الرقم التسلسلي: .....

جامعة سعيدة – الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

أطروحة

مقدمة لنيل شهادة

دكتوراه الطور الثالث

التخصص : قانون جنائي وعلوم جنائية

الفرع : حقوق

من طرف :

خرشي عثمان

عنوان الأطروحة:

إجراءات سير الدعوى العمومية في الجرائم المعلوماتية

أطروحة مناقشة بتاريخ 2021/07/04 أمام لجنة المناقشة المشكلة من :

الرقم	اللقب و الإسم	الرتبة	المؤسسة	الصفة
01	السيد بوشنتوف بوزيان	أستاذ التعليم العالي	جامعة سعيدة – د. مولاي الطاهر	رئيسا
02	السيد نابي عبد القادر	أستاذ محاضر-أ-	جامعة سعيدة – د. مولاي الطاهر	مشرفا
03	السيد خنفوسي عبد العزيز	أستاذ محاضر-أ-	جامعة سعيدة – د. مولاي الطاهر	مشرفا مساعدا
04	السيد بوسندة عباس	أستاذ التعليم العالي	جامعة سيدي بلعباس– جيلالي ليابس	ممتحنا
05	السيد بواب بن عامر	أستاذ التعليم العالي	المركز الجامعي بالبيض – نور البشير	ممتحنا
06	السيدة مراح نعيمة	أستاذ محاضر-أ-	جامعة سعيدة – د. مولاي الطاهر	ممتحنا

السنة الجامعية:2020 /2021 م 1442/1441هـ

بسم الله الرحمن الرحيم

" شَهِدَ اللَّهُ أَنَّهُ لَا إِلَهَ إِلَّا هُوَ وَالْمَلَائِكَةُ وَأُولُو الْعِلْمِ قَائِمًا بِالْقِسْطِ لَا إِلَهَ إِلَّا هُوَ الْعَزِيزُ الْحَكِيمُ ".

صدق الله العظيم سورة آل عمران: الآية 18

إهداء

أحمد الله عز وجل أن وفقني لإنجاز هذا البحث من غير حول مني ولا قوة فلله الحمد والمنة والفضل.

ونصلي ونسلم على حبيبنا ونبينا محمد صلاة نُكفى بها الهموم وتغفر بها الذنوب.

إلى روح والدي الطاهرة، أسأل الله أن يجدد عليه الرحمات ويجعل قبره روضة من رياض الجنة وأن يسكننا وإياه جنته جنة النعيم.

إلى والدتي الكريمة حفظها الله وأطال الله في عمرها وأرضاها عني في الدنيا والآخرة.

إلى إخوتي وأخواتي وجميع أقاربي وأصدقائي أسأل الله أن يحفظكم ويفتح عليكم في جميع مناحي حياتكم وأن يوفقكم في الدنيا والآخرة.

هذا وأتوجه بجزيل الشكر لجميع الأساتذة الذين شرفوني بتدريسهم لي وبنصائحهم القيمة عبر مختلف الأطوار.

وأتوجه بالشكر الخاص للأساتذة: الدكتور نابي عبد القادر والدكتور خنفوسي عبد العزيز والأستاذة الدكتورة عمارة فتيحة الذين رافقوني طيلة هذا العمل بالإشراف والتوجيه فجازاكم الله خيرا.

إلى كل هؤلاء وإلى كل من ساعدني ولو بالقليل... أهدي عملي هذا

خرشي عثمان

قائمة المختصرات

ط: الطبعة

د ط: دون طبعة

ص: الصفحة

ق إ ج: قانون الإجراءات الجزائية

ق ح ط: قانون حماية الطفل

ق ع: قانون العقوبات

ق م: القانون المدني

ج ر: الجريدة الرسمية

P: page

المقدمة

لقد صاحب الثورة الصناعية منذ منتصف القرن الماضي تطورات وتغيرات مست كل جوانب الحياة في المجتمع ومنها القانون بطبيعة الحال، حيث تم تطويع نظرياته وأحكامه ليتلاءم مع الظروف والمشاكل المستحدثة التي خلقتها تلك الثورة، والتي مهدت من خلال التقدم التقني في مجال الحاسبات الآلية، أين أصبحت قادرة على تجميع واستيعاب كم هائل من المعلومات بعدما كانت تقوم بعمليات حسابية معقدة فقط بل وأصبحت قادرة على استرجاع تلك المعلومات بسرعة فائقة وبدقة متناهية[1] وبعد أن كانت المعلومات مشكلة تؤرق الذين يهتمون بها ويحتاجون إليها أصبحت في متناول اليد بأقل مجهود وفي حيز قليل جدا.

ولم يشهد العالم خلال تاريخه الطويل تغيرات في نمط الاتصال والتبادل بل وفي أسلوب الحياة بالعمق والشمول والسرعة التي يشهدها عالمنا منذ أن دخلت حياتنا هذه التقنيات الحديثة للمعلومات والاتصال

[2]؛ لذا ليس غريبا أن نرى الحاسبات الآلية قد غزت مجالات عديدة ومتنوعة في المجتمع أين أصبحت الاستعانة بها واستخدامها ضرورة لا غنى عنها على مستوى أجهزة الدولة ومختلف مرافقها وبالتالي أصبح استخدامها أمرا لا مفر منه حاليا في الدول المتقدمة مقارنة بدول العالم الثالث والذي سيأتي يوم تكون فيه الحاجة إليها ملحة.

هذا وقد كانت الاتصالات في وقت مضى مبنية على التليفون والتلغراف والتلكس والفاكس بحيث كانت تقتصر على إجراء حوار كلامي بين طرفين أو عدد من الأطراف، وكذلك كانت تشتمل على نقل رسائل مكتوبة ومعلومات وبيانات من مكان إلى مكان آخر كالبنوك فيما بينها، ولقد كان التلكس يقوم بهذه الوظيفة ثم عُمل بالفاكس لأنّه أسرع في نقله للمعلومات والبيانات فاستُغني عن

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، د ط، الدار الجامعية للطباعة والنشر، بيروت، لبنان، 1999 ص5.

[2] جهاد رضا الحباشنة، الحماية الجزائية لبطاقات الوفاء، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص13.

التلكس، وتطورت الاتصالات بعد ذلك تطورا مذهلا بأن أصبحت تشتمل على الشبكات الدولية المعروفة بالإنترنيت[1]، التي يمكن عن طريقها نقل مصنفات ومعلومات وبيانات هائلة بسرعة فائقة.

ففي يومنا هذا كميات هائلة من ثروات المجتمع يتم تطويرها أو تخزينها أو نقلها أو انتقاؤها باستخدام الحاسب، فمثلا الصناعة الأمريكية لوحدها تحول مليارات الدولارات من العمليات المالية يوميا من خلال شبكات الحاسب حتى أن هناك من يرى بأننا سنصوت قريبا من خلال جهاز الحاسب مباشرة[2]؛ هذا بالإضافة إلى أنّ التطور الكبير في مناحي الحياة الاقتصادية والاجتماعية والثقافية والسياسية صاحبه تزايدا ونموا واعتمادا ملحوظا على النظم المعلوماتية الآلية والتكنولوجيا القائمة على الحاسوب، وذلك كوسيلة أساسية من أجل الحفاظ على البيانات وتشغيلها ومعالجتها داخل معظم المؤسسات التابعة للدولة أو غير التابعة لها، إلى درجة يصعب معها تخيل أنّ أي مجال لم يتأثر بهذه الظاهرة الحديثة السريعة النمو، فالمعلوماتية الآن أصبحت قضية الجميع ولم تعد محدودة النطاق أو مقصورة على قطاع معين[3].

وإذا كانت المعلوماتية قد قضت ما يقرب من نصف قرن قبل أن يصبح حالها على هذا النحو وقبل أن تحدث ثورة حقيقية في العديد من المجالات، فقد بات مألوفا وصف العصر الذي نعيش فيه الآن بعصر المعلوماتية، حتى أن هذه الأخيرة أصبحت عاملا حاسما في تحديد ملامح مستقبلية بل وأصبحت ظاهرة كثيرة التشعب والتأثير في حياة المجتمعات حاضرا ومستقبلا وعنصرا حاسما في أوجه النشاط الإنساني المختلفة وفي شتى المشاريع المختلفة، وذلك نظر لما لها من قدرة فائقة خاصة مع ظهور

---

[1] حسني عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الانترنيت (دراسة مقارنة بين الشريعة والقانون)، د ط، دار النهضة العربية القاهرة، مصر 2011، ص5.

[2] عبد الكريم خالد الردايدة، الظواهر الإجرامية المستحدثة وسبل مواجهتها، ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن 2010، ص93.

[3] نبيلة إسماعيل رسلان، التأمين في مجال المعلوماتية والشبكات، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص3.

الأجيال الجديدة من الحاسبات التي لم تعد تقتصر في قدرتها على تخزين واسترجاع البيانات فقط بل على تحليلها وحل العديد من المسائل[1].

لهذا لم يكن بالإمكان الاستمرار في ملاحظة تدفق وانفجار المعلومات في مختلف مجالات الفكر البشري ولاسيما على الصعيد الدولي من دون إيجاد الوسائل المنظمة لكيفية التعامل مع تلك المعلومات من الناحية القانونية، وسن قوانين وعقد اتفاقيات مساهمة في التفاهم على الأقل في تجنيب التعدي على أجهزة الاستعلام والوسائط الناقلة لها[2]، وهو ما ظهر في الآونة الأخيرة من خلال سن التشريعات الغربية لقوانين مدنية وأخرى جزائية تواجه التطور الهائل في مجال المعلوماتية وتكافح مختلف الجرائم المصاحبة لها.

فالتطور الكبير في المجال التكنولوجي أدى إلى ازدياد أهمية الكمبيوتر في شتى نواحي الحياة المعاصرة إلى درجة أصبحت فيها كل الفروع من أي نشاط إلاّ ويستخدم فيها الكمبيوتر كالبنوك والشركات والهيئات وغيرها، والذي جلب معه نشوء جرائم نتجت عن استخدامه فمنها ما يقع على الكمبيوتر ذاته ومنها ما يقع بواسطته، فالحاسب الآلي أصبح وسيلة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية[3]، وبينما كانت حياتنا غير متصلة بالإنترنت منذ 15 إلى 20 عامًا فقد توسعت الإنترنت بأن شملت جميع مناحي الحياة الاجتماعية ذلك أنّ الناس يعيشون باستمرار جزءًا من حياتهم داخلها بدءًا من التسوق والتواصل للعمل والوقوع في الحب وحتى شن حملات سياسية[4] فالإنترنيت وصل به الحال الآن أن أصبح ساحة سياسية يتم من خلالها إنشاء السلطة السياسية.

---

[1] محمد حسن قاسم، مراحل التفاوض في عقد الميكنة المعلوماتية، ط ثانية، دار الجامعة الجديدة، الإسكندرية، مصر، 2016 ص4.

[2] غسان رباح، الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، ط أولى، منشورات الحبلى الحقوقية، بيروت لبنان، 2008، ص105.

[3] محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، د ط، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004، ص7.

[4] Vasileios Karagiannopoulos, A Short History of Hacktivism: Its Past and Present and What CanWe Learn from It, fom books of, Tim owen-jessica marshall rethinking cybercrime, critical debates, Palgrave macmillan, Cham Switzerland AG 2021, p63.

لذا فإنّ ظهور الحاسب وانتشار شبكة الإنترنيت فتح معه مجالات عديدة للاستفادة منها لكن في نفس الوقت أدى إلى انتشار ثقافة منافية لعادات وطبائع الكثير من المجتمعات[1]، وكذا ظهور عدة جرائم مرتبطة بها كصناعة ونشر الفيروسات والاختراقات غير المشروعة وتعطيل أجهزة الآخرين ومضايقة وملاحقة الآخرين المتعاملين مع الشبكة بالإضافة إلى استخدام الانترنيت في نشر وإعلان الصور الإباحية والدعوة لممارسة الجنس عبر الشبكة؛ وكذلك جرائم النصب عن طريق الإعلان عن بيع سلع وهمية عبر الشبكة إلى غيرها من الجرائم التي لازالت في التزايد وتسجل كل حين[2].

وكأصل عام فإن الجرائم تتعلق بوجود الإنسان وهي تتطور بتطوره خاصة في ظل التطور المستمر والسريع لتكنولوجيا المعلومات والاتصال، هذه التكنولوجيا التي يحاول العلماء والأفراد العقلاء والصالحين الاستفادة منها وكذلك بالمقابل يحاول المجرمون استغلالها في أعمالهم الإجرامية، فتكنولوجيا المعلومات والاتصال أصبحت منصة مباحة للجميع للصالحين منهم والمجرمين، هذه الفئة الأخيرة استطاعت اكتساب خبرات ومهارات أكثر في تعاملها مع الإنترنت والتي أهلتها لارتكاب أنواع مختلفة من الجرائم المعلوماتية.

هذه الجرائم الأخيرة المبتكرة والمستحدثة هي الآن تمثل ضربا من ضروب الذكاء الإجرامي الذي أوجب على مختلف الأنظمة التشريعية الجنائية الوطنية والدولية تطوير وتحديث تشريعاتها التقليدية بذكاء مماثل للذكاء الإجرامي الذي تُعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب تلك التقنيات وأبعادها الجديدة[3]؛ من غير الخروج عن مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى.

---

[1] ضياء مصطفى عثمان، السرقة الإلكترونية دراسة فقهية، ط أولى، دار النفائس للنشر والتوزيع، عمان، الأردن، 2011 ص37.

[2] محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، د ط ، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003، ص9.

