي كونه يمس بخصوصية الإنسان وحرمة حياته[1].

الفرع الرابع:

إقحام مزودي خدمات الاتصالات الإلكترونية في مسار الوقاية من الجرائم الإلكترونية

يظهر ذلك من خلال فرض مجموعة من الالتزامات عليهم والمذكورة في المواد 10،11 و12 من القانون 04 – 09الخاص بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال الالتزام بالتعاون مع مصالح الأمن المكلفة بالتحقيق القضائي عن طريق جمع المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات.

المبحث الثاني:

التحقيق والمحاكمة في الجريمة الإلكترونية.

تعتبر الجريمة الإلكترونية من الجرائم المنصوص عليها في قانون العقوبات والقوانين الأخرى مثلها مثل الجرائم التقليدية، فلذا نجدها تتسم بالدعوى العمومية، وهذه الدعوى تتم بمراحل، بداية بمرحلة جمع الاستدلالات وهي المرحلة الأولى، وصولا إلى مرحلتي التحقيق والمحاكمة.

[1] سعيداني نعيم، مرجع سابق، ص 184.

تعد البيئة الرقمية مسرحا لارتكاب الجريمة الإلكترونية والتي تستدعي جميع الإجراءات المستحدثة التي تتلاءم مع الطبيعة المادية والتقنية لهذا النوع من الجرائم من اجل الوصول إلى الدليل الرقمي الخاص بها.

وسنتطرق في هذا المبحث إلى دراسة إجراءات التحقيق (المطلب الأول) والمحاكمة في الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول:

التحقيق في الجريمة الالكترونية

التحقيق في الجريمة الإلكترونية يعتبر المرحلة الثانية بعد مرحلة جمع الاستدلالات، فهو من اختصاص قاضي التحقيق، وصولا إلى مرحلة المحاكمة والتي تعتبر بمثابة آخر مرحلة من مراحل الدعوى العمومية والتي تؤدي إلى انقضائها.

الفرع الأول:

آليات البحث والتحري في الجرائم الإلكترونية

ما لا شك فيه أن إدانة المتهم من عدمه مرتبط باستجلاء الحقيقة، إقامة الإسناد المادي على مرتكبها بأدلة الإثبات عن طريق التحقيق، فهو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة باختلاف أنواعها.

إن عملية التحقيق الجنائي تمر بمرحلتين، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى هي مرحلة جمع الاستدلالات يباشرها أعضاء الضبط القضائي، حسب المادة 12/3 من قانون الإجراءات الجزائية الجزائري والتي تنص " **و يخاطب الضبط القضائي مهمة البحث والتحري عن**

الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبها ما دام لم يبدأ فيها بتحقيق قضائي"[1].

والمرحلة الثانية تدخل في اختصاص قاضي التحقيق، حسب المادة 38 من القانون رقم 06-22 المتعلق بالإجراءات الجزائية التي تنص " **و يناط قاضي التحقيق إجراءات البحث والتحري ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق وإلا كان ذلك الحكم باطلا"**[2].

ولهذا يمكن القول إن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أو ابتدائيا.

وإذا كان التحقيق بصفة عامة يعتمد على ذكاء وفطنة المحقق وقوة ملاحظته وسرعة البديهة لديه، محاولا بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة والبحث فيها وفي الأدلة وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطوير لأساليب ارتكابها وتكليف جهات مختصة لممارسته من أجل مواكبة الجريمة فيهذه البيئة[3].

أولا: الأجهزة المختصة في البحث والتحرير

إن ارتفاع نسبة الجرائم المعلوماتية قد طرح عدة تحديات لأجهزة الضبط القضائي، مما دفع إلى ضرورة تطوير هذه الأجهزة لمسايرة التطور الحاصل في مجال الجريمة، ونتيجة لذلك نجد معظم الدول قامت بإحداث أجهزة متخصصة لمواجهة الجريمة الإلكترونية، والتي تتولى مهمة التحاليل عن الجرائم المرتكبة في العالم الافتراضي، وقد تحمل هذه الأخيرة تسميات مختلفة منها فرقة التحري عن جرائم

[1] أنظر المادة 12 من قانون الإجراءات الجزائية الجزائري، المرجع السابق.

[2] أنظر المادة 38 من قانون الإجراءات الجزائية الجزائري المرجع السابق.

[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، ص 43.

المعلوماتية إلى غير ذلك من التسميات، إلا أن هذه الأجهزة لا يقتصر دورها على المستوى الوطني، بل هناك أجهزة خصصت للمستوى الدولي ففي هذه النقطة نحاول ذكر بعض الأجهزة سواء كان دورها على المستوى الوطني أو الدولي كالتالي:

أ- الأجهزة المختصة بالبحث والتحري عن الجريمة الإلكترونية على المستوى الوطني

نظرا للخصوصية التي تتميز بها الجريمة الإلكترونية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة بعملية البحث والتحري عن الجريمة الإلكترونية لمنعها، والتخفيف من حدتها والكشف عنها، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني فعلى مستوى جهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني، المخبر المركزي للسلطة العلمية بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، بالإضافة إلى وجود على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر[1].

أما على مستوى الدرك الوطني يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي وجرائم الإلكترونية ومكافحتها التابع لمديرية الأمن العمومي للدرك الوطني[2].

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر عن غيرها على كشف

[1] بوبقرة خيرة، مرجع سابق، ص 46 – 47.

[2] بوبقرة خيرة، مرجع نفسه، ص 48.

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[1].

ومن أجل اشتراك مزودي خدمات الانترنت والاتصالات التابعة والمتنقلة في محاربة الجرائم الإلكترونية يلزم القانون رقم 09 – 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال و مكافحتها هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها[2].

ب-الأجهزة المختصة بالبحث والتحري عن الجريمة الإلكترونية على المستوى الدولي

تعرف الجريمة الإلكترونية ضمنها ذات دولي عابر للحدود الوطنية، يمكن أن يتعدى أثرها عدة دول، فإن مكافحتها لا يتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، كما أن التحقيقات المتبادلة في الجريمة الإلكترونية وملاحقتها قضائيا تؤكد أهمية المساعدة القانونية المتبادلة بين الدول، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر[3] ما يلي:

1- **على الصعيد الدولي:** تعد المنظمة الدولية للشرطة الجنائية (الإنتربول)[4]، من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم الإلكترونية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في دول الأطراف على نحو فعال من اجل مكافحة

[1] عثمان عز الدين، إجراءات التحقيق والتفتيش في المساء بأنظمة الاتصال والمعلوماتية، مجله دائرة البحوث والدراسات القانونية والسياسية-مخبر المؤسسات والنظم السياسية، المركز الجامعي مرسلي عبد الله، تيبازة، المجلد الثاني، العدد 04، 2018، ص 52.

[2] أحمد مسعود مريم، مرجع سابق، 2013، ص66.

[3] عثمان عز الدين، مرجع نفسه، ص 49، 50 ،51.

[4] بعد انتهاء الحرب العالمية الثانية عقد في بروكسل (بلجيكا) مؤتمر دولي في الفترة من 9-سبتمبر 1946 انتهى إلى احياء اللجنة الدولية للشرطة (ICPO)ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول ووضع ميثاق هذه المنظمة في الفترة 7 واعتبر نافذا اعتبارا من 13جوان 1956.

الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية، وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

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

الثانية: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم بناءا على طلبات تقديم صادرة من المحكمة إلى دول الأطراف للتعاون معها.

تعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم الإلكترونية بوضع قائمة اسمية لضباط مختصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم الإلكترونية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة الإلكترونية من خلال خلق فرق عمل وورشات التكوين[1]،أنشأت هذه المنظمة وحدة متخصصة في مكافحة هذا النوع من الجرائم تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الجرائم وكيفية التدريب على مكافحتها.

2- على الصعيد الإقليمي:

أولا: الشرطة الأوروبية أو الأوروبول

هو جهاز على مستوى الاتحاد الأوروبي تم إنشائه في لوكسمبور 1992 مقره لاهاي بهولندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية لدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرام المعلوماتي، يهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف دول الأعضاء وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة

[1]Myriam QUEMENER. Cybercriminalite-droit pénal, appliqué. economica, septembre 2010.p 208

في أي دولة عضو بخصوص هذه الجرائم، وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم Internet Crime Reporting Online System في سنة 2010 بغرض التنسيق في مجال مكافحة الجريمة الإلكترونية على مستوى دول الأعضاء .

يوجد أيضا جهاز 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 دولتان على الأقل من دول 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.

ثانيا: موقف المشرع الجزائري

تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشاهدها البشرية من قبل، ورغبة منه في التصدي لظاهرة الإجرام الالكتروني وما يصاحبها من أضرار من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، قام من خلال ذلك إصدار مجموعة من القوانين منها قوانين عامة وقوانين خاصة لمواجهة وقمع الاعتداءات الواردة على المعلوماتية، بموجب القانون رقم 04 15 المتضمن تعديل قانون العقوبات وهذا بإدراجه قسما كاملا (المواد من 394 إلى 394 مكرر8) يتضمن العقوبات المقررة للمساس بأنظمة المعالجة الآلية للمعطيات، ثم سنة 2009 بموجب القانون رقم 09 -04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ثم سنة 2015 بإقراره لقانونين الأول تحت رقم 03-15 المتعلق بعصرنة قطاع العدالة،

والثاني تحت رقم 04 -15 المتعلق بالقواعد المطبقة على التوقيع والتصديق الإلكتروني تناول من خلالهما بعض النصوص التجريمية ضد الاعتداء على منظومة التوقيع والتصديق الإلكترونين.

الفرع الثاني:

إجراءات التحقيق في الجرائم الإلكترونية

أدى التطور السريع الحاصل في مجال المعلوماتية وما صاحب هذا التطور من انعكاسات على الجرائم في الوسائل المستعملة في ارتكاب هذه الجرائم والمحل الذي تقع عليه باعتباره بيانات ومعطيات غير مادية ونوع الجنات الذين يرتكبونها جعل هذه القوانين غير مواكبة لها، الأمر الذي دفع المشرع الجزائر إلى ضرورة إعادة النظر في بعض الإجراءات التقليدية وقوانين الإجراءات الجزائية، باستحداث نوعي من القواعد الإجرائية تتلاءم مع هذه الجرائم ذات طبيعة خاصة وتقنيات عالية.

ومما لا شك فيه أن التحقيق في الجرائم التقليدية يختلف كليا عن التحقيق في الجرائم الإلكترونية المرتكبة في مسرح افتراضي غير مادي، لكون الجريمة الإلكترونية تحتاج إلى تطوير تلك الإجراءات التي تثير العديد من المشكلات نظرا لخصوصيتها، كالتفتيش، الضبط، المعاينة والخبرة، وتحيينها لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها[1].

أولا: المعاينة

تعتبر المعاينة من المراحل الأولى للاستدلال ومن أهم إجراءات التحقيق، وكون الجريمة الإلكترونية من الجرائم المستحدثة، فالمعاينة تعتبر من الإجراءات المهمة بما توفره من أدلة إثبات إذا تعلق الأمر بالجرائم الإلكترونية.

[1] محمد قدري حسن عبد الرحمان، جرائم الاحتيال الالكتروني، مجله الفكر الشرطي، عدد 79، صادر من مركز بحوث الشرطة، القيادة التامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص 159.

تعرف المعاينة بأنها" الكشف الحسي المباشر لإثبات حاله شيء أو شخص"[1] وتعرف أيضا بأنها إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما يفيد في كشف الحقيقة، المعاينة من الوجهة القانونية ليست وسيلة بل هي إجراء استقصائي كاشف لأبعاد الجريمة وأركانها[2].

فالمعاينة من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها، وكلما رأت ضرورة لذلك، حيث تنص المادة 79 من قانون الإجراءات الجزائية الجزائري على أنه" يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها"،

غير أنها تختلف حسب طبيعة الجريمة الإلكترونية التي تم ارتكابها، فإذا كانت واقعة على الحاسب الآلي أو الأشرطة، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ومن ثم ضبطها ووضعها في أحراز مفتوحة تقدم للنيابة العامة[3].

غير أن الحال بالنسبة للجرائم الإلكترونية خاصة جرائم الاعتداء على الأشخاص التي من الممكن أن يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوعها واكتشافها مما يؤدي إلى محو آثارها أو تلفها أو العبث بها[4].

فبالنسبة لمعاينة مسرح الجريمة الإلكترونية قد أجمع الخبراء باعتباره مستودع سرها، وعليه فإن عملية جمع الأدلة من خلال مسرح الجريمة الإلكترونية يقتضي التعامل على أساس أن هناك مسرحين، مسرح تقليدي ومسرح سيبيراني.

---

[1] عبد الصبور عبد القوي على مصري، التجارة الالكترونية والقانون، الطبعة الأولى، لعلوم النشر والتوزيع، القاهرة، 2010، ص 316.

[2] المرجع نفسه، ص 260.

[3] ياسر محمد الكرمي محمود ابو حطب، الحماية الجنائية والمنية للتوقيع الالكتروني منشاة المعارف، الإسكندرية، 2014، ص 243.

[4] هروال هيبة نبيلة ، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013، ص 217.

مسرح تقليدي يقع خارج بيئة التقنية تقوم فيه على عناصر مادية وملموسة مثلا: أشرطة الحاسب والكابلات الخاصة به وشاشة العرض ويترك الجاني فيها آثار عديدة كالبصمات والمتعلقات الشخصية، ويتعامل معها أعضاء فريق المعاينة كل حسب تخصصه بدون أية صعوبة.

مسرح سيبيراني وهو عكس التقليدي يقع في بيئة رقمية والعالم الافتراضي من خلال وسائل إلكترونية يتكون من البيانات الرقمية التي يتم التعامل بواسطتها في بيئة الحاسوب وشبكاته وفي ذاكرته وفي الأقراص الموجودة بداخله والتعامل مع الأدلة الموجودة في هذا المسرح غير أن هناك المادية المحسوسة لمكان وقوعها مقهى الانترنت مثلا وهو أكثر صعوبة تعترض المختص كون عملية المعاينة جد معقدة في البيئة الرقمية، بحيث لا تتم إلا عن طريق خبير متخصص تلقى تكوينا عاليا في التعامل مع الأدلة الرقمية والمحافظة عليها[1].

ثانيا: التفتيش

أن طبيعة الجريمة الإلكترونية تجعلها تتميز عن غيرها من الجرائم الأخرى كونها من الجرائم التي يصعب إثباتها لذلك أجاز المشرع الجزائري ضمن القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في المادة 05 للسلطات القضائية المختصة بالتفتيش في المنظومة المعلوماتية ضد جريمة يحتمل وقوعها وتتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم الأخرى، نظرا لسرعة ارتكابها ومحو آثارها وتخطيها للحدود الوطنية[2].

[1] محمد ابن نصير محمد السرحاني، مهارات التحقيق الفني في جرائم الحاسوب والانترنيت، رسالة ماجستير في العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، قسم الشرطة، الرياض، 2004، ص 77.

[2] انظر المادة 05 من الأمر 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع السابق.

لذا يعتبر التفتيش إجراء من إجراءات البحث والتحقيق يهدف إلى استخلاص الدليل الالكتروني قبل أن يقوم المجرم بحذفه أو تدميره أو إخفائه، فالتفتيش في عالم التقنية يختلف عن التفتيش العادي لأنه منصب على بيئة رقمية تتكون من مكونات مادية ومعنوية فلقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانه التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه أنه "**إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجر ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك**"[1].

ثالثا: ضبط الأدلة في الجريمة الإلكترونية

الضبط هو الوسيلة القانونية التي بواسطتها تضع السلطة المختصة يدها على الأشياء والوسائل التي وقعت عليها الجريمة أو استخدمت لاقترافها، أو نتجت عنها فهو إذا الأثر المباشر للتفتيش[2]، والضبط كقاعدة عامة يقع على المكونات المادية الملموسة للكمبيوتر دون المعنوية وباعتبار البيانات المعالجة إلكترونيا محل الضبط في الجرائم الإلكترونية، أدى إلى انقسام الفقه إلى اتجاهين، فالبعض يرى أن بيانات الحاسب لا تصلح أن تكون محلا للضبط لكونها بيانات معنوية فمن المستحيل ضبطها إلا بعد نقلها على كيان مادي ملموس أما الاتجاه الثاني يرى أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية مغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية وهذا الخلاف دفع بالمشرعين في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمجال التفتيش والضبط ليشمل إلى جانب الأشياء المادية، البيانات الإلكترونية، إذا نجد المشرع الجزائري قد تدخل بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، لاستكمال الفراغ

[1] انظر المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري.

[2] محمد طارق عبد الرؤوف الخان، التعليم الالكتروني و التعليم الافتراضي، المجموعة العربية للتجريب و النشر، القاهرة، 2014، ص 290.

التشريعي في المنظومة التشريعية، حيث استحدث المادة 06 التي تنص على أنه" **عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث و اللازمة لفهمها على دعامة التخزين تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية**"، أما فيما يخص الصعوبات التي يثيرها ضبط مكونات الحاسوب فهنا لا يجب الخلط بين ضبط المكونات المادية وضبط المكونات الدولية للحاسوب.

فيما يخص المكونات المادية للنظام فلا يثير ضبطها أي صعوبات إذ يمكن ضبط جهاز الكمبيوتر وملحقاته، في حين تكمن الصعوبة في ضبط النظام كله أو الشبكة كلها.

فمن المشكلات التي تواجهها عملية الضبط للوسائل المعنوية نجد ضخامة البيانات التي من الواجب فحصها من قبل المحقق نتيجة حجم الشبكة الأمر الذي يتطلب من الخبرة الفنية ما ينجم لتحديد البيانات التي تصلح كأدلة جنائية من عدمه[1].

كما يشكل أحيانا اعتداء على الحقوق والحريات الفردية عند عدم مراعاة الضمانات المقررة لحماية هذه الحقوق والحريات.

ومن المشكلات المثيرة عند ضبط البيانات المخزنة لجهاز الحاسوب مشكلة أخذ نسخة من تلك البيانات عند ضبط النسخة الأصلية حينما تكون هذه الأخيرة مستحيلة في النظام أو بالشبكة التي تربط بين عدة أجهزة إذ لا يمكن اعتبارها نسخة أصلية لاحتمال أنه قد تم التلاعب بها[2].

[1] وفي هذا الصدد قضت المحكمة الفيدرالية الألمانية بإلغاء المحضر الذي ورد على 220 قرص صلب بالإضافة إلى الوحدة المركزية للحسب بحجة مخالفة سلطة التحقق التناسب، مشار إليه عند سعيدني نعيم، مرجع سابق، ص 162.

[2] محمد طارق عبد الرؤوف الخان، مرجع سابق، ص 290 .

وطبقا للمادة 11 من قانون الإجراءات الجزائية أن إجراءات التحري والتحقيق سرية ما لم ينص القانون على خلاف ذلك، كما يجب على ضباط الشرطة القضائية تدوين جميع إجراءات الضبط في محضر خاص بعد تسجيلها وقيدها في سجل خاص.

رابعا: الخبرة التقنية

الخبرة التقنية إجراء يستهدف استخدام قدرات الشخص الفنية والعلمية والتي لا تتوافر لدى رجال القضاء من اجل الكشف عن دليل أو قرينة تفيد في كشف الحقيقة في ارتكاب الجريمة ونسبتها إلى المتهم أو تحديد صفات شخصيته الإجرامية[1].

ففي مجال الجريمة الإلكترونية للخبرة التقنية أهمية بالغة، لا يستطيع أن يتعامل معها إلا شخص ذو دراية وخبرة في هذا المجال، فالخبرة إذا طريقة من الطرق التي يلجأ إليها الخصوم لإثبات بعض الحقوق، ولتكون وسيلة تساعد القاضي في الوصول إلى الحقيقة في النزاع المعروض عليه وفصل الخصومات القائمة بين الأفراد[2].

فالخبير الإلكتروني لابد أن تتوفر لديه المقدرة الفنية والإمكانيات العلمية في مسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية[3]، مع مراعاة الخبرة العملية التي تحقق الكفاءة الفنية من اجل كشف الغموض عن الجريمة وجمع أدلتها والتحفظ عليها ومساعدة المحقق في إيجاد جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[4].

[1] الشلقاني أحمد شوقي، مبادئ الإجراءات في التشريع الجزائري، ص 59.

[2] صغير يوسف، مرجع سابق، 2013، ص 89.

[3] صغر يوسف، مرجع نفسه، ص 88،89.

[4] عبد الفتاح بيومي حجازي، مرجع سابق، ص 137.

فقد نص المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون رقم 09 – 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه" **يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لا نجاز مهمتها**" فالمشرع هنا قد قام بتوسيع دائرة المساعد القضائية في مجال مكافحة الجريمة الإلكترونية لتشمل إلى جانب الخبير، جميع المتخصصين في مجال تكنولوجيات الإعلام والاتصال، وفي هذا الصدد نجد المشرع قد قام بإنشاء هيئات وأجهزة متخصصة في مكافحة الجريمة، أهمها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

المطلب الثاني:

إجراءات المحاكمة في الجريمة الإلكترونية

إن القضية الخاصة بالجريمة الإلكترونية لا يمكن بأي حال من الأحوال أن تبقى رهينة التحقيق والتحريات، بل لابد لها أن تدخل في مرحلة جديدة لتصل إلى أروقة المحاكم التي تختص بمحاكمة أو متابعة مرتكبي الجريمة الإلكترونية، وبالتالي وجود جهاز قضائي من اجل محاكمة هؤلاء المجرمين، يختص بالفصل في هذا النوع من الجرائم نظرا لخطورتها، وهو ما ستتطرق إليه في هذا المطلب، اختصاص المحكمة وتشكيلها (الفرع الأول) والإجراءات والقواعد العامة للمحاكمة (الفرع الثاني).

[1] مرسوم رئاسي رقم 15– 261 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العد 53 المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 53، صادر في 08 أكتوبر 2015.

الفرع الأول:

اختصاص المحكمة وتشكيلها

نظرا للطبيعة القانونية الخاصة التي تتميز بها الجريمة الإلكترونية و السيمات أو الخصوصيات التي تمتاز بها ولعل أهمها اعتبارها جريمة عابرة للحدود، جعلها تستعصي على القواعد التي تحكم مسألة الاختصاص المكاني، التي تخضع لها الجرائم التقليدية، فطابعها الافتراضي جعلها لا تتلاءم مع معيار محل وقوع الجرم الذي يتم اعتماده لتمديد المحكمة المختصة[1].

إضافة إلى الاختصاص النوعي الذي يتحدد حسب نوع الجريمة التي ينظر فيها هذا ما سنتطرق إليه في النقط التالية:

أولا: اختصاص المحكمة

لقد نص قانون الإجراءات الجزائية المعدل في المواد 37، 40، 329 منه على تمديد الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وكذا المحكمة إلى دائرة اختصاص المحاكم الأخرى، عن طريق التنظيم في الجرائم المذكورة على سبيل الحصر، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات اذ أنشاء محاكم أو أقطاب جزائية متخصصة ذات اختصاص إقليمي ومحل موسع وهو ما سنتناوله من خلال الاختصاص المحلي (أ) والاختصاص النوعي (ب).

[1] المناعسة أسامة أحمد، مرجع سابق، ص 296.

أ- الاختصاص الإقليمي أو المحلي في الجريمة الإلكترونية

أصبحت الأقطاب الجزائية المتخصصة أمرا مهما لابد منه، فنجدها تتميز بأنها ذات اختصاص محلي موسع طبقا لقانون الإجراءات الجزائية[1].

وبصدور المرسوم التنفيذي رقم 06-348الذي تم بموجبه تعيين وتحديد المحاكم ذات الاختصاص الإقليمي الموسع وكذا الجهات القضائية لهذه المحاكم، حيث تم تنصيب أربعة أقطاب ممثلة فيما يلي[2]:

القطب الجزائي بالجزائر سيدي محمد ويمتد اختصاصه الإقليمي إلى المجالس التالية: الجزائر، الشلف، الاغواط، البليدة، البويرة، تيزي وزو، الجلفة، بومرداس[3].

القطب الجزائي بقسنطينة يمتد اختصاصه المحلي ليشمل المجالس القضائية التالية: قسنطينة، أم البواقي، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج[4]

القطب الجزائي بوهران ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية: وهران، بشار، تلمسان، سعيدة، سيدي بلعباس، مستغانم، معسكر، غليزان[5]

القطب الجزائي بورقلة ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية: ورقلة، ادرار، تمنراست، اليزي، غرداية[6]

---

[1] أنظر المواد 37، 40، 329 من قانون الإجراءات الجزائية الجزائري المرجع السابق.

[2] المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية.

[3] أنظر المادة 02 من المرسوم التنفيذي رقم 06 – 348 مؤرخ في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، الجريدة الرسمية، عدد 63 ، صادر في 08 أكتوبر 2006 .

[4] أنظر المادة 03 من المرسوم التنفيذي 06 – 348 مرجع نفسه.

[5] أنظر المادة 04 من المرسوم التنفيذي 06 -348 مرجع نفسه.

[6] أنظر المادة 05 من المرسوم التنفيذي 06 -348 مرجع نفسه.

ومما لا شك أن الاختصاص الإقليمي الموسع للقطب الجزائي المتخصص يشمل جميع مراحل الدعوى العمومية ابتداء من جمع الاستدلالات إلى غاية المحاكمة فالسلوك الإجرامي في نطاق الجرائم الإلكترونية قد يرتكب في مكان معين كجريمة الإتلاف عن طريق إدخال الفيروس، وتتحقق النتيجة بتدمير المعلومات في مكان آخر فالاختصاص ينعقد إما في مكان وقوع السلوك أو مكان تحقيق النتيجة، وتعد الجريمة الإلكترونية إذ تمت عن طريق الانترنت جريمة مستمرة، حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت فيها الجريمة

فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني، أو إذا ارتكبت من طرف شخص أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي[1].

ب- الاختصاص النوعي في الجريمة الإلكترونية

الاختصاص النوعي للمحاكمة يتحدد بالفصل في القضية المعروضة عليها حسب نوع الجريمة المرتكبة اذ تختص محكمة الجنايات بالفصل في الأفعال الموصوفة بجنايات وأفعال إرهابية أو تخريبية،

المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص أيضا المحاكم بالنظر في الجنح والمخالفات وذلك فيما عاد الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 من الإجراءات الجزائية[2].

[1] أنظر المادة 05 من القانون 09 – 04 االمرجع السابق.

[2] أنظر المادة 328 من قانون الإجراءات الجزائية.

ونظرا للطبيعة التقنية المعقدة للجرائم الإلكترونية تشترط على رجال القضاء تكوين في هذا المجال يمكنهم من متابعة هذه الجرائم إلى جانب جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب وتلك المتعلقة بالتشريع الخاص بالصرف، لذا جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى وهذا ما نصت عليه المواد 37 و40 والمادة 329 من قانون الإجراءات الجزائية الجزائري أثر التعديل الذي جاء به القانون رقم 04-14 الذي حددت أحكامه في المرسوم التنفيذي رقم 06 – 348 المتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة قسنطينة، وهران، ورقلة[1].

ثانيا: تشكيلة المحكمة

إن المحكمة الجزائية تختلف بحسب قسم ونوع كل جريمة، فعلى مستوى المحكمة قسم الجنح يتشكل من قاضي فرد يساعده كاتب الضبط و بحضور وكيل الجمهورية أو أحد مساعديه، بينما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فيها ثلاثية، فهي تتشكل من رئيس الغرفة ومستشارين اثنين بالإضافة إلى كاتب الضبط وبحضور النائب العام لوحده أو أحد مساعديه، أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفينوكاتب الضبط والنيابة العامة أو من يمثلها[2].

الفرع الثاني:

الإجراءات والقواعد العامة للمحاكمة

سنتطرق في هذا العنصر إلى إجراءات المحاكمة (أولا)، ثم القواعد العامة للمحاكمة (ثانيا).

[1] أنظر المواد 37، 40، 329 من القانون رقم 04 -14 المرجع السابق.

[2] أنظر المادة 30 و258 من قانون الإجراءات الجزائية الجزائري المرجع السابق.

أولا: إجراءات المحاكمة

تبدأ المحكمة جلستها بالإعلان أولا على افتتاحها بالقول "**باسم الشعب الجزائري الجلسة المفتوحة**" ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها.

وإذ لم تكن الدعوى مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة، ففي مثل هذه الحالة وطبقا لأحكام المادة 339 مكرر 6 المستحدثة بموجب الأمر رقم 15 -02 من قانون الإجراءات الجزائية الجزائري[1] تتخذ المحكمة إحدى الإجراءات التالية:

ترك المتهم حرا، إخضاع المتهم لتدبير أو أكثر من تدبير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 من قانون الإجراءات الجزائية، أو وضع المتهم في الحبس المؤقت، و لا يجوز الاستئناف في الأوامر التي تصدرها المحكمة وفقا لهذه المادة.

ففي حالة ما إذا سبق حبس المتهم من طرف قاضي التحقيق عن طريق الحبس المؤقت موجب إجراء المثول الفوري، فإنه يساق بواسطة القوة العمومية لحضور الجلسة في اليوم المحدد لها، و يخطره رئيس الجلسة بأن له الحق في اختيار محامي للدفاع عنه، فإن طلب ذلك أمهله القاضي مهلة لا تقل عن ثلاثة أيام لتحضير دفاعه طبقا للمادة 339 مكرر 5 من الأمر 15 -02 المعدل والمتمم قانون الإجراءات الجزائية[2].

[1] أنظر المادة 339 مكرر 6 المستحدثة بموجب الأمر رقم 15 -02 المعدل والمتمم لأمر 66- 155 المتضمن قانون الإجراءات الجزائية.

[2] أنظر المادة 339 مكرر 5 المستحدثة بموجب الأمر 15 -02 المعدل والمتمم الأمر 66- 155 المتضمن قانون الإجراءات الجزائية.

ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها من طرف القاضي وبعدها يقوم القاضي بسماع الشهود، وبعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية، لتقوم النيابة العامة بعد ذلك بالمرافعة والتقديم التماساتها في الشق الجزائي فقط، وفي الأخير يقوم الدفاع المتهم بتقديم مرافعته وتقديم التماساتها، ويكون بعدها للنيابة العامة والمدعي الحق في الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه، ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق المنطق بالحكم[1].

ثانيا: القواعد العامة للمحاكمة

تتقيد المحاكمة بمجموعة من المبادئ تنطبق على المحكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية، سنحاول شرح بداية بعلانية الجلسة (أ)، شفوية المرافعات (ب)، حضور أطراف الخصومة (ج)، ثم تدوين التحقيق النهائي (د).

أ- علانية الجلسة

معظم التشريعات تأخذ بمبدأ علانية الجلسة، وذلك أن العلنية تسمح للجمهور بالاطلاع على إجراءات المحاكمة بمراقبة عمل المحكمة، ومنه الاطمئنان والشعور بالعدالة وهذا عكس التحقيق الأولي الذي يقوم به ضباط الشرطة القضائية، وكذا التحقيق الابتدائي الذي تقوم بهجهات التحقيق، فكلاهما يتم في سرية، إلا أن العلانية ليست في جميع الجلسات، بل للقاضي السلطة التقديرية لإخراج القصر من الجلسة، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على النظام العام والآداب العامة، إلا أن الحكم

[1] أنظر المادة 304 من قانون الإجراءات الجزائية الجزائري.

يجب أن يصدر في جلسة علانية، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري[1].

ب-شفوية المرافعات

الحق لأطراف الخصومة في مناقشة كل دليل يعرض بالجلسة، حتى يتمكن الجميع من الدفاع عن نفسه، ولا يتم الاكتفاء بالتحقيقات الأولية والابتدائية التي سبقت المحاكمة فقانون الإجراءات الجزائية يقرر أن تكون المرافعات لجميع الوقائع علنا وشفاهية، فيقدم الخصوم طلباتهم فتناقش شفاهة وعلنا عملا بالأحكام الواردة في المواد 233، 287، 288، 289، 304، 353 من قانون الإجراءات الجزائية الجزائري، فتنص مثلا المادة 304 من قانون الإجراءات الجزائية الجزائري "**متى انتهي التحقيق بالجلسة سمعت أقوال المدعي المدني أو محاميه**"، "**وتبدي النيابة طلباتها** "" **و يعرض المحامي والمتهم أوجه الدفاع ويسمح المدعي المدني والنيابة العامة بالرد، ولكن الكلمة الأخيرة للمتهم ومحاميه دائما**"[2].

ج-حضور أطراف الخصومة

من المستحيل إجراء المحاكمة دون أطراف الخصومة؛ لذلك أوجب المشرع حضور كل من الضحية والمتهم، أما بالنسبة للنيابة فهي جزء من التشكيلة، ويقرر القانون لأطراف القضية حق الحضور، تمكينا له من إبداء أوجه دفاعهم إمام الجهة القضائية المختصة، حيث نصت عليه مجموعة من المواد في قانون الإجراءات الجزائية[3].

[1] أنظر المادة 285 من قانون الإجراءات الجزائية الجزائري المرجع السابق.

[2] أنظر المواد 233، 287، 288، 314، 333، 353 من قانون الإجراءات الجزائية الجزائري المرجع السابق.

[3] لمزيد من التفاصيل ينظر المواد 287، 2889، 290، 294، 296، 343، 344، 345، 345، 347، 348، 349، 31، 33، 355، 407، من قانون الإجراءات الجزائية الجزائري مرجع نفسه.

د-تدوين التحقيق النهائي

لا يجوز للمحكمة أن تنعقد في غياب أمين الضبط لأن دوره يستجد في تدوين كل ما يدور بالجلسة، حيث يقوم كاتب الضبط بالهيئة الجزائية أو أمين الضبط وجوبا بتحضير محضر الجلسة، يدون فيه جميع الإجراءات التي تتم فيها، ويوقع عليه طبقا لأحكام المواد 257، 314، 340، 380، 429 من قانون الإجراءات الجزائية الجزائري، لتتاح للقاضي الجزائي أو هيئة القضاء الجزائي التفرغ كليا لإدارة الجلسة وجمع المعلومات والسماع للمرافعات التي من شأنها أن تتيح له أو لهم تكوين اقتناعهم وإصدار الأحكام على ضوء ما اقتنعوا به[1].

وكخلاصة القول نستنتج أن الجريمة الإلكترونية رغم أنها جريمة مستحدثة ولكن لم يخصص لها إجراءات محاكمة خاصة بها وإنما تخضع لنفس إجراءات الجريمة التقليدية.

خلاصة الفصل الثاني

وأخيرا وبعدما تطرقنا في هذا الفصل إلى الأحكام الإجرائية للجريمة الإلكترونية، حيث بينا الإجراءات العامة التي تخضع لها الجريمة الإلكترونية والتي تشترك فيها مع الجريمة التقليدية في مرحلة جمع الاستدلالات، ومنها إجراءات مادية تقتصر فقط على المعاينة التقنية والتفتيش المعلوماتي الذي يخضع تارة إلى أحكام قانون الإجراءات الجزائية، وتارة أخرى إلى أحكام القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وأخرى شخصية تتمثل في الخبرة، وشهادة شاهد الكتروني، والتسرب وهو من أساليب التحري الخاصة، التي جاء بها تعديل قانون الإجراءات الجزائية، والذي لا يقرر إلا على الجرائم الخطيرة ذات الإجراءات الخاصة التي تطبق على الجرائم الموصوفة بالخطيرة، كالجرائم الإلكترونية، تتمثل في مراقبة الاتصالات الإلكترونية

[1] لمزيد من التفاصيل أنظر المواد 314 340 380 429 من قانون الإجراءات الجزائية الجزائري مرجع نفسه.

وحفظ المعطيات المتعلقة بحركة السير والتي جاء بها القانون رقم 09-04 المتعلق القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذا أثناء مرحلة البحث والتحري في الجريمة الإلكترونية.

أما في مرحلة التحقيق الابتدائي أو القضائي فقد عرفت الجريمة الإلكترونية في هذا المجال خصوصية خاصة من حيث اختصاصات قاضي التحقيق سواء كان الاختصاص المحلي (باعتبارها جريمة عابرة للحدود الدولية)أو الاختصاص النوعي، ونظرا للخصوصيات التي تتميز بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتطورها السريع والمستمر، جعل من الدول ومنها الجزائر إلى وضع آلية قانونية جديدة للحد من خطورة هذه الجريمة على المجتمع ككل من خلال تمديد الاختصاص المحلي لبعض المحاكم لقضاء التحقيق، ووكيل الجمهورية من خلال آلية قضائية جديدة تعرف بالقطب الجزائري المتخصص، ومن خلال عرض وجيز لاختصاص هذه الأقطاب الجزائية طبقا لنص، المادة 37 من قانون الإجراءات الجزائية الجزائري وكذا توسيع اختصاصها المحلي ليشمل بعض المجالس القضائية، حددها في أربعة أقطاب طبقا للمرسوم التنفيذ رقم 06 – 348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، بالإضافة إلى إظهار تشكيلة المحكمة وعرض الإجراءات والقواعد العامة للمحاكمة.

خاتمة

الجريمة الإلكترونية هي وليدة الثروة المعلوماتية والتكنولوجية، حيث لم تسلم منها كل دول العالم المتطورة كانت أو النامية على حد سواء، مما جعل الجريمة الإلكترونية متميزة عن الجريمة التقليدية من حيث تسميتها وتعريفها وخصائصها. وكذا الأركان التي تقوم عليها وصولا إلى الإجراءات المتابعة فيها.

ومن خلال هذه الدراسة تم الإلمام بالجوانب القانونية للجريمة الإلكترونية في شقها الموضوعي والإجرائي حيث ميزت بينها وبين الجريمة التقليدية مستندة في ذلك على تعديل قانون العقوبات بموجب القانون رقم04- 15 المتعلق بالقواعد المطبقة على التوقيع والتصديق الإلكتروني والقانون رقم09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى قانون الإجراءات الجزائية.

ومما لا شك أن لهذه القوانين أهمية كبيرة فيتدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري، كما أن هذا التعديل يعد قفزة في مجال التشريع، كونه واكب التشريعات المقارنة بتجسيده لمعظم أحكام الاتفاقية الدولية للإجرام المعلوماتي.

ومما سبق ذكره، ارتأينا أن نضع مجموعة من النتائج يمكن إجمالها فيها يلي:

عدم وجود تعريف جامع مانع للجريمة الإلكترونية، فهي لا تزال محل خلاف فقهي وقضائي وهذه الجرائم يمكن أن تمس الشخص الطبيعي كما يمكن أن تمس الشخص المعنوي فهي تشكل خطر على أمن الدولة نظرا لطبيعتها المتعدية للحدود وارتباطها بشبكة الانترنت.

عدم وجود مصطلح موحد للجريمة الإلكترونية، فهناك من يسميها الجريمة المعلوماتية أو السيبرانية أو جريمة الياقات البيضاء أو جريمة الانترنت إلى.... الخ، حتى المشرع الجزائري لم يستقر على تسمية

واحدة، حيث سماها طبقا للقانون رقم 04-15 المتعلق بالقواعد المطبقة على التوقيع والتصديق الإلكتروني بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال طبقا للقانون رقم09 -04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ورغم هذه الاختلافات إلا أنها تصب كلها في معنى واحد.

إن ما يميز الجريمة الإلكترونية عن الجريمة التقليدية هو وسيلة ارتكابها، وكذلك محل الجريمة حيث تقع على نظام المعالجة الآلية بمكوناته الغير المادية.

الجرائم الإلكترونية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق، ويتصف المجرم المعلومات فيها بالذكاء والسرعة والدقة والتخصص في مجال تكنولوجيا المعلومات واعتماده على التقنيات الحديثة في ارتكاب هذا النوع من الجرائم.

من أهم مميزات الجريمة الإلكترونية أنها صعبة الاكتشاف والإثبات فهي تقع على أشياء غير ملموسة عكس الجرائم التقليدية، إذ يمكن للجاني إخفاء آثاره عن طريق البرامج المختلفة.

رغم كل الاختلافات بينها وبين الجريمة التقليدية إلا أنها تتوافق معها في مدى توفر القصد الجنائي العام.

رغم اجتهاد وتدارك المشرع الجزائري للفراغ القانوني في مجال الإجرام الإلكتروني إلا انه لم يستطيع التصدي لهذه الجريمة، بالتالي عجز القواعد الإجراءات الجزائية والنصوص العقابية التقليدية وقصورها عن مواجهة الجرائم الإلكترونية والمجرم الإلكتروني.

إن عملية البحث والتحقيق في الجرائم الإلكترونية تعتريها صعوبات كثيرة، نظرا للطبيعة الخاصة التي تتميز بها، فالطابع العابر للحدود الذي تتسم به قد يثير العديد من المشاكل القانونية ومشكلات الاختصاص القضائي والقانون الواجب التطبيق.

وعلى ضوء هذه النتائج التي أظهرتها الدراسة قد توصلت إلى التوصيات والاقتراحات التالية:

ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل كل السلوكيات المجرمة ويكون متفقا عليه على المستوى العالمي ويتلاءم مع تطور التكنولوجي.

ضرورة تقنين قواعد جديدة لمكافحة الجرائم الإلكترونية كما ينبغي تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع هذه الجرائم المستحدثة.

ضرورة تخصيص شرطة جنائية خاصة لمكافحة جرائم الانترنت، مع تكوين لجان خبراء لهذا الشأن.

تعزيز وتنسيق التعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم الإلكترونية.

يتعين تدريب وتأهيل وتحديث أفراد الضبطية القضائية وكذلك النيابة العامة والقضاء على كيفية التعامل مع هذا النوع من الجرائم.

ضرورة وضع إجراءات خاصة للتحقيق والمحاكمة في الجريمة الإلكترونية تختلف عن الجريمة التقليدية.

ضرورة توعية المجتمع بمخاطر التعامل مع المواقع السيئة على شبكة الانترنت وخلق ثقافة اجتماعية جديدة على هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبه العقوبات جزائية.

الأخذ بالتجارب السابقة بالنسبة للدول المتطورة التي ساهمت في محاربة الجريمة الإلكترونية كالولايات المتحدة الأمريكية وكندا.

إعادة النظر في مدى تطبيق القوانين من عدمه.

تأسيس مقاربة شمولية تستوعب الصور الجديدة للعلاقات الإنسانية، وتكفل حماية حقوق ومصالح الأفراد والمؤسسات، تحقيق الأمن الالكتروني.

قائمة المحتويات

الموضوع **الصفحة**

مقدمة..... **1**

الفصل الأول

خصوصية الأحكام الموضوعية الخاصة لمواجهة الجريمة الإلكترونية..... **6**

المبحث الأول: الطبيعة القانونية الخاصة لمواجهة للجريمة الإلكترونية 7

المطلب الأول: مفهوم الجريمة الإلكترونية 8

الفرع الأول: المقصود بالجريمة الإلكترونية وخصائصها.....9

أولا: تعريف الجريمة الإلكترونية.....9

أ- التعريف الفقهي للجريمة الالكترونية 9

1- تعريف الجريمة الالكترونية على أساس وسيلة ارتكابها 10

2- تعريف الجريمة الالكترونية على أساس موضوعها 11

3- تعريف الجريمة الالكترونية على أساس المعرفة التقنية.....11

ب-التعريف التشريعي للجريمة الالكترونية.....12

ثانيا: خصائص الجريمة الإلكترونية.....13

الفرع الثاني: عناصر الجريمة الإلكترونية 15

أولا: أطراف الجريمة الإلكترونية.....15

أ- المجني عليه في الجريمة الالكترونية (الضحية) 16

ب- الجاني في الجريمة الالكترونية (المجرم المعلوماتي).....17

1- مجرمين مستعملين الانترنت 18

2- مجرمين مبرمجين 19

ثانيا: الأجهزة الالكترونية المستعملة في الجريمة الإلكترونية 20

أ- الوسائل الالكترونية 21

ب- شبكة المعلومات المحلية والعالمية 21

المطلب الثاني: الوصف القانوني للجريمة الإلكترونية وأركانها 23

الفرع الأول: الوصف القانوني للجريمة الإلكترونية 23

الفرع الثاني: أركان الجريمة الإلكترونية 25

أولا: الركن الشرعي 26

ثانيا: الركن المادي ..... 26.

أ – السلوك الإجرامي (الفعل) 27

ب – النتيجة الإجرامية 27

ج – العلاقة السببية 28

ثالثا: الركن المعنوي 28

1- القصد الجنائي العام 29

2- القصد الجنائي الخاص 30

المبحث الثاني: القواعد الموضوعية الخاصة لمحاربة الجريمة الإلكترونية 31

المطلب الأول: الأحكام الخاصة لمحاربة الجريمة الالكترونية في القانون الجزائري 31

الفرع الأول: محاربة الجريمة الالكترونية في ظل قانون العقوبات 32

الفرع الثاني: محاربة الجريمة الالكترونية في ظل القوانين الخاصة وأحكام الاتفاقيات الدولية ...32

أولا: في ظل القوانين الخاصة 33

أ _ قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها 33

ب-قانون رقم 18-05المتعلق بالتجارة الالكترونية 33

ج – قانون رقم 18 –07 المتعلق بحماية الأشخاص الطبيعيين.....34

ثانيا: في ظل أحكام المعاهدات والاتفاقيات الدولية 34

أ _ المعاهدات الدولية والإقليمية.....34

ب – معاهدات تسليم المجرمين 36

المطلب الثاني: الجزاءات المترتبة عن ارتكاب الجريمة الالكترونية والهيئات المكلفة بالوقاية منها ومحاربتها 37

الفرع الأول: الجزاءات المقررة للجريمة الالكترونية 37

أ –عقوبات المجرم الالكتروني كشخص طبيعي 37

ب –عقوبات المجرم الالكتروني كشخص معنوي 40

الفرع الثاني: الهيئات المكلفة بالوقاية من الجريمة الالكترونية ومحاربتها 42

أولا: الهيئات الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال.....42

ثانيا: الهيئات القضائية الجزائية المتخصصة.....42

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام 43

الفصل الثاني: الأحكام الإجرائية الخاصة لمواجهة الجريمة الإلكترونية.....45

المبحث الأول: كشف الجريمة الإلكترونية 47

المطلب الأول: كشف الجريمة الإلكترونية وفقا للأحكام التقليدية 48

الفرع الأول: التحري 48

الفرع الثاني: تلقي البلاغات والشكاوى.....49

الفرع الثالث: الإقرار بالجريمة.....50

الفرع الرابع: الشهادة في الجريدة الالكترونية 51

المطلب الثاني: كشف الجريمة الإلكترونية وفقا للأحكام المستحدثة.....51

الفرع الأول: أسلوب اعتراض المراسلات والتسجيل الأصوات والتقاط الصور 52

الفرع الثاني: التسرب 52

الفرع الثالث: المراقبة الإلكترونية 53

الفرع الرابع: إقحام مزودي خدمات الاتصال الإلكترونية في مسار الوقاية من الجرائم الإلكترونية..

.....54

المبحث الثاني: التحقيق والمحاكمة 54

المطلب الأول: التحقيق في الجريمة الإلكترونية 55

الفرع الأول: آليات البحث والتحري في الجرائم الإلكترونية.....55

أولا: الأجهزة المختصة في البحث والتحري.....56

أ- الأجهزة المختصة بالبحث والتحري عن الجريمة الالكترونية على المستوي الوطني....

.....57

ب- الأجهزة المختصة بالبحث والتحري عن الجريمة الالكترونية على المستوي الدولي...

.....58

1- على الصعيد الدولي 59

2- على الصعيد الإقليمي 60

أولا: الشرطة الأوروبية أو الأوروبول 60

ثانيا: موقف المشرع الجزائري 60

الفرع الثاني: إجراءات تحقيق في الجرائم الإلكترونية 61

أولا: المعاينة 62

ثانيا: التفتيش 64

ثالثا: ضبط الأدلة في الجريمة الإلكترونية 65

رابعا: الخبرة التقنية 67

المطلب الثاني: إجراءات المحاكمة في الجريمة الإلكترونية 68

الفرع الأول: اختصاص المحكمة وتشكيلها 68

أولا: اختصاص المحكمة 69

أ - الاختصاص الإقليمي أو المحلي في الجريمة الإلكترونية 69

ب- الاختصاص النوعي في الجريمة الإلكترونية 71

ثانيا: تشكيلة المحكمة 72

الفرع الثاني: الإجراءات والقواعد العامة للمحاكمة 72

أولا: إجراءات المحاكمة 72

ثانيا: القواعد العامة للمحاكمة 74

أ - علانية الجلسة 74

ب - شفوية المرافعات 74

ج- حضور أطراف الخصومة.....75

د- تدوين التحقيق النهائي.....75

الخاتمة 77

قائمة المصادر والمراجع باللغة العربية

أولا: الكتب

1- **الخان محمد طارق عبد الرؤوف**، التعليم الالكتروني والتعليم الافتراضي، المجموعة العربية للتجريب والنشر، مصر، 2014.

2- **أسامة أحمد بلال محمد**، جرائم تقنية نظم المعلومات الالكترونية، الطبعة 3، عمان،2014

3-**أشرف توفيق شمس الدين**، شرح قانون العقوبات، القسم العام النظرية العامة للجريمة والعقوبة، الطبعة الخاصة لطلاب التعليم المفتوح بكلية الحقوق بجامعة بنها، 2009.

4-**السلامة محمد عبد الله**، موسوعة الجرائم المعلوماتية جرائم الكمبيوتر والانترنت، المكتب حي العربي الحديث الإسكندرية، مصر، 2007.

5-**الشلقاني أحمد شوقي**، مبادئ إلى إجراءات في التشريع الجزائري،

6-**الملط احمد خليفة**، الجرائم المعلوماتية، ط2 دار الفكر، الإسكندرية، 2006.

7-**المناعسة أسامة احمد** وآخرون، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل، عمان، 2001.

8- **بالطي غنية**، الجريمة الالكترونية، الدار الجزائرية، الجزائر، 2015.

9- **بالعاليات إبراهيم**، أركان الجريمة الالكترونية وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، الدار برتي، الجزائر، 2007

10- **حسن بوسقيعة**، الوجيز في القانون الجزائي العام، ط10، دار هومة، الجزائر ،2011.

12- **خليفة محمد**، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر،2007.

13- **سامي جلال فقي حسين**، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، 2011.

14- **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي، دار الجامعة الجديدة، مصر،2009.

15- **طوني ميشال عيسى**، التنظيم القانوني لشبكة الانترنت، دار صادر للمنشورات الحقوقية، لبنان. 2001 .

16- **عباد الفتاح بيومي حجازي**، التزوير الكمبيوتر والانترنت، دراسة مقارنة، منشأة المعارف، مصر،2010.

17- **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والانترنت الجرائم الالكترونية، دراسة مقارنة، في النظام المعلوماتية والانترنت منع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية لبنان،2007.

18- **عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، 2006.

19- **عبد الله سليمان**، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية، الجزائر1995.

20- **عبد الصبور عبد القوي على**، مصري التجارة الالكترونية والقانون، الطبعة الأولى، دار العلوم التكبير والتوزيع، مصر، 2010.

21- **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجزائية في الجرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.

22- **عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، مصر، 2004.

23- **عفيفي كامل**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية،بيروت،2013.

24- **فضل سليمان احمد**، المواجهة التشريعية والأمنية للجرائم الناشئة، المعلومات الدولية الأنترنت، دار النهضة العربية القاهرة، 2013.

25- **هروال هية نبيلة،** الجوانب الإجرائية لجرائم الأنترنت، الطبعة الثانية، دار الفكر الجامع، مصر،2011.
26- **محمد سامي الشوا،** ثوره المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية مصر،1994.
27- **محمد سليم العواء،** في أصول النظام الجنائي الإسلامي، دار المعارف2006 .
28- **محمود نجيب حسن،** شرح قانون العقوبات_ القسم الخاص، دار النهضة العربية، مصر، 1992.
29- **مدحت عبد الحليم رمضان،** الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة، القاهرة،2001.
30- **محمود محمد لطفي صالح،** المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية، دراسة مقارنة، دار الكتب القانونية، البرمجيات، مصر، 2014.
31- **محمود احمد عبابنة،** جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2015 .
32- **هدى حامد قشقوش،** جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.
33- **هدى حامد قشقوش،** الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، مصر،2000.
34- **ياسر محمد الكومي محمود ابو حطب،** الحماية الجنائية والملية للتوقيع الالكتروني، منشأة المعارف، مصر،2014.
35- **يوسف أبو الحجاج،** أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، سوريا،2010.

ثانيا: الرسائل والمذكرات الجامعية

أ: رسائل الدكتوراه

1- **إياد احمد البطانية**، النظام القانوني لعقود برامج الحاسوب دراسة مقارنة، أطروحة الدكتوره، كلية القانون في جامعه بغداد، 2002 .

2- **هروال هيبة نبيلة**، جرائم الانترنت دراسة مقارنه، أطروحة لنيل شهادة الدكتوره، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2014 .

ب: المذكرات الجامعية

1) مذكرات الماجستير

1 **محمد ابن نصير محمد السرحاني**، مهارات التحقيق الفني في جرائم الحاسوب والانترنت، رسالة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية. كلية الدراسات العليا ،الرياض، 2004

2 **أحمد مسعود مريم**، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة الماجستير في القانون الجنائي، كليه الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة ، 2013 .

3 **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية،2013.

4 **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة الماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.

5 **يونس خالد عرب**، جرائم الحاسوب، رسالة ماجستير مقدمة إلى كلية الحقوق، الجامعة الاردنية، عمان، 1994.

2)مذكرات الماستر:

1 **بوبقرة خيرة،** آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس، مستغانم2020.

2 **بوعمرة محمد بنينال سيدي علي،** جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الأعمال كلية الحقوق والعلوم السياسية. قسم القانون الخاص، جامعه اكلي مجلد أولحاج البويرة، 2020 .

3 **بوشعرة أمينة، موساوي سهام،** الإطار القانوني للجريمة الالكترونية دراسة مقارنة، مذكرة الماستر في الحقوق، تخصص قانون خاص وعلوم جنائية، كليه الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية ، 2018 .

4 **مرابط حياة،** الجريمة الالكترونية في التشريع الجزائري، مذكرة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية جامعة عبد الحميد ابن باديس ،مستغانم، 2019 .

ثالثا: المقالات والمداخلات

أ: المقالات

بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية جامعة زيان عاشور، المجلد الثاني، العدد 23, 2015، ص 76 – 98.

2- **سعد الحاج بكري،** شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الامنية والتدريب،العدد11، 1990، ص 244-248.

3- **عبد الرحمن الشنيقي،** المواجهة الأمنية الجرائم الحاسبات الآلية، مجلة الأمن والحياة، العدد 129، 1993، ص 244 -248.

4- **فايز الظفيري،** الأحكام العامة للجريمة الالكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين الشمس، 2002 ص 131 – 149.

5- **قجاج يوسف،** الإطار الإجرائي الدولي في مجال البحث عن الجريمة الالكترونية، مجلة الفقه القانون / عدد196/28، 2015 ، ص 182 -186.

6 **محمد قدري وحسن عبد الرحمان**، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي صادر عن مركز بحوث الشرطة القيادة التامة لشرطة الشارقة الإمارات العربية المتحدة، المجلد عشرين، العدد 4، 2011، ص. 55-147.

ب- المداخلات

1 **اقلولي ولد رابح صافية**، الطبيعة القانونية للجريمة المعلوماتية، مداخلة في ملتقى الدولي حول الجريمة المعلوماتية، جامعة بسكرة، الجزائر يومي 16 و 17نوفمبرص ص1689 -1708

2 **توفيق شمبور** وآخرون، السرية المصرفية، أسعات ومناقشات الندوة التي نظمها. المصارف العربية، لبنان, 1993 ص 8 – 358.

3 **هشام محمد فريد رستم**، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح آلية عربية موحدة للتدرب التخصصي، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، من 1 إلى 3 ماي 2000، ص 588 – 607

رابعا- النصوص القانونية

أ المعاهدات

العهد الدولي المتعلق الخاص بالحقوق المدنية والسياسية المصادق عليها من طرف الجمعية العامة للأمم المتحدة المؤرخ في 16 ديسمبر 1966، دخل حيز التنفيذ في 23 مارس 1976، التي وقعت عليها الجزائر في 10 ديسمبر 1968 و صادقت عليها في 12 سبتمبر 1989.

ب النصوص التشريعية

1 قانون رقم 04- 14مؤرخ في 10 نوفمبر 2004المعدل و المتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، عدد 71 صادر في 10 نوفمبر 2004.

2 قانون رقم 04-09مؤرخ في 5 أوت يتضمن القواعد الخاصة الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها ، الجريدة الرسمية ، عدد 47 صادرفي16اوت 2009 .

3 قانون رقم 15-04 مؤرخ في 1 فبراير2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين، الجريدة الرسمية، عدد 6 صادر في 10 فبراير2015.

4 قانون رقم 18- 05مؤرخ في 10 مايو 2018، يتعلق بالتجارة الالكترونية، الجريدة الرسمية، عدد 28 صادر في 1 مايو 2018.

5 قانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 46 صادر في 29 يونيو 2018.

6 قانون رقم 19-10 مؤرخ في 11ديسمبر 2019، يعدل الأمر رقم 66-155، المؤرخ في 08 يونيو 1966، والمتضمن قانون الإجراءات الجزائية الجزائري، الجريدة الرسمية، عدد 78، المؤرخ في ديسمبر 2019.

7أمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية المعدل و المتمم بموجب الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 .

8 أمر رقم: 20-01 ، يعدل ويتمم الأمر رقم 66- 156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات الجزائري، الجريدة الرسمية ،العدد 44، الصادرة في 20 يونيو 2020

9 أمر رقم 21 - 11 المؤرخ في 25 أغسطس 2021، يتمم الأمر رقم 66 - 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 65 الصادرة في 26 غشت سنة 2021.

ج- النصوص التنظيمية

1 مرسوم تنفيذي رقم 98-257 مؤرخ في 25 أوت 1998 الذي يضبط شروط و كيفيان إقامة خدمات "**انترنت** " و استغلالها، الجريدة الرسمية، 63 صادر في 26 أوت 1998

2 مرسوم رئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015. يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية عدد 53 المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية عدد 53 صادر في 08 أكتوبر سنة 2015 .

3 مرسوم رئاسي رقم 19 / 172 مؤرخ في يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و كيفيات سيرها، الجريدة الرسمية، عدد 37 صادر في 9 يونيو سنة 2019 .

د- الوثائق

بعد انتهاء الحرب العالمية الثانية عقد في بروكسل (بلجيكا) مؤتمر دولي في الفترة من 9 سبتمبر 1946 انتهى إلى إحياء اللجنة الدولية للشرطة (ICPO)ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول ووضع ميثاق هذه المنظمة في الفترة 7 واعتبر نافذا اعتبارا من 13جوان 1956.

قائمة المصادر والمراجع باللغة الاجنبية

01 David Johnson, Electronic privacy, stoddar. canada, 1997.

02 Myriam QUEMENER. Cybercriminalité-droit pénal, appliqué. economica, septembre 2010.

ملخص خصوصية الجريمة الالكترونية في القانون الجزائري

أدى التطور التكنولوجي المذهل في مجال صناعة الحوسبة والاتصال, إلى بروز عالم تقنية المعلومات, وهي تمس كافة أوجه النشاط الإنساني, لكن بالمقابل نتج عن إساءة استخدامها جرائم مستحدثة تسمى" بالجرائم الالكترونية" تختلف في مفهومها ووسائلها وأساليب ارتكابها على الجرائم التقليدية, فهي جرائم تتم في بيئة رقمية عابرة للحدود و يصعب على المحققين اكتشافها و إثباتها حيث تتسبب في أضرار نفسية و اجتماعية و اقتصادية بالغة, و بالتالي كان لزما على المشرع عند وضعه لسياسته الجنائية بشقيها الموضوعي و الإجرائي الإحاطة الشاملة بماهية هذه الجرائم المستحدثة و بكافة أشكالها الفعالية في مكافحتها و ضمان لعدم إفلات المجرم الالكتروني من العقاب.

هذا ما دفع المشرع الجزائري في كل مرة بالتصدي لهذه الجرائم وذلك ضمن وضع آليات جديدة تعمل على الحد منها والكشف عنها وهذا باستحداث وتعديل قانون العقوبات ووضع سياسة جنائية فعالة ومتكاملة لمكافحة الجرائم الالكترونية.

Résumé

Le développement technologique impressionnant dans le domaine de l'informatique et de l'industrie de la communication a conduit à l'émergence du monde des technologies de l'information, qui affecte tous les aspects de l'activité humaine. Cependant, en contrepartie, l’utilisation abusive de cette technologie a entraîné de nouveaux crimes appelés « cybercriminalité » qui différent dans leur concept, leurs moyens et leurs méthodes des crimes traditionnels. Cesont des crimes commis dans un environnement numérique transfrontalier difficiles à détecter et à prouver pour les enquêteurs causant ainsi des dommages psychologiques, sociaux et économiques considérables. Il était nécessaire donc pour le législateur, lors de l'élaboration de sa politique pénale de fond et de procédure de bien comprendre la nature de ces nouvelles formes de criminalité et de prendre des mesures efficaces pour les combattre afin de garantir que les cybercriminels ne restent pas impunis.

C'est ce qui a poussé le législateur algérien à lutter continuellement contreces crimes en mettant en place de nouveaux et de mettre en place une politique criminelle efficace et intégrée pour lutter contre la cybercriminalité.