الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية **ميدان: الحقوق**

قسم الحقوق ***تخصص: قانون جنائي***

مذكرة مكملة لنيل شهادة الماستر أكاديمي

تحت عنوان

الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري

إعداد الطالبة:
نايت الصغير حليمة

إشراف الأستاذ:
د. داود كمال

لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
برابح السعيد	أستاذ محاضر –أ -	رئيسا
داود كمال	استاذ محاضر –أ-	مشرفا و مقررا
مهدي رضا	أستاذ محاضر –أ-	ممتحنا

السنة الجامعية: 2021- 2022

استمارة معلومات

المعلومات الشخصية:

الاسم: حليمة — اللقب: سايت الصغير

اسم الأب: كمال الدين — اسم ولقب الأم: دبابي يمينة

تاريخ الازدياد: 13 ماي 1999 — مكان الازدياد: برج بوعريريج

رقم الهاتف: 0658683605

البريد الالكتروني: halimahalouma13599@gmail.com

العنوان الشخصي: حوزة 365 مسكن شارع "أ" رقم 1 باب 7 - القرية الشمالية - برج بوعريريج.

الباكالوريا:

المعدل: 10,00 — الشعبة/التخصص: علوم تجريبية — سنة الحصول على شهادة الباكالوريا: 2017

الليسانس:

تخصص الليسانس: قانون عام — الدفعة/ سنة التخرج: 2020 - 2019

الماستر:

تخصص الماستر: قانون إداري — الدفعة/ سنة التخرج: 2022 - 2021

معدل الترتيبي للماستر: (المعدل العام)

الوضعية المهنية:

موظف: ☐ — عاطل عن العمل: ☒ X

في حالة موظف:

وظيف عمومي — قطاع خاص:

المصلحة المستخدمة — اسم المؤسسة / الشركة:

الرتبة في العمل:

الصيغة:

موظف رسم — موظف في إطار عقود: — نوع العقد:

امضاء الطالب

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد بوضياف بالمسيلة

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية الحقوق والعلوم السياسية

قسم : الحقوق

المرجع: القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز البحث

أنا الممضي أدناه،

السيد(ة) ثابت المغير حليمة

الصفة: طالب، أستاذ باحث، باحث دائم طالبة

الحامل لبطاقة التعريف الوطنية رقم: 401015816

الصادرة بتاريخ 2022-03-16 عن دائرة/ بلدية برج بوعريريج

المسجل(ة) بكلية الحقوق والعلوم السياسية قسم : الحقوق

والمكلف بانجاز أعمال بحث (مذكرة ماستر، مذكرة ماجيستير، أطروحة دكتوراه) الموسومة بـ :

مذكرة ماستر :

الجريمة الإلكترونية وعاجز اليات مواجهتها في التشريع الجزائري.

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ 2022/06/20

إمضاء المعني

401015816
2022-03-16

من رئيس المجلس الشعبي البلدي
و بتفويض منه
عون رئيس مصلحة الحالة المدنية
بلواهري فتيحة

شكر وعرفان

نتوجه بادئ ببدء الشكر العميق لله العليم الخبير الذي أمدنا بعظيم نعمته

ووفقنا إلى إنهاء هذا العمل المتواضع وكلنا أمل أن نكون قد وفقنا إلى حد ما في

توصيل الأفكار والمعلومة في هاته الدراسة

وكما روى الإمام الترميذي عن أبي هريرة رضي الله عنه قال : قال رسول الله صلى

الله عليه وسلم :" من لا يشكر الناس لا يشكر الله "

وعليه أتقدم بالشكر والعرفان لأمي الغالية التي كانت السند الحقيقي في كل وقت وحين ،

ولكل الاساتذة الذين كان لهم الفضل الكبير في وصولنا لهذه المرحلة ، وبالخصوص

الأستاذ المشرف الدكتور داود كمال الذي لم يبخل علينا في مد يد العون

لإنجاز هذا العمل المتواضع .

مقدمة

مقدمة:

الجريمة ظاهرة ليست بحديثة فقد شغلت العديد من الدول التي تحاول وضع سياسة جنائية ناجعة تمكنها من مواجهتها والحد منها تحقيقا للأمن والاستقرار داخل المجتمع وتطبيقا للعدالة في ظل الموازنة بين حقوق الأفراد وواجباتهم. ومما لا شك فيه أن اختلاف المجتمعات من حيث درجة التطور في شتى المجالات يؤثر على الجريمة كظاهرة مرنة مرتبطة بالبيئة السياسية الاجتماعية والثقافية والعقائدية لكل مجتمع.

و قد مست الثورة التكنولوجية أغلب الدول على جميع الأصعدة، وساهمت بشكل كبير في تسهيل حياة الأفراد واختصارهم الوقت والجهد وقضت على المسافات وأثرت بشكل إيجابي كبير على مردودية المجتمعات في جميع المجالات، ومن جهة أخرى ظهرت انعكاساتها السلبية لسوء استخدامها واستعمالها بصورة وكيفية تضر بمصالح الأفراد وحقوقهم وأمنهم وبالدولة ككل، بل تعدى ذلك المستوى الداخلي ليمس الأمن الدولي ومصالح المتجمع الدولي بمختلف مكوناته، وهذا التطور العلمي جعل الدول وأجهزتها تواجه جرائم مستحدثة من حيث الارتكاب والتنفيذ وحتى الأثر ، اصطلح على تسميتها بالجرائم الإلكترونية، وتبعا لذلك استغل المجرمون القصور التشريعي وطوروا من أنفسهم وأساليب ارتكابهم لهذه الجرائم بكيفيات يستغلون فيها مميزات وخاصية هذه الجرائم من جهة وكذا نقص خبرة الدول في التصدي لهذه الأخيرة على المستويين التشريعي والتطبيقي الميداني. فمن الصعب التحكم في معطيات تحدث في عالم افتراضي وتتعلق بأفعال مرتكبة بتقنية عالية ومعقدة، إضافة لمعوقات عملية تحول دون تتبع آثار الجريمة والكشف عنها والوصول لأدلة مادية ملموسة ومن ثم إثباتها، عكس الجرائم التقليدية.

- أسباب اختيار الموضوع:

-أسباب ذاتية:

تتعلق هذه الأسباب بالرغبة الشخصية في دراسة هذا الموضوع والوقوف على أهم عناصره وأدق تفاصيله المهمة للتعرف عليه على نحو علمي قانوني يثري رصيدنا الفكري، إضافة لميولنا لكل ما هو مستحدث فيما تعلق بالإجرام، ونحن في الواقع جزء منه هذه التقنية ومعرضون في كل وقت لنكون طرفا فيه كضحايا هذا أو جناة مع انتفاء قصدنا.

- الأسباب الموضوعية:

- الجرائم الإلكترونية موضوع ذو قيمة علمية تستحق المتابعة والدراسة وكونها أخذت حيزا كبيرا على مستوى الحياة الخاصة والعامة. إضافة للخطورة البالغة لهذه الجرائم على المستوى الوطني والدولي لدرجة انهيار دولة كاملة بجميع مؤسساتها بسبب جريمة إلكترونية مست الجانب الأمني أو العسكري أو الاقتصادي للدولة. وهذا الموضوع يزامن تطور التفكير الإجرامي الذي يعتبر الخطوة الأولى في محاربته أن يتم فهمه وتأطيره ليسهل التحكم فيه.

- وقد عالجه المشرع الجزائري بتعديله لمختلف قوانينه محاولا التكيف مع التطور الحاصل وليوفر الحماية حماية شاملة لمعطيات المعالجة الآلية، فتنوعت أوجه الحماية لهذه المعطيات دوليا من خلال إبرام الاتفاقيات الدولية المنظمة لهذا الموضوع وداخليا من خلال العمل على ضرورة توفير حماية جنائية فعالة بسن نصوص تشريعية عقابية.

- أهمية الموضوع:

- تظهر أهمية الموضوع من خلال ما يقدمه من أفكار ومعلومات عن الجريمة الإلكترونية من حيث بيان تعريفها ومجالات استخدامها وأهم مميزاتها التي تمكن متناوله من تمييزها بسهولة عن غيرها من الجرائم وتتشكل لديه فكرة مختصرة وفي نفس الوقت ملمة بأهم ما يجب معرفته عنها كجرائم حديثة منتشرة وخطيرة في مجتمعنا.

– كما أن موضوعنا يركّز بشكل كبير على الإجراءات التي اعتمدها المشرع الجزائري في مكافحة هذه الجرائم فالعبرة بالجانب العملي التطبيقي الميداني وهو أهم ما يجب التركيز عليه والوقوف على تفاصيله، إذ لا فائدة من نصوص تشريعية تجرم وتعاقب دون إمكانية تطبيقها في الواقع وتحقيق الهدف عموما، وموضوعنا يقف على مختلف الضوابط العملية لمكافحة هذه الجرائم في جميع المراحل مع بيان مدى فعاليتها وتقييمها حسب انعكاس آثار تطبيقها ميدانيا.

– **أهداف الدراسة:** نهدف من هذه الدراسة إلى ما يلي:

- بيان مفهوم الجريمة الإلكترونية وخصائصها ومجالات استخدامها.
- بيان الأجهزة المتخصصة في متابعة الجرائم الإلكترونية ودورها ومهامها في مكافحة هذه الأخيرة.
- تحديد الإجراءات المتبعة في التحري والتحقيق وحتى المحاكمة بالنسبة لهذه الجرائم.
- توضيح مدى فعالية إجراءات مكافحة الجرائم الإلكترونية في الجزائر وكذا التعاون الدولي في هذا المجال.

– **إشكالية الموضوع:**

في السابق كان من الصعب تصور الوضع الحالي الذي يرتكز على التكنولوجيا بشكل أساسي وكبير، وقد انتشرت الجرائم الإلكترونية وتفاقمت آثارها وأضرارها العامة والخاصة ورغم هذا يبقى الاستغناء عن استخدام هذه التقنية شبه مستحيل فلا مجال يخلو من الحاسب الآلي والتكنولوجيا الحديثة عموما، ونظرا لخطورة هذا النوع من الجرائم دفعنا موضوع دراستنا إلى طرح الإشكالية الرئيسية التالية:

- ما مدى فعالية النصوص الإجرائية الجنائية في مكافحة الجريمة الإلكترونية في التشريع الجزائري؟

- و تندرج تحت هذه الإشكالية إشكالات فرعية تتمثل في:
- ما هو مفهوم الجرائم الإلكترونية، وما موقف المشرع الجزائري من ذلك؟

- فيما تتمثل أهم خصائص وتصنيفات الجرائم الإلكترونية وما هي الجهات المختصة في متابعتها؟
- ما مدى كفاية الإجراءات الجزائية التقليدية في جمع الأدلة الإلكترونية والبحث والتحري عن هذه الجرائم، ولأي مدى يمكن القول بأن أساليب التحري الخاصة والجديدة تحترم وتطبق معايير المشروعية؟
- ما هي أهم إجراءات التحقيق المستحدثة وما مدى فعالتها في هذا مكافحة الجرائم الإلكترونية؟
- هل المحاكمة في الجرائم الإلكترونية مميزة عن باقي الجرائم الأخرى، وما الإشكالات التي تحدثها؟
- لأي درجة يمكن القول بأن المجتمع الدولي نجح في مكافحة الجرائم الإلكترونية عن طريق الإجراءات التي فرضها والتعاون الدولي في هذا المجال؟

-صعوبات الموضوع:

من بين أكبر الصعوبات التي واجهتنا في معالجة الموضوع عدم كفاية الوقت لإنجاز بحث بصورة أفضل ونقص الإمكانيات للتنقل وإثراء الموضوع أكثر كونه يميل بنسبة كبيرة لإبراز الجانب التطبيقي وبيان الاختلال على المستوى العملي الميداني. إضافة لنقص المراجع التي تتناول الموضوع بدقة وخصوصا المعمقة والتي تعالجه من الجانب التطبيقي الواقعي ورغم ذلك حاولنا إنجازه بالمراجع والمصادر المتوفرة.

- منهج الدراسة:

للإجابة عن الإشكالية المطروحة اتبعنا المنهج الوصفي وذلك بوصف وتعريف الجريمة الإلكترونية وبيان مجالات استخدامها وتوضيح الأجهزة المختصة في متابعتها (تشكيلها العضوي والوظيفي) بالإضافة إلى التطرق للإجراءات العملية الخاصة بمكافحة الجرائم الإلكترونية في التشريع الجزائري.

- خطة الدراسة:

تم تقسيم الموضوع إلى فصلين رئيسيين حيث:

الفصل الأول تحت عنوان ماهية الجرائم الإلكترونية، والذي قسمته لمبحثين، المبحث الأول تحدثت فيه عن مفهوم الجريمة الإلكترونية، بينما تناولت في المبحث الثاني مجالات استخدام الجريمة الإلكترونية والأجهزة المختصة في متابعتها.

بينما الفصل الثاني خصصته لدراسة إجراءات مواجهة الجريمة الإلكترونية، حيث قسمته لثلاثة مباحث، الأول تناولت فيه إجراءات التحري وجمع الاستدلالات في الجرائم الإلكترونية، والمبحث الثاني تطرقت فيه للتحقيق في الجرائم الإلكترونية، وأخيرا المبحث الثالث الذي تناولت فيه المحاكمة في الجرائم الإلكترونية.

لنختم موضوعنا بخاتمة تحتوي على أهم النتائج المتوصل إليها واقتراحات للمشرع الجزائري يتخذها من أجل ضمان المكافحة الفعالة للجرائم الإلكترونية.

الفصل الأول

ماهية الجريمة الإلكترونية

الفصل الأول:

ماهية الجريمة الإلكترونية

خلقت الثورة المعلوماتية نمطا جديدا من الإجرام تجسد في انتشار الجرائم الإلكترونية باعتبار الجريمة ظاهرة إجتماعية تتأثر طبيعتها وحجمها بالتحولات الاقتصادية والإجتماعية والثقافية دوليا ووطنيا، مما أدى بالضرورة لزعزعة العديد من المفاهيم التقليدية التي ظلت سائدة فترة طويلة من الزمن.

و اتسعت هذه الظاهرة لتصبح إجراما لا حدود له على مستوى العالم الافتراضي بشكل كبير ومروع يمس جميع الأشخاص أيا كانت، وتعدت خطورة هذه الجرائم لتكون ملجأ غير ممسوس بالنسبة للجناة الفعليين فقد تكيف المجرمون أيضا مع الوضع الجديد وابتدعوا أساليب ووسائل جديدة أجبرت أغلب التشريعات لتكييف ترسانتها القانونية مع هذا النمط الإجرامي الحديث.(1)

و في إطار ضرورة مكافحة هذه الظاهرة بسبل قانونية وجب التعرف على جميع حيثياتها ومن ثم مكافحتها عمليا لإسقاط الجناة وتوفير الحماية القانونية والفنية اللازمة للأشخاص التي تستعمل هذه الشبكات لمصالحها الخاصة والعامة، وهذا ما سنحاول معالجته من خلال التطرق في هذا الفصل لماهية الجريمة الإلكترونية وذلك في مبحثين:

- المبحث الأول نبين فيه مفهوم الجريمة الإلكترونية.

- أما المبحث الثاني نتعرف فيه على مجالات استخدام الجريمة الإلكترونية والأجهزة المختصة في متابعتها.

المبحث الأول: مفهوم الجريمة الإلكترونية:

(1)- زعيطي آمنة: مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري، مقال في مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، المجلد 4، العدد 7، جوان 2017، ص 4.

لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم أو التسمية الدقيقة لمصطلح الجريمة الإلكترونية لوجود مجموعة من المفاهيم المتقاربة والمشتقة من الإجرام الإلكتروني وهذا ما يطرح مسألة التشابه والاختلاف بين مصطلح الجريمة الإلكترونية وغيرها من المصطلحات المماثلة لها؛ ومن جهة أخرى فلهذه الجريمة خصائص تميزها عن غيرها من الجرائم والتي تتفرد بها لوحدها [1]، ولتحديد مفهوم الجريمة الإلكترونية بدقة ووضوح وجب التطرق لتعريف الجريمة الإلكترونية في المطلب الأول وخصوصية الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول: تعريف الجريمة الإلكترونية:

يصعب تحديد نطاق هذه الجريمة لإختلاف تعاريفها، ونظرا لطبيعتها الخاصة باعتبار أنها تقع في عالم إفتراضي ، لذا سأتعرض في هذا المطلب للتعريف اللغوي للجريمة الإلكترونية (الفرع الأول)، وكذا التعريف الفقهي الذي تباينت فيه الآراء إلا أنني سأتناول أبرزها (الفرع الثاني)، إضافة للجانب الأهم وهو التعريف التشريعي للجريمة الإلكترونية (الفرع الثالث).

الفرع الأول: التعريف اللغوي للجريمة الإلكترونية:

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجرمه الرجل على قومه وإليهم، ذنب وجنى جنئته.[2]

توجد مفاهيم منبثقة من الإجرام الإلكتروني والغش المعلوماتي والانحراف الذي يقع بواسطة الحاسب الآلي أو جرائم الإنترنت ويلاحظ تشابه بين الجريمة الإلكترونية والجريمة المعلوماتية. حيث ترى الدكتورة غنية باطلي في هذا الشأن: أن استعمال مصطلح الجريمة الإلكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها

---

(1)– زيوش عبد الرؤوف: الجريمة المعلوماتية في التشريع الجزائري مجله العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد الرابع، العدد الثالث، سبتمبر 2019 ، ص 3.

(2)– غنية باطلي: الجريمة الإلكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع الجزائر، 2015، ص 12– 13.

البعض الجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الإنترنت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة للأفراد والجماعة، مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص.[1]

إن مصطلح الجريمة الإلكترونية يعد أوسع من الجريمة المعلوماتية التي يقصد بها الجرائم المرتكبة على الكمبيوتر وجرائم الإنترنت فالجريمة الإلكترونية هي جريمة محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر أو أية وسيلة إلكترونية أخرى وهذا ما أكدته اتفاقية بودابست [2] أو الاتفاقية المتعلقة بالجريمة الإلكترونية والتي صادق عليها المجلس الأوربي في بودابست في المجر في 23 نوفمبر 2001. [3]

الفرع الثاني: التعريف الفقهي للجريمة الإلكترونية:

انقسم الفقه إلى اتجاهين، منهم من ضيق من مفهوم الجريمة الإلكترونية **و**منهم من وسع من مفهومها.