[3] إبراهيم رمضان، إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية) مجلة كلية الشريعة والقانون، العدد الثلاثون، الجزء الثاني، جامعة الأزهر بطنطا، مصر، 2015، ص360.

فالطبيعة الخاصة للجرائم المعلوماتية من حيث خطورتها و صعوبة الكشف عنها و غياب الدليل المادي الذي يدين مرتكبها في غالب الأحيان، أصبحت طاغية على الساحة الإجرامية بشكل كبير نتيجة لغياب إستراتيجية فعالة لمحاربتها أو على الأقل التقليل منها على المستوى الدولي خاصة في ظل قلة الاتفاقيات الدولية وصعوبة التعاون الدولي للحد منها[1]، هذا بالإضافة إلى صعوبة مسألة تحديد قائمة جرائمها وتحديد أنماط سلوكها الإجرامي والأفعال المكونة لها، وكذلك تباين الفقهاء في مختلف النظم القانونية حول مدى انطباق نصوص القوانين الجنائية التقليدية على هذه الجرائم، والذي مع تنامي الدراسات البحثية وتطور ظاهرة الجرائم المعلوماتية فيما بعد أظهر عدم قابلية هذه النصوص وعجزها وعدم كفايتها للانطباق على هذه الأنماط من الجرائم المعلوماتية[2].

ولعل البدايات الأولى للجرائم المعلوماتية كانت مع ظهور برامج قياس درجات الأمان في أنظمة الحاسبات الآلية، والتي تم استخدامها لالتقاط المعلومات والتلاعب بأنظمة الحاسبات التي تحتوي عليها واستغلالها لأغراض غير مشروعة أين يستطيع الجاني من خلالها أن يسيطر على النظام ومن ثم يقوم بنشاطه الإجرامي الذي يعقبه بمحو كل أثر يُمَكن من كشف الجريمة[3]، لهذا فإن عملية دراسة مختلف الإجراءات الواجب اتخاذها في مواجهة الجريمة المعلوماتية يقودنا للزوم معرفة الدوافع والأسباب التي تؤدي بالمجرم المعلوماتي لارتكابها، والتي من المنطق أن تختلف من مجرم لآخر كل حسب مركزه وظروفه داخل المجتمع هذا الاختلاف الذي أفرز عدة جرائم معلوماتية تباينت درجة خطورتها من جريمة لأخرى، لدرجة عجز الفقهاء وتشريعات الدول عن إيجاد تقسيم موحد لها عالميا.

---

[1] ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية مجلة دراسات وأبحاث، المجلد 1، العدد 1، جامعة زيان عاشور الجلفة، الجزائر، سبتمبر 2009، ص241.

[2] محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن 2007 ص61.

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، ط أولى، منشورات الحبلى الحقوقية بيروت لبنان، 2005، ص36.

وهو ما انعكس على مفهومها فلا يزال هناك تباين وعدم ثبات للمصطلحات والتسميات التي تطلق على هذه الظاهرة الإجرامية الحديثة التي باتت تهدد الدول قبل الأفراد، هذا التباين والاختلاف الذي ربما يعود لنشأة وتطور وتمحور ظاهرة تكنولوجيا المعلومات من جهة، وإلى اختلاف وجهات النظر بين المختصين في مجال الإعلام وبين رجال القانون وعلماء الاجتماع وعلم النفس[1] من جهة أخرى، فالجرائم المعلوماتية أو كما يسميها البعض بالجرائم الإلكترونية أو جرائم الحاسب الآلي والانترنيت أو جرائم الغش المعلوماتي أو جرائم الاحتيال المعلوماتي، رغم محاولة الكثير من الفقهاء وبذل الجهد في إيجاد ووضع تعريف جامع[2] وشاف لها، لم يسفر إلى الوصول للنتيجة المطلوبة.

ومن خلال هذه المسميات حول هذه الجريمة المستحدثة نرى بأنّ الاتجاه المناسب والذي نميل إليه من خلال دراستنا هذه هو تفضيل اصطلاح الجرائم المعلوماتية على المصطلحات السابقة، ذلك أنّه عام ويتسع ليشمل التقنيات الحالية والمستقبلية كلها والمستخدمة في التعامل مع المعلومات أيا كان نوعها بما في ذلك الحاسوب وشبكة الانترنيت، وتكون فيه المعلومات محلا لهذه الجريمة إمّا بذاتها أو بما تمثله.

فهذه الجريمة المستحدثة تختلف عن الجريمة التقليدية لكونها تتسم بطابع خاص في أنّها جريمة عابرة للحدود قد ترتكب في العديد من الدول ويكون تأثيرها ممتد ليصل إلى عدد غير محدود من الدول عكