وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون إعلام آلي وأنترنت

الموسومة بـ

خصوصية التحقيق في الجريمة الإلكترونية

إعداد الطلبة:

- بن عزوز أسماء
- سارة بن محمود

إشراف الدكتور:

* سي حمدي عبد المومن

أجيزت يوم:2024/06/20.

لجنة المناقشة:

الإسم واللقب	الصفة	الرتبة
رفاف لخضر	رئيسا	أستاذ محاضر قسم أ
سي حمدي عبد المومن	مشرفا	أستاذ محاضر قسم أ
زاوي رفيق	مناقشا	أستاذ محاضر قسم أ

السنة الجامعية 2024/2023

شكر وعرفان

لقوله "لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ"

أولا بعد حمد الله حمدا يليق بجلال قدره وعظيم سلطانه وبعد الصلاة والسلام على خير خلق الله سيدنا محمد عليه الصلاة والسلام

نتقدم بكلمة شكر وعرفان إلى الأستاذ المشرف سي حمدي عبد المومن الذي لم يبخل علينا بنصائحه وتوجيهاته التي أعانتنا على إتمام هذا العمل

إلى أعضاء لجنة المناقشة الموقرة

وأخيرا نرجوا أن نكون وفقنا في هذا العمل ونسأل الله أن يجعله في ميزان حسناتنا.

إهداء

الحمد لله الذي أعانني على إتمام هذا العمل والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين

أهدي عملي هذا إلى رمز العطاء والوفاء والدي الكريمين أسأل الله أن يحفظهما ويطيل في عمرهما وإلى أخواتي وإخواني سندي في هذه الحياة

وإلى زوجي ورفيق دربي وإلى براعم بيتي مرام ورؤيا وأياد حفظهم الله ورعاهم إلى أختي وزميلتي بن عزوز أسماء التي كانت لي عونا وسندا وإلى كل من ساعدنا من قريب أو بعيد أهدي ثمرة عملي هذا

صارة بن محمود

إهداء

إلى روح أبي الطاهرة

إلى سندي في الحياة أمي الغالية

إلى قرة عيني أبنائي "إيناس وأنيس"

إلى إخوتي وأخواتي الأعزاء

وإلى كل من ساعدني من قريب أو بعيد

إلى أعز زميلة وصديقة بن محمود سارة التي كانت عونا وسندا لي

أسماء

الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

إذن بالإيـــداع

أنا الممضي أسفله الأستاذ: ....

الرتبة : ....

المشرف على مذكرة الماستر الموسومة بـ : ....

....

من إعـــداد :

الطالب الأول : ....

الطالب الثاني : ....

أوافق على إيداع الطالب (الطالبين) لمذكرة التخرج لدى الإدارة من أجل برمجتها للمناقشة.

إمضاء الأستاذ المشرف

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): بن محمود نعيمة الصفة: طالب، أستاذ، باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم 402705924 والصادرة بتاريخ 2022-08-23

المسجل(ة) بكلية / معهد الحقوق قسم علوم سياسية وعلاقات دولية

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: حوكمة الحقوق في ظل رقمنة الإدارة

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

التاريخ: 2024.06.04

توقيع المعني (ة)

04 جوان 2024

المركز الجامعي لتيبازة
مكتب التكوين في الدكتوراه

* ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): بن عزوز أسماء الصفة: طالب، أستاذ، باحث طالبة

الحامل(ة) لبطاقة التعريف الوطنية رقم 100662312 والصادرة بتاريخ 18-04-2016

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم علوم الإعلام والاتصال

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: خصوصية التحقيق في الجريمة الإلكترونية

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

التاريخ: 04-05-2024

بن عزوز أسماء
100662312
2016/04/18

توقيع المعني (ة)

04 جوان 2024

مقدمة

مقدمة

تعتبر التكنولوجيا الإلكترونية الحديثة من أبرز صفات وسمات العصر الحديث وأصبح المجتمع حاليا يقاس بمدى تطور وسائل تبادل المعلومات فيه عبر منظومة الانترنت الذي شاع استعماله في مجتمعنا والذي ساهم في تعزيز التواصل الحضاري والثقافي وتعزيز التفاهم الإنساني وكسر الحواجز بين الشعوب حتى أصبح العالم كقرية صغيرة ومع هذا التطور الهائل رافقته موجات اختراق وتعديات وإساءة استخدام هذا التطور في أنشطة غير مشروعة مما يؤدي إلى وقوع ضرر بالمصالح المادية والمعنوية للأشخاص والتعدي حتى على سيادة الدول وكيانات المؤسسات الوطنية والدولية، وهو ما يعرف بالجريمة الإلكترونية وهي من الجرائم المستحدثة وقد عرفها الفقهاء بتعريفات مختلفة نذكر منها أنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه"[1]، وأيضا عرفت على أنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى"[2]، أما المشرع الجزائري فقد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04[3] على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية تخصص علم الإجرام والعقاب، جامعة باتنة، 2012/2011، ص 14.

[2] حمزة بن عقون، نفس الرسالة، ص 13.

[3] القانون رقم 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إلي 394 مكررا 7 وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية، وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية ومن أمثلة الجريمة الالكترونية المرتكبة في الجزائر تسرب أسئلة البكالوريا 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية والذي ألقي القبض عليه من طرف الشرطة الفيدرالية العالمية. [1]

وباعتبار الجريمة الإلكترونية من الجرائم المستحدثة وجب مواكبتها من ناحية الأنظمة الجزائية والتشريع لحماية حقوق الأفراد والمؤسسات وحتى الدول واستخدام الوسائل والأساليب المتطورة في مجال التحقيق بتلك الجرائم وضبط مرتكبيها وتتبعها وكشفها وجمع الأدلة القائمة حولها باعتبار أن التحقيق في الجريمة الإلكترونية يعتبر أهم إجراء في سير الدعوى الجزائية الذي يستلزم البحث في خصوصياته المتعلقة بالجرائم الالكترونية كأساس موضوع التحقيق المستحدث ومختلف عناصر التحقيق فيها والآليات اللازمة لمواجهة هذه الجرائم.

ولقد تطرقنا في دراستنا إلى هذا الموضوع بسبب الفضول الشخصي والمعرفي من أجل الإلمام بجوانب هذه الجريمة المستحدثة وطرق التحقيق فيها ومعرفة كل ما يتعلق بها وكيفية التصدي لها، أما بالنسبة للأسباب الموضوعية فهو البحث وتعميق المعرفة في مجال

[1] نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة أحمد دراية، 2017/2016، ص 09.

التحقيق في الجرائم الإلكترونية من حيث التطرق لأهم عناصره وأساليبه وكيفية مجابهة هذه الجرائم.

ويهدف هذا الموضوع إلى عدة نقاط نذكر منها ما يلي:

- تسليط الضوء على إجراءات التحقيق في الجريمة الالكترونية.

- إبراز أهم التحديات التي تواجه التحقيق في ج.إ.

- إبراز المساعي الدولية لمواجهة هذه الجرائم.

ومما سبق يمكن طرح الإشكالية الآتية:

- ما هي خصوصية التحقيق في الجريمة الالكترونية ؟

وانطلاقا من الإشكالية الرئيسية يمكن طرح التساؤلات التالية:

- فيما يتمثل التحقيق في الجريمة الالكترونية ؟ وما هي آليات التحقيق في الجريمة الالكترونية وسبل تفاديها ؟

واعتمدنا في بحثنا على المنهج الوصفي التحليلي باعتباره أنسب منهج لمعالجة موضوعنا والإلمام بجوانبه مع تحليل بعض المواد القانونية.

وللإجابة على إشكالية الموضوع ارتأينا اعتماد خطة ثنائية تتضمن فصلين، كل فصل يتضمن مبحثين حيث تناولنا في الفصل الأول الإطار المفاهيمي للتحقيق في الجريمة الالكترونية الذي تعرضنا فيه إلى مفهوم ومعوقات التحقيق، أما الفصل الثاني فتضمن آليات التحقيق في مواجهة الجريمة الالكترونية وكذا سبل التعاون الدولي في مجابهتها.

الفصل الأول:

الإطار المفاهيمي للتحقيق في الجريمة الالكترونية

الفصل الأول: الإطار المفاهيمي للتحقيق في الجريمة الالكترونية

إن جرائم الانترنت تعتبر تهديدا مباشرا لتقدم البشرية بواسطة أعمال إجرامية يقوم بها أشخاص يسيئون استخدام التكنولوجيا الحديثة وهذه الجرائم تستمر بزيادة صعوبتها وتعقيدها، كما أن ملاحقة مرتكبيها لا تكاد تخلو من الصعوبات والعراقيل التي تصادف المحقق الجنائي في الجرائم الالكترونية، لذا سنتطرق في هذا الفصل إلى دراسة الإطار المفاهيمي للتحقيق في الجريمة الإلكترونية من خلال مفهوم التحقيق في الجريمة الالكترونية (المبحث الأول)، والصعوبات التي تواجه التحقيق في ج.إ (المبحث الثاني).

المبحث الأول: مفهوم التحقيق في الجريمة الالكترونية

إن التحقيق بصفة عامة يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها توصلا لإظهار الحقيقة. [1]

تعريف التحقيق:

أ- **لغة:** إثبات المسألة بدليلها.

ب- **اصطلاح فقهاء القانون:** هي عبارة عن جميع إجراءات التحقيق التي يباشرها المحقق عند وقوع جريمة أو حادثة توصلا إلى معرفة الحقيقة.

تعريف إجراءات التحقيق:

أ- **لغة:** جمع إجراء ومصدره أجرى، أجرى الماء ونحوه أساله وجعله يجري وأجرى الأمر أمضاه وأنفذه، وضعه في حيز التنفيذ.

ب- **اصطلاح فقهاء القانون:** هي جميع الأعمال التي تشكل بمجموعها شكل التحقيق الجنائي وهي تمثل جميع الأوامر والنظم التي تحكم أعمال التحقيق الجنائي وتضمن سير العدالة الجنائية وحمايتها من أسباب التعثر والانحراف.

التحقيق في الجرائم المعلوماتية من أهم الإجراءات التي تتخذ في الدعوى، إن لم تكن أهمها على الإطلاق ومن ثم فإن المحقق يجب أن يتبصر ببعض الأمور التي يجب أن ينتبه لها أثناء التحقيق في هذا النوع من الجرائم سيما وأن هذا الموضوع يتسم بالحداثة وبتقنية علمية وذكاء عالي.

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، ط1، الإسكندرية، 2018، ص 13.

إن التحقيق هو مجموعة من القواعد القانونية والفنية التي تباشرها السلطة المختصة لتمحيص الأدلة والكشف عن الحقيقة. [1]

التحقيق في الجرائم الإلكترونية هو نشاط قانوني يتعلق بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الاستدلالات التي يتطلبها التحقيق فهو الضبط القضائي للجاني والدليل على إدانته أو براءته.

ويعرفه العقيد عبد الواحد إمام بأنه: "مجموعة الإجراءات والوسائل المشروعة قانونا والتي يقوم بها المحقق لكشف واستجلاء غموض الحادث والتوصل إلى فاعله وإسناد الاتهام قبله". [2]

تعريف التحقيق الجنائي في الجرائم الإلكترونية: يمكن تعريفه بأنه عمل قانوني يقوم به مأمور التحقيق القضائي المختص والمتخصص لضبط الجرائم الإلكترونية والرقمية من فاعل ودليل إلكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون مختصة في هذه النوعية من الجرائم لإقامة العدل.

فالتحقيق هو مجموعة من الإجراءات التي يقوم بها شخص خوله القانون سلطة اتخاذ كافة الإجراءات القانونية والوسائل المشروعة في حال وصول إلى علمه وقوع جريمة يهدف إلى الكشف عن الأدلة وضبط فاعلها وتقديمه إلى المحاكمة، وقد عبر عنه المشرع الجزائري بقاضي التحقيق وأعطى تعريفه في نص المادة 68 من ق إ ج. [3]

---

[1] أجعود فطيمة، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر في الحقوق تخصص قانون إعلام آلي وانترنت، جامعة محمد البشير الإبراهيمي، 2022/2021، ص 08.

[2] مصطفى محمد موسى، التحقيق الجنائي في ج.إ، بدون دار نشر، طبعة 1، القاهرة، ص 165-166.

[3] آيت عبد المالك نادية، فلاح عبد القادر، التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، جامعة خميس مليانة، سنة 2019، ص 164.

المادة 68: (القانون رقم 01-08 المؤرخ في 26 يونيو 2001) يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أدلة الاتهام وأدلة النفي. [1]

يحتاج التحقيق في هذه النوعية من الجرائم، لإمكانيات مادية وقواعد وإجراءات تختلف عن التحقيق في الجرائم التقليدية سواء من حيث طبيعة السلوك الإجرامي الإلكتروني أو من حيث طبيعة الدليل الإلكتروني أو وسائل وآليات كشف الجريمة والوصول إلى الدليل الإلكتروني.

من مميزاته أن يكون التحقيق في الجريمة الإلكترونية بسرية وهذا ما نصت عليه المادة 11 من ق.إ.ج "أي عدم الإطلاع على مجريات التحقيق"، ويتميز أيضا بتدوين جميع إجراءات التحقيق في محاضر رسمية ويصادق عليها لتكون حجية في الإثبات، كذلك وضع خطة للتحقيق فيبدأ المحقق بجمع الاستدلالات ويساعده فريق تقني مؤهل في هذا النوع من الجرائم الخطيرة لأنه يتطلب وسائل مادية وبشرية للبحث والتحري وضبط مرتكبيها. [2]

وما يميز التحقيق في الجرائم الإلكترونية عن التحقيق في الجرائم التقليدية أن مرتكبو الجرائم الإلكترونية لديهم قدرة تقنية وذكاء خارق في سرعة إتلاف وتشويه وإضاعة الدليل الإلكتروني الرقمي في وقت قصير، وإنها جرائم لا تترك أثرا ماديا في مسرح الجريمة الالكتروني. [3]

[1] انظر المادة 68 من قانون الإجراءات الجزائية، النص الكامل للقانون وتعديلاته إلى غاية 11 يوليو سنة 2018، مدعم بالاجتهاد القضائي، الطبعة 15، ص 56.

[2] انظر المادة 11 من قانون الإجراءات الجزائية.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 13.

المطلب الأول: عناصر التحقيق في الجريمة الإلكترونية

لقد تماشى تطور الجريمة وأساليب ارتكابها مع تطور وسائل التحقيق الجنائي، فبعد أن كان التعذيب والعنف من وسائل التحقيق للوصول إلى الدليل أصبح قائما على الأساليب العلمية واستخدام شبكة الانترنت هي الصفة المميزة والغالبة.

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها الضبطية القضائية بشأن واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لها، وهو ما يمهد الطريق أمام القضاء باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة وهدف التحقيق هو الكشف عن الحقيقة وللوصول إلى الحقيقة يلجأ المحقق إلى مجموعة إجراءات بعضها بهدف الحصول على الدليل الرقمي وتسمى إجراءات جمع الأدلة، وبعضها الآخر يعرف بالإجراءات الاحتياطية ضد المتهم كالقبض و الحبس المؤقت. [1]

والجريمة الإلكترونية لا تختلف عن أي جريمة أخرى، إذ تتطلب لتحقيقها الأركان المتفق عليها وعلى ضرورة توفرها في أي جريمة لكي تتواجد على أرض الواقع وهي الركن الشرعي والمادي والمعنوي. [2]

الفرع الأول: الركن الشرعي

ولقد نصت عليه المادة الأولى من قانون العقوبات الجزائري"لا جريمة ولا عقوبة أو تدبير أمن بغير قانون" فالمقصود هنا وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل.

---

[1] أجعود فطيمة، المرجع السابق، ص 11.

[2] بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة المسيلة، السنة الجامعية 2013-2014، ص 30.

ولقد خصص المشرع الجزائري منذ تعديل 2004 وتبعته تعديلات 2006 القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والذي يندرج ضمن الباب الثاني الجنايات والجنح ضد الأفراد، الفصل الثالث الجنايات والجنح ضد الأموال (المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري).

جاء القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها كجانب وقائي من وقوع الجرائم المعلوماتية من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية. [1]

الفرع الثاني: الركن المادي

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالأنترنت وبطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجتها، فمثلا يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيوم بتحميل الكمبيوتر ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد دائرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها، لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق ج.إ. [2]

ويتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقيق الركن المادي دون تحقق النتيجة.

[1] أجعود فطيمة، مرجع سابق، ص 22.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 52.

فهو كل فعل أو سلوك إجرامي صادر عن إنسان عاقل سواء كان ايجابيا أو سلبيا يؤدي إلى نتيجة تمس حقا من الحقوق التي يكفلها الدستور والقانون. [1]

ويقوم الركن المادي في هذه الجريمة بانعقاد إرادتين أو أكثر واجتماعهما على موضوع معين، يتمثل في الإعداد لجريمة أو أكثر سواء جريمة الدخول أو البقاء، جريمة التلاعب بالمعطيات، جريمة التعامل في المعطيات غير مشروعة وهو ما نصت عليه المادة 394 مكرر 5 يقوم بغض النظر عن الوقت الذي استغرقه سواء كان منظما أو عارضا اقتصر إعطاؤه على مجرد العزم، ويشترط لقيام الجريمة تعدد الجناة الحد الأدنى هو شخصين، كلاهما مسؤول جزائيا فإذا لم يكن إحداهما مسؤولا جزائيا لا يقوم الاتفاق. [2]

وقد قسم الدكتور رضا فرح الركن المادي إلى ثلاث عناصر: السلوك الإجرامي، النتيجة الإجرامية، العلاقة السببية بين الفعل والنتيجة. [3]

– **السلوك الإجرامي:** يكون بصورتين إما بالفعل الإيجابي أو بالفعل السلبي، ويمكن أن نجده في الجريمة الالكترونية بنوعيه الايجابي والسلبي، فلا ننسى التطور الكبير في محتوى وطبيعة السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل.

– **النتيجة الإجرامية:** هو الأثر المادي الذي يحدثه السلوك الإجرامي.

– **العلاقة السببية بين الفعل والنتيجة:** هي العلاقة بين الفعل والنتيجة ويثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وإسناد الفعل للنتيجة هو شرط أساسي لتقرير المسؤولية.

---

[1] أجعود فطيمة، مرجع سابق، ص 22.

[2] اومدور رجاء، المرجع السابق الذكر، ص 26.

[3] يوسف جفال، المرجع السابق الذكر، ص 16.

ليس كل جريمة تستلزم وجود أعمال تحضيرية، فيصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق وبرامج فيروسات ومعدات لفك الشفرات وكلمات المرور وحيازة صور دعارة للأطفال فمثل هذه الأشياء تشكل جريمة بحد ذاتها. [1]

أ- في جريمة الدخول أو البقاء عن طريق الغش في المنظومة المعلوماتية: يتمثل السلوك الإجرامي إما في الدخول أو البقاء في المنظومة المعلوماتية الغير مفتوح للجمهور، هذا ما أشارت إليه المادة 394 مكرر من قانون العقوبات "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" فنرى أنه لم يشترط صفة معينة في الشخص ولا وسيلة أو طريقة معينة للدخول المهم أن يكون مخالفا لإرادة صاحب النظام أي ليس له ترخيص، فيعتبر الدخول مشروع والبقاء غير مشروع. [2]

ب- في جريمة التلاعب بالمعطيات: هي جرائم ضرر أي جرائم مادية بالتالي هي ذات نتيجة، لأنه لا يكفي أن تهدد سلامة المعطيات بل يشترط تغيير حالة المعطيات. [3]

ج- في جريمة التعامل في معطيات غير مشروعة: حسب نص المادة 394 مكرر 2 الغاية من التجريم هنا وقائية لأن هذه الجرائم هي جرائم خطر يهدف المشرع من خلال تجريمها إلى منع وقوع الضرر في حالة التعامل في معطيات صالحة لارتكاب الجريمة، وفي حالة حدوث هذه الأخيرة يحاول القضاء على أثار الجريمة. [4]

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 52-53.

[2] اومدور رجاء، المرجع السابق الذكر، ص 22.

[3] نفس المرجع، ص 23.

[4] نفس المرجع، ص 23-24.

الفرع الثالث: الركن المعنوي

يتكون الركن المعنوي من عنصري العلم والإرادة. [1]

فالركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني. [2]

يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون. [3]

المطلب الثاني: الهيئات وأجهزة التحقيق في الجرائم المعلوماتية

بدأت التشريعات –ومن بينها التشريع الجزائري– تواجه خطورة الجرائم المعلوماتية من خلال استحداث هيئات قضائية وغير قضائية وهو ما سنتناوله في هذا المطلب.

الفرع الأول: الهيئات القضائية الجزائية المتخصصة

يعتبر إنشاء هيئات قضائية جزائية متخصصة توجها جديدا لتطويق نطاق الجرائم الخطيرة ومن بينها الجرائم المعلوماتية.

أولا: إنشاء الهيئات القضائية الجزائية المتخصصة

نشأت هيئات قضائية جزائية متخصصة منذ تعديل قانون الإجراءات الجزائية الجزائري بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لـ ق اج ج.

---

[1] بشير حماني، المرجع السابق الذكر، ص 11.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 53.

[3] يوسف جفال، المرجع السابق الذكر، ص 17.

باستقراء نص المادة 37 و 40 منه، يتضح أن المشرع الجزائري خروجا عن القواعد العامة للاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحددة بـ:

- مكان وقوع الجريمة..

- محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها.

- المكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر.

فقد أجاز المشرع بموجب الفقرة الثانية من المادة 37 ق ا ج تمديد اختصاص وكيل الجمهورية في جرائم محددة على سبيل الحصر ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات إلى دائرة محاكم أخرى محددة عن طريق التنظيم، وهو نفسه بالنسبة لتمديد اختصاص قاضي التحقيق بموجب الفقرة الثانية من المادة 40 ق ا ج.

كما نصت الفقرة الأخيرة من المادة 329 من قانون الإجراءات الجزائية الجزائري، على تمديد الاختصاص المحلي للمحكمة في الجرائم المحددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وما يفسر خروج المشرع عن معايير الاختصاص الأصلي[1] في الجرائم المعلوماتية هو:

- اتساع مكان ارتكاب الجرائم المعلوماتية خارج حدود الاختصاص الإقليمي التقليدي، وانتشار الأعمال المكونة هذه الجرائم داخل وخارج حدود الدولة.

[1] كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11، العدد 01، سنة 2015، ص 121.

– التمسك بالمعايير الأصلية للاختصاص يشكل عائقا أمام مواجهة الجرائم المعلوماتية.

– الطبيعة الخاصة لهذه الجرائم.

وقد حدد المشرع سنة 2006، بموجب المرسوم التنفيذي رقم 06–348 تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق حيث يمتد الاختصاص المحلي لمحكمة سيدي محمد ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران ووكلاء الجمهورية وقضاة التحقيق في هذه المحاكم، إلى محاكم المجالس القضائية التابعة لمختلف ولايات الوطن (48 ولاية) حسب الجهة. [1]

وما يعاب على المشرع الجزائري في مسألة تمديد الاختصاص أنه لجأ إلى ذلك إلا أنه لم يستحدث أقساما متخصصة ولا تشكيلة خاصة لدى الجهات القضائية ولا قضاة متخصصين في الجرائم المحددة حصرا في هذه المواد ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، عكس ما ذهب إليه القانون الفرنسي في المادة 706–75 من ق ا ج فرنسي أن المحاكم ذات الاختصاص الموسع تشمل على فرع للنيابة وتشكيلات للتحقيق والمحاكمة متخصصة بالنظر في الجرائم محل الاختصاص الذي وضح أن تمديد الاختصاص للمحاكم لا يخص إلا القضاة المعينين في فروع متخصصة في حين أن قانون 04–14 جاء عاما حيث جعل من تمديد الاختصاص لكل القضاة الموجودين في المحاكم ذات الاختصاص الموسع. [2]

[1] أنظر المادة 2–3–4–5 المرسوم التنفيذي رقم 06–348، المؤرخ في 5 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد 63، الصادرة في 8 أكتوبر 2006، ص 30.

[2] كريمة علة، مرجع سابق، ص 123.

ثانيا: توسيع صلاحيات ضباط الشرطة القضائية

تجدر الإشارة أن المادة 16 من ق ا ج ج عالجت مسألة تمديد اختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني فيما يتعلق بالبحث ومعاينة جرائم محددة بنص المادة ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وأجازت المادة 47 التفتيش والمعاينة والحجز في هذه الجرائم في أي ساعة من النهار والليل بإذن من وكيل الجمهورية كما يجوز لقاضي التحقيق بالتفتيش والحجز ليلا أو نهارا في كامل التراب الوطني، أو يأمر ضباط الشرطة القضائية المختصين بذلك.

كما مكن المشرع الجزائري بموجب المادة 51 من نفس القانون، تمديد آجال التوقيف للنظر مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وهنا لابد من مراعاة ضمانات المتهم خلال مرحلة التوقيف للنظر.

الفرع الثاني: الهيئات غير القضائية

تتمثل الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتية في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى السلطة الوطنية لمعالجة المعطيات ذات طابع شخصي، ووكالة أمن الأنظمة المعلوماتية.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

1- مفهوم الهيئة: في سبيل ضمان فاعلية التحقيق أنشأ المشرع الجزائري بموجب المادة 13 من القانون 09-04 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وترك تحديد تشكيلتها وتنظيمها وكيفيات سيرها عن طريق التنظيم، حيث نظمت

وفقا لعدة مراسيم بداية بالمرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015 [1]، الذي عرف الهيئة بموجب المادة 02 منه على أنها: سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل ثم جاء المرسوم الرئاسي 19-172 المؤرخ 6 يونيو 2019 [2] وأعاد تعريف الهيئة بموجب المادة 02 منه، على أنها: مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني، وأعيد تنظيم الهيئة من جديد بموجب المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020 [3]، حيث عرفت الهيئة بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية.

2- مهام الهيئة: أبقى المرسوم الرئاسي لسنة 2020 على مهام الهيئة تحت رقابة السلطة القضائية والمتمثلة في [4]:

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

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1] مرسوم رئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 53، الصادرة بتاريخ 8 أكتوبر 2015، ص 16.

[2] مرسوم رئاسي رقم 19-172، مؤرخ في 6 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر، عدد 37، الصادرة بتاريخ 9 جوان 2019، ص 05.

[3] مرسوم رئاسي رقم 20-183، مؤرخ في 13 جويلية 2020، يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 40 الصادرة بتاريخ 18 جويلية 2020، ص 05.

[4] أنظر المادة 04 من المرسوم الرئاسي 20-183 سالف الذكر، ص 05 ص 06.

– مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لاسيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

– ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

– تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

– تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

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

– المساهمة في تحيين المعايير القانونية في مجال اختصاص الهيئة.

3– تنظيم الهيئة: وضع المرسوم الرئاسي لسنة 2020 كل من مجلس التوجيه ومديرية عامة، تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما. [1]

مجلس التوجيه: أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة لمجلس التوجيه بموجب المرسوم الرئاسي لسنة 2019، غير أنه عدل التشكيلة برئاسة رئيس

[1] المادة 05 من المرسوم الرئاسي رقم 20–183 ، ص 06.

الجمهورية ويمكنه أن يفوض ممثله، حيث يتشكل مجلس التوجيه من الوزير المكلف بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية وقام المرسوم بإضافة كل من المدير العام للأمن الداخلي وقائد الدرك الوطني والمدير العام للأمن الوطني وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوطني ويعين رئيس الجمهورية ممثلي رئاسة الجمهورية ووزارة الدفاع الوطني. وأضافت المادة 08 منه أن اجتماع مجلس التوجيه في دورة عادية مرتين في السنة، بناء على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية، كلما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

المديرية العامة: يريدها مدير عام، تعيينه أو إنهاء المهام يكون بموجب مرسوم رئاسي.

أسندت للمديرية العامة نفس الصلاحيات المنصوص عليها في مرسوم 2019، غير أن الاختلاف يكمن في أن المرسوم الجديد جعل من صلاحيات المديرية العامة مقيدة بوجوب موافقة مجلس التوجيه، على مشروع ميزانية الهيئة وإعداد وتنفيذ برنامج عمل الهيئة، ووجوب رفع التقرير السنوي لنشاطات الهيئة لمصادقة مجلس التوجيه.

كذلك أعيدت صياغة أسماء المديريات والمصالح التابعين للمديرية العامة، حيث تضم الهيئة[1]:

- **مديرية للمراقبة الوقائية واليقظة الالكترونية:** حيث أضافت المادة 15 صلاحية اليقظة الالكترونية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهو سبب تغيير المصطلح الذي كان في المرسوم الرئاسي لسنة 2019 "مديرية تقنية".

- **مديرية للإدارة والوسائل:** لم يتغير محتوى المادة في المرسوم الجديد.

[1] المادة 11 من المرسوم الرئاسي رقم 20-183، سالف الذكر، ص 7.

- **مصلحة الدراسات والتلخيص:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 19 منه.

- **مصلحة التعاون واليقظة الالكترونية:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 20 منه.

ثانيا: السلطة الوطنية لحماية المعطيات ذات طابع شخصي

استحدث المشرع الجزائري بموجب القانون 18-07 سلطة وطنية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي وهي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية وبالاستقلال المالي والإداري تضمن عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات.

ثالثا: وكالة أمن الأنظمة المعلوماتية

استحدثت منظومة وطنية لأمن الأنظمة المعلوماتية توضع لدى وزارة الدفاع، والتي تتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، والوكالة الوطنية لأمن الأنظمة المعلوماتية التي من بين مهامها إجراء التحقيقات الرقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية. [1]

وتعتبر وكالة أمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يقع مقرها في مدينة الجزائر.

[1] مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04، الصادر في 26 جانفي 2020، ص 05.

سير الوكالة:

تدير الوكالة لجنة توجيه وتزود بلجنة علمية، وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطة المدير العام الذي يسير بدوره الوكالة ويسهر على تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنفيذ المخططات والبرامج المسطرة من قبل لجنة التوجيه.

الفرع الثالث: الوحدات المكلفة بالتحقيق في الجرائم المعلوماتية

إن الأجهزة التابعة للأمن والدرك الوطني تسهر على المواجهة التنظيمية للجرائم المعلوماتية بشكل عمودي كل في مجال اختصاصه.

أولا: وحدات الدرك الوطني

تلعب مؤسسة الدرك الوطني دور فعال في مواجهة الجرائم المعلوماتية وتطويق نطاق الجرائم المعلوماتية من خلال استحداثها لتقنيات خاصة، وإنشاء وحدات خاصة.

أ- **المعهد الوطني للأدلة الجنائية وعلم الإجرام INCC /GN:** وهو جهاز تابع للدرك الوطني أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183 [1]، يتكون من 11 دائرة متخصصة في عدة مجالات تضمن الخبرة والتكوين والتعليم وتقديم المساعدات التقنية والبحوث والدراسات والتحاليل في علم الجريمة.

حيث تكلف دائرة الإعلام الآلي والإلكترونيك بمعالجة تحليل وتقديم كل دليل الكتروني وتماثلي للعدالة، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

[1] مرسوم رئاسي 04-183 المؤرخ في 26 جوان 2004، يتضمن أحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، عدد 41، الصادرة في 27 جوان 2004، ص 18.

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تحيين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية.

ولإنجاز المهام المنوطة بها تنقسم الدائرة إلى ثلاثة مخابر وكل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل:

1- مخبر الإعلام الآلي: يختص بتحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش)، كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية.

2- مخبر الفيديو: يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، كما يعمل على تحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات، ومقارنة الأوجه وشرعية الصور والفيديو.

3- مخبر الصوت: يختص بمعرفة وتحديد المتكلم، وتحديد شرعية التسجيلات الصوتية، ويعمل على تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة. [1]

ب- مركز الوقاية من جرائم المعلوماتية ومكافحتها CPLCIC /GN: وهو مركز تابع لأجهزة الدرك الوطني بدأ عمله منذ سنة 2004، والذي يكلف بمهمتين رئيستين:

المهمة الأولى: قبلية تتعلق بالتدقيق والوقاية.

المهمة الثانية: بعدية تتعلق بردع الجرائم الماسة بالطفولة.

وحديثا أنشأ مكتب خاص بحماية الأحداث عبر الانترنت بغرض تقديم الدعم التقني للوحدات الإقليمية في التحري وجمع الأدلة الجنائية.

[1] عرض مقدم من طرف: هواري عياش، المعهد الوطني للأدلة الجنائية، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، بسكرة، الجزائر.

في 2017 عالج المركز 100 جريمة تتعلق بالأطفال والمراهقين، و 20 جريمة مالية، حيث أن الجرائم المالية مازالت محدودة لأن التجارة الالكترونية والدفع الالكتروني مازال في بدايته، ويتوقع زيادة هذا النوع من الجرائم خلال السنوات المقبلة بعد تعميم التجارة الالكترونية، مما يتطلب الاستعداد لمواجهة من الجرائم المتعلقة بالتجارة الالكترونية عن طريق إنشاء مكتب خاص بالجريمة الاقتصادية ومختلف تحديات الفضاء السيبراني، وهذا يستدعي إطار قانوني متكامل من الجوانب العملية والتقنية وذلك عن طريق تكوين مختصين في الجرائم المعلوماتية في كل مجالاتها. [1]

ج- المصلحة المركزية للتحريات الجنائية SCIC /GN: تعد المصلحة المركزية للتحريات الجنائية مصلحة تابعة لأجهزة للدرك الوطني تقوم بالتحقيق التقني والعملي، ويبقى إجراء التحقيق في الجرائم المعلوماتية ليس بالأمر السهل، باعتبار أن هذا النوع من الجرائم المعاصرة لا يعترف بحدود المكان والزمان، كما أن إجراءات جمع الأدلة وتحديد هوية مرتكبي هذه الجرائم أو المشتبه بهم تبقى معقدة في ظل التكنولوجيات الحديثة.

وجدير بالذكر أن المحققين على المستوى المحلي من فصائل الأبحاث التي تشمل محققي جرائم الإعلام الآلي، يختصون بالتحقيق ومقاربة تقنية أولية [2]، وهو كذلك بالنسبة لخلايا الشرطة العلمية والتقنية على المستوى المحلي.

[1] مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الالكترونية تم حلها بنجاح، موقع الإذاعة الجزائرية، الدخول يوم 25-05-2019، على الساعة 05:34.

[2] عرض مقدم من طرف: عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، بسكرة، الجزائر.

ثانيا: وحدات الأمن الوطني

تتولى المديرية العامة للأمن الوطني التحقيق في الجرائم المعلوماتية عن طريق قسمين يشمل القسم الأول المخابر، ويشمل القسم الثاني الفرق، وفي سبيل نجاعة التحقيق لها دور فعال في مواجهة الجرائم المعلوماتية.

أ- **المخابر:** يوجد مخبر مركزي للشرطة العلمية في الجزائر العاصمة، ومخبر جهوي في قسنطينة ووهران [1] وقد استحدثت أقسام متخصصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة الكترونية قصد استخراج وتتبع ما من شأنه أن يفيد في التحقيق ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع، وأهم الأجهزة المستغلة من طرف هذه الأقسام:

1- أدوات التخزين الرقمية (أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة).

2- أجهزة الكمبيوتر ولواحقها. [2]

وحسب المعطيات الإحصائية لدائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية بقسنطينة، فقد شهد سنة 2014 ما يقارب 250 قضية محل تحقيق، أبرزها قضيتين تتعلق بالإنابة القضائية الدولية عن طريق مكتب الأنتربول أقدم فيهما شابين من ولاية قسنطينة بالاعتداء وتعطيل نظام معلوماتي خاص بموقع وزارة الخارجية الكويتية، والقيام باحتيال الكتروني على أهداف بالولايات المتحدة الأمريكية، وسجل الثلاثي الأول سنة

[1] وتجدر الإشارة أن هناك مخابر أخرى قيد الانجاز في ورقلة، بشار، تمنراست.

[2] حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، بسكرة، الجزائر، ص 08.

2015، 60 قضية تتعلق أغلبها بسوء استخدام مواقع التواصل الاجتماعي من خلال قضايا المساس بالأشخاص في صورة الابتزاز، القذف والتشهير... [1]

ب- وجود فرقة على مستوى كل أمن ولاية: في سبيل ضمان فاعلية التحقيق في مواجهة الجرائم المعلوماتية تم إنشاء ما يعرف بالمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي مصلحة تابعة لمديرية الشرطة القضائية مقرها على مستوى الجزائر العاصمة، ثم أنشأت خلايا تابعة للفرق الاقتصادية والمالية على مستوى أمن الولايات، تشمل خلية مكافحة الجرائم المعلوماتية، ثم مع تطور الجرائم واعتماد Modem و 3g، تم ترقية الخلية لتصبح فرقة في حد ذاتها، حيث أصبحت مستقلة وتابعة للفرق الولائية للشرطة القضائية، وتوجد فرق على مستوى 48 ولاية.

وكمثال عن بعض الإحصائيات على مستوى الفرق، كانت القضايا المنجزة من خلال فرقة مكافحة الجرائم المعلوماتية في أمن ولاية قالمة تقدر 153 قضية منجزة خلال الثلاث سنوات الأخيرة والموضحة في الجدول التالي:

المبحث الثاني: صعوبات التحقيق في الجريمة الإلكترونية

يتسم التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها جنائيا بالعديد من الصعوبات التي يمكن أن تعرقل وتصعب عملية التحقيق ومن أهم هذه المعوقات التي تواجه القائمين على مكافحة الجرائد الالكترونية والتحقيق فيها، عوائق تتعلق بالجريمة وعوائق تتعلق بالجهات المتضررة أو الضحية.

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة 1، 2016، ص 181.

المطلب الأول: صعوبات خاصة بالجريدة الإلكترونية

الفرع الأول: صعوبات تتعلق بالجريمة الإلكترونية

من المعوقات المتعلقة بالجريمة الإلكترونية هي:

1- إخفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه.

2- افتقاد أكثر الآثار التقليدية.

3- إعاقة الوصول إلى الدليل لاحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها والإطلاع عليها أو استنساخها.

4- سهولة محو الدليل أو تدميره في زمن قصير جدا، ومن الأمثلة على ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية، لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخرين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة.

فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده وبالتالي تتصله من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة.

ناهيك عن الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بالانترنت من قبل بعض الأطراف المعنية. [1]

الفرع الثاني: صعوبات تتعلق بجهات التحقيق

بعض هذه المعوقات ترجع إلى شخصية المحقق مثل التهيب من استخدام جهاز الكمبيوتر واستخدام الانترنت بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية والبعض الآخر يتعلق بالنواحي الفنية كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارة في استخدام الكمبيوتر والانترنت وعدم توفر المعرفة بأساليب ارتكاب الجرائم الكمبيوتر والانترنت والمعرفة باللغة الإنجليزية. [2]

إزاء ذلك يرى البعض أنه من المستحسن أن توكل مهمة التحقيق في مثل هذا النوع من الجرائم إلى بيوت الخبرة المتخصصة في هذا المجال لاسيما مع وجود شركات عالمية متخصصة للتحقيق في الجرائم المعلوماتية حققت النجاح في الكثير من المجالات. [3]

الفرع الثالث: صعوبات تتعلق بمرتكب الجريمة

مرتكب الجريمة الالكترونية يتطلب قدرا من الذكاء والمعرفة الدقيقة بالحاسب الآلي والشبكة المعلوماتية التي لا تتوفر لدى الشخص العادي، وعادة ما يكون مرتكب هذه الجرائم شخصا يتمتع بذكاء خارق يسمح له بخرق الأنظمة المعلوماتية ويقسم إلى صنفين:

- **المتسللون:** هم أشخاص يصلون بطرق غير قانونية إلى المعلومات في نظام حاسوبي ويبادرون في تعديل هذه المعلومات.

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 65 ص 66.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 69.

[3] أجعود فطيمة، مرجع سابق، ص 50.

– **المخربون:** فدورهم لا يقتصر على خرق المعلومات فقط وإنما يقومون بالعبث في البيانات والمعلومات المخزنة في الحاسوب. [1]

الفرع الرابع: صعوبات تتعلق بالدليل الالكتروني

إن الدليل الرقمي هو ذلك الدليل الذي يجد له رجال الضبطية القضائية أساسا في العالم الافتراضي يعود إلى الجريمة[2]، ويواجه المحقق صعوبات في التعامل مع الأدلة الإلكترونية نذكر منها ما يلي:

– مشاكل الدليل باعتباره غير مرئي ولا وجود لأثار مادية تقليدية مع صعوبة الوصول إلى الدليل بسبب استخدام وسائل حماية فنية ككلمات السر حول المواقع تمنع الوصول إليها أو تدميرها أو تشفيرها لإعاقة الوصول لها، والاطلاع على محتواها أو استنساخها:

– سهولة محو الدليل الإلكتروني أو تدميره في مدة قصيرة.

– وجود كم هائل من المعلومات والبيانات المتعين فحصها وعبورها لحدود الدولة الواحدة.

– إمكانية تخزين البيانات والمعلومات المتعلقة بالجريمة بأنظمة وشبكات الكترونية موجودة في دول مختلفة، ارتكاب الجريمة عن بعد، سرعة تنفيذ الجرائم المعلوماتية، مساس إجراءات التفتيش بخصوصيات الأفراد. [3]

[1] أجعود فطيمة، مرجع سابق، ص 49.

[2] عبير بعقيقي، فيصل بصيغة، الإثبات في الجرائم المعلوماتية على ضوء 09-04، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02، 2018، جامعة بسكرة، ص 35.

[3] أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم الالكترونية، أطروحة شهادة دكتوراه، الطور الثالث ل م د، تخصص قانون خاص، جامعة محمد البشير الإبراهيمي ب ب ع، كلية الحقوق، 2021/2020، ص 127.

المطلب الثاني: صعوبات خاصة بالضحية في الجريمة الإلكترونية

إن التحقيق في الجريمة الالكترونية خاصة فيما يتعلق بالضحية أو الجهة المتضررة يواجه عدة صعوبات في الكشف أو التوصل للدليل الإلكتروني للأسباب التالية:

الفرع الأول: أسباب خاصة بالضحية في الحرية الإلكترونية

إن الضحية في الجريمة المعلوماتية هو كل من أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع للتقنيات الالكترونية الرقمية. [1]

نتيجة لقلة خبرة الضحايا وكشفهم عن بعض المعلومات الشخصية عن حياتهم اليومية أو استعمالاتهم المفرطة لوسائل التواصل الاجتماعي، قد يؤدي إلى زيادة ارتكاب الجرائم المعلوماتية خاصة جرائم السب والشتم والابتزاز الإلكتروني، سرقة المعلومات الشخصية والاعتداء على حرمة الحياة الخاصة وقد يكون امتناع الضحايا عن التبليغ سببا في عدم مباشرة إجراءات التحقيق في الجرائم المعلوماتية ومن هذه الأسباب نذكر:

– قد يعود إلى الجهل بالقانون حيث أن عدم الإدراك بوجود نصوص تجرم وتعاقب على أشكال الجرائم المعلوماتية قد يكون سببا مباشرا في عدم التبليغ.

– عدم معرفة الضحية بالإجراءات التي يمكنه إتباعها في حالة التعرض للجرائم المعلوماتية.

– امتناع الشركات أو المؤسسات عن التبليغ خوفا على سمعتها وكيانها، وقد تكون الخشية بسبب أن التبليغ قد يكون فرصة ذهبية أمام الهجوم المعلوماتي لمعرفة ثغرات النظام المعلوماتي للمؤسسة ومختلف نقاط الضعف فيها.

[1] أومدور رجاء، مرجع سابق، ص.

– تخوف المؤسسات التجارية من استغراق التحقيق لفترة زمنية طويلة مع احتمالية احتفاظ جهات التحقيق بأجهزة الحاسب مما يؤثر على حسن سير العمل بتلك الشركات.

– امتناع الشركات والمؤسسات المالية (البنوك) عن التبليغ خشية من اهتزاز ثقة المتعاملين معها وبالتالي سحب ودائهم واستثماراتهم، ولا يقف الأمر على عدم التبليغ فقط بل يتعداه إلى الامتناع عن تقديم أي مساعدة لجهات التحقيق. [1]

الفرع الثاني: أسباب تتعلق بتحديد نطاق الضحايا

ويعود السبب في ذلك إلى أنهم في أغلب الأحيان لا يعلمون شيئا عن الجريمة إلا بعد وقوع الفعل وفي هذه الحالة يرون من الحكمة عدم الإبلاغ عنها كما لا يحبذ أكثرهم أن يعترف بأن نظامها المعلوماتي قد وقع هذه اعتداء وهذا السلوك السلبي يعتبر مغريا لمرتكبي الجرائم للاستمرار في أنشطتهم. [2]

اعتقاد بعض الضحايا بعدم قدرة الأجهزة الأمنية على التوصل لمرتكبي الجرائم بسبب نقص خبرتهم وعدم توفر الإمكانيات اللازمة للتوصل إلى المجرمين.[3]

التخوف من الإساءة للسمعة والفضيحة خاصة في الجرائم الإباحية والتشهير بالنساء أو في حالات الاعتداء الجنسي على الأطفال، وعرض صور إباحية لهم في مواقع الانترنت، كما أن تخوف الموظف من الحرمان من خدمة الانترنت، قد يكون سببا في

[1] مرجع سابق، ص 35–36.

[2] فتوح الشاذلي، عفيفي كامل عفيفي، جرائد الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقي، بيروت، 2003، ص 34.

[3] أومدور رجاء، مرجع سابق، ص 36.

امتناعه عن التبليغ حيث يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لمواقع غير مؤمنة أو غير مسموح بزيارتها. [1]

[1] أومدور رجاء، مرجع سابق، ص 128.

خلاصة الفصل الأول

مع تنامي ظاهرة الجرائم الإلكترونية وتخطي أثارها حدود الدول أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكشف عملية التحقيق وإثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثرا ماديا ملموسا كما هو الحال في الجرائم التقليدية.

ورغم الجهود المبذولة فإن هذه التحديات تبقى عصية على الحل في كثير من الأحيان في غياب إستراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها.

فضلا عما يثيره من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض إجراءات التحقيق كالمعاينة والتفتيش والضبط في نطاق البيئة الافتراضية.

الفصل الثاني:

آليات التحقيق في الجريمة الالكترونية

الفصل الثاني: آليات التحقيق في الجريمة الالكترونية

إن التحقيق بشكل عام يعتمد على ذكاء المحقق وفطنة وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق والبحث فيها ومتابعتها والبحث في الأدلة والتنقيب عنها وصولا إلى إظهار الحقيقة.

ولقد تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة وتطور أساليب ارتكابها فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الانترنت هي الصفة المميزة والغالبة ومرد ذلك هو حدوث طفرة علمية من مجال تكنولوجيا المعلومات. [1]

ولتوضيح ذلك تطرقنا في هذا الفصل في المبحث الأول إلى الإجراءات المتبعة للتحقيق في الجريمة الالكترونية (العادية والمستحدثة) أما الحديث الثاني فخصصناه إلى آليات التعاون الدولي للتحقيق في الجريمة الإلكترونية.

[1] د. عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جانفي 2018، ص 50.

المبحث الأول: الإجراءات المتبعة للتحقيق في الجرائم المعلوماتية

إن طبيعة الوسط الافتراضي، يتطلب إعادة تقييم منهج الإجراءات التقليدية، خاصة وأن الوسائل المستخدمة في ارتكاب الجرائم المعلوماتية تختلف عن الوسائل التقليدية، مما يتطلب مواكبة الإجراءات للتطورات الحاصلة في المجال المعلوماتي، لتسهيل التعامل مع الحاسب الآلي وكافة الأجهزة الحديثة والمحافظة على الأدلة المستخلصة منها، مع مراعاة عدم المساس بالحريات وحقوق الإنسان، إلا لمقتضيات التحري والتحقيق مع مراعاة الضمانات المقررة قانونا بشأنها، سواء أكانت هذه الإجراءات عادية أو مستحدثة.

المطلب الأول: الإجراءات العادية للتحقيق في الجريمة الإلكترونية

ويمكن القول أن هذه الإجراءات تكمن في إجراء التفتيش المعلوماتي والمعانية والخبرة.

الفرع الأول: إجراء التفتيش المعلوماتي

ويمكن تعريف التفتيش المعلوماتي على أنه: إجراء من إجراءات التحقيق يهدف إلى الوصول إلى أدلة منبثقة من جناية أو جنحة لإثبات ارتكابها ونسبتها إلى المتهم، بشرط أن يكون تحقق وقوعها فعلا داخل نظم المعالجة الآلية للمعطيات. [1]

أولا: تفتيش الحاسب الآلي

يشتمل الحاسب الآلي على مجموعة من المكونات المادية المتمثلة في الوحدات المختلفة (وحدات الإدخال كلوحة المفاتيح والماسح الضوئي والميكروفون، وحدات الإخراج كالشاشة والطابعة والسماعات)، كما يشتمل على مجموعة من المكونات المعنوية المتمثلة

[1] أومدور رجاء، موضع سابق، ص137.

في المعلومات والبيانات المعالجة آليا، غير أن التساؤل يثور حول مدى قابلية هذه المكونات للتفتيش؟

أ- بالنسبة لتفتيش مكونات الحاسب الآلي المادية

لا يوجد إشكال حول إمكانية خضوعها للتفتيش غير أن ذلك يتوقف على طبيعة المكان: فإذا كان المكان خاصا؛ لا يجوز تفتيشه إلا بنفس الضمانات المقررة قانونا في التفتيش التقليدي، أما إذا كان المكان عاما؛ لا يجوز التفتيش إلا بنفس الضمانات والقيود المرتبطة بتفتيش الأشخاص. [1] وهناك بعض التشريعات تبين ضوابط التفتيش لمكونات الحاسب الآلي، ومنها قانون المنافسة الكندي، حيث يتيح للقائم بالتفتيش إمكانية استخدام أي نظام الأجهزة الحاسب الآلي لتفتيش أي بيانات وبإمكانه أن يعمل على تسجيل تلك البيانات في شكل مطبوعات أو مخرجات أخرى. [2]

ب- بالنسبة لتفتيش مكونات الحاسب الآلي المعنوية

هي محل خلاف فقهي، حيث يرى جانب من الفقه أن المكونات المعنوية لا تصلح بطبيعتها لأن تكون محلا للتفتيش والضبط باعتبار أن التفتيش يهدف إلى ضبط أدلة مادية وهذا يقتضي أحكاما خاصة تكون أكثر ملائمة لتفتيش وضبط تلك البيانات غير المحسوسة،

أما عن موقف المشرع الجزائري يمكن اعتباره جعل التفتيش يمتد ليشمل جميع المكونات المادية والمعنوية، وتبرير ذلك نص المادة 81 من قانون الإجراءات الجزائية "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة" حيث استعمل في نص المادة مصطلح "أشياء".

[1] خالد عياد الحلبي، الدليل الالكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017، ص 159.

[2] يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري (دراسة مقارنة)، ط1، دار النهضة العربية، القاهرة، 2017، ص 341.

ثانيا: تفتيش شبكات الحاسب الآلي

قد تمتد شبكات الحاسب الآلي في الدولة نفسها أو إلى عدة دول:

أ- في حالة اتصال حاسب المتهم بحاسب آخر في نفس الدولة

وقد تطرق المشرع الجزائري لتوسيع الصلاحيات في تفتيش الجرائم المعلوماتية إلى كامل امتداد التراب الوطني، حيث يجوز إجراؤه في كل محل سكني أو غير سكني، وفي أي وقت، بناء على إذن مسبق من وكيل الجمهورية المختص، كما يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين بذلك، مع إمكانية اتخاذ تدابير أخرى أو الأمر باتخاذ تدابير تحفظية بناء على تسخير النيابة العامة أو طلب من ضباط الشرطة القضائية. [1]

ب- في حالة اتصال حاسب المتهم بحاسب آخر خارج حدود الدولة

وقد انتهج المشرع الجزائري إمكانية امتداد التفتيش إلى خارج الإقليم الوطني وذلك وفقا لمبدأ المعاملة بالمثل وبمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات ذات الصلة وهذا في حالة اتصال حاسب المتهم بحاسب آخر خارج الدولة. [2]

الفرع الثاني: المعاينة والخبرة في الجرائم المعلوماتية

تعتبر الخبرة والمعاينة من أكبر العقبات التي تواجه الإثبات في الجرائم المعلوماتية، فالمعاينة قد تكون شخصية تتعلق بشخص المجني عليه، كما قد تكون مكانية تتعلق بمكان

[1] انظر الفقرة 03 و 04 من المادة 47 من الأمر 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[2] ونصت في ذلك المادة 5 فقرة 3 من القانون 09-04 على أنه: (... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل...).

ارتكاب الجريمة، وتتعلق المعاينة العينية بالأشياء والأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الأمر الاستعانة بخبير وفي هذه الحالة نكون أمام إجراء آخر من إجراءات التحقيق وهو الخبرة التي تعد أهم وسائل الأدلة.

أولا: المعاينة في الجرائم المعلوماتية

المعاينة هي إجراء يتضمن وصف مكان الحادث بما فيه من أشياء، أشخاص، مع الفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان، والتي تشير إلى شخصيته وشركائه، وما يفيد في إثبات ارتكاب الجريمة وتوضح قدرا من الاستنتاجات التي تشكل في حد ذاتها الأساس الذي يقوم عليه التحقيق.

ويقصد بمعاينة مسرح الجريمة المعلوماتية معاينة الآثار والبصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه، أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي والشبكة العالمية، أو التي من الممكن أن يطلق عليها البصمات المعلوماتية، وذلك مع ضرورة مراعاة مبدأ الشرعية والخصوصية المعلوماتية للأفراد ودون البحث في المحتوى إلا في حدود السلطات القصرية الممنوحة لجهات التحقيق.[1]

1- الإجراءات المتخذة قبل وأثناء إجراء المعاينة

يشير الفقه إلى أن ارتكاب الجريمة على المكونات المادية للحاسب الآلي مثل جرائم الاعتداء على أشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومفاتيح التشغيل والأقراص وغيرها، لا تثير صعوبة في معاينتها والتحفظ على الأشياء التي تعد أدلة مادية تدل على ارتكاب الجريمة ونسبتها إلى مرتكبها، في حين أن المكونات المعنوية كالجرائم

[1] أومدور رجاء، مرجع سابق، ص153.

الواقعة على برامج الحاسب الآلي وبياناته أو بواسطتها، تثير العديد من الصعوبات أهمها قلة الآثار المادية التي قد تتخلف عن هذه الجرائم، كذلك تردد عدد كبير من الأشخاص على مسرح الجريمة خلال مدة زمنية طويلة نسبيا تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها، مما يمنح فرصة لحدوث تغيير أو عبث بالآثار المادية أو زوال بعضها، كذلك إمكانية التلاعب بالبيانات عن بعد أو حذفها، مما يتطلب الحذر عند إجراء المعاينة واتخاذ مجموعة من الإجراءات قبل وأثناء المعاينة. [1]

أ- الإجراءات الواجب إتباعها قبل معاينة مكان الجريمة المعلوماتية

إن أهم إجراء لابد من إتباعه قبل معاينة مكان الجريمة المعلوماتية هو توفير معلومات مسبقة عن مكان الجريمة، ونوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها. [2]

ونظرا لخطورة الجرائم المعلوماتية وإمكانية تلف الأدلة أو ضياعها فينبغي قبل المعاينة الإعداد الجيد لعدم تسرب الأدلة أو ضياعها، واصطحاب خبراء متخصصين لمرافقة فريق التحقيق، كما ينبغي اصطحاب وسيلة توليد كهرباء بديلة وآمنة، حتى لا ينقطع التيار الكهربائي أثناء الفحص لتفادي تلف الأدلة، إضافة إلى ضرورة وجود مجموعة من البرامج المساعدة على فحص مكونات الحاسب الآلي كالمتعلقة باستعادة الملفات المحذوفة، وبرامج كسر كلمات المرور وبرامج فحص الهواتف المحمولة. [3]

ب- الإجراءات الواجب إتباعها أثناء القيام بالمعاينة

تصوير الجهاز والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة، وملاحظة طريقة إعداد نظام الحاسب بعناية، واثبات حالة

[1] أومدور رجاء، مرجع سابق، ص 155.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 157.

[3] حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017، ص 57.

التوصيلات والكابلات المرتبطة بالحاسب والتي تكون متصلة بمكونات النظام، وهذا لتسهيل القيام بالمقارنة والتحليل عند عرض الموضوع على المحكمة، وينبغي عدم التسرع في نقل أية مادة معلوماتية من مكان وقوع الجريمة لعدم إتلاف البيانات المخزنة. [1]

كذلك لابد من فحص سلة المهملات لمعرفة الملفات المحذوفة مؤخرا بالإضافة إلى استخدام برامج استعادة الملفات المحذوفة، التحفظ على المستندات الخاصة بالإدخال وملحقات الحاسب الآلي المادية الورقية المرتبطة بالجريمة وكل الآثار التي تفيد التحقيق، الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز وكذلك التأكد من وجود نسخة منها محفوظة على الحاسب نفسه، والفحص بدقة لكل ملفات الجهاز، خاصة ملفات Log file للتعرف على العمليات التي قام بها المستخدم والمواقع التي ارتادها على شبكة الانترنت. [2]

2- ضوابط المعاينة بعد وقوع الجريمة في المجال الالكتروني

- استعداد فريق التحقيق الذي سيتولى إجراء المعاينة من الناحية الفنية والعملية، ولابد من قصر المعاينة على ذوي الخبرة في المجال المعلوماتي.

- إعداد خطة عمل للمعاينة وكيفية إجرائها.

- تأمين جميع الأجهزة الالكترونية بما في ذلك الشخصية والمحمولة وإبعاد أي شخص لا علاقة له بمهمة التحقيق.

[1] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، مصر، 2011، ص 111.

[2] حازم محمد حنفي، مرجع سابق، ص 57.

– تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، مع تسجيل وقت ومكان التقاط كل صورة، مع التركيز بصفة خاصة على الأجزاء الخلفية للحاسب الآلي وملحقاته، ومراعاة وقت وتاريخ ومكان التقاط كل صورة. [1]

– دقة ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، ليتمكن المحقق من المقارنة والتحليل فيما بعد عند عرض الأمر على المحكمة.

– مراعاة عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة على الوسائط المعلوماتية. [2]

– التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة، والشرائط والأقراص الممغنطة، وفحصها ورفع البصمات ذات الصلة بالجريمة، كذلك التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، ولابد أن تتم الإجراءات وفقا لمبدأ المشروعية وفي إطار ما تنص عليه القوانين الإجرائية.

– تحريز الأدلة الالكترونية المتحصلة من مسرح الجريمة من خلال ضبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، مراعاة ظروف الحرارة والرطوبة لتخزينها والالتزام بالقواعد الفنية المتعلقة بنقلها، مع تأمين البرامج المضبوطة قبل تشغيلها فنيا وعمل نسخ احتياطية سليمة وكاملة، وتمييز كل دليل الكتروني عن غيره بوضع علامة مادية خاصة به. [3]

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 164.

[2] أومدور رجاء، مرجع سابق، ص 157.

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 177.

ثانيا: الخبرة في مجال الجرائم المعلوماتية

الخبرة هي عبارة عن إجراء من إجراءات التحقيق التي تستوجب الإلمام بمجموعة من المعلومات الفنية التي تساعد في استخلاص الأدلة اللازمة للتوصل إلى الحقيقة القضائية.

وتعرف الخبرة القضائية على أنها استشارة فنية يستعين بها قاضي التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه بحكم تكوينه، ولعل دواعي اللجوء إلى الخبير كثيرة وهي في تزايد مستمر نتيجة المستجدات على الساحة العلمية ولجوء الجناة إلى وسائل عصرية متطورة في ارتكاب الجريمة، حيث لا يمكن كشفها إلا بواسطة ذوي الاختصاص وما يزيد في الحاجة إلى الخبير هو طبيعة تكوين قضاة التحقيق الذي يغلب عليه العمومية. [1] في حين أن للخبير كفاءة في اختصاص معين بذاته.

وفي ذلك يعد الخبير التقني شخص مؤهل علميا وعمليا يتميز بالكفاءة والتخصص التعامل مع شبكة الانترنت وأنظمة وبرمجيات الحاسب الآلي وفهم لغته.

1- ندب الخبراء

تعتبر الخبرة في مجال التحقيق الجنائي أحد ذروع المحقق الجنائي في الجرائم المعلوماتية وتظهر أهميتها بصفة عامة في كونها إجراء تحقيق تتحرك به الدعوى الجنائية وذلك بانتداب الخبير، وتظهر أهمية انتداب هذا الأخير في الجرائم المعلوماتية في كونه مؤثرا في سير الدعوى الجنائية، فبعد أن يدلي برأيه شفاهية لسلطة التحقيق أن تقرر عدم إحالة المتهم إلى المحاكمة وأن تأمر إلا وجه لإقامة الدعوى الجنائية، هذا فضلا عن كون الخبير التقني أحد أعضاء فريق التحقيق في الجرائم المعلوماتية ابتداء.

[1] أحسن بوسقيعة، التحقيق القضائي، ط10، دار هومة، 2012، ص 107-108.

يكتسي ندب الخبراء أهمية قصوى في إجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين و تحليلها وكشف أي تلاعب في البرامج و المعلومات. [1]

ولقد أوجبت المادة 143، 146 من قانون الإجراءات الجزائية الجزائري على قاضي التحقيق أن يحدد بدقة في الأمر بندب خبير المهمة المطلوبة منه والأسئلة الفنية أو العملية التي يطلب الاستفسار فيها، وأن هذه المهمة لا يجوز أن تتعلق إلا بفحص مسائل ذات طابع فني، ولا يفوض فيها أي جزء من جوانب اختصاصه، لأن ذلك قد يعرض أمره للبطلان ولابد أن تجرى الخبرة تحت مراقبة وإشراف قاضي التحقيق، ويتعين على الخبير اطلاع القاضي بكل ما توصل إليه من نتائج ويعلمه بتطورات الأعمال التي يقوم بها، لاتخاذ الإجراءات اللازمة.

2- دور الخبرة في مجال الجرائم المعلوماتية

للخبير التقني دور وقائي وهو حماية وتأمين النظام محل الاعتداء من استمرار التهديد المعلوماتي ضده، كالحد من استمرار انتشار الفيروسات التي يمكن أن تنتقل وتسجل أوتوماتيكيا على الحاسبات والتي يمكن أن تدمر ما تبقى من النظام المعلوماتي، أو أن يساعد على وقف التجسس المعلوماتي بنسخ الملفات أو بمنع سرقة وقت الآلة. [2]

كما تساعد الخبرة في مجال الجرائم المعلوماتية في الكشف عن الدليل الالكتروني وتحديد خصائصه المميزة وخصائص كل جزء منه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، الأصوات وغيرها، ويقوم الخبير بعمل نسخة أصلية منه للتأكد من عدم وجود معلومات مفقودة أثناء استخلاصه ويمكن إجراء اختبارات عليه للتحقق من أصالته

[1] أومدور رجاء، مرجع سابق، ص 160.

[2] محمد كمال شاهين، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2018، ص 335.

ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون، كما تساعد الخبرة في إصلاح الدليل وإعادة تجميعه من المكونات المادية للحساب الآلي، وفي جمع الآثار المعلوماتية الرقمية، واستخدام خوارزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله. [1]

يكون عمل الخبير بحضور وتحت إشراف المحقق، ويرى الفقه أن حضور المحقق هو بمثابة رقابة إجرائية لتسهيل مهمة الخبير ومساعدته في تعيين مكان البحث وتوفير الظروف الموضوعية، غير أنه لا يجوز للمحقق التدخل في الأعمال الفنية التي يجريها الخبير، وينحصر دور الخبير في إبداء رأيه في المسائل الفنية التي حددها له المحقق، وله أن يستعين بغيره من الخبراء نظرا لعدم وجود خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها ولا خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع بواسطة أو على الحاسب الآلي. [2]

وبالإسقاط على ما جاء في قانون الإجراءات الجزائية الجزائري فقاضي التحقيق أو القاضي الذي تعينه الجهة القضائية له أن يراقب أعمال الخبرة، وإذا ظهر للخبير مسألة تقنية خارجة عن اختصاصه فيجوز للقاضي أن يصرح لهم بضم فنيين متخصصين، ويؤدي الفنيون المعينون على هذا الوجه نفس يمين الخبراء ويرفق تقريرهم بكامله بتقرير الخبراء. [3]

حجية تقرير الخبرة

عند الانتهاء من الخبرة يحرر الخبراء تقريرا، وبالرجوع إلى المادة 153 من قانون الإجراءات الجزائرية الجزائري فتقرير الخبرة لابد أن يشتمل على وصف ما قام به الخبراء من أعمال ومختلف النتائج التي تم التوصل إليها، وعليهم أن يشهدوا بقيامهم بالأعمال المطلوبة

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 302.

[2] محمد كمال شاهين مرجع سابق، ص 338.

[3] المادة 149 من قانون الإجراءات الجزائية.

منهم شخصيا، ومن ثم يقومون بالتوقيع على تقرير الخبرة ويودع لدى كاتب الجهة القضائية التي أمرت بالخبرة وتثبيت الإبداع بموجب محضر. [1]

المطلب الثاني: الإجراءات المستحدثة للتحقيق في الجريمة الإلكترونية

الفرع الأول: الإجراءات المتعلقة بالبيانات الإلكترونية المتحركة

نص المشرع على المراقبة التقنية لضروريات التحقيق، نظرا للتطور الهائل في مجال التكنولوجيا، وما جاءت به من صعوبة اكتشاف الجريمة وتتبع آثار المجرم المعلوماتي.

أولا: مراقبة الاتصالات الإلكترونية

نص المشرع الجزائري على هذا الإجراء من خلال المواد 65 مكرر 5 إلى 65 مكرر 10 قانون إجراءات جزائية، وذلك تحت الفصل الرابع بعنوان: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور فهي تعتبر استثناءا لمبدأ الحق في الخصوصية، وعمل المشرع الجزائري على استحداث القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في الفصل الثاني المادة 04 التي نظم فيها الحالات التي يسمح باللجوء إلى مراقبة الاتصالات. [2]

على هذا النحو خرج المشرع الجزائري عن القاعدة العامة التي تقضي تنفيذ إجراءات التحقيق عند ارتكاب الجريمة لجمع الأدلة والقرائن وجعل من مراقبة الاتصالات الالكترونية مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة من خلال القيام بعمليات المراقبة المسبقة، هذا ما نصت عليه المادة 3 من القانون 09-04 التي أقرت أو حددت الدواعي

[1] أومدور رجاء، مرجع سابق، ص 162.

[2] مرزوقي كريمة، مراقبة الاتصالات الالكترونية وحق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 5، العدد 2، 2020، جامعة تيزي وزو، ص 1370.

من القيام بمراقبة الاتصالات الالكترونية، المتمثلة في مقتضيات حماية النظام العام ومستلزمات التحريات أو التحقيقات القضائية الجارية.

يقصد بمراقبة الاتصالات الالكترونية وفقا للقانون 09-04 المادة 2 فقرة و الاتصالات الالكترونية "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".[1]

وحالات اللجوء إلى المراقبة الالكترونية التي نظمها المشرع الجزائري في المادة 4 من القانون 09-04 هي: [2]

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

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

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ثانيا: التفتيش في المنظومة المعلوماتية

موضوع التفتيش في الجريمة المعلوماتية: إذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر تطبق القواعد التقليدية للتفتيش.[3]

[1] المادة 2 من القانون 09-04 المذكور سابقا.

[2] ومن الشروط اللازمة لإجراء المراقبة وجود الإذن بالمراقبة والتزام بالسرية أثناء إجراء التحقيق واستعمال المعطيات المتحصل عليها في إطار القانون.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 187.

ولكن الصعوبة تكمن في الجرائم الواقعة على برامج الكمبيوتر وبياناته لأنه بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش، عبر إرسالها من خلال نظام معلوماتي من مكان لآخر، وعلى اعتبار أن التفتيش عن هذه البيانات يستوجب الكشف عن الرقم السري، ولا أحد يعرفه سوى الجاني ولا يمكن إجباره على البوح به. [1]

ولتخطي هذه الصعوبات أوضح المشرع الجزائري في الفقرة 2 من المادة 5 من القانون 09-04 ".....انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك مسبقا".[2]

يجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

كما حددت المادة 7 من القانون 09-04 "الحجز عن طريق من الوصول إلى المعطيات": "..... يتعين على السلطة التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة". [3]

ثالثا: التسرب

هو إجراء يقوم به ضابط الشرطة القضائية أو أحد أعوانه تحت مسؤوليته بتنسيق العملية لمراقبة الأشخاص المشتبه فيهم بإيهامهم أنه فاعل معهم أو شريك لهم. [4]

---

[1] المرجع السابق، ص 189.

[2] المادة 05 من القانون 09-04.

[3] المادة 07 من القانون 09-04.

[4] أومدور رجاء، المرجع السابق ، ص 177.

وهو إجراء جديد نظمه قانون الإجراءات الجزائية في الفصل الخامس تحت عنوان التسرب من المواد 65 مكرر 11 إلى 65 مكرر 18، إذا اقتضت ضرورة التحري والتحقيق اللجوء له في الجرائم السبعة المحددة على سبيل الحصر وتتمثل في: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.[1] ولصحة هذا الإجراء عند اقتضاء ضرورات التحري والتحقيق في الجرائم المذكورة أعلاه يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط في المواد أدناه.[2]

الفرع الثاني: الإجراءات المتعلقة بالبيانات الالكترونية المخزنة

تعطي البيانات الالكترونية المخزنة أهمية بالغة في مجال التحقيق في الجرائم المعلوماتية، لهذا ينبغي حمايتها والمحافظة عليها من كل ما يؤدي إلى تلفها أو تعديلها. [3]

وتكمن أهمية الحفاظ عليها في اعتبارها أدلة إثبات، تستخدمها سلطات التحقيق التي تشكل دليلا في مواجهته، كما يمكن من خلالها تتبع آثار المجرم ومعرفة هويته.[4]

وقد نصت المادة 2 فقرة **د** من القانون 09-04 على المقصود بمقدمة الخدمات.

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

[1] المادة 65 مكرر 11 من قانون إجراءات جزائية، ص 50.

[2] أومدور رجاء، نفس المرجع، ص 178.

[3] أومدور رجاء، نفس المرجع، ص 182.

[4] نفس المرجع، ص 182.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها. [1]

أولا: الالتزامات العامة لمقدمي الخدمات

في إطار الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نص المشرع الجزائري على مساعدة مقدمي الخدمات للسلطات المكلفة بالوقاية ومكافحة هذا الإجرام الالكتروني.

وقد حدد المشرع الجزائري في المادة 11 من القانون 09-04 المعطيات التي يلتزم مقدمو الخدمات بحفظها على سبيل الحصر وتشمل:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل الاتصال.

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها. [2]

- بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

[1] المادة 2 من القانون 09-04.

[2] المادة 11 من القانون 09-04.

كما نص المشرع الجزائري على العقوبات المقررة في حالة الإخلال أو عدم احترام الالتزامات المنصوص عليها في هذه المادة، فعندما يؤدي إلى عرقلة سير التحقيقات والتحريات القضائية تقوم المسؤولية الجزائية سواء بالنسبة للأشخاص الطبيعيين أو المعنويين، وتقرر العقوبة للشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات وبغرامة مالية تقدر من 50.000 دج إلى 500.000 دج أما بالنسبة للأشخاص المعنوية تقدر بغرامة مالية وفقا لقانون العقوبات.

ثانيا: الالتزامات الخاصة بمقدمي الخدمات

إضافة على الالتزامات المفروضة على مقدمي الخدمات التي جاءت بها المادة 10 من القانون 09-04 المتمثلة في تقديم المساعدة للسلطات وحفظ المعطيات المتعلق بحركة السير، فقد أضاف المشرع الجزائري بعض الالتزامات الخاصة من خلال المادة 12 من القانون السالف الذكر.

المادة 12 زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه يتعين على مقدمي الخدمات ما يلي: [1]

أ- التدخل الفوري لسحب محتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

[1] المادة 01 من القانون 09-04.

المبحث الثاني: التعاون الدولي في مواجهة الجرائم الإلكترونية

في ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظرا للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديها سواءا كانوا أفرادا أم مؤسسات أم مجتمعات محافظة بأكملها، وهو ما دفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الانترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة. [1]

إن تفاقم الإجرام العابر للحدود أدى إلى تكثيف الجهود الدولية للحد من انتشار هذه الجرائم عبر القارات. [2]

وهذا ما جاء به القانون 09-04 في الفصل السادس تحت عنوان "التعاون والمساعدة القضائية الدولية – الاختصاص القضائي – المادة 15".... تختص المحاكم الجزائرية بالنظر في الجرائد المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني. [3]

المطلب الأول: آليات التعاون الدولي في مواجهة الجرائم الالكترونية

مع تفشي ظاهرة الإجرام الالكتروني وانتشاره في العالم كان لزاما على جميع الدول ومهما بلغت قوتها أن توحد جهودها للقضاء على هذه الجرائم الالكترونية، فكان من الضروري أن تكون القوانين متجانسة بين مختلف الدول فيما يتعلق بالإجراءات والآليات المتفق عليها فالهدف واحد وهو منع وقوع مثل هذه الجرائم والحد منها.

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 393.

[2] أومدور رجاء، مرجع سابق، ص 217.

[3] انظر المادة 15 من القانون 09-04.

وتتمثل أشكال التعاون الدولي في:

الفرع الأول: المساعدة القضائية

تعرف المساعد القضائية الدولية بأنها "كل إجراء تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم.

فهي في الغالب تتم عن طريق اتفاقيات دولية تنطوي على تبادل السلطات المعلومات لمعاقبة وإلقاء القبض على مرتكبي الجريمة الالكترونية. [1]

في إطار التحقيق في الجرائم الالكترونية، منح القانون السلطات المختصة إمكانية تبادل المساعدة القضائية في إطار التعاون الدولي في شكل الكتروني مع رفض أي طلب مساعدة من شأنه أن يمس بالسيادة الوطنية أو النظام العام.

هذا ما أكدته الفقرة الأولى من المادة 16 والمادة 18 من القانون 09-04.

أولا: صور المساعدة القضائية

تتخذ المساعدة القضائية ثلاث صور وهي:

1- تبادل المعلومات: يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، إما عن الاتهامات التي وجهت إلى رعاياها في الخارج أو الإجراءات التي اتخذت ضدهم وقد يشمل التبادل السوابق القضائية للجناة.

مما لتبادل المعلومات من أهمية قصوى بوصفه وسيلة لمكافحة الجرائم بصفة عامة والجريمة الالكترونية بصفة خاصة، لما توفره هذه المعلومات من مساعدة لأجهزة تنفيذ

[1] أجعود فطيمة، مرجع سابق، ص 71.

القانون، ويشمل هذا المبدأ تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة الكترونية.

وهذا ما نصت عليه اتفاقية بودابيست في الفقرة 1 من المادة 25 توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو بجمع أدلة جريمة جنائية في شكل الكتروني. [1]

ونجد أن الجزائر من ضمن الدول المتفقة على تبادل المعلومات هذا بالرجوع إلى المادة 17 من القانون 09-04 "تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل". [2]

2- نقل الإجراءات

يقصد به قيام دولة ما بناءا على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة أهمها التجريم المزدوج وأهمية الإجراءات في الوصول إلى الحقيقة.

الطبيعة الخاصة للجرائم الالكترونية بعبورها للحدود الوطنية وصعوبة إقامة الدليل على ارتكابها ومدى قبول التشريعات الدولية للأدلة المستمدة من الحاسب الآلي كذلك ما

[1] أجعود فطيمة، مرجع سابق، ص 72.

[2] المادة 17 من القانون 09-04.

يتعلق بمسائل الضبط والتفتيش في البيئة الافتراضية وهو ما يؤدي إلى صعوبة إثبات الجرائم ونسبتها لمرتكبيها مما استدعى التعاون الدولي في مجال تفتيش أجهزة الحاسب الآلي. [1]

3- الإنابة القضائية

وهو إجراء من إجراءات الدعوى تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها. [2]

ولضرورة الفصل في مسألة معروضة على سلطة قضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، ويهدف هذا الإجراء إلى تسهيل الإجراءات بين الدول بما يخص إجراءات التحقيق اللازمة كتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمتع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل إقليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش. [3]

ثانيا: القيود الواردة على طلبات المساعدة القضائية

لكي تكون هذه الطلبات صحيحة وقانونية لابد من

- أن يكون في تنفيذ طلبات المساعدة القضائية عدم المساس بالسيادة الوطنية والنظام العام.

- ضرورة المحافظة على سرية المعلومات المتبادلة.

- عدم استعمال هذه المعلومات في غير موضع الطلب.

[1] أجعود فطيمة، ص 73.

[2] أومدور رجاء، المرجع السابق الذكر، ص 222.

[3] محمد أحمد سليمان عيسى، المرجع السابق الذكر، ص 56.

هذا ما أكده المشرع الجزائري في المادة 18 من القانون 09-04 "القيود الواردة على طلبات المساعدة القضائية الدولية".[1]

الفرع الثاني: تسليم المجرمين

هي عملية في الغالب يكون منصوص عليها في الاتفاقيات والمعاهدات الدولية، والمشرع الجزائري نص في القانون 09-04 على اختصاص السلطات القضائية في المادة 15 "..... عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية".[2]

غير أن المشرع الجزائري اغفل على تسليم المجرمين في القانون السالف الذكر، في حالة فرار المجرم المعلوماتي غير أنه وطبقا للاتفاقية العربية لمكافحة الجرائم تقنية المعلومات اشترطت على ضرورة وجود اتفاقية من أجل تسليم المجرمين في هذا النوع من الجرائم.

بينما نصت اتفاقية بودابيست على المبادئ ذات الصلة بتسليم المجرمين من خلال نص المادة 24 التي تضمنت الأحكام الخاصة بتسليم المجرمين.

كما اخضع المشرع الجزائري بعض جوانب نظام تسليم المجرمين إلى أحكام دستورية والتي قضت بعدم جواز تسليم أحد خارج التراب الوطني إلا بناءا على طلب تسليم المجرمين وعدم جواز تسليم اللاجئين السياسيين.

وهذا ما تضمنته ق إ ج في الكتاب السابع المتعلق بعلاقات بين السلطات القضائية الأجنبية حيث وضع شروط تسليم المجرمين بموجب المواد 694 إلى 701 من ق إ ج و

[1] المادة 18 من القانون 09-04 السالف الذكر ص 8.

[2] المادة 15 من القانون 09-04.

إجراءات التسليم من المواد 702 إلى 713 من ق إ ج وآثار التسليم في المواد 714 إلى 718 من نفس القانون السالف الذكر.

وأقرت المادة 718 على عدم جواز إعادة التسليم أي عند تسليم دولة ما مجرم لا يجوز على الدولة المستلمة إعادة تسليمه إلى دولة أخرى إلا بشروط معينة. [1]

1- شروط تسليم المجرمين: لصحة هذا الإجراء لابد من:

- التجريم المزدوج: أن يكون الفعل المجرم في كلتا الدولتين الطالبة والمطلوب منها.

- اختصاص الدولة طالبة التسليم بملاحقة الشخص المطلوب تسليمه من جهة، ومن جهة أخرى يجب أن يكون الفعل المعاقب عليه طبقا للقانون الجزائري.

- عدم جواز تسليم اللاجئين السياسيين.

2- إجراءات التسليم: يقم طلب التسليم ويكون كتابة إلا في حالة الاستعجال و هذا ما نصت علية المادة 16 في الفقرة 2 من القانون 09-04 "..... قبول طلبات المساعدة القضائية الواردة في الفقرة أ إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

- دراسة الطلب ثم الرد عليه في النهاية.

الفرع الثالث: التعاون الأمني على المستوى الدولي

هو وسيلة لمحاربة الجريمة الالكترونية، حيث تمكن الدول من تتبع المجرمين خارج الحدود الوطنية من خلال أجهزته التي تعمل بمساعدة الدول للحد من هذه الجرائم، فالتعاون

[1] أجعود فطيمة، مرجع سابق، ص 75.

الأمني يشمل المجال الشرطي والقضائي والقانوني، فلتحقيق الأمن يتطلب تنفيذ إجراءات تتعلق بتلك المجالات مجتمعة. [1]

فالتعاون الدولي الأمني من أهم أشكال التعاون الدولي بالخصوص في الجرائم الالكترونية، لهذا تقوم المنظمة الدولية للشرطة الجنائية الانتربول بدور أساسي في ترسيخ دعائم هذا التعاون.

أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة. [2]

المطلب الثاني: معوقات التعاون الدولي في مواجهة ج.إ وسبل تفاديها

رغم وجود اتفاقيات ومعاهدات دولية، وجل التشريعات تنادي بالتعاون الدولي إلا إن هناك صعوبات تقف دون تحقيق هذا التعاون.

ومن أهم هذه الصعوبات:

الفرع الأول: الصعوبات التي تواجه التعاون الدولي (على المستوى الوطني والدولي)

أولا: الصعوبات التي تواجه التعاون الدولي على المستوى الوطني

1- عدم ملائمة القوانين الجنائية الداخلية: إن إصدار العديد من الدول التشريعات المتعلقة بالجرائم الالكترونية وانضمامها للعديد من الاتفاقيات الدولية التي تجرم الأفعال المخالفة

[1] حشيفة عبد الهادي، المرجع السابق الذكر، ص 38.

[2] محمد أحمد سليمان عيسى، المرجع السابق الذكر، ص 52.

للمعاهدات المنظمة لهذه الجرائم، إلا أن هذه النصوص غير كافية لمعالجة سائر الجرائم المرتكبة في مجال الكمبيوتر والانترنت، الأمر الذي يؤدي لتقليل جهود رجال الشرطة عند ضبط الجرائم والكشف عن مرتكبيها.

فالكثير من نصوص القوانين الجنائية الداخلية لبعض الدول لا تكفي بوضعها الحالي لمواجهة تلك الصور المستحدثة من الجرائم.

2- صعوبة إثبات الجرائم الالكترونية: من خلال الأسباب التالية:

- أنها لا تترك أثرا بعد ارتكابها - صعوبة الاحتفاظ الفني بآثارها إن وجدت.

- تحتاج إلى خبرة فنية لا تتوفر عند المحقق العادي، تعتمد على قمة الذكاء بارتكابها. [1]

ثانيا: الصعوبات التي تواجه التعاون الدولي على المستوى الدولي

1- الصعوبات التي تواجه المساعدة القضائية

يصادفها العديد من العقبات والمعوقات منها:

- عدم وجود نموذج موحد للنشاط الإجرامي. [2] أي عدم وجود اتفاق مشترك بين الدول حول نماذج عن إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر.

- عدم القدرة على جمع الأدلة والمعلومات، كان لابد من وجود نظام اتصال للجهات القائمة بالتحقيق الاتصال بالجهات الأجنبية لجمع أدلة معينة ومعلومات مهمة.

[1] حشيفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانوني جنائي وعلوم جنائية، كلية الحقوق، جامعة الجلفة، 2020، ص 48 ص 49.

[2] أومدور رجاء، المرجع السابق الذكر، ص 223.

بطء إجراءات المساعدة القضائية: أي تباطؤ في الرد على طلبات المساعدة من الدولة متلقية الطلب وهذا لعدة أسباب منها فوارق الإجراءات والصعوبات اللغوية. [1]

2- الصعوبات التي تواجه إجراءات تسليم المجرمين

- مشكلة التنازع في الاختصاص: اختلاف التشريعات والنظم القانونية الذي قد ينجم عنه التنازع في الاختصاص.

- تعدد طلبات تسليم المجرمين: قد يرتكب الشخص المراد تسليمه عدة جرائم تمس في نفس الوقت مصالح أساسية لعدة دول، ففي هذه الحالة تقدم عدة طلبات لتسليم المجرم، فهنا لابد للدول المتضررة تقديم الأدلة الخاصة بالجريمة. [2]

الفرع الثاني: سبل تفادي الصعوبات التي تواجه التعاون الدولي

من السبل التي تقلل من حجم الصعوبات التي تواجه ت.د والتي تكون خلال الإجراءات التالية:

- استخدام بعض تقنيات التحقيق الخاصة، مما يخفف من غلو واختلاف النظم القانونية والإجرائية ويزيد من فاعلية التعاون الدولي.

- تحديث تشريعات محلية خاصة بالجرائم الالكترونية وإبرام اتفاقيات خاصة تراعى فيها هذا النوع من الجرائم.

- إبرام اتفاقيات دولية ثنائية أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي.

[1] أومدور رجاء، المرجع السابق، ص 226.

[2] أومدور رجاء، المرجع نفسه، ص 236.

– إقرار إجراءات مستحدثة في مجال المساعدة القضائية، نتيجة القصور في إجراءات المساعدة التقليدية، مما جعلها غير مجدية في مواجهة الجريمة الالكترونية.

– إيجاد طريقة أو وسيلة تتسم بالسرعة في إجراء طلب الإنابة القضائية كالاتصال المباشر من جهات التحقيق، للقضاء على مشكلة البطء.

– إدراج أحكام عامة في المعاهدات والاتفاقيات الدولية المعنية تسليم المجرمين من خلال سرد الأفعال التي تتطلب أن تجرم كجرائم وأفعال مجرمة بمقتضى قوانين الدولتين معا. [1]

[1] أجعود فطيمة، مرجع سابق، ص 78.

خلاصة الفصل الثاني

تعتبر الجريمة الالكترونية جريمة مستحدثة ومتطورة مع تطور التكنولوجيا وأساليب التحقيق فيها معقدة ومن أجل التصدي لها وتفادي أكبر قدر من تأثيرها على المجتمعات والدول كان لزاما أن يتماشى هذا التطور التكنولوجي مع أساليب وإجراءات لتفادي هذه الجرائم من تشريعات وقوانين، وتخطي الدولة الواحدة لأساليب الحماية الوطنية إلى الحماية الدولية من خلال عقد اتفاقيات وقوانين وسياسات من أجل نجاعة أكثر وحماية أوفر.

لكن رغم هذه الجهود المبذولة في هذا الإطار فإن الصعوبات لا تزال قائمة وتمثل تعديا لهذه الدول مع المحاولة المستمرة في إيجاد حلول لها وسبلا لتفاديها.

خاتمة

خاتمة

إن خصوصية التحقيق في الجريمة الإلكترونية تختلف وتتغير بتطور البيئة الرقمية وبأساليب التحقيق المتبعة كون المحقق في هذه الجريمة يجب أن يتمتع بصفات ومؤهلات خاصة ومميزة وعلى الدولة أن تتماشى مع هذا التطور بين قوانين وتشريعات من أجل فعالية أكثر في التصدي لهذه الجريمة وحماية أكبر للأفراد والمؤسسات سواء داخل الدولة أو خارجها.

ولقد توصلنا في بحثنا هذا إلى مجموعة من النتائج والتوصيات.

النتائج:

1- لم يتم الاتفاق على تحديد مفهوم جامع مانع لهذه الجرائم كونها جرائم مستحدثة ومتطورة وأساليب التحقيق فيها مختلفة.

2- أن المحقق في الجريمة الإلكترونية يجب أن يتمتع بمؤهلات وقدرات خاصة.

3- أن المشرع الجزائري أستحدث هيئات غير قضائية تتمثل في إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال بموجب القانون 09-04.

4- وجود صعوبات في الحصول على الدليل الإلكتروني والحفاظ عليه.

5- يجب مراعاة الحق في الخصوصية باعتباره تحديا يواجه إجراءات التحقيق في الجريمة الالكترونية.

6- يمكن للضحية في الجريمة الإلكترونية أن يكون عائقا أمام عملية التحقيق.

7- يجب تحديد العناصر اللازمة للتحقيق لتوضيح القانون الواجب تطبيقه في هذه الجرائم سواءا داخل أو خارج النطاق الإقليمي للدولة.

8- إن آليات التعاون الدولي في مجال التحقيق في الجرائم الالكترونية غير كافية ويجب تطويرها وتحسينها.

التوصيات:

1- استعمال واستخدام أساليب وتقنيات جديدة ومتطورة من طرف أجهزة التحقيق في الجريمة الإلكترونية من أجل الوصول لفعالية أكثر في عملية التحقيق.

2- مسايرة التطورات التقنية الحاصلة في المجال المعلوماتي بتطوير النظم والقوانين والتشريعات وتحيينها بما يتناسب مع ذلك.

3- استخدام الدليل الالكتروني كأداة إثبات أساسية من أدوات الإثبات الجنائي.

4- تشجيع المبادرات التوعوية والتحسيسية من طرف المؤسسات ووسائل الإعلام بخطورة الجرائم الإلكترونية والتبليغ عنها.

5- محاولة اكتساب الخبرة والاستفادة من تجارب بعض الدول الرائدة في المجال المعلوماتي.

6- تفعيل دور التعاون الدولي في مجال محاربة الجريمة الالكترونية من خلال الاتفاقيات الدولية والإقليمية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

قائمة المراجع والمصادر

القوانين:

1- القانون 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 47 صادرة بتاريخ 16 أوت 2009.

الأوامر:

1- أمر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

المراسيم:

1- مرسوم رئاسي رقم 21-439 مؤرخ في 7 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الكتب:

1- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دراسة تطبيقية، ط1، الإسكندرية، 2009.

2- مصطفى محمد موسى، التحقيق الجنائي في الجريمة الالكترونية، بدون دار نشر، ط1، القاهرة.

3- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ط1، .2018

4- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، .2003

5- يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري (دراسة مقارنة)، ط1، دار النهضة العربية، القاهرة، .2017

6- خالد عياد الحلبي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017.

7- رامي متولي القاضي، مكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، مصر، 2011.

8- حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، .2017

9- أحسن بوسقيعة، التحقيق القضائي، ط10، دار هومة.

10- محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2018.

المقالات:

1- مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد 1، 2014.

2- آيت عبد المالك نادية، فلاح عبد القادر، التحقيق الجنائي في الجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ والباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، جامعة خميس مليانة، 2019.

3- رضا عسال، عماد عبد الرزاق، الجريمة الالكترونية والمجرم المعلوماتي – مقارنة مفاهيمية – التحقيق في الجريمة الالكترونية، مجلة ديلير حيليا، دراسات ومكتبات المعلومات، العدد 5، issn 2661-7781.

4- رمزي حوحو، منيرة بلورغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، جامعة بسكرة، العدد 2، 2014.

5- عز الدين عثماني، إجراءات التحقيق والتفتيش في الجريمة الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسة الدستورية والنظم السياسية، العدد 4، 2018.

6- عبير بعقيقي، فيصل بسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، جامعة بسكرة، المجلد 9، العدد 2، 2018.

7- مرزوقي كريمة، مراقبة الاتصالات الإلكترونية وحق الفرد في الخصوصية المعلوماتية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة تيزي وزو، المجلد 5، العدد 2، 2020.

8- محمد أحمد سليمان عيسى، التعاون الدولي في مجال مكافحة الجريمة الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2، 2016.

الأطروحات والرسائل الجامعية:

1- أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، الطور الثالث ل م د، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2021.

2- بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الالكترونية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق تخصص ق ج، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2013.

3- بشير حماني، خصوصية التحقيق في الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة المسيلة، 2018.

4- يوسف جفال، التحقيق في الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، تخصص ق ج، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2016.

5- بن لغوم خالد أمين، إجراءات التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قانون خاص، جامعة مستغانم، 2019.

6- حشفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الالكترونية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص ق ج وعلوم جنائية، كلية الحقوق، جامعة الجلفة، 2020.

7- أجعود فطيمة، خصوصية التحقيق في الجريمة الالكترونية، مذكرة لنيل شهادة ماستر في الحقوق، تخصص قانون إعلام آلي وانترنت، جامعة محمد البشير الإبراهيمي، 2022/2021.

فهرس المحتويات

فهرس المحتويات:

الملخص:

لقد تناولنا في بحثنا هذا خصوصية التحقيق في الجريمة الإلكترونية وهذا الموضوع يعتبر من المواضيع المهمة والمعاصرة وقسمنا بحثنا إلى فصلين تطرقنا في الفصل الأول إلى الإطار المفاهيمي للتحقيق في الجريمة الإلكترونية الذي يحتوي على مبحثين كالتالي

مفهوم التحقيق والصعوبات التي تواجهه أما الفصل الثاني تناولنا آليات التحقيق في الجريمة الإلكترونية من خلال مبحثين الإجراءات المتبعة في التحقيق والتعاون الدولي في مواجهة الجرائم الإلكترونية.

الكلمات المفتاحية: التحقيق، الجريمة الإلكترونية، الإجراءات المتبعة.

Summary:

In our research, we have discussed the specificity of investigating cybercrime, and this topic is considered one of the important topics in a moderate evening. We divided our research into two chapters to introduce us in the first chapter to the conceptual framework in cybercrime, which contains two sections called

The concept of investigation and the difficulties facing it. Chapter Two: We dealt with the investigation of electronic crime through two sections, examining the measures followed in the international joint investigation in confronting electronic dances.

Keywords: investigation, cybercrime, preventive measures