---

(1)– ضياء مصطفى عثمان: السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011، ص 32.

(2)– اتفاقية بودابست: والمعروفة أيضا باتفاقية الجرائم الحاسوبية واعتمدت الاتفاقية وتقريرها التوضيحي من قبل لجنة وزراء مجلس أوربا في 8 نوفمبر 2001 ودخلت حيز التنفيذ في سنة 2004 وتعتبر الاتفاقية أول معاهدة دولية بشأن الجرائم المرتكبة عبر الإنترنت وشبكات الكمبيوتر الأخرى، هدفها الرئيسي هو اتباع سياسة جنائية مشتركة تهدف لحماية المجتمع من الجرائم الإلكترونية لاسيما من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي.

(3)– ضياء مصطفى عثمان: المرجع السابق، ص 24.

- الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية:

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها. ومن التعريفات التي وضعها أنصار هذا الاتجاه أن "الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى".

- الاتجاه الذي يوسع من مفهوم الجريمة الإلكترونية:

فقد عرفها أصحابه بأنها "سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي جريمة تتم في محيط أجهزة الكمبيوتر، أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"، كما عرفها الفقيهان Michels & Credo بأنها "سوء استخدام الحاسب أو جريمة الحسابات تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه البيانات الخاصة، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وأيضا الاستخدام غير المشروع أو سرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته.(1)

و قد تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها "جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".(2)

(1)– سميرة معاشي: ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة بسكرة، ص 276.

(2)– ربيحة زيدان: الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 44.

الفرع الثالث: التعريف التشريعي للجريمة الإلكترونية:

بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة بتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية. وبهذا وفق المشرع في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية، ولولا هذه النظم المعلوماتية وشبكات الاتصال ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم».(1)

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

و حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه وهذا ما يوسع مجال نطاق الجرائم الإلكترونية في التشريع الجزائري.(2)

المطلب الثاني: خصوصية الجريمة الإلكترونية:

يسّر التقدم العلمي الكبير في مجال المعلوماتية حياة الإنسان ووفر عليه جهداً كبيراً وطبع شتى معاملاته بالسرعة الفائقة مما جعله يوفر الوقت والمال أيضا، لكن في المقابل فقد ارتبط استعمال هذه الوسائل الفنية الحديثة بظهور جرائم جديدة لم تكن معروفة من قبل،

(1)- أنهلة عبد القادر المومني: الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 52.

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

كما ارتبط بزيادة في حدة بعض الجرائم التي كانت موجودة من قبل، فهذه التقنية أوجدت ألوانا جديدة من الجرائم طبعتها بطابعها وأسبغت عليها خصائص ميزتها عن غيرها من الجرائم [1]. ومن أبرز الخصائص التي يمكننا أن نميز فيها الجريمة الإلكترونية عن غيرها من الجرائم التقليدية أنها ترتكب من مجرم غير تقليدي (الفرع الأول)، وكونها جريمة صعبة الاكتشاف والإثبات (الفرع الثاني)، لاسيما أنها تعتبر من الجرائم العابرة للحدود (الفرع الثالث).

الفرع الأول: ترتكب الجريمة الإلكترونية من مجرم غير تقليدي:

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات لا يوجد لها مثيل لدى غيره، كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لإرتكاب الجريمة مختلفة عنده أيضا فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي، أي أنه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أن هذا المجرم إنسان ذكي، إذ أنه يستغل ذكاءه في تنفيذ جريمته، ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا، ويفسر هذا أن هذا المجرم من ذوي المستويات العلمية العالية غالبا. وما يميز مجرم المعطيات أيضا هي الدوافع التي تدفعه لارتكاب الجريمة، فهي متعددة ومختلفة فقد تكون السعي لتحقيق الربح وقد تكون الرغبة في الانتقام من رب العمل وقد تكون الرغبة في قهر النظام والتفوق على وسائل التقنية وتعقيدها وقد يرتبط الدافع بحب التعلم والاستكشاف، كما قد يرتبط بالسياسة والإيديولوجيا- إلى غير ذلك من البواعث كما يتميز مجرم المعطيات أيضا بفئاته وأنماطه المختلفة وهو ينقسم إلى نوعين رئيسيين، الأول هم الهواة المولعون بالمعلوماتية، والثاني هم محترفو الجرائم المعلوماتية وأساس التمييز بين

---

(1)- محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 8 ماي 45 قالمة، ص 371.

النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة، بينما هو ساذج لدى النوع الأول لا يتعدى الرغبة في الإستطلاع والإستكشاف ، فهو خبيث لدى النوع الثاني، والذي قد يكون ماليا أو سياسيا أو غيره.[1]

الفرع الثاني: جريمة صعبة الاكتشاف والإثبات:

تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات تخريب، شواهد مادية)، وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة، والنظام العدلي وعدم كفاية القوانين القائمة.[2]

لا تحتاج جرائم الإعتداء على برامج ومعلومات الحاسب الإلكتروني إلى أي عنف أو جثث أو سفك دماء أو آثار اقتحام لسرقة الأموال وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الإلكتروني، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها.[3]

من المفترض أن اكتشاف هذه الجرائم يتم عن طريق الفحص والتدقيق أو عن طريق الشكاوى التي يقدمها المجني عليهم، والوضع بخصوص جرائم المعطيات بالغ التعقيد في الأمرين معا، فجهات التحقيق لم تصل إلى تلك المعرفة أو الخبرة التي تملكها حيال التحقيق في الجرائم التقليدية، لأن الأمر يتطلب معرفة واسعة وإحاطة كاملة بهذه التكنولوجيا الحديثة، وتحديث هذه المعارف يوميا، هذا من جهة، ومن جهة أخرى فالضحية في هذه الجرائم تمتنع

---

[1]– عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الطبعة الثانية، القاهرة 2002، ص36.

[2]– ذياب موسى البداينة: الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من 2–3 /2014/09، ورقة علمية بعنوان الجرائم الإلكترونية: المفهوم والأسباب، كلية العلوم الإستراتيجية، عمان، 2014، ص 20.

[3]– عادل يوسف عبد النبي الشكري: الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، جامعة الكوفة « كلية القانون »، العدد السابع، 2008، ص 116.

في الغالب عن التبليغ عنها وقد يسعى إلى التعتيم علي المحققين وتضليلهم حتى لا يكتشفوا هذه الجرائم.كما أن إثبات هذه الجرائم يعترضه الكثير من الصعوبات، فطبيعة هذه الجرائم غير مرئية في الغالب لأنها تتعلق بمعطيات في شكل نبضات أو ذبذبات إلكترونية، ويسهل علي الجاني محو الأدلة المتعلقة بها وتدميرها في وقت وجيز.[1]

الفرع الثالث: جريمة عابرة للحدود الدولية:

الجريمة الإلكترونية ذات بعد دولي، أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.[2]

و ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحاسبات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان في دولة معينة على مجني عليه في دولة أخرى في وقت يسير جدا مكبّدة أفدح الخسائر لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت، خاصة في مجال التجارة الإلكترونية وإزدياد إعتماد البنوك عليها. وتثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى.[3]

---

[1]- سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 95.

[2]- إبراهيم رمضان إبراهيم عطايا: الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مجلة كلية الشريعة والقانون بطنطا، الجزء الثاني، العدد 30، ص 374.

[3]- نائلة عادل محمد فريد قورة: جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003، ص 49.

و قد تتأثر دول كثيرة بهذه الجريمة في آن واحد بسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها، ومن أهم القضايا التي أكدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة إيدز، وتتلخص وقائعها عام 1942 حيث قام أحد الأشخاص وهو "كوزيف بيب" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الإيدز، لكن في الحقيقة يحتوي هذا البرنامج على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الفاعل أو الجاني بطلب مبلغ مالي للحصول على عنوان إلكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني بإرسال البرنامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الإنجليزي إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية.[1]

فهذا النوع من الجرائم يمتاز بالنعومة وعدم استخدامه للعنف كما في الجرائم التقليدية.

---

[1]- سويد سفيان: الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2003، ص 23.

المبحث الثاني

مجالات استخدام الجرائم الإلكترونية والأجهزة المختصة في متابعتها

إذا كنا بصدد الحديث عن مجالات استخدام الجريمة الإلكترونية (المطلب الأول) أو نطاقها فحتما سنجده واسعا يشمل جميع مناحي حياة المجتمع وأفراده، فنطاق الجريمة الإلكترونية يطال حياة الأشخاص الخاصة وأموالهم ومؤسساتهم وجرائم أخرى تمس حتى بأمن الدولة كجرائم الإرهاب والجرائم المنظمة. ونجد أيضا من يصنف الجرائم الإلكترونية تبعا لمرتكبها **أو** لطريقة تنفيذها،أو وفقا للغرض أو هدف الاعتداء. وفي ظل هذا التعدد عمدت أغلب الدول لإسناد مهمة متابعة هذه الجرائم لأجهزة مختصة ومحددة محاولة بذلك مكافحتها قانونيا **و**تتبع ذلك تطبيقيا وميدانيا ، والحد منها وتأطيرها عمليا لحد ما (المطلب الثاني).

المطلب الأول: مجالات استخدام الجرائم الإلكترونية:

مع اختلاف تصنيفات الجرائم الإلكترونية مجالات استخدامها المتعددة نميز صنفين رئيسيين: الأول شكلي ونجد فيه الجرائم الإلكترونية التقليدية أي المعروفة سابقا لكنها مرتكبة بتقنية حديثة كالسرقة الإلكترونية، وجرائم إلكترونية مستحدثة تعتمد بشكل كلي ورئيسي في تنفيذها على تقنيات رقمية ، أما الصنف الثاني ألا وهو التصنيف العملي والذي سنركز عليه بشكل كبير والذي ينقسم بدوره لثلاثة أنواع وهي:

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي:

و هي جرائم يتم ارتكابها بواسطة تقنيات رقمية إذ يعتبر النظام المعلوماتي في حد ذاته أو برامجه وسيلة لتنفيذ الجريمة، ويسهل فيها الحاسب الآلي نتيجتها الإجرامية ويضاعف من جسامتها ويهدف الجاني لربح مادي غير مشروع [1]. وتنقسم بدورها إلى:

---

[1]- نمديلي رحيمة: المرجع السابق، ص 102.

أولا: الجرائم الواقعة على الأشخاص:

للحياة الشخصية خصوصية وحرمة تمنع اقتحامها من طرف أي شخص كالاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، ويمكن أن تقوم هذه الجريمة بالاطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته.

و يتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها عبر الإنترنت، أما الركن المعنوي وهو توفر القصد الجنائي بعنصريه أي قصد نشر الصور والعلم والإرادة بذلك. [1]

ونجد أيضا جرائم انتحال شخصية الغير والاستدراج وذلك من خلال استخدام شخصية الضحية بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيرها من الأسباب، وكذا انتحال شخصية المواقع وهذا النمط بكثرة في المجال التجاري، إضافة للإستدراج ، أي إيهام المجرم الإلكتروني لضحاياه وأغلبهم صغار في تكوين صداقة عبر الشبكة تتحول إلى لقاء واقعي.[2]

ثانيا: جرائم واقعة على الأموال:

أصبحت معظم المعاملات التجارية من خلال شبكة الإنترنت، كالبيع والشراء، مما أنجر عليه تطور وسائل الدفع والوفاء، وتبعا لذلك أنتهز المجرمون فرصتهم في السطو على

---

[1]- يوسف خليل يوسف العفيفي: الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة"، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون "الجامعة الإسلامية، غزة، 2013، ص 25.

[2]- عمرو موسى: الجرائم المعلوماتية (جرائم الحاسب الآلي في مصر وفي الدول العربية)، المكتب الجامعي، الإسكندرية، مصر، 2006، ص102.

المعاملات التجارية وابتكروا طرقا لأجل ذلك كالتحويل الغير مشروع للأموال وقرصنة البطاقات الممغنطة .[1]

و من أبرز أنواع الجرائم التي تتعرض لها المعاملات التجارية الحديثة ما يلي:

- السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني الغير مشروع.

- القمار وغسيل الأموال عبر الإنترنت.

- جريمة السرقة والسطو على أموال البنوك.

- تجارة المخدرات عبر الإنترنت.[2]

ثالثا: جرائم واقعة ضد أمن الدولة:

و تتمثل في جرائم الإرهاب والتجسس والجريمة المنظمة ؛ ظاهرة الإرهاب ظاهرة عالمية، حيث ظهرت الكثير من التنظيمات التي تتبنى هذا الفكر في مختلف دول العالم وبمختلف التسميات، وتظهر العلاقة بين الإرهاب والجريمة الإلكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الإلكتروني، كما يتم تبني العمليات الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الإلكترونية بما يحقق أهدافها.[3]

إضافة للتجسس والجريمة الإلكترونية ، فالتطور المعلوماتي سهل للمجرم الإلكتروني سواء كان فردا أو تنظيما ، وينفذ ذلك على الأشخاص أو المنظمات وحتى الدول وأجهزتها. وسواء كأن تجسسا عسكريا أو اقتصاديا أو سياسيا، وكذا الجريمة المنظمة والجريمة

---

(1)– صغير يوسف: الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون "تخصص القانون الدولي الأعمال"، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2013، ص 44.

(2)– حفوظة الأمير عبد القادر وغرداين حسام: الجريمة الإلكترونية وآليات التصدي لها، الملتقى الوطني "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 93.

(3)– صغير يوسف: المرجع السابق، ص 96.

الإلكترونية وذلك من خلال الإمكانيات المتاحة إلكترونيا في التخطيط والتوجيه وتنفيذ المخططات الإجرامية بسهولة ، مخترقة حدود الدول بأقل تكلفة ودون مخاطرة.[1]

و في ذات السياق يعد التجسس العسكري من أخطر الجرائم إذ أتاحت الإنترنت للدول ممارسته على دول أخرى، وذلك بالإطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول كثيرة النزاعات، ولاسيما المساس بالأمن الفكري والذي يخلق فوضى عن طريق التأثير على معتقدات وتقاليد مجتمعات بأكملها.[2]

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي:

هناك نوع آخر من الجرائم الإلكترونية والتي تقع على النظام المعلوماتي بحد ذاته وتستهدف مكوناته المادية أو المنطقية أو المعلومات المدرجة فيه.

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

المكونات المادية في الأجهزة والمعدات الملحقة بالنظام والمستخدمة في تشغيله كالأسطوانات والشرائط والكابلات، وطبيعة هذه المعدات المادية تجعل من الجرائم الواقعة عليها جرائم تقليدية، كأن تكون محلا للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل وهذا يرتب خسائر كبيرة؛ وقد حدث هذا النوع في فرنسا وأدى إلى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية ، وتم تقدير الخسائر بخمسة ملايين فرنك فرنسي.[3]

---

[1]- رحموني محمد: خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة العدد 41، جامعة أحمد دراية، أدرار، 2018، ص ص 448- 449.

[2]- ناصر محمد البقهي: أثر التحويل مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري والمفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة السعودية، 22-25 جمادى الأولى 1430 هـ، ص 18.

[3]- نمديلي رحيمة: مرجع سابق، ص ص 103- 104.

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

تعتبر هذه الصورة الأكثر انتشارا وخطورة لأنها تتم بواسطة الاحتيال لإدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها أو تغييرها.[1]

بداية تجب الإشارة إلى أن فعل الدخول والبقاء الغير مشروع في نظام المعالجة الآلية للمعطيات يشكل جريمة لوحده. وقد نص المشرع الجزائري في المادة 394 مكرر من قانون العقوبات الجزائري على أنه " يعاقب بالحبس من ثلاث (3) أشهر إلى سنة (1)، وبغرامة من 50.000 دج إلى 10.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف **أو** تغيير المعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 إلى 150.000 دج." [2]

و المستنتج من النص السابق أن الدخول والبقاء الغير مشروع في نظام المعالجة الآلية للمعطيات يتجلى في صورتين بحيث أن مجرد الدخول والبقاء غير المشروع في النظام يشكل الصورة البسيطة لهذا الفعل المجرم، والصورة المشددة تتحقق بتوفر ظروف التشديد وهي إما بالحذف أو تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروع، أو تخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين.[3]

و يجتمع فعل البقاء والدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، مثل أن لا يكون للجاني حق الدخول ويدخل عن طريق الغش ويبقى ، حيث نصت المادة 394

---

[1]– سمية عكور: الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانوني والأمني، الملتقى العلمي حول " الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الإستراتيجية، الأردن، 02– 04/ 09/ 2014 ، ص 12.

[2]– مولود ديدان: قانون العقوبات، قانون رقم 09– 01، المؤرخ في 25 فبراير 2009، د. ط، ص 120.

[3]– نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط 1، 2005، ص 223.

مكرر من قانون العقوبات الجزائري على فعل البقاء غير المشروع، على غرار القانون الفرنسي في المادة 323/1 في قانون العقوبات الفرنسي.(1)

الفرع الثالث: الجرائم الواقعة على البرامج الإلكترونية:

ينقسم هذا الصنف من الجرائم ينقسم إلى نوعين، الأول وهو الجرائم التي تقع على البرامج التطبيقية [1]، وهذا بتحديد البرنامج أولا ثم التلاعب به أو تعديله. ونذكر على سبيل المثال كأن يقوم أحد المسؤولين على البرمجة بالبنوك الأمريكية بتعديل برنامج ما، كأن يضيف دولارا واحدا على كل حساب يزيد عن عشرة دولارات ويقوم بتقييد المصاريف الزائدة في حساب خاص به.(2)

و النوع الثاني يتعلق بالجرائم الواقعة على برامج التشغيل [2]، أي تلك البرامج المسؤولة عن عمل النظام المعلوماتي من ضبط وترتيب للعمليات الخاصة بهذا الأخير، وتقوم هذا الجريمة عن طريق تزويد البرنامج بتعليمات إضافية للوصول إليها بشفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي. ومثال ذلك تصميم برنامج وهمي تنفذ به الجريمة كقيام إحدى شركات التأمين الأمريكية بتصميم برنامج تصنيع وثائق تأمين أشخاص وهميين بهدف تقاضي هذه الشركة العمولات من اتحاد شركات التأمين.(3)

(1)– أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الجزائر، ط 2، 2007، ص 110.

1– البرامج التطبيقية: هي كل البرامج التي تعمل على الحاسب مثل معالج الكلمات والجداول الإلكترونية وقواعد البيانات وأدوات العروض وبرامج الناشر المكتبي والألعاب وبرامج الوسائط المتعددة.

(2)– بوضياف إسمهان: الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف– المسيلة، العدد الحادي عشر ، 2018.

2– برامج التشغيل: وهي المشغل الرئيسي لجهاز الحاسوب ويعرّف نظام التشغيل بأنه مجموعة من البرامج الأساسية التي تدير جهاز الحاسوب، وتنظم جميع المهام التي يقوم بها، وتسهل على المستخدم الاستفادة من المعدات والملحقات التي يتكون منها الجهاز.

(3)– نمديلي رحيمة: المرجع السابق، ص 104.

المطلب الثاني: الأجهزة المختصة في متابعة الجرائم الإلكترونية:

كيّف المشرّع الجزائري ترسانته القانونية حسب التطورات الحاصلة في مختلف المجالات وما تبعه من ظهور جرائم جديدة تستدعي مواجهتها قانونيا وعمليا، وقد أشار المشرع في مختلف قوانينه إلى هذا النوع من الجرائم وخصص أجهزة لمتابعتها، فالجرائم الإلكترونية تنفرد بإجراءات خاصة نظرا لانفرادها بخصائص دون باقي الجرائم التقليدية، وهذا ما جعل المشرع يتبع نصوصه القانونية الهادفة لمكافحة الجريمة الإلكترونية بنصوص أخرى تجعل من الأولى تطبق ميدانيا، وذلك من خلال أنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الفرع الأول)، وهيئات أخرى قضائية جزائية (الفرع الثاني)، إضافة إلى هيئات تابعة للجهاز الأمني (الفرع الثالث).

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

استحدثت هذه الهيئة بموجب المادة 11 من القانون 64–67 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال السالف الذكر، حيث نصت على: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته"، وقد أحالت الفقرة الثانية من ذات المادة مسألة تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها للتنظيم، وهو ما تضمنه المرسوم الرئاسي رقم 15 –261.[1]

أولا: طبيعة تشكيل الهيئة ومهامها:

حسب المادة الثانية من المرسوم الرئاسي 15–261 تعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، يوجد مقرها بالجزائر وضعت لدى الوزير المكلف بالعدل، وعليه فقد تضمنت النصوص تحديد تشكيل الهيئة، وتبيان المهام الموكلة لها.

وفقا للمادة السادسة من نفس المرسوم تشكل الهيئة من:

[1]– المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر. ج. ج. ع. 53. الصادرة بتاريخ 8 أكتوبر 2015.

أ- لجنة مديرة يترأسها الوزير المكلف بالعدل:

و تتشكل من: وزير الداخلية، الوزير المكلف بالبريد وتكنولوجيا الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني ممثل عن رئاسة الجمهورية ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا [1]، وطبقا للمادة الثامنة فمن مهامها:

- ❖ توجيه عمل الهيئة والإشراف عليه ومراقبته.
- ❖ دراسة المسائل المتعلقة باللجوء للمراقبة الوقائية للاتصالات الإلكترونية.
- ❖ ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه.
- ❖ تقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة.
- ❖ اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ❖ بالإضافة إلى دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه دون إغفال دراستها للتقرير السنوي لنشاطات الهيئة والمصادقة عليه.

ب- المديرية العامة :

يديرها مدير عام بموجب مرسوم رئاسي وتنتهي مهامه بنفس طريقة تعيينه [2] وعليه السهر على:

- ❖ العمل على حسن سير الهيئة الوطنية بتنفيذ برنامج عملها.
- ❖ تحفيز نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها.
- ❖ تحضير اجتماعات اللجنة المديرة.
- ❖ تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية.[3]

---

[1]- المادة السابعة من المرسوم الرئاسي 15-261.

[2]- تنص المادة التاسعة من المرسوم الرئاسي 15-261 على: " يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي. وتنهى مهامه حسب الأشكال نفسها ".

[3]- لتفاصيل أكثر حول هذه النقطة، أنظر السادة العاشرة من المرسوم الرئاسي 15-261.

ت- مديرية المراقبة والوقاية واليقظة الإلكترونية: تمارس مديرية المراقبة العديد من المهام أهمها ما يلي:

❖ القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها.

❖ تقوم بإرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة.

❖ العمل على تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة، وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.

❖ تولّي مهمة جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

❖ تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرة، وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة.

- السهر على حسن سيرة والحفاظ على الحالة الجيدة لمنشآته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة.[(1)]

ت - مديرية التنسيق التقني:

في سبيل قيام الهيئة بكافة المهام المنوطة بها على أكمل وجه، تكلف مديرية التنسيق التقني بممارسة مهام يمكن إجمالها في:

❖ إنجاز الخبرات القضائية في مجال اختصاص الهيئة.

---

(1)- لتفاصيل أكثر حول هذه النقطة، أنظر المادة الحادية عشر من المرسوم الرئاسي 15- 261.

❖ تكوين قاعدة معطيات تحليلية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال واستغلالها.

❖ إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

❖ القيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها.(1)

ج- مركز العمليات التقنية:

طبقا للمادة الثالثة عشر من المرسوم الرئاسي 15-261 تم تزويد مركز العمليات بالمنشات والتجهيزات والوسائل المادية، وبالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الإلكترونية مع العلم أن المركز تابع لمديرية المراقبة الوقائية واليقظة الإلكترونية.(2)

بالنسبة لمهام هذه الهيئة فقد أحالت المادة الرابعة من المرسوم 15-261 إلى السادة 14 من المرسوم 09- 04 حيث تمارس الهيئة العديد من المهام والتي يمكن إجمالها في:

❖ - اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

❖ تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

❖ مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها فيما يتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات وإنجاز الخبرات القضائية، مع ضمان المراقبة والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص.

---

(1)- لتفاصيل أكثر حول هذه النقطة، أنظر المادة الثانية عشر من المرسوم الرئاسي 15-261.

(2)- المادة الرابعة عشر من المرسوم الرئاسي 15-261.

❖ تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

❖ ضرورة العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

❖ تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بالإضافة إلى المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.(1)

ثانيا: طريقة سير الهيئة:

طبقا للمادة السادسة عشر من المرسوم 15-251 تجتمع الهيئة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها، إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه وفقا لنص المادة السابعة عشر من المرسوم الرئاسي السالف الذكر، حيث يتم تزويدها بقضاة، وضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني، ويتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية، وطبقا للمادة الثامنة عشر من ذات المرسوم تزود الهيئة بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني، كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل (2). وفي سبيل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة بمراقبة الاتصالات الإلكترونية

(1)- لتفاصيل أكثر حول هذه النقطة، أنظر: آمال بن صويلح: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة الملتقى الدولي حول "الإجرام السيبراني المفاهيم والتحديات"، 11-12 أفريل 2017، جامعة 8 ماي 1945، قالمة، الجزائر، ص ص 5- 7.

(2)- المادة 19 من المرسوم الرئاسي 15-261 السالف الذكر.

وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص، وذلك طبقا لنص المادة الحادية والعشرين من المرسوم 15-261.

و يمكن للهيئة وضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية، ويشارك في عملية مراقبة الاتصالات الإلكترونية أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة، كما يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة بالاتصال مع المسؤولين المعنيين في الهيئة من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة.[1]

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة في متابعة الجرائم الإلكترونية:

أنشئت بموجب القانون 04- 14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية [2]. وتختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37- 329- 40 قانون إجراءات الجزائية.[3]

اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/ 06 المؤرخ في 2006/1/5 إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 04/09.

و تم توسيع صلاحيات الضبطية القضائية عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني المادة 16 قانون

---

(1)- المادة 24 من المرسوم الرئاسي 15-261 السالف الذكر.

(2)- سالم عبد الرزاق: ملتقى حول المنظومة التشريعية الجزائرية في محال الجريمة المعلوماتية، بمحكمة سيدي محمد، ص 14.

(3)- مولود ديدان: قانون الإجراءات الجزائية، الأمر 11-02، دار بلقيس، الجزائر، ص 18.

إجراءات الجزائية، كما يمكن تفتيش المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية حسب المادة 47 قانون الإجراءات الجزائية.

و قد نصت المادة 65 مكرر 5 قانون الإجراءات الجزائية على أساليب تحري خاصة تتعلق باعتراض المراسلات الإلكترونية والمدرجة بموجب القانون 06-22 المؤرخ في 20/ 12/ 2006.

- التسرب المادة 65 مكرر 11 من قانون الإجراءات الجزائية.
- تفتيش المنظومة المعلوماتية المادة 5 من القانون رقم 04/09.
- حجز المعطيات المعلوماتية المادة 5 رقم 04/09.
- نسخ المعطيات على دعامة تخزين الكترونية.
- إمكانية منع الوصول إلى معطيات تحتويها المنظومة.
- منع الاطلاع على المعطيات التي يشكل محتواها جريمة.[1]

الفرع الثالث: الهيئات التابعة للجهاز الأمني:

كلف المشرع الجزائري هيئات تابعة للجهاز الأمني بالتدخل للمواجهة العملية على المستوى التطبيقي للجرائم الإلكترونية، وتصنف الهيئات التابعة للجهاز الأمني والمكلف بمكافحة الجرائم ذات الصلة إلى نوعين:

أولا- الهيئات التابعة لسلك الأمن الوطني: يوجد على مستوى جهاز الأمن الوطني ثلاث وحدات مهمتها البحث والتحقيق في الجرائم الإلكترونية وهي:

أ- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

---

[1]- سالم عبد الرزاق: المرجع السابق، ص ص 18- 19.

ب- المخبر الجهوي للشرطة العلمية بقسنطينة.

ت- المخبر الجهوي للشرطة العلمية بوهران.

و يتولى كل مخبر سواء المركزي أو الجهوي لولاية قسنطينة أو وهران، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها.[1]

ثانيا- الوحدات التابعة للقيادة العامة للدرك الوطني:

تلعب مختلف المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني دورا هاما في مجال مكافحة الجريمة الإلكترونية، وتتميز مختلف الفصائل بخبرة وكفاءة عالية في مكافحة الجريمة الإلكترونية [2]، كما يوجد على المستوى المركزي هيئات تتكفل بمكافحة هذه الأخيرة وهي:

أ- المعهد الوطني للأدلة الجنائية وعلم الإجرام:

أنشأ المعهد بموجب المرسوم الرئاسي 04- 183 [3]، وهو مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلف بإجراء الفحوص العلمية في إطار التحريات الأولية، وإجراء بحوث متعلقة بالكشف عن الجرائم باللجوء إلى التكنولوجيا الدقيقة [4]، ويحتوي على: مصلحة البصمات، ومصلحة الإعلام الآلي حيث يتم على مستوى هذه

---

(1)- لتفاصيل أكثر حول هذه النقطة، أنظر: ربيعي حسين: آليات البحث والتحري في الجرائم المعلوماتية، أطروحة دكتوراه علوم، جامعة باتنة، 2015- 2016، ص 177- 178.

(2)- سعيدة بورنون: مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، مجلد 30، عدد 03، 2019، ص 52- 53.

(3)- مرسوم رئاسي 04- 183 المؤرخ في 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، ج. ج. ج. ع. 41، الصادرة بتاريخ 27 يونيو 2004.

(4)- لتفاصيل أكثر حول هذه النقطة، أنظر: المادة الرابعة من المرسوم الرئاسي 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني السالف الذكر.

المصلحة: رصد ومراقبة وتتبع عمليات الاختراق والقرصنة الإلكترونية وتفكيك البرامج الإلكترونية.[1]

ب- مركز الوقاية من جرائم الأعلام الآلي والجرائم الإلكترونية للدرك الوطني:

أنشأ هذا المركز سنة 2008 ويهدف إلى تحليل معطيات وبيانات الجرائم الإلكترونية، وتحديد هوية أصحابها سواء كانوا فرادى أو جماعات، والتي قد تستهدف خاصة المؤسسات الرسمية، البنوك وحتى الأفراد،

كما يهدف إلى:

- مساعدة باقي الأجهزة الأخرى في أداء مهامها وخاصة ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.

- المشاركة في عمليات التحري والتسرب عبر شبكة الإنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.

المشاركة في قمع الجرائم الإلكترونية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.[2]

---

[1]- هواري عياش: مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، جامعة بسكرة، كلية الحقوق، 2016، ص 12.

[2]- رابح سعاد: ضوابط مكافحة الجريمة المعلوماتية مجلة القانون العام الجزائري والمقارن، جامعة جيلالي الياس- سيدي بلعباس، المجلد السابع، العدد 01، جوان 2021.

ت- مديرية الأمن العمومي والاستغلال:

و هي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمراكز التقنية العلمية في مجال أعمال البحث والتحري في الجرائم الإلكترونية.

ث- المصلحة المركزية للتحريات الجنائية:

و هي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال.[1]

---

[1]- لتفاصيل أكثر حول هذه النقطة، أنظر: ربيعي حسين: آليات البحث والتحري في الجرائم المعلوماتية، المرجع السابق، ص 183.

الفصل الثانـي

إجراءات مواجهة الجريمة الإلكترونية

الفصل الثاني:

إجراءات مواجهة الجريمة الإلكترونية

قام المشرع الجزائري بصدد التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة ومحاولة منه تدارك الفراغ القائم في هذا المجال إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية وعلى رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية ورغم تأخر الجزائر في استخدام تكنولوجيا المعلومات والإنترنت لم يحل ذلك دون أن تصدر تشريعات تضمن الحماية الجنائية للأنظمة المعلوماتية، وتحفظ حقوق الأفراد من مخاطر الاستخدام السيء لتكنولوجيا المعلومات، وضرورة عدم الاكتفاء بالنصوص التقليدية، بالإضافة إلى ذلك فقد ضمن الحماية الجزائية للنظم المعلوماتية من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66- 156 المتضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات [1]، والذي تم تعزيزه بالقانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد قطع المشرع خطوة لا بأس بها إذ جرم الأعمال الإلكترونية بتعديله قانون العقوبات بموجب القانون رقم 04-15 المتمم للأمر رقم 66- 156 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات إضافة لتعديل سنة 2006، وكذا تجريم الأعمال الإلكترونية في القوانين الخاصة كالحماية في قانون التأمينات الاجتماعية رقم 08- 01، وقانون الملكية الأدبية والفنية الأمر رقم 03-05، الحماية في نصوص التوقيع الإلكتروني القانون رقم 15-03، وباقي التدابير والإجراءات المستحدثة في قانون الإجراءات الجزائية وغيرها والتي سنتطرق إليها فيما بعد، بحيث يتم تطبيق الإجراءات خلال مراحل سير الدعوى المتعلقة بالجرائم الإلكترونية وهذا ما سنفصل فيه لاحقا.

---

[1]- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66 – 156 مؤرخ في 08-06- 1966 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 71 لسنة 2004 المعدل والمتمم.

و في ذات السياق فمواجهة الجريمة الإلكترونية كخطوة عملية أولى تتمثل في المرحلة الأولى وهي مرحلة التحري وجمع الاستدلالات (المبحث الأول)، ثم مرحلة التحقيق في الجرائم الإلكترونية (المبحث الثاني) وأخيرا مرحلة المحاكمة في الجريمة الإلكترونية (المبحث الثالث).

المبحث الأول: التحري وجمع الاستدلالات في الجرائم الإلكترونية

حدد المشروع الجزائري بعض القواعد والضوابط في ظل مواجهة الجرائم الإلكترونية ومرتكبيها ولحماية معطيات الحاسب الآلي خاصة في مرحلة جمع الاستدلالات، حيث أن أجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة لمعاينة مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة [1]، وتخص هذه المرحلة التي تسمى بمرحلة البحث والتحري أي جمع الاستدلالات كل الإجراءات المتخذة من طرف الضبطية القضائية منذ معرفتها وعلمها باحتمال وقوع الجريمة وما يليها من تحرير محاضر بشأن تلك الإجراءات ونتائجها وتقديمها أمام الجهات المختصة [2]، وقد نص المشرع على تشمل واختصاص الضبطية القضائية في قانون الإجراءات الجزائية.[3]

و انطلاقا مما سبق سنتطرق في هذا المبحث إلى:

المطلب الأول: تلقي البلاغات والشكاوي في الجرائم الإلكترونية:

المتحري هو شخص مكلف بإجراء التحري بواسطة الحاسب الإلكتروني عن المتحري عنه، وعليه أن يمتلك القدرة على إجراء مهامه وأن يميز من الحقائق والأقوال والآراء والاستنتاجات، إضافة لتمتعه بدقة الملاحظة لتتبع المتهمين والشهود أثناء التعامل معهم وسرعة الأداء والتأني والصبر وقوة الذاكرة.[4]

و الحديث للغير في مجال التحري يكون في حدود توجيه الأسئلة والاستفسارات، فيجب أن تكون مقنعة مليئة بالثقة، في حين أن كتابة المحاضر يجب أن تتميز بالوضوح والتسلسل المنطقي والإقناع لتصل إلى العدالة، وكخطوة سابقة لكل ما تحدثنا عنه هو أن يتلقى رجال

---

[1]- خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 147.

[2]- أحمد شوقي الشلقاني: مبادئ الإجراءات الجزائية في التشريع الجزائري- الجزء 2، الطبعة الخامسة، ديوان المطبوعات الجامعية، الجزائر، ص 159.

[3]- لتفاصيل أكثر حول تشكيل واختصاص الضبطية القضائية، أنظر :المواد 15، 16 قانون الإجراءات الجزائية الجزائري.

[4]- مروك نصر الدين: محاضرات في الإثبات الجنائي، دار هومة، الجزائر، 2011، ص 81.

الضبطية القضائية أو المتحرون بلاغات (الفرع الأول) وشكاوى (الفرع الثاني) تمكنهم حينئذ من مباشرة إجراءات التحري.

الفرع الأول: تلقي البلاغات في الجرائم الإلكترونية:

الأصل أنه يجب على رجال الشرطة قبول البلاغات التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند وردها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ بدعوى عدم الاختصاص المكاني أو النوعي بها، في حين أن الواجب اتخاذ الإجراءات المقرة بشأنها، ثم إخطار جهة الاختصاص والمحضر إليها.

و يقوم المتحري بجمع الأدلة وفحص البلاغ بإجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.[1]

و يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الإنترنت أو ما يسمى بالبلاغ الرقمي، وذلك بإرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجوه صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية مثلا تتضمن التبليغ عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال.

و المعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المتحري عند تلقيه البلاغ، ويمكن الحصول عليها من خلال طرح أسئلة عن تاريخ وقت تلقي البلاغ،

[1]- خالد عباد الحلي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، الأردن، 2011، ص 79.

المعلومات الخاصة، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة.[1]

الفرع الثاني: الشكوى في الجرائم الإلكترونية:

تتطور النزاعات بين الأفراد بشكل مستمر نتيجة لتطور المشاكل داخل المجتمع، لذا كان من الضروري أن تطرح هذه الصراعات أمام المحاكم لإيجاد حل لها حفاظا على امن المجتمع واستقراره.[2]

لهذا وضعت وزارة العدل حيز الخدمة أرضية إلكترونية جديدة تسمع للأشخاص بتقديم الشكاوى **أو** العرائض عن بعد وذلك في إطار مواصلة تطوير وتحسين نوعية الخدمات المقدمة للمواطنين وأفراد الجالية الجزائرية بالخارج، حسب ما أفاد به بيان وزارة العدل يوم الثلاثاء 28 جويلية 2020.

و للاستفادة من هذه الخدمة يتعين على مقدم الشكوى الولوج إلى أرضية النيابة الإلكترونية المخصصة لهذا الغرض والمتاحة عبر البوابة الإلكترونية لوزارة العدل، قصد ملء استمارة تسجيل شكوى عن بعد بمجموعة من المعلومات الشخصية الخاصة بهويته كاملة وعنوان إقامته ورقم هاتفه: ونوع شكواه ومضمونها.

كما أن الشكوى المودعة سيتم تحويلها بصفة آلية إلى ممثل النيابة (وكيل الجمهورية بالمحكمة **أو** النائب العام بالمجلس القضائي) لاتخاذ الإجراء المناسب.

---

[1]- محمد بوعمرة، سيد علي بنينال: جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية- تخصص القانون الأعمال، جامعة أكلي محند أولحاج – البويرة، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2019- 2020، ص 42.

[2]- نجاة زعزوعة، ليلى بن قلة: النيابة العامة الإلكترونية في التشريع الجزائري، مجلة الدراسات القانونية والاقتصادية Issn 2602-7321، 2021، ص 301.

و بعد تصرف ممثل النيابة في الشكوى، يتم إعلام المعني بمآلها والإجراءات المتخذة أو المطلوب اتخذاها، وذلك عبر أرضية النيابة الإلكترونية وكذا عبر رسالة نصية قصيرة وبريده الإلكتروني. [1]

و هنا نميز بين حالتين حالة عدم قبول الشكوى أو رفضها وذلك مع تبيان سبب الرفض وحالة قبولها وإحالتها الملف إلى الجهة المختصة. وذلك حتى يتمكن المعني بالأمر من متابعة مآل دعواه أمام الجهة المختصة التي حددتها النيابة العامة.

و يلاحظ من خلال ما سبق ذكره بأن إجراءات تقديم الشكوى أمام النيابة العامة الإلكترونية تتسم بالسهولة بالنسبة للشاكي والنيابة العامة ذلك أنه إذا كان الأمر أصبح يسيرا على الشاكي باعتبار أنه يتفادى مشقة الانتقال إلى المحكمة وانتظار اليوم المحدد للاستقبال من طرف وكيل الجمهورية لعرض شكواه وقيدها لدى كتابة الضبط بل يمكنه القيام بذلك عن بعد وفي أي وقت كان، فإن الأمر أصبح أيضا يسيرا على النيابة من خلال معالجتها لهذه الشكوى عن بعد تفاديا للاكتظاظ والازدحام داخل مقر المحكمة، ومن جهة ثالثة فإن هذه الطريقة تدعم شفافية العمل القضائي مما يدعم ويعزز الاطمئنان في نفوس المتقاضين.[2]

المطلب الثاني: أساليب التحري الخاصة:

أثارت الجرائم الإلكترونية مشكلة إجرائية نظرا لطبيعتها الخاصة وهذا ما أدى لعدم إمكانية الاستعانة بإجراءات التحري التقليدية كالتفتيش والضبط، الأمر الذي حتم إلى ضرورة التنصيص على إجراءات حديثة أطلق المشرع الجزائري على تسميتها بأساليب التحري الخاصة.

---

[1]- أرضية إلكترونية جديدة تسمح للأشخاص بتقديم الشكاوي عن بعد، نشر يوم الثلاثاء 28 جويلية 2020، وتم الاطلاع على موقع وكالة الأنباء الجزائرية يوم 29 ماي 2022، على الساعة 14:52، ورابط الموقع:
https://www.aps.dz/ar/algerie/9025-2020-07-28-17-13-13

[2]- نجاة زعزوعة، ليلى بن قلة: المرجع السابق، ص 303.

يعرف الفقه أساليب التحري الخاصة أنها تلك العمليات أو الإجراءات أو التقنيات التي تستخدمها الضبطية القضائية تحت مراقبة وإشراف السلطة القضائية، بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات وجمع الأدلة عنها والكشف عن مرتكبيها، وذلك دون علم ورضا الأشخاص المعنيين.[1]

الفرع الأول: أساليب التحري الخاصة وفقا لقانون الإجراءات الجزائية والقانون المتضمن القواعد الخاصة:

أولا: أساليب التحري الخاصة وفقا لقانون الإجراءات الجزائية:

أ- مراقبة الأشخاص والأشياء والأموال:

وفقا للمادة 16 مكرر من قانون الإجراءات الجزائية فأنه يمكن لضباط الشرطة القضائية الحق بمراقبة الأشخاص والأشياء والأموال ومتحصلات الجريمة، وذلك على امتداد التراب الوطني وفقا للقانون.[2]

و تعني المراقبة وضع شخص أو وسائل نقل أو أماكن أو مواد تحت رقابة سرية ودورية بهدف الحصول على معلومات لها علاقة بالشخص محل الاشتباه، أو بأمواله، أو بالنشاط الذي يقوم به. وحسب المادة المذكورة سابقا تتم المراقبة بعد إخبار وعدم اعتراض وكيل الجمهورية المختص إقليميا ويكون الإخبار كتابة لأنه يتضمن تمديد الاختصاص الإقليمي والمساس بحرية الأشخاص، كما يتم تحت إشراف وإدارة النائب العام. وبعد الانتهاء من المراقبة أو خلالها لابد من تدوين ما تم التوصل إليه ضمن محاضر تحقيق للرجوع إليه واستعمالها أثناء جميع مراحل الخصومة الجزائية.

---

[1]- عبد الرحمان خلفي: محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010، ص ص 68- 69.

[2]- لتفاصيل أكثر، يرجى الاطلاع على نص المادة 16 مكرر، الأمر رقم 66- 155 مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية، معدل ومتمم بالقانون رقم 18- 13 مؤرخ في 11 يوليو سنة 2018.

ب- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

نظمها المشرع في قانون الإجراءات الجزائية، المواد 65 مكرر 5 إلى غاية مكرر 10 التي تجيز لضباط الشرطة القضائية وأعوانهم القيام بهذه الأعمال.

و يقصد باعتراض المراسلات عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب الجريمة.[1]

و المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، كل تراسل أو إرسال أو استقبال علامات أو إشارات أو متابات أو صور أو أصوات أو معلومات مختلفة عن طريق الإعلام أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية حسب المادة 8-21 من القانون رقم 2000-3 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.[2]

أما تسجيل الأصوات والتقاط الصور هو تسجيل المحادثات الشفوية التي تحدث بن الأشخاص بصفة سرية أو خاصة وفي مكان عام أو خاص وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.[3]

و للإشارة فالإجراءات المذكورة سابقا مقيدة بشروط لتكون إجراءات صحيحة ومنتجة لآثارها وهذا في المادة 65 مكرر 5 قانون الإجراءات الجزائية.

حيث حدد الجرائم فيها على سبيل الحصر تحت طائلة البطلان [4]، إضافة للحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع مراعاة المواعيد المحددة في

---

(1)- عبد الرحمان خلفي: محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010، ص 72.

(2)- الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: السنة السابعة والثلاثون، العدد 48، الصادرة في 2000/08/06، ص 7.

(3)- عبد الرحمان خلفي: المرجع السابق، ص 73.

(4)- نصر الدين هنوني، دار بن يقدح: الضبطية القضائية في القانون الجزائري، دار هومة، الجزائر، 2011، الطبعة الثانية، ص 78.

المادة 47 من ذات القانون. وتنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختصة وفي حالة فتح تحقيق قضائي تتم بناءا على إذن قاضي التحقيق وتحت مراقبته المباشرة.[1]

ج – التسرب:

يعتبر تقنية جديدة بالغة الخطورة على أمن الضبطية القضائية، وتتطلب جرأة وكفاءة ودقة العمل، قننها المشرع الجزائري في تعديله لقانون الإجراءات الجزائية لسنة 2006 وعرفته المادة 65 مكرر 12 بأنه "قيام ضابط عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة المكلف بتنشيط العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف ".

و الأفعال التي يقوم بها رجل الضبطية تعتبر جريمة في الظروف العادية كما أنها متناقضة مع قاعدة نزاهة ومشروعية الحصول على الدليل والمذكورة في المادة 65 مكرر 14 ق. إ. ج. ولكن هذه الإباحة المشروعة قانونا بهدف الوصول لحماية المجتمع ومكافحة الجريمة تقييده بعدم وصول أفعاله لحد التحريض فسلطة الرجل المتسرب تمنحه السير مع المجموعة لا المبادرة أو الأمر أو التحريض.[2]

و تتم عملية التسرب وفقا لشروط محددة في نصوص الإجراءات الجزائية والمتمثلة في:

– أن يتم اللجوء إلى التسرب إذا اقتضت ضروريات التحري ذلك مع توفر الإذن من طرف وكيل الجمهورية أو من طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية.

---

[1]– تفاصيل أكثر أنظر: في إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم: 06–22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المرجع السابق، ص 8– 9.

[2]– نجيمي جمال: إثبات الجريمة على ضوء الاجتهاد القضائي، دراسة مقارنة، دار هومة، الجزائر، 2011، ص ص 451– 452.

– أن يكون الإذن مكتوبا مسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويكون الإذن يحدد مدة عملية التسرب على أن لا تتجاوز أربعة 04 أشهر ويمكن تجديدها حسب مقتضيات التحري ضمن نفس الشروط الشكلية والزمنية، كما يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت، يوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

– لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، ويعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة، من 50.000 دج إلى 200.000 دج. وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 200.000 دج إلى 500.000 دج. وإذا تسبب الكشف في وفاة أحد هؤلاء الأشخاص فتكون عقوبة الحبس من عشر سنوات إلى عشرين سنة والغرامة من 500.000 دج إلى 1.000.000 دج دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.

– إذا تقرر وقف العملية أو انقضاء المهلة المحددة وفي حالة عدم تمديدها، يمكن للعون المتسرب مواصلة إجراءات التسرب للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على أن لا تتجاوز المدة أربعة أشهر، مع إخبار القاضي الذي رخص بالإجراء في أقرب الآجال فبانقضاء مهلة الأربعة أشهر دون تمكن العون من توقيف نشاطه في ظروف تضمن آمنة، يمكن للقاضي أن يرخص بتمديدها لأربعة أشهر على الأكثر.

– يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية.[1]

ثانيا: أساليب التحري الخاصة وفقا للقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (مراقبة الاتصالات الإلكترونية):

نظم المشرع نظام مراقبة الاتصالات الإلكترونية في الفصل الثاني من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و نص المشرع الجزائري في المادة 04 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية (مع وجوب الحصول على إذن مسبق من السلطات القضائية المختصة) هي:

أ– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. (في هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته المنصوص عليها في المادة 13 من نفس القانون إذنا لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير بين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها والمتمثلة في تجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية

[1]– أنظر إجراءات التسرب: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم: 06– 22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66– 155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية الجزائري، المرجع السابق، ص 9–10 ؛ كشلك: عبد الله أوهايبية: شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة الجزائر، 2015، ص ص 319– 322.

والاعتداءات على أمن الدولة ومكافحتهما وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير).[1]

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- مقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية.

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

الفرع الثاني: تقدير مدى مشروعية أساليب التحري الخاصة:

لتقدير مشروعية أساليب التحري الخاصة التي منحها المشرع الجزائري للضبطية القضائية يجب الوقوف على القيود التي وضعتها الاتفاقيات الدولية للسلطات القضائية عند الإذن باتخاذ أساليب للتحري قد تمس بالحقوق والحريات المعترف بها للفرد.

أولا: مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية وفقا للاتفاقيات الدولية لحقوق الإنسان:

من ضمانات مشروعية إجراءات جمع الأدلة الرقمية في الاتفاقيات الدولية، فقد نصت المادة 03 من الإعلان العالمي لحقوق الإنسان على أن لكل فرد الحق في الحياة والحرية وسلامة شخصه، وأضافت المادة 12 من نفس الإعلان على أنه لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات). بينما المادة 92-2 منه أجازت إمكانية المساس بتلك الحقوق حيث نصت على أنه يخضع الفرد في ممارسة حقوقه وحرياته لتلك القيود التي يقرها القانون فقط لضمان الاعتراف بحقوق الغير

[1]- أنظر في: الإجراءات المتعلقة بمراقبة الاتصالات الإلكترونية: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية قانون رقم 09- 04 المؤرخ في 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرجع السابق، ص 6.

وحرياته واحترامها ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي).[1]

أشارت المادة 17 الفقرة الأولى من العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة 1966 على أنه: (لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته)، وقد نصت المادة 19 فقرة ثنية منه: (لكل إنسان الحق في حرية التعبير، ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها). وقد سمحت نفس المادة في فقرتها الثالثة على إخضاع الحقوق المنصوص عليها في الفقرة الثانية لبعض القيود ولكن شريطة أن تكون محددة بنص القانون وأن تكون ضرورية لاحترام حقوق الآخرين أو سمعتهم، أو الحماية الأمن القوي أو النظام العام أو الصحة العامة أو الآداب العامة. ومن جهة أخرى فإن المادة 5 من العهد ذاته نصت في فقرتها الأولى: (ليس في هذا العهد أي حكم يجوز تأويله على نحو يقيد انطواءه على حق لأي دولة أو جماعة أو شخص بمباشرة أي نشاط أو القيام بأي عمل يهدف إلى إهدار أي من الحقوق أو الحريات المعترف بها في هذا العهد أو إلى فرض أي قيد أو تضييق على أي من حقوق الإنسان الأساسية المعترف بها أو النافذة في أي بلد تطبيقا لقوانين أو اتفاقيات أو أنظمة أو أعراف بذريعة كون هذا العهد لا يعترف بها أو كون اعترافه بها أضيق مدى).[2]

---

[1]- الإعلان العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة 217 ألف (د-3) المؤرخ في 10 كانون الأول/ ديسمبر 1948، من خلال الموقع الرسمي الإلكتروني لهيئة الأمم المتحدة، http://www.un.org/ar/documents/index.html، بتاريخ: 13 /2022/05، على الساعة 20:15.

[2]- أنظر هذه المواد من خلال الموقع الإلكتروني للمعهد الدولي الخاص بالحقوق المدنية والسياسية:

file:///C:/Users/user/Downloads/Documents/ccpr.pdf، بتاريخ: 2022/05/25 على الساعة 18:00.

و نصت المادة 15 من اتفاقية بودابيست، على مجموعة من الشروط والضمانات التي يجب على الدول الأطراف مراعاتها لضمان مشروعية الإجراءات الجزائية المتبعة في التحري والتحقيق عن الجرائم الإلكترونية حيث:[1]

– كل طرق أن يحرص على تأسيس وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في القسم الخالي، والتي تخضع للشروط والاحتياجات المقررة في قانونه الداخلي، والذي يجب أن يضمن حماية حقوق الإنسان وحرياته خصوصا الناشئة عن الالتزامات التي تعهد بها في ظل اتفاقية المجلس الأوربي عام 1950 لحماية حقوق الإنسان وحرياته الأساسية والاتفاقية الدولية للحقوق المدنية والسياسية للأمم المتحدة لعام 1966، والاتفاقيات العالمية الأخرى المطبقة والخاصة بحقوق الإنسان والتي يجب أن تتكامل مبدأ التناسب.

و الشروط السابقة الذكر يجب أن تشمل بطبيعة السلطة والإجراء المعني بشأنه على إشراف قضائي أو أية أشكال أخرى للإشراف المستقل ، البواعث المبررة للتطبيق، تحديد نظام التطبيق، والمدة الزمنية للسلطة أو الأجراء.

و في نطاق يسع المصلحة العامة، وبالأخص حسن تطبيق العدالة، ويجب على كل طرف أن يفحص أثر السلطات والإجراءات الواردة في هذا القسم على الحقوق والمصالح القانونية للطرف الثالث.

ثانيا: مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة الإلكترونية وفقا للقانون الجزائري:

انقسم الفقه بين مؤيد ومعارض لاستعمال الأساليب التقنية الحديثة وذلك كما يلي:

[1]– هلالي عبد الله أحمد: كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة،2011، ص 174.

أ- الرأي المعارض:

انتقد المعارضون بشدة أساليب التحري الخاصة وذلك من حيث حجيتها من جهة، فهي وسائل غير مضمونة لأنها لا تعكس الحقيقة دائما فمقاطع الصوت أو الصورة يمكن تغييرها أو حذفها كليا أو جزئيا وكذا تركيبها بشكل يغير الحقيقة؛ ومن جهة أخرى من حيث مشروعيتها، إذ أن الدستور يحمي حرمة الحياة الخاصة وكذا مراسلاته واتصالاته بكل أشكالها، إضافة لقانون العقوبات الذي يعاقب على المساس بحرمة الحياة الخاصة للمواطن فيما يتعلق بالمكالمات والصور من خلال المواد: المادة 137 (قانون رقم 06-23 مؤرخ في 20 ديسمبر 2006) المادة 303 (قانون 06- 23 مؤرخ في 20 ديسمبر 2006) المادة 303 مكرر: (قانون 06- 23 مؤرخ في 20 ديسمبر 2006).[1]

لهذا يرى بعض الفقهاء أن الاتجاه الجديد للسياسة الجنائية التي جاء بها المشرع بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية لم يوازن بين حماية الصالح العام وحق الأفراد في احترام حياتهم الخاصة وهذا ما جسدته السلطات الواسعة الممنوحة لضباط الشرطة القضائية تحت غطاء مقتضيات التحري والتحقيق التي تتضمن مساس صارخا لحقوق الأفراد وحرياتهم الشخصية المكفولة حمايتها دستوريا. فالمشرع تكفل بكافة الأعمال والإجراءات التي تضمن القيام بالمهمة على أكمل وجه ولكنه لم يفكر في الإنسان المهدورة حقوقه بعد أن تتضح براءته، فكان يجدر به أن ينصّ على تعويض يتناسب وحجم الأضرار التي لحقت به مع العلم أن أي تعويض يقدم له لن ينصف حقه.[2]

---

[1]- نجيمي جمال: المرجع السابق، ص ص 443- 444.

[2]- أنظر في ذلك: نصر الدين هنوني ودارين يقدح: الضبطية في القانون الجزائري، دار هومة، الجزائر 2011، الطبعة الثانية، ص 77؛ وكذا تدخل القاضي لوعيل بمحكمة الشراقة، مجلس قضاء البليدة، Débat de la journée ، 2010 de 02 mai، مقال منشور ضمن مجلة: محاربة الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، ملتقى دولي يومي 05- 06 ماي 2010، الجزائر، ص 107.

ب- الرأي المؤيد:

يرى المؤيدون أن الفائدة العلمية والعملية خصوصا لهذه الوسائل يجعل التشريعات تعتمد عليها في سبيل الكشف عن الجريمة والبحث عن المجرمين، بل اعتمد على هذه الوسائل حتى الدول التي تتغنى بحماية حقوق الإنسان، ونادت بضرورة استخدامها الاتفاقيات الدولية في ظل التطورات الخطيرة التي يشهدها الإجرام المنظم وجرائم المخدرات وتبييض الأموال والفساد وغيرها، والجزائر ليست بمنأى عن هذا التطور وفي سبيل الوقاية بكل الطرق المستحدثة عليها تأطير هذه الإجراءات ووضع الآليات اللازمة لتطبيقها، مع إعطاء ضمانات كافية بغية احترام الحريات الفردية وحقوق الإنسان مع جعلها تتم تحت إشراف القضاء وسلطته مع تضييق مجال تطبيقها.[1]

و التعديل الدستوري الجزائري في 2016 نص في المادة 46 على أنه:

1. لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون.
2. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.
3. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.
4. حماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه. [2]

و بإسقاط قانون الإجراءات الجزائية وقانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يمكننا القول أن المشرع عند تقريره لإجراءات حديثة للتحري عن بعض الجرائم ومنها الإلكترونية وهذا لثبوت عدم كفاية الإجراءات التقليدية لمكافحة هذه الجرائم المستحدثة تقول أنه حاول الموازنة بين

---

[1]- عبد الرحمان خلفي: المرجع السابق، ص 70؛ أنظر كذلك: نجيمي جمال، المرجع السابق، ص 446.

[2]- الجريدة الرسمية للجمهورية الديمقراطية الشعبية: قانون رقم 16-01 مؤرخ في 6 مارس سنة 2016، يتضمن التعديل الدستوري، العدد 14، السنة الثالثة والخمسون، الصادرة في 7 مارس سنة 2016، ص 11.

الحفاظ على حق الجماعة في توقيع العقاب وعدم إفلات المجرمين منه وكذا تقريره لضمانات وشروط يجب على الضبطية القضائية اتباعها عند التحري حفاظا على الحرية الفردية إزاء هذه الإجراءات، مما جعل هذه الإجراءات الحديثة تكتسي طابع المشروعية.[1]

فطالما أحاط المشرع الجزائري أساليب التحري الخاصة الممنوحة للضبطية القضائية بضمانات قانونية فهي إجراءات تتسم بالمشروعية وذلك بنصه عليه في الاتفاقيات الدولية والتعديل الدستوري 2016، فلا يمكن للضبطية القضائية أن تقوم بأي إجراء إلا بناءا على إذن مكتوب ومسبب صادر من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، تحت رقابته المباشرة، كما أن هذه الإجراءات لا يمكن الإذن بها إلا إذا اقتضت ضرورات التحري وعدم كفاية إجراءات التحري التقليدية.

[1]- شرف الدين وردة: مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الفكر، العدد الخامس عشر جوان 2017، ص 555.

المبحث الثاني: التحقيق في الجرائم الإلكترونية:

إن التصدي للجرائم الإلكترونية يتطلب التحقيق الفعال والقدرة على جمع الأدلة والإثبات الجنائي، وهذا النهج يتطلب بداية تحديد نموذج تحقيق أمثل، وثانيا الاستجابة للتحديات القانونية التي تعرقل تنفيذ القانون وصولا للتحقيق في الجريمة الإلكترونية وإثباتها. وقد أدركت الدول أهمية تكنولوجيا المعلومات كمفتاح لتحسين أداء الإدارة والأمن على السواء، لذلك أولى المشرع اهتماما بمتابعة إجراءات التحقيق في الجريمة الإلكترونية وحاول سد الثغرات التشريعية وكذا استحداث إجراءات تتناسق وتتناسب مع خصوصية هذه الجرائم وترفع من مستوى فعالية التحقيق في هذه الأخيرة [1]. ومما لا شك فيه أن مرحلة التحقيق مرحلة جد مهمة تساهم بشكل كبير في توجيه الدعوى ومنه النتائج والآثار التي تترتب على، ومع التطور التكنولوجي المستمر والسريع صعبت مواكبته لمعوقات تعترض التحقيق ذلك في جرائم مستحدثة ومجرمين ذو خبرة واحتراف تقني عالي.

و انطلاقا مما سبق سنتعرف على خصائص التحقيق والمحقق في الجرائم الإلكترونية (المطلب الأول) إضافة لإجراءات التحقيق في هذه الجرائم (المطلب الثاني)، وأخيرا معوقات التحقيق (المطلب الثالث).

المطلب الأول: خصائص التحقيق والمحقق في الجرائم الإلكترونية:

يعتمد التحقيق على مميزات خاصة في المحقق تجعله يظهر الحقيقة بكل حيثياتها وفي وقت وجيز وبمهارة عالية ونتائج دقيقة، ومواكبة لحركة الجريمة وتطور أساليب ارتكابها في البيئة الإلكترونية، لم تعد خصائص التحقيق والمحقق هي نفسها السابقة، أو بصيغة أخرى يمكن القول أن التحقيق والمحقق يتغيران كلاهما ليكونا في مستوى متناسب من الفعالية، مع طبيعة الجرائم الإلكترونية المستحدثة ومرتكبيها.

---

[1]- مصطفى عبد الباقي: التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة دراسات علوم الشريعة والقانون، المجلد 45، عدد 4، ملحق 2، 2018، ص 286.

الفرع الأول: خصائص التحقيق:

التحقيق محطة جد مهمة وفاصلة فيما يتعلق بالجريمة الإلكترونية، إذ تعتبر الإجراءات المتخذة خلالها ونتائجها لها الأثر البالغ في مصير الدعوى ومنحى العدالة، فما يتم جمعه من معلومات وأدلة رقمية إلكترونية في المرحلة الموالية لارتكاب الجريمة قد لا يبقى متاحا بعد مرور مدة جد قصيرة على ارتكابها فهي ذات طبيعة تقنية ومسرح إفتراضي خطير يصعب فيه التحكم في الأدلة والحصول عليها والحفاظ عليها ومن ثم إثباتها .

و التحقيق الجنائي عموما هو علم له قواعد ثابتة وراسخة بدونها ما كان التحقيق ليتمتع بتلك الصفة وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي يخضع لها المحقق ويمتثل لها، أما الثانية فتتميز بالمرونة وهنا تبرز خبرة المحقق وفطنته ومهارته في صنع الفارق.[1]

و يعرف التحقيق أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل لكشف الحقيقة وإظهارها.[2]

و عرف أيضا أنه: مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق، طبقا للشروط والأوضاع التي يحددها القانون، بهدف البحث عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقدير لزوم محاكمة المدعى عليه أو عدم لزومها.[3]

و التحقيق في الجريمة الإلكترونية بالخصوص يعرف بأنه: عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل إلكتروني رقمي لتقديمه إلى سلطات التحقيق القضائي في هذه الجرائم لإقامة العدل.[1]

---

[1]- خالد محمود إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 56.

[2]- عمر بن إبراهيم بن حماد العمري: إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، رسالة ماجستير، جامعة نايف العربية، 2007، ص 22.

[3]- عمر بن إبراهيم بن حماد العمري: المرجع السابق، ص 23.

الفرع الثاني: خصائص المحقق:

المحقق هو الشخص القائم بأعمال إجراءات التحقيق الجنائي، أي من عهد له القانون تحري التحقيق في البلاغات والحوادث الجنائية، فيكشف الغموض ليصل إلى معرفة حقيقة الحادث وكشف مرتكبه لتتم محاكمته.[2]

و عرف كذلك بأنه: كل شخص يقوم بأحد أعمال التحقيق، سواء بصورة أصلية أو استثنائية، إذ يقوم بهذه الأعمال بناء على تخويل مباشر من قبل المشرع، أو بصفة غير مباشرة بناءا على ندب أو تكليف من جهة لها الاختصاص الأصيل والأساسي وذلك يكون ضمن نطاق الإجراء الذي خول له القيام به.[3]

أما المحقق في الجرائم الإلكترونية فهو المكلف بالبحث عن الحقيقة في الجريمة الإلكترونية والكشف عن مرتكبيها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم للقضاء، فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق كل حسب اختصاصه.[4]

و ليقوم المحقق بعمله باحترافية وفعالية وتقنية عالية يجب أن تتوفر فيه بعض الخصائص وهي كالتالي:

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والإنترنت والتي تتعلق بالجريمة المرتكبة، ووصول الإخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والإنترنت من الفنيين الذين يعملون على تلك الأجهزة.
- اتباع الإجراءات الصحيحة والمشروعة من اجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة، وتخزينها في الأقراص المعدة لذلك ومنه حذفها.

---

(1)- مصطفى محمود موسى: التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009، ص 156.

(2)- خالد محمود إبراهيم: المرجع السابق، ص 86.

(3)- محمود حماد مرهج الهيتي: أصول البحث والتحقيق الجنائي، دار الكتاب القانونية، القاهرة، مصر، 2014، ص 123.

(4)- مصطفى محمود موسى: المرجع السابق، ص 253.

- تشكيل فريق تحقيق فني، وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش في مسرح الجريمة.
- البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول إلى البرامج المخزنة وكيفية الحصول على الأرقام السرية والشفرات التي تمكنهم من الدخول إلى الحاسوب.
- وضوح خطة عمل مع جميع أعضاء فريق التحقيق، والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها.

الفرع الثالث: السلطة المختصة بالتحقيق في الجزائر:

جدير بالذكر أن المشرع الجزائري قد أسند سلطة التحقيق الابتدائي ووفقا لقواعد الاختصاص المحلي للنيابة العامة وفقا للمادة 37 من قانون الإجراءات الجزائية.[1]

يتضح من خلال النص السابق أن النيابة العامة في التشريع الجزائري تعد هي صاحبة الاختصاص الأصيل بالتحقيق الابتدائي، إما بالنسبة لقاضي التحقيق، وفيما يخص الاختصاص المحلي، فقد نظمته المادة 40 من ق. إ. ج. ج والتي أخذت بالمعايير المنصوص عليها في المادة 37 من ق. إ. ج. ج، وطبقا لنص المادة 67 فإنه لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية.

لكن لما كانت جريمة المساس بأنظمة المعالجة الآلية للمعطيات جريمة قد ترتكب في مكان معين وتكون

آثارها في مكان آخر فأن المشرع بموجب المادة 37 فقرة 2 من ق.إ.ج.ج. أجاز تمديد الاختصاص المحلي لكل من وكيل الجمهورية وكذا قاضي التحقيق بالقطب الجزائي المتخصص إلى دائرة الاختصاص محاكم لأخرى المحددة في التنظيم.[1]

[1]- تنص المادة 37 من ق. إ.ج. ج على ما يلي: « يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشبوهين... »

المطلب الثاني: إجراءات التحقيق في الجرائم الإلكترونية:

في بداية ظهور الإجرام الإلكتروني لم يكن خيار للتصدي له سوى الاعتماد على النصوص الإجرائية الجزائية القائمة، ومما لا شك فيه أن المشرع حين أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الإلكترونية، فإنه يقصد بها الإجراءات التي تثير إشكالات وعقبات عملية تعود لخصوصية هذه الجرائم، كالتفتيش والضبط، المعاينة والخبرة والتي تحتاج لتطوير دون غيرها من الإجراءات (سماع المتهم أو الشهود، الاستجواب والمواجهة) التي لا توجد أية صعوبات في اتخاذها.[2]

الفرع الأول: التفتيش وضبط الأدلة:

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق، المتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات واستثناءا خول للضبطية القضائية في حالات محددة قانونا.[3] بينما الضبط يعتبر الأثر المباشر الذي ينتج عن التفتيش.

أولا: التفتيش في البيئة الإلكترونية:

---

[1]- المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/10 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

[2]- محمد قدري حسن عبد الرحمان: جرائم الاحتيال الإلكتروني، مجلة الفكر الشرطي، عدد 79 صادر عن مركز بحوث الشرطة والقيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص 172.

[3]- من بينها حالة التحقيق في جناية أو جنحة متلبس بها المنصوص عليها في المادة (41) من ق. إ. ج. ج.، وفي التحقيق الابتدائي المنصوص عليه في المواد (63) وما يليها من ق. إ. ج. ج.، أنظر: الأمر رقم (66-155) مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم.

التفتيش إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا.[1]

و باعتبار فالتفتيش عملية إثبات مادي غايته ضبط أدلة مادية خاصة بالجريمة فالظاهر أنه يتنافى مع الطبيعة الغير مادية البرامج وبيانات الحاسب الآلي، فهو مسرح افتراضي ومعطيات غير محسوسة، ولكن في الواقع محل التفتيش هو مستودع تلك البيانات والمعطيات الخاصة، أي الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية كوحدات المعالجة المركزية وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم، ومكونات أخرى منطقية كبرامج النظام الأساسية، البرامج التطبيقية، البيانات المعاجلة آليا، وشبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى محلي ودولي.[2]

في حين أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها يخضع لإجراءات التفتيش المألوفة، لأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد فيه ما إذا كان عاما أو خاصا [3]. فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكمه، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاتها وبالإجراءات والضمانات المقررة قانونا في التشريعات المختلفة لذلك ففي القانون الجزائري تشترط المواد من (44 إلى 47) من ق. إ. ج. للقيام بإجراء تفتيش مسكن في الجرائم

---

[1]- عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، دار الفكر الجامعي، الإسكندرية، 2006، ص 192.

[2]- علي محمود علي محمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 إلى 28 أفريل 2003، ص 135.

[3]- عادل عبد الله خميس المعمري: التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد 22 عدد 86، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، 2013، ص 260.

المتلبس بها، الحصول مسبقا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار بهذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش، على أن يتم التفتيش نهارا في الفترة الممتدة من الخامسة إلى الثامنة مساءا وبحضور صاحب المسكن أو ممثله وإن تعذر ذلك استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته.[1]

و منه فتفتيش المكونات المادية لجهاز الحاسب وملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير آية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، كمراعاة وقت التفتيش، الإذن بالتفتيش، الأشخاص القائمين بالتفتيش، والأشخاص المطلوب حضورهم عند التفتيش، مع مراعاة الاختصاص المكاني وعدم فض الأوراق المحرزة. كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الإلكترونية دون الحاجة إلى أن تكون الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى.[2]

أما بالنسبة للمكونات الغير مادية أي المنطقية والمعطيات المعلوماتية للحاسب، فقد استحدث المشرع الجزائري نصوصا قانونية أجاز تفتيشها ومن بينهم، المادة الخامسة من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والمادة الرابعة من هذا القانون، الدخول بغرض التفتيش ولو

---

[1]- تجدر الإشارة إلى أنه بعد التعديل الذي ألحقه المشرع على ق. إ. ج. ج. بالقانون 22/06 المؤرخ في ديسمبر 2006 استغنى في الفقرة الأخيرة من المادة 45 والفقرة الثانية من المادة 47 والفقرة الثالثة من المادة 64 عن تطبيق كل الضمانات المقررة لتفتيش المساكن عندما يتعلق الأمر بالتفتيش في الجرائم الإلكترونية وأصبح من الممكن التفتيش في هذه الجرائم في أي ساعة من الليل أو النهار ودون حاجة لرضائه ولا لحضوره أثناء التفتيش.

[2]- فايز محمد راجح غلاب: الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة نيل شهادة الدكتوراه في القانون، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق جامعة الجزائر 1، الجزائر،2011 ، ص 309.

عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية.[1]

ثانيا: ضبط الأدلة في الجرائم الإلكترونية:

و يقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها وعن مرتكبيها، ووضعها في أحراز مختومة ولتقدم إلى الجهة القضائية المختصة كدليل إثبات [2]. وتحصيل الأدلة في الجرائم الإلكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، الأشرطة الممغنطة، الطباعة، البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الإنترنت مثل المودم، ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية [3]. وقد يرتبط الدليل الإلكتروني بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الإلكترونية التي يجري تبادلها عبر شبكة الإنترنت والبريد الإلكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيرا حول مدى إمكانية ضبطها وفقا لقواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية [4]، وتبني في القانون رقم 09-4 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 0/05 الفرع الأول: التفتيش وضبط الأدلة.

---

[1]- أنظر المادة 05 من القانون رقم 09-5 المؤرخ في 14 شعبان 1430 هـ الموافق ل 05 عشت سنة 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر. عدد 47، صادر بتاريخ 25 شعبان 1430 هـ الموافق لـ 16 أوت 2009.

[2]- خالد عباد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان،2011، ص 170.

[3]- لتفاصيل أكثر، أنظر المواد (45 و46 و84) من قانون الإجراءات الجزائية الجزائري.

[4]- عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت دار الفكر الجامعي، الإسكندرية، 2006، ص218.

2009/8، إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها تحت عنوان "حجز المعطيات المعلوماتية" وخصص لها عددا من المواد التي تذكرها على النحو التالي:

– نصت المادة 06 على أنه: "عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات محزنة مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية..."

– أضافت المادة 07 فيما يخص الحجز عن طريق منع الوصول إلى المعطيات بأنه "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة ".

– أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت المادة 08 على أنه "يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك ".[1]

[1]– أنظر المواد (6، 7، 8) من القانون رقم 09– 04 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

بالإضافة إلى هذه التدابير وضع المشرع الجزائري على عاتق مقدمي خدمات الإنترنت جملة من الالتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش والضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحقيق.[1]

الفرع الثاني: المعاينة وندب الخبراء:

تعتبر المعاينة من أهم إجراءات التحقيق نظرا لما توفره من اكلة إثبات وتزداد أهميتها إذا تعلق الأمر بالجرائم الإلكترونية، إضافة للخبرة التقنية ودورها في تقويم الإثبات الرقمي بحيث أصبح من الضروري الاستناد إليها في هذا المجال بالتحديد تحقيقا لمبدأ التخصص.

أولا: المعاينة:

وهي إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في كشف الحقيقة [2]، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقيقة، أو بناء على طلب من الخصوم. والأصل أن تجرى المعاينة بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة. [3]

و تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الإلكترونية كجرائم الاعتداء على

---

[1]- أحمد مسعود مريم: آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة ماجستير في القانون الجنائي ، جامعة قاصدي مرباح، ورقلة،2013، ص 103.

[2]- فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق بجامعة القاهرة، 2012، ص 266.

[3]- محمد أبو العلاء عقيدة: " التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية " ص 07، مقال منشور في الموقع التالي: www.osamabahar.com

الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة [1]. أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الإنترنت فيكون الانتقال للمعاينة هذا افتراضيا أو إلكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الإلكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الإنترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الإنترنت أو إحدى المقرات المزودة بخدمات الإنترنت [2].

ثانيا: ندب الخبراء في الجرائم الإلكترونية:

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجا إليه القضاء وسلطات التحقيق على حد سواء، وذلك كل ما استعصى عليهم الأمر، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الإلكترونية، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الإلكترونيات.[3]

و الخبير في الجريمة الإلكترونية هو الفني المتخصص وصاحب الخبرة في التقنية الإلكترونية وشبكاتها، والذي يكون قد رأى أو سمع أو أدرك بحواسه معلومات هامة لازمة

---

[1]- ياسر محمد الكومي، محمود أبو حطب: الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف، الإسكندرية، 2014، ص 243.

[2]- وليد عاكوم: التحقيق في جرائم الحاسوب، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منعقد بإمارة دبي في الفترة الممتدة من 26 إلى 28 أفريل 2003.

[3]- صغير يوسف: الجريمة المرتكبة عبر الإنترنت، المرجع السابق، ص 87.

للدخول في نظام المعالجة الآلية الرقمية للبيانات، إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الإلكتروني داخله ويتمثل الخبراء الإلكترونيون في ما يلي: [1]

- المبرمجون.
- المحلل هو الشخص الذي يضع خطوات العمل ويجمع بيانات نظام معين.
- مهندس الصيانة والاتصالات.
- مشغل الحاسوب الآلي وشبكاته.
- مدير النظام المعلوماتي.

و باعتبار الخبرة من إجراءات التحقيق فهي تخضع لضوابط قانونية وأخرى فنية، يتعلق الأمر بأن يتم اختيار الخبير من جدول الخبراء الذي تعده المجالس القضائية بعد استطلاع رأي النيابة، هذا كأصل وكاستثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء يجوز لجهات التحقيق أن تختار بقرار مسبب خبراء ليسو مقيدين في أي من هذه الجدأول [2]. وأوجب المشرع الجزائري في المادة 145 من ق. إ. ج. ج. على الخبير في كل مرة أن يختار فيها وقبل أداء مهامه أن يحلف اليمين القانونية، غير أنه إذا كان خبيرا مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى مادام قد أدى اليمين عند تقييده بالجدول أول مرة.[3]

أما عن الضوابط المتعلقة بالخبرة، فتتمثل في التزام الخبير بالقيام بأعمال الخبرة بنفسه دون أن يكلف بها غيره ويتقيد بالمهام المنوطة به والمحددة في أمر التعيين على أن يتولي

---

[1]- مصطفى محمود موسى: المرجع السابق، ص 172.

[2]- أنظر: نص المادة 144 من قانون الإجراءات الجزائية.

[3]- عبد الناصر محمد محمود وعبيد سيف سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، بحث مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي والمنعقد بالرياض في الفترة الممتدة بين 12- 14/ 11/ 2007، ص 24.

مهامه تحت رقابة القاضي الذي أمر بإجراء الخبرة ولا يستلزم ذلك حضوره فعلا أثناء أداء أعماله، بل يكفي أن يبقى على اتصال مستمر معه وإحاطته علما بكل المستجدات التي تطرأ بعمله، على اعتبار الخبير ليس سوى مساعد فني للقاضي.[1]

المطلب الثالث: معوقات التحقيق في الجرائم الإلكترونية:

هناك العديد من المشاكل التي تؤثر على عملية التحقيق نظرا للخصوصية والطبيعة التي انفردت بها الجرائم الإلكترونية عن غيرها من الجرائم التقليدية. فالجرائم المستحدثة لا تعترف بالحدود الجغرافية مما يثير عدة عقبات فعلية خاصة مسألة تنازع الاختصاص بين الدول في مسألة التحقيق (الفرع الأول)، إضافة للقصور التشريعي والصعوبات المتعلقة بالشق الميداني (الفرع الثاني).

الفرع الأول: إشكالية تنازع الاختصاص بالتحقيق في الجرائم الإلكترونية:

من بين أكبر التحديات التي تواجهها عملية التحقيق في الجرائم الإلكترونية هو موضوع تنازع الاختصاص، لاتسام هذه الأخيرة بالبعد الدولي وطابعها المتخطي لحدود الدولة الواحدة إضافة لارتباط سلوكها الإجرامي بالعالم الافتراضي والرقمي.

ترتبط الجرائم الإلكترونية بأكثر من ولاية قضائية ويجتمع فيها أكثر من معيار واحد من معايير إسناد الاختصاص مما يؤدي إلى تنازع ايجابي بين عدة جهات قضائية.[2]

و وفقا لمبدأ الإقليمية ينعقد الاختصاص للقضاء الوطني كما في حالة نشر الصور الإباحية أو العبارات التي تخص على الكراهية العنصرية المنتشرة على شبكة الإنترنت بصرف النظر عن الدولة التي صدر منها هذا العمل الإجرامي طالما يمكن أن تتحقق النتيجة الإجرامية على الإقليم الوطني، كما يختص القضاء الوطني وسلطة التحقيق وفقا

---

[1]– QUEMENER Myriam: CHARPENEL Yves, Cybercriminallité- Droit Pénal Appliqué, édition Economica, Paris, 2010, p. 183.

[2]– CHAWKI Mouhammed: Combattre le Cyber Criminalité, Edition de Saint Amans, Paris, 2008, p. 318.

لمبدأ إقليمية النص الجنائي بالجرائم الإلكترونية المرتكبة على السفن والطائرات الوطنية بصرف النظر عن جنسية مرتكب الجريمة أو المجني عليه فيها.[1]

و قد يتجاوز مدى هذه الجرائم حدود الدولة ويتجزأ ركنها المادي ويتوزع على أكثر من مكان، إذ يمكن أن يقع السلوك في مكان وتتحقق النتيجة في مكان آخر، ولتفاقم هذه المسألة باعتبارها أدت لوجود صعوبة فعلية أمام التصدي لهذا النوع من الجرائم، تدخل الفقه الجنائي وقدم حلا لهذه المشكلة والمتمثلة في إعطاء أولوية النظر في الجريمة الإلكترونية للدولة التي تتوفر على أحد معايير تحديد الاختصاص الذي يكون الأكثر فعالية لملاحقة الجرمين.

أما المشرع الجزائري فقد اكتفى في هذا الشأن بالفقرة الثانية من نص المادة 15 من القانون 09- 04 والتي تنص: «تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الأعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني ».

و أمام الكم الهائل للإغراق المعلوماتي بكل ما فيه من سلبيات تهدد الهوية الوطنية والنظام العام والآداب العامة يمكن القول أن مبادرة المشرع الجزائري لا ترقى للمستوى المطلوب لمواجهة هذا النوع من الجرائم، حيث يظهر أن المشرع أعاد صياغة نص المادة 588 من ق. إ. ج. ج. والتي نصت على مبدإ الاختصاص العيني، ولم يأتي بأية إضافة جديدة إلى قواعد الاختصاص.[2]

---

[1]- محمد كمال شاهين: مرجع سابق، ص 190.

[2]- حيمي سيدي محمد: معوقات التحقيق في الجرائم الإلكترونية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة أبو بكر بلقايد- تلمسان، المجلد السادس، العدد الأول، سنة 2022، ص 1742.

الفرع الثاني: عدم مواكبة النصوص الجزائية لخصوصية الجرائم الإلكترونية:

أصبحت تقريبا جميع المعاملات والإجراءات إلكترونية، الأمر الذي يحتم توضيح السلوكات الإجرامية الإلكترونية الغير مشروعة وهذا عن طريق تنظيم تشريعي يستند إلى مبدأ المشروعية، ولكن في الواقع غياب التنظيم التشريعي في هذا الجانب يجعل من المحقق غير قادر على مواجهة هذا الإجرام المستحدث إذ أنه يباشر في إجراءات باطلة تتعارض ومبدأ المشروعية لغياب نص يحكم تلك الإجراءات بالرغم من فعاليتها ووجوب القيام بها للكشف عن الحقيقة ومعرفة مرتكبي الجريمة.[1]

و منه فالنصوص الجنائية القائمة عاجزة عن التطبيق على الجرائم الإلكترونية، فالنصوص التقليدية قد وضعت لتطبق وفق معايير معينة، في حين أن محل الجريمة الإلكترونية هي معطيات ذات طبيعة معنوية، كما أن هناك العديد من الأفعال الجديدة خاصة في الدول مرتبطة باستعمال الإنترنت وغير مجرمة وفقا للقواعد العقابية التقليدية ولا تعتمد إليها لمواجهتها رغم تهديدها للمصالح العامة. فالدخول مثلا لنظام حاسب مملوك للغير وسرقة المعلومات منه لا يعد جريمة بمفهوم القوانين التقليدية إن السرقة لا ترد إلا على المال المنقول، وهذه الصفة لم تثبت بعد للمعلومات كونها تعتبر أفكارا معنوية بحتة، زيادة على ذلك فالسرقة بالمفهوم التقليدي يعني أخذ مال الغير بدون وجه حق في حين أن اختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها لذا فإنها لا يحميها المقرر في جرائم الأموال.[2]

و لم يتوقف عند قصور النصوص العقابية في مواجهة الجرائم الإلكترونية بل تعدى إلى القوانين الإجرائية، إذ أن معظم إجراءات التحقيق والمتابعة الجزائية التي تتضمنها

---

[1]- خالد عباد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان- الأردن، الطبعة الأولى، 2011، ص 220.

[2]- غنام محمد غنام: عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات في الفترة الممتدة من 01 إلى 03 ماي 2003، ص 325.

التشريعات التقليدية لا تتلاءم مع طبيعة هذه الجرائم وأحيانا تتعارض حتى مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها المعلومات أو البيانات بشتى أنواعها، وهذا الأمر يشكل عقبة كبيرة أمام رجال الضبطية القضائية من عدة نواحي.

و في ذات السياق فجهات التحقيق والسلطات القائمة عليه لا تتناسب مع الإجرام الإلكتروني المتطور، وهذا راجع لقلة خبرة المحققين، حيث أن هذه الجرائم تقع على تقنية تكنولوجية وهذه التقنية دائمة التطور وبشكل سريع، ومنه فالمحقق يجب أن يكون على دراية بالغة بالحاسوب والمعلوماتية، إضافة إلى أن التحقيق في هذه الجرائم يحتاج إلى تكوين هؤلاء المحققين الأمر الذي يحتاج التنظيم تشريعي فعال يعدل ويكيف أجهزة التحقيق في هذا النوع من الجرائم.

الفرع الثالث: الصعوبات المتعلقة بالشق الميداني:

أولا: صعوبة الحصول على الدليل وإخفائه:

نظرا لوقوع الجريمة في بيئة رقمية، يواجه المحققون صعوبات في استخراج الدليل الرقمي فهو دليل غير مرئي، فهو عبارة عن نبضات مغناطيسية تشكل بيانات رقمية في العالم الافتراضي، ومنه فعدم رؤية الدليل الرقمي يشكل العديد من المعوقات والصعوبات من خلال جمعه وتحليله مما يستوجب أن يكون المحققون في مستوى تقني عالي للتعامل هذا النوع من الأدلة.[1]

و تمثل صعوبة الحصول على الدليل الرقمي أحد أبرز الصعوبات فكثيرا ما يلجأ مرتكبو الجريمة الإلكترونية إلى أهم الوسائل لعرقلة جميع أدلة الإدانة، ومن بين أهم هذه الوسائل نجد مسألة استخدام التشفير أو استخدامهم كلمة السر أو القيام بإخفاء هويتهم، وخاصة عند استخدامهم لشبكة الإنترنت وذلك بالاستعانة بالبرامج والتطبيقات التي تعمل على طمس هويتهم في شبكة الإنترنت.

[1]- عماد بلغيث: صعوبات التحقيق في الجرائم الإلكترونية مجلة الرسالة للدراسة والبحوث الإنسانية، مخبر سوسيولوجية جودة الخدمة العمومية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد السادس، العدد الثالث، سبتمبر 2021، ص 79.

يتميز المجرم الإلكتروني بالذكاء والإتقان لعملهم الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك يتمكن من إخفاء الأفعال غير المشروعة التي يقوم بها أثناء تشغيله للوسائل الإلكترونية ويستخدم في ذلك التلاعب غير المرئي في النبضات والذبذبات الإلكترونية التي يتم عن طريقها تسجيل البيانات.[1]

ثانيا: العزوف عن التبليغ بوقوع الجريمة الإلكترونية وصعوبة اكتشاف مرتكبيها:

غالبا ما يتكتم المجني عليه ولا يبلغ السلطات المختصة عن وقوع الجريمة الإلكترونية بعد اكتشافها، ويظهر هذا جليا لدى المؤسسات التجارية والمالية أو العمومية التي لا تكشف عن الاعتداءات الإلكترونية التي تتعرض لها حرصا على سمعتها وثقة متعامليها في كفاءتها وحماية مصالحهم.[2]

و للتقليل من ظاهرة التكتم عن الجرائم الإلكترونية، عمدت بعض الدول إلى فرض التزامات على عاتق جهات المجني عليها بالإبلاغ عن هذه الجرائم بمجرد علمهن بوقوعها، وجعلت أي تقصير أو إخلال بهذا الالتزام يعرض صاحبه إلى عقوبات جزائية، ولكن هذا الحل تم انتقاده بشدة، فليس من المقبول تحويل المجني عليه إلى مجرم يتم معاقبته لمجرد عدم تبليغه عن كونه ضحية لجريمة إلكترونية، في حين يبقى الجرم الحقيقي دون عقاب.[3]

إضافة لأكثر صعوبة تواجهها السلطات المختصة في مكافحة الجرائم الإلكترونية هو أن المجرم المعلوماتي يعمل بذكاء على إخفاء هويته للحيلولة دون تعقبه وكشف هويته وذلك

---

[1]- المرجع نفسه: ص 79.

[2]- هشام محمد فريد رستم: "الجرائم المعلوماتية- أصول التحقيق الجنائي الفني واقتراح آلية عربية موحدة للتدريب التخصصي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، من 1- 3 ماي 2000، ص ص 435- 436.

[3]- هشام محمد فريد رستم: المرجع السابق، ص 438.

حتى تظل أعمالهم الإجرامية بعيدة كل البعد عن السلطات المعنية بمكافحة هذا النوع من الجرائم.[1]

[1]- عماد بلغيث: المرجع السابق، ص 81.

المبحث الثالث: إجراءات المحاكمة والتعاون الدولي في الجرائم الإلكترونية:

كمرحلة إجرائية مهمة موالية لما سبق وتطرقنا له في إطار مواجهة الجرائم الإلكترونية، فالدعوى تمر على جهاز قضائي من أجل محاكمة مرتكبي تلك الجرائم وتوقيع العقاب المستحق تحقيقا للردع في ظل العدالة والموازنة بين حقوق الأفراد وحق المجتمع في توقيع العقاب. وللتعرف على هذه المرحلة الإجرائية المهمة وجب التعرف على الجهات التي تتولى الحكم في هذه الجرائم (المطلب الأول)، وكما ذكرنا سابقا فالجهود الداخلية في مكافحة هذه الجرائم ليست في غنى عن التعاون الدولي في هذا المجال (المطلب الثاني).[1]

المطلب الأول: المحاكمة في الجرائم الإلكترونية:

الفرع الأول: قواعد الاختصاص جهة الحكم في الجريمة الإلكترونية:

أولا: الاختصاص المحلي:

طبقا لنص المادة 38 من ق. إ. ج. يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط في أو المكان إقامة المتهم أو مكان ضبط كما نصت أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة اختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران.

و في نطاق الجرائم الإلكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان آخر، فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، وتعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الإنترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها.

---

(1)_

و متى كانت الجريمة الإلكترونية، أيا كان نوعها، فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيات الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.[1]

ثانيا: الاختصاص النوعي:

و يتحدد الاختصاص النوعي للمحكمة الفصل في القضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من ق. إ. ج. كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الإستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 من ق. إ. ج.

و نظرا للطبيعة التقنية المعقدة للجرائم الإلكترونية خصها المشرع بإجراءات خاصة، مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبيض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف إذا جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى وهذا ما نصت عليه المواد 37، 40 والمادة 329 من ق. إ.ج. ج، إثر التعديل الذي جاء به القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من

[1]- المرسوم التنفيذي رقم 06-348 المؤرخ في أكتوبر 2006 المتضمن الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج. ر.، عدد 63، ص29.

الجزائر العاصمة، قسنطينة، وهران، ورقلة.[1]

الفرع الثاني: إجراءات المحاكمة:

بخصوص تشكيلة المحكمة فتختلف بحسب قسم ونوع قسم الجنح خاصة بالجريمة المعلوماتية على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو مساعديه.

أما الغرفة الجزائية على مستوى المجلس قضائي فتتشكل من رئيس غرفة ومستشارين اثنين بالإضافة إلى كاتب ضبط وبحضور النائب العام أو أحد مساعديه.

أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها.[2]

و تستهل المحكمة جلستها بالإعلان عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها، وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها **إلى** أقرب جلسة، وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر 6 المستحدثة بموجب الأمر 15-02 المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية تتخذ المحكمة إحدى الإجراءات التالية: فإما تترك المتهم حرا، أو تخضعه لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 من ق. إ.ج. ج.، أو وضع المتهم في المؤقت، وهذه التدابير لا تقبل الاستئناف.

---

[1]- القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية، جريدة عدد 71، ص 4.

[2]- عبد الرحمان خلفي: المرجع السابق، ص 321.

و إذا حبس المتهم من طرق قاضي التحقيق عن طريق الحبس المؤقت بموجب إجراءات المثول الفوري فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بحقه في اختيار محام للدفاع عنه. ومن ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي وبعدها يقوم القاضي بسماع الشهود وبعد الانتهاء من التحقيق تعطى كلمة للطرف دون المطالبة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساتها في الشق الجزائي وفقط، وفي الأخير يقوم دفاع المتهم بتقديم مرافعته، ويكون بعدها للنيابة العامة والمدعي حق الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه. ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو لأجل متعلق بالحكم.

المطلب الثاني: التعاون الدولي في مجال مكافحة الجريمة المعلوماتية:

ينبثق التعاون القضائي من التعاون التشريعي، ومنه فعالية الملاحقة القضائية في الجرائم الإلكترونية إما عن طريق مساعدة من سلطات دولة منشأ الجريمة، أو من سلطات الدولة التي عبر من خلالها السلوك الإجرامي للوصول إلى الهدف أو النتيجة، أو حيث توجد أدلة الجريمة. كما أن الأحكام والقرارات التي تصدر من الهيئات القضائية بالنسبة لهذه الجرائم لا تسري على إقليم دولة أخرى ولا ترتب أي أثر قانوني ما لم تعترف بها هذه الأخيرة، وعليه فلا تتأتي هذه الأمور إلا في إطار التعاون القضائي الدولي المتبادل.

الفرع الأول: المساعدة القضائية الدولية:

و تتم غالبا بمقتضى اتفاقيات ومعاهدات دولية تنطوي على تبادل السلطات القضائية المختصة المعلومات لمعاقبة وإلقاء القبض على مرتكبي الجريمة الإلكترونية ألا وهو المجرم الإلكتروني وذلك نظر لكون الجريمة الإلكترونية عابرة للحدود.

من أجل ذلك ولمواجهة أخطارها واتخاذ تدابير وإجراءات تحفظية لجمع الأدلة الإلكترونية في إطار مبدأ المعاملة بالمثل على تقديم المساعدة القضائية [1]. وهي تبادل السلطات المختصة المعلومات واتخاذ إجراءات تحفظية لجمع الأدلة الإلكترونية الخاصة بجرائم الماسة بالمعطيات في الأحوال العادية، وفي الحالة الغير عادية يتم استعمال وسائل الاتصال السريعة كالفاكس وغيرها من الوسائل الإلكترونية وذلك لما توفره هذه الوسائل من شروط أمن كافية لتتأكد من صمتها.[2]

و حتى تكون طلبات المساعدة القضائية الدولية المتبادلة صحيحة، لابد من التقيد والالتزام بقيود قانونية، تتمثل في:

- ألا يكون في تنفيذ طلبات المساعدة مساس بالسيادة الوطنية أو النظام العام.
- ضرورة المحافظة على سرية المعلومات المبلغة.
- عدم استعمال هذه المعلومات في غير موضع في الطلب.[3]

الفرع الثاني: تسليم المجرمين:

و هي العملية التي في الغالب يكون منصوصا عليها في الاتفاقيات والمعاهدات الدولية وقد نص المشرع الجزائري في القانون 04/09 على اختصاص السلطات القضائية الجزائية الجزائرية إذا كان مرتكب الجريمة الماسة بالمعطيات أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني، لكنه أغفل على تسليم المجرمين في حالة فرار المجرم الإلكتروني، غير أنه وطبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات اشترطت على ضرورة وجود اتفاقية من أجل تسليم المجرمين في هذا النوع من الجرائم واستبعدت وجود اتفاقيات تسليم بين الدول الأطراف في هذه الاتفاقية [4].

---

[1]- أنظر: المادة 02/16 قانون 04/09.

[2]- أنظر: المادة 17 من القانون 04/09.

[3]- أنظر: المادة 18 الفقرة الأخيرة من قانون 04/09.

[4]- أنظر: البند 03 و04 من المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

إلا أن هذا التسليم تحكمه مجموعة من الإجراءات الواجب إتباعها من قبل كل دولة طرف طلبت التسليم وهي:

– التجريم المزدوج: ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبة التسليم، وكذلك في تشريع الدولة المطلوب إليها التسليم أيا كانت صورة العقاب.[1]

– اختصاص الدولة طالبة التسليم (مختصة) بملاحقة الشخص المطلوب تسليمه من جهة، ومن جهة أخرى يجب أن يكون الفعل المعاقب عليه طبقا للقانون الجزائري.[2]

– عدم جواز تسليم الرعايا ممنوحي اللجوء السياسي.[3]

و يتم التسليم بتقديم طلب التسليم ويكون كتابة إلا في حالة الاستعجال مع إرفاق طلب التسليم بمجموعة من المستندات الدالة على ارتكاب الشخص الجرم محل التسليم.[4]

---

[1]– أنظر: المادة 2/667 من ق. إ. ج. ج.

[2]– أمير فرج يوسف: الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية بمكافحتها، الاسكندرية ،ومكتبة الوفاء القانونية ، 2011، ص 54– 55.

[3]– هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والتطبيق، الطبعة الاولى ،دار النهضة العربية ،القاهرة ، 2006، ص 281.

[4]– سليمان عبد المنعم: الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، د. ط.، دار الجامعة الجديدة، 2007، ص220.

خاتمة

الخاتمة :

تغيرت معايير التطور والنمو واصبحت تقاس تبعا لمدى مواكبة الشعوب للتطور التكنولوجي ، اذ اصبحت التقنيات الحديثة ضرورية في جميع مجالات الحياة ولازمة في جميع المؤسسات باختلافها ، الأمر الذي سهل القيام بالعديد من الوظائف في وقت وجهد وكلفة ومسافة أقل من السابق ، ولكن للاسف بالرغم من المميزات الكثيرة والقيّمة التي استفادت البشرية منها ، إلا أن الإستخدام الغير الجيد لها جعل منها مصدرا للعديد من المشاكل التي باتت تؤثر بشكل خطير على الدول والمجتمعات في مختلف الأصعدة ، اذ تعدى ذلك من الضرر بمصالح الأفراد للضرر بمصالح الدولة وأمنها واستقرارها حتى أنه يمس أحيانا تها الحساسة . وفي وقت وجيز وجدت أغلب التشريعات نفسها في مواجهة غير متكافئة مع الجرائم الالكترونية ، فلم يعد الاجرام والمجرم التقليدي يأخذ نفس الصور الالمعهودة ، بل بدوره شهد تغيرات وتطورات غيرت كل المفاهيم ومن جهة اخرى اصبحت سبل مكافحة هذه الجرائم كذلك غير مجدية ولا ملائمة للتصدي للنشاطات الاجرامية الحديثة ومرتكبيها . فالجريمة الالكترونية جريمة مستحدثة تتمتع بطبيعة قانونية مختلفة ومميزة عن الجريمة التقليدية، الأمر الذي أجبر أغلب التشريعات على الإجتهاد في ايجاد سياسة ناجعة لمكافحة هذا الاجرام المستحدث ، والمشرع الجزائري بدوره يحاول الاجتهاد في هذا المجال، ويظهر ذلك جليا من حيث تبنيه سياسة مزدوجة في مواجهة الاجرام المستحدث، بتعديله للقوانين العامة وكذا الخاصة ، وحرصا منه على تفادي افلات المجرم الالكتروني من المتابعة والعقاب بادر المشرع لاستحداث قواعد اجرائية تتناسب مع البيئة الرقمية وذلك في مختلف مراحل الدعوى وهذا ما دعت اليه الضرورة العملية ، فالضبط والتحقيق في العالم الافتراضي يختلف كل الاختلاف عن العالم الحقيقي ، اذ لا وجود للماديات بل مجرد معطيات رقمية الكترونية ، ومنه فالأساليب المستحدثة خلال جميع مراجل الدعوى تتوافق لحد ما مع طبيعة هذه السلوكات الالكترونية المجرمة ومرتكبيها . والجدير بالملاحظة أنه رغم كل الجهود والتعديلات والاستحداثات على المستويين الموضوعي والاجرائي وما سبق ذكره ، يبقى تحقيق الهدف المرجو من ذلك بعيد الأمد، فالجرائم الالكترونية تتطور بشكل مستمر وسريع مما يزيد من خطورتها على أمن وسلامة الأفراد أو المؤسسات أو الحكومات، اضافة للطابع العالمي العابر للحدود الذي يصعب مهمة التحكم في هذه الجرائم وتأطيرها بشكل صحيح وفعال يحد أو على الأقل يقلل من انتشارها .وأصبح من الضروري خطوة خطوات

مدروسة لسد الفراغ التشريعي في هذا المجال لاسيما ربطه بالواقع العلمي، مع ايجاد حلول للمعوقات الاجرائية التي تحول دون التصدي لها على المستوى الميداني وطنيا ودوليا ، ولن يتحقق هذا سوى بوضع مخطط محكم وفعال يقوم عليه مختصون يبلغون مستوى لا بأس به من الاحترافية والتخصص ويعتمدون في ذلك على تجارب ودول سبقتنا في هذا المجال بأشواط معتبرة ، ومراعين في ذلك طبيعة مجتمعنا وأجهزتنا القائمة على مكافحة هذه الجرائم ، فالعبرة بالاصلاح الفعلي والناجع والاستفادة من خبرة غيرنا في مكافحتهم لهذا الاجرام المستحدث بطريقة عقلانية مرنة لا تزيد من الاشكالات التطبيقية ولا تتعارض مع سياستنا واحداثياتها .ومن النتائج المستخلصة في دراستنا هذه :

_المشرع الجزائري تصدى للجرائم الالكترونية بتعديله الجوانب الموضوعية والاجرائية لهذه الاخيرة من جهة ، واستحدث قوانين اخرى خاصة من جهة اخرى .

_فشل المشرع نسبيا في مواجهة الجرائم الإلكترونية فقد طغت طبيعتها الخاصة على محاولاته ويمكن القول أنه لغاية الآن لا تزال مختلف الأجهزة المكلفة بمتابعة هذه الجرائم تتخبط في إشكالات تطبيقية وتحاول ايجاء حلول مشروعة في غياب النص الصريح الذي يقيدها أو يمنحها اتخاذ الاجراءات المناسبة لمواجهة هذه الجرائم .

_ يظهر جليا نقصر خبرة السلطة القائمة على مكافحة هذه الجرائم على المستوى الداخلي وحتى الخارجي ، فالجزائر لوحدها وبالإمكانيات المحدودة لا يمكزها مواجهة هذا الاجرام المستحدث ،فالاشكالية القائمة منذ الازل إما عدم نجاعة وفعالية السياسة التي تتبناها الجزائر في مكافحة مثل هذه الظواهر الإجرامية ، أو عدم وجود الآليات الحقيقية والميدانية المشروعة لتنفيذ وتطبيق تلك السياسة بشكل إحترافي يضمن تحقيق الهدف المرجو .

ونقدم بعض التوصيات لتخطي العقبات الموضحه سابقا :

- ضرورة الإلتزام بحماية الحقوق المكفولة دستوريا وعدم التهوان والإستخفاف والتماطل في تعديل وإستحداث نصوص قانونية توسع من دائرة تجريم النشاطات الإلكترونية .
- ضرورة التركيز على تحقيق هدف الردع بنوعيه ، فالمواجهة الحقيقية تكون نتيجها إما الحد من هذه الجرائم أو على الأقل التقليل منها ،ولكن في الواقع نحن نسجل تزايد مستمر لهذه الظاهرة ،ببساطة العقوبات المقررة لهذا النوع من الجرائم ينبغي أن

تتناسب وخطورتها فهي تمس بحقوق خاصة وعامة وأثرها بالغ الخطورة على جميع الاصعدة .

- -من الضروري وجود نصوص قانونية توضح حدود سلطات البحث والتحري أثناء ادائهم لمهامهم فهذا الجانب جد مهم ، اذ من غير المنطقي أن ننادي بحماية الحياة الخاصة للأفراد وأثناء تحقيق ذلك نسلب هذا الحق للكثير من الاشخاص بداعي البحث عن الحقيقة ، يجب على المشرع تكوين الاجهزة المخول لها التحري والتحقيق ليقومو بعملهم باحترافية دون تسجيل تجاوزات وتعسف من قبلهم في ظل غياب نص صريح ودقيق في هذا الخصوص .
- من واجب السلطة المعنية أن تمارس وظيفتها الوقائية التوجيهة القبلية ، والتي تساهم في توعية الأفراد بحقوقهم وواجباتهم وكيفية التعامل الصحيح مع التقنيات التي بين أيديهم ، ومن جهة أخرى يجب خلق فكر قانوني وإرجاع الثقة في العدالة والقانون ،ليتم التبليغ عن هذه الجرائم فور وقوعها وكذا المساهمة في الكشف عنها وعن مرتكبيها .
- تعزيز التعاون مع وسائل الإعلام كونها تؤثر بشكل مباشر وكبير في افكار المجتمع بل يمكن القول أنها يمكن أن تساهم بشكل كبير في تحقيق الكثير من الاهداف التي يسعى إليها المشرع ولكن بطريقة أخرى .
- يجب الانفتاح على المجتمع الدولي وتخصيص هيئات ومراقبة عملها لتاتي بحلول لهذه الظاهرة وترفع من مستوى الإحترافية والدقة والنجاعة في التعامل مع المعطيات الرقمية في العالم الإفتراضي.

قائمة المصادر والمراجع

قائمة المراجع:

أولا: النصوص القانونية .

- 1القوانين :

1- القانون 04-14المؤرخ في 10نوفمبر 2004المعدل والمتمم للأمر 155/66المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية العدد 71، سنة 2004 .

2-القانون رقم 04-15المؤرخ في 10نوفمبر 2004المعدل والمتمم للأمر 66-156مؤرخ في 08-06-1966المتضمن قانون العقوبات ،الجريدة الرسمية العدد 71، سنة 2004 .

3- القانون رقم 06-22المؤرخ في 20ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155المؤرخ في 8يونيو سنة 1966والمتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية العدد 84، سنة 2006 .

4- القانون رقم 09-04المؤرخ في 5غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، الجريدة الرسمية العدد 47، سنة 2009 .

- 5 القانون رقم01-16 مؤرخ في 6 مارس سنة 2016، يتضمن التعديل الدستوري ، الجريدة الرسمية العدد 14، سنة 2016 .

-1الأوامر :

1- الأمر رقم 66-155مؤرخ في 8يونيو سنة 1966يتضمن قانون الاجراءات الجزائية ،معدل ومتمم بالقانون رقم 18-13مؤرخ في 11يوليو سنة 2018 .

-2المراسيم :

1 -المرسوم الرئاسي رقم 15-261المؤرخ في 8أكتوبر 2015المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، ج.ر.ج.ج.ع. 53، الصادرة بتاريخ 8أكتوبر 2015 .

2- المرسوم الرئاسي 04-183المؤرخ في 26يونيو 2004يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني ، ج.ر.ج.ج.ع. 41الصادرة بتاريخ 27يونيو 2004 .

3- المرسوم التنفيذي رقم 06-348المؤرخ في 5أكتوبر سنة 2006والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، الجريدة الرسمية العدد 63، سنة 2006 .

ثانيا: الكتب .

- الكتب بالعربية :

1- أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري – الجزء 2، الطبعة الخامسة ، ديوان المطبوعات الجامعية ، الجزائر ، 1999 .

2- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومة ، الجزائر ، 2017 .

3- أمير فرج يوسف ، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر ، د ط ، مكتبة الوفاء القانونية ، الإسكندرية ، 2011 .

4- أنهلة عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، االاردن 2008 .

5- خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان ، 2011 .

6- خالد محمود إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، مصر ، 2009 .

7- زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري الدولي ، دون طبعة ، دار الهدى ، عين مليلة ، الجزائر ، 2011 .

8- سعيد عبد اللطيف حسن ، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، الطبعة الأولى ، دار النهصة العربية ، القاهرة 1999 . ،

9- سليمان عبد المنعم ، الجوانب الاشكالية في النظام القانوني لتسليم المجرمين ، د ط ، دار الجامعة الجديدة ، 2007 .

10-ضياء مصطفى عثمان ، السرقة الالكترونية ، الطبعة الأولى ، دار النفائس ، عمان ،2011 .

11-غنية باطلي ، الجريمة الالكترونية ،دراسة مقارنة ، د ط ، الدار الجزائرية للنشر والتوزيع ، الجزائر ، 2015 .

12 - عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، د ط ، دار الفكر الجامعي ، الإسكندرية ، مصر ، . 2006

13- عبد الله حسين محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2002 .

14 -عمرو موسى ، الجرائم المعلوماتية (جرائم الحايب الآلي في مصر وفي الدول العربية) ، د ط ، المكتب الجامعي الحديث ، الإسكندرية ، مصر ، 2006 .

15 - محمود حماد مرهج الهيني ، أصول البحث والتحقيق الجنائي ، د ط ، دار الكتب القانونية ، القاهرة ، مصر ، 2014 .

16 - مصطفى محمود موسى ، التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، 2009 .

17 - مولود ديدان ، قانون العقوبات ، حسب تعديل القانون رقم 11-14المؤرخ في 02-08-2011، د ط ، دار بلقيس ، الجزائر ، 2009 .

18- مولود ديدان ، قانون الإجراءات الجزائية ، الأمر 11-02، د ط ، دار بلقيس ، الجزائر ، 2009 .

19 - نائلة عادل محمد فريد قورة ، جرائم الحاسب الإقتصادية ، دراسة نظرية وتطبيقية ، د ط ،دار النهضة العربية ، القاهرة ، 2003 .

20 - نجيمي جمال ، إثبات الجريمة على ضوء الإجتهاد القضائي ،دراسة مقارنة ، د ط ، دار هومة ، الجزائر ، 2011 .

21 - نصر الدين هنوني ، درين يقدح ، الضبطية القضائية في القانون الجزائري ، الطبعة الثانية ، دار هومة ، الجزائر ، 2011 .

22 - هشام عبد العزيز مبارك ، تسليم المجرمين بين الواقع والتطبيق ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2006 .

23 - هلالي عبد اللاه أحمد ، كيفية الواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست ، د ط ، دار النهضة العربية ، القاهرة ، 2011 .

24- ياسر محمد الكومي محمود ابو حطب ، الحماية الجنائية والأمنية للتوقيع الإلكتروني ، د ط ، منشأة المعارف ، الإسكندرية ، 2014 .

A – Ouvrages

1- CHAWKI Mouhammed , Combattre le cyber criminalité , Edition de Saint Amans , Paris , 2008 .

2- QUEMENER Myriam , CHARPENEL Yves , Cybercriminallité– Droit pénal appliqué , édition Economica, paris , 2010 .

ثالثا : المقالات .

1- ابراهيم رمضان إبراهيم عطايا ، " الجريمة الإلكترونية وسبل مواجهتها في الشريعة الاسلامية والأنظمة الدولية " ، مجلة كلية الشريعة والقانون بطنطا ، جامعة الأزهر ، المجلد 30،العدد 2، افريل 2015 .

2- بوضياف إسمهان ، " الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر " ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف ، المسيلة ، العدد 11، 2018 .

3- حيمي سيدي محمد ، " معوقات التحقيق في الجرائم الالكترونية" ، المجلة الاكاديمية للبحوث القانونية والسياسية ، جامعة أبو بكر بلقايد – تلمسان ، المجلد 06، العدد 01، سنة 2022 .

4- رابح سعاد ، " ضوابط مكافحة الجريمة المعلوماتية " ، مجلة القانون العام الجزائري والمقارن ، جامعة جيلالي ليابس سيدي بلعباس ، المجلد 7، العدد 01، جوان 2021 .

5- رحموني محمد ، " خصائص الجريمة الإلكترونية ومجالات إستخدامها ، مجلة الحقيقة ، جامعة أحمد دراية ، أدرار ، العدد 41، 2018 .

6- زعيطي آمنة ، " مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري " ، مجلة حقوق الإنسان والحريات العامة ، جامعة مستغانم ، المجلد 4، العدد 7، جوان 2017 .

7 – زيوش عبد الرؤوف ، " جريمة المعلوماتية في التشريع الجزائري " ، مجلة العلوم القانونية والإجتماعية ، جامعة زيان عاشور بالجلفة الجزائر ، المجلد الرابع ، العدد 3، سبتمبر 2019 .

8– سعيدة بوزنون ، " مكافحة الجريمة الإلكترونية في التشريع الجزائري " ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري قسنطينة ، المجلد 30، العدد 03، سنة 2019 .

9 – سميرة معاشي ، " ماهية الجريمة الإلكترونية " ، مجلة المنتدى القانوني ، جامعة بسكرة ، العدد 7، مارس 2018 .

10–شرف الدين وردة ، " مشروعية اساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري "، مجلة الفكر ، جامعة محمد خيضر ، بسكرة ، العدد 15، جوان 2017 .

11–عادل عبد الله خميسي المعمري ، "التفتيش في الجرائم المعلوماتية " ، مجلة الفكر الشرطي ، صادر عن مركز بحوث الشرطة ، القيادة العامة لشرطة الشارقة ، الإمارات العربية المتحدة ، المجلد 22، العدد 86، 2013 .

12–عادل يوسف عبد النبي الشكري ، " الجريمة المعلوماتية وأزمة الشرعية الجزائية " ، مجلة مركز دراسات الكوفة ، جامعة الكوفة ، كلية القانون ، العدد 7، سنة 2008.

13 – عماد بلغيث ، " صعوبات التحقيق في الجرائم الإلكترونية ، مجلة الرسالة للدراسة والبحوث الإنسانية ، مخبر سوسيولوجية جودة الخدمة العمومية ، جامعة محمد بوضياف المسيلة ، الجزائر ، المجلد 06، العدد 03، سبتمبر 2021 .

14 – محمد خليفة ، " خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها " ، البوابة الجزائرية للمجلات العلمية ، كلية الحقوق والآداب والعلوم الإجتماعية ، جامعة 8ماي 45قالمة ، سبتمبر 2009 .

15– محمد قدري حسن عبد الرحمان ، " جرائم الإحتيال الإلكتروني " مجلة الفكر الشرطي ، مركز بحوث الشرطة ، القيادة العامة لشرطة الشارقة ، الامارات العربية المتحدة ، العدد 79، أكتوبر . 2011

16 – مصطفى عبد الباقي ، "التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين " دراسة مقارنة ، دراسات علوم الشريعة والقانون ، جامعة بيرزيت ،كلية الحقوق والإدارة العامة ، رام الله ، فلسطين ، المجلد 45، العدد 4، الملحق 2، 2018 .

17– نجاة زعزوعة ، ليلى بن قلة ، " النيابة العامة الإلكترونية في التشريع الجزائري " ، مجلة الدراسات القانون والإقتصادية ، جامعة تلمسان ، الجزائر ، المجلد 04، العدد 02، جوان 2021 .

رابعا : المداخلات العلمية .

1- حفوظة الامير عبد القادر وغرداين حسام ،" الجريمة الإلكترونية وآليات التصدي لها " ، ورقة مقدمة ضمن فعاليات الملتقى الوطني بعنوان : آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر ، 29مارس 2017 .

2- ذياب موسى البدانية ، " الجرائم الإلكترونية : المفهوم والاسباب " ورقة علمية مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية العلوم الاستراتيجية ،عمان ، الموسم بعنوان : الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من . 2-2014/09/3 .

3- سالم عبد الرزاق ، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية ، بمحكمة سيدي محمد .

4- سومية عكور ، " الجرائم المعلوماتية وطرق مواجهتها – قراءة في المشهد القانوني والامني " ، ورقة بحثية مقدمة للملتقى العلمي المنظم من طرف كلية العلوم الاستراتيجية بعنوان " حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ، الاردن ، في الفترة 02-2014/09/04 .

5- عبد الناصر محمد محمود وعبيد سيف سعيد السمساري ، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية ، دراسة تطبيقية مقارنة ، بحث مقدم للمؤتمر العربي الأول لعلوم الادلة الجنائية والطب الشرعي ، المنعقد بالرياض في الفترة الممتدة بين . 12-2007/11/14

6- علي محمود علي محمودة ، " الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي " ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، نظمته أكاديمية شرطة دبي ، في الفترة من 26إلى 28أفريل . 2003

7- غنام محمد غمام ، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات في الفترة الممتدة من 01الى 03ماي . 2003

8-ناصر محمد البقهي ، "أثر التحويل المعلوماتي على الأمن الفكري "، المؤتمر الوطني الأول للأمن الفكري والمقاهوَن والتحديات ، كرسي نايف بن عبد العزيز لدراسات الامن الفكري بجامعة الملك سعود ، المملكة السعودية ، 22-23جمادى الأولى 1430هـ .

9- نمديلي رحيمة ، " خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة " ، كتاب أعمال مؤتمر الجرائم الإلكترونية الدولي الرابع عشر ، طرابلس ، لبنان ، بتاريخ 24-25مارس 2017 .

10-هشام محمد فريد رستم ، " الجرائم المعلوماتية - أصول التحقيق الجنائي الفني واقتراح آلية عربية موحدة للتدريب التخصصي " ، بحوث مؤتمر القانون والكمبيوتر والانترنت ، جامعة الإمارات المتحدة ، كلية الشريعة والقانون ، الملجد الثاني ، الطبعة الثالثة ، من 1-3ماي2000 .

11- هواري عياش ، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ، جامعة بسكرة ، كلية الحقوق ، 2006 .

12- وليد عاكوم ، التحقيق في جرائم الحاسوب ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، منعقد بإمارة دبي في الفترة الممتدة من 26إلى 28أفريل 2003 .

خامسا : المذكرات والأطروحات الجامعية .

1 - ربيعي حسين ، آليات البحث والتحري في الجرائم المعلوماتية ، أطروحة دكتوراه علوم ، جامعة باتنة ، 2015-2016 .

2 - فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني ، أطروحة نيل شهادة الدكتوراه في القانون ، فرع القانون الجنائي والعلوم الجنائية ، جامعة الجزائر 1، كلية الحقوق ، الجزائر ، 2011 .

3- سويد سفيان ، الجرائم المعلوماتية ، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام ، جامعة أبو بكر بلقايد ، كلية الحقوق ، تلمسان ،الجزائر ، 2003 .

4 - صغير يوسف ، الجريمة المرتكبة عبر الأنترنت ، مذكرة لنيل شهادة الماجستير في القانون " تخصص القانون الدولي للأعمال " ، جامعة مولود معمري ، كلية الحقوق والعلوم السياسية ، تيزي وزو ، 2013 .

5- يوسف خليل يوسف العفيفي ، الجرائم الإلكترونية في التشريع الفلسطيني " دراسة تحليلية مقارنة " ، رسالة لنيل شهادة الماجستير في القانون العام ، الجامعة الإسلامية ، كلية الشريعة والقانون ، غزة ، 2013 .

6 - أحمد مسعود مريم ، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة ماجستير في القانون الجنائي ، جامعة ورقلة ، كلية قاصدي مرباح ، 2013 .

7 – محمد بوعمرة ، سيد علي بنينال ، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري ، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية – تخصص قانون أعمال ، جامعة أكلي محند أولحاج ، كلية الحقوق والعلوم السياسية ، قسم القانون الخاص ، البويرة ، 2019–2020 .

سادسا : المطبوعات .

1– عبد الرحمان خلفي ، محاضرات في قانون الإجراءات الجزائية ، دار الهدى ، الجزائر ، . 2010

2 – مروك نصر الدين ، محاضرات في الإثبات الجنائي ، دار هومة ، الجزائر ، 2011.

سابعا : المواقع الالكترونية .

1–" أرضية إلكترونية جديدة تسمح للاشخاص بتقديم الشكاوى عن بعد" ، نشر يوم الثلاثاء 28جويلية 2020، موقع وكالة الانباء الجزائرية ، تم الإطلاع عليه يوم 29ماي 2022الساعة 14:15، رابط الموقع :

https://www.aps.dz/ar/algerie/9025–2020–07–28–17–13–13.

2– الاعلان العالمي لحقوق الإنسان ، المعتمد بموجب قرار الجمعية العامة 217الف (د– (3المؤرخ في كانون الأول / ديسمبر 1948، من خلال الموقع الرسمي الإلكتروني لهيئة الأمم المتحدة ، تم الإطلاع على الموقع بتاريخ 2022/05/13،على الساعة 20:15، رابط الموقع :

http://www.un.prg/ar/documents/index.html .

3– العهد الدولي الخاص بالحقوق المدنية والسياسية ، تم الاطلاع بتاريخ 2022/05/25على الساعة 18:00، رابط الموقع : file:///C:/Users/user/Downloads/Documents/ccpr

فهرس المحتويات

فهرس المحتويات

شكر وعرفان	
إهداء	
مقدمة	1
الفصل الأول: ماهية الجريمة الإلكترونية .	7
المبحث الأول: مفهوم الجريمة الإلكترونية .	8
المطلب الأول: تعريف الجريمة الإلكترونية .	9
الفرع الأول: التعريف اللغوي للجريمة الإلكترونية .	9
الفرع الثاني: التعريف الفقهي للجريمة الإلكترونية .	10
الفرع الثالث: التعريف التشريعي للجريمة الإلكترونية .	11
المطلب الثاني: خصوصية الجريمة الإلكترونية .	12
الفرع الأول: ترتكب الجريمة الإلكترونية من مجرم غير تقليدي .	13
الفرع الثاني: جريمة صعبة الاكتشاف والإثبات .	14
الفرع الثالث: جريمة عابرة للحدود الدولية .	15
المبحث الثاني: مجالات استخدام الجرائم الإلكترونية والأجهزة المختصة في متابعتها.	16
المطلب الأول: مجالات استخدام الجرائم الإلكترونية .	17
الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي.	17
أولا: الجرائم الواقعة على الأشخاص .	17
ثانيا: جرائم واقعة على الأموال.	18
ثالثا: جرائم واقعة ضد أمن الدولة.	19
الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي.	20
أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي.	20
ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي.	20
الفرع الثالث: الجرائم الواقعة على البرامج الإلكترونية.	21
المطلب الثاني: الأجهزة المختصة في متابعة الجرائم الإلكترونية.	22
الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.	23
أولا: طبيعة تشكيل الهيئة ومهامها.	23
ثانيا: طريقة سير الهيئة.	27

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة في متابعة الجرائم الإلكترونية.	28
الفرع الثالث: الهيئات التابعة للجهاز الأمني.	29
أولا– الهيئات التابعة لسلك الأمن الوطني.	29
ثانيا– الوحدات التابعة للقيادة العامة للدرك الوطني .	30
الفصل الثاني: إجراءات مواجهة الجريمة الإلكترونية.	33
المبحث الأول: التحري وجمع الاستدلالات في الجرائم الإلكترونية.	35
المطلب الأول: تلقي البلاغات والشكاوي في الجرائم الإلكترونية.	36
الفرع الأول: تلقي البلاغات في الجرائم الإلكترونية.	37
الفرع الثاني: الشكوى في الجرائم الإلكترونية.	38
المطلب الثاني: أساليب التحري الخاصة.	39
الفرع الأول: أساليب التحري الخاصة وفقا لقانون الإجراءات الجزائية والقانون المتضمن القواعد الخاصة	40
أولا: أساليب التحري الخاصة وفقا لقانون الإجراءات الجزائية.	40
ثانيا: أساليب التحري الخاصة وفقا للقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.	44
الفرع الثاني: تقدير مدى مشروعية أساليب التحري الخاصة.	45
أولا: مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية وفقا للاتفاقيات الدولية لحقوق الإنسان.	45
ثانيا: مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة الإلكترونية وفقا للقانون الجزائري.	47
المبحث الثاني: التحقيق في الجرائم الإلكترونية.	50
المطلب الأول: خصائص التحقيق والمحقق في الجرائم الإلكترونية.	51
الفرع الأول: خصائص التحقيق.	51
الفرع الثاني: خصائص المحقق.	53
الفرع الثالث: السلطة المختصة بالتحقيق في الجزائر.	54
المطلب الثاني: إجراءات التحقيق في الجرائم الإلكترونية.	55
الفرع الأول: التفتيش وضبط الأدلة.	55

أولا: التفتيش في البيئة الإلكترونية.	55
ثانيا: ضبط الأدلة في الجرائم الإلكترونية.	58
الفرع الثاني: المعاينة وندب الخبراء.	60
أولا: المعاينة.	60
ثانيا: ندب الخبراء في الجرائم الإلكترونية.	61
المطلب الثالث: معوقات التحقيق في الجرائم الإلكترونية.	63
الفرع الأول: إشكالية تنازع الاختصاص بالتحقيق في الجرائم الإلكترونية.	63
الفرع الثاني: عدم مواكبة النصوص الجزائية لخصوصية الجرائم الإلكترونية.	64
الفرع الثالث: الصعوبات المتعلقة بالشق الميداني .	66
أولا: صعوبة الحصول على الدليل وإخفائه.	66
ثانيا: العزوف عن التبليغ بوقوع الجريمة الإلكترونية وصعوبة اكتشاف مرتكبيها.	67
المبحث الثالث: إجراءات المحاكمة والتعاون الدولي في الجرائم الإلكترونية.	68
المطلب الأول: المحاكمة في الجرائم الإلكترونية.	69
الفرع الأول: قواعد الاختصاص جهة الحكم في الجريمة الإلكترونية.	69
أولا: الاختصاص المحلي.	69
ثانيا: الاختصاص النوعي.	69
الفرع الثاني: إجراءات المحاكمة.	70
المطلب الثاني: التعاون الدولي في مجال مكافحة الجريمة المعلوماتية.	71
الفرع الأول: المساعدة القضائية الدولية.	72
الفرع الثاني: تسليم المجرمين.	73
خاتمة	
قائمة المصادر والمراجع	
فهرس المحتويات	

الملخص:

أدى الاستخدام السيء لتكنولوجيا الحديثة لظهور الجرائم الالكترونية ، وهي كل نشاط اجرامي غير مشروع يمس أنظمة معالجة المعطيات أو أي منظومة معلوماتية او اتصالاتية ، وقد صعب على اغلب الدول التصدي لها نظرا لطبيعتها وخصائصها التي تميزها عن الجرائم التقليدية اضافة لتعدد مجالات استخدامها ،فقد أصبح الافراد والمؤسسات والدول ككل لا يستغنون عن التكنولوجيا في جميع المجالات مما ادى لظهور تجاوزات غير مشروعة على مستوها ، ومما لا شك فيه أن المشرع الجزائري بدوره يحاول مواجهة هذا الاجرام المستحدث ،اذ خصص أجهزة لمتابعتها دون غيرها ، فقد بلغت درجات من الخطورة لا يستهان بها ، فالمشرع يملك ترسانة قانونية في هذا المجال لا بأس بها رغم بعض النقائص ، ولعل الاهتمام الأوفر يجب أن يرتكز على الجانب الاجرائي اضافة للموضوعي، وفي هذا الخصوص تم استحداث قواعد اجرائية عديدة خلال جميع مراحل الدعوى ، خصوصا تلك المتعلقة باستحداث أساليب تحري وتحقيق عن الجرائم الالكترونية تتناسب والطبيعة الخاصة لهذه الأخيرة .

Summary :

The bad use of modern technology has led to the emergence of cybercrime, which is every illegal criminal activity that affects data processing systems or any information or communication system. And countries as a whole do not dispense with technology in all fields, which has led to the emergence of illegal transgressions on their level, and there is no doubt that the Algerian legislator, in turn, is trying to confront this new crime, as it has allocated devices to follow it without others, it has reached degrees of seriousness not to be underestimated, the legislator has There is a good legal arsenal in this field, despite some shortcomings, and perhaps the most attention should be based on the procedural aspect in addition to the objective. for this last one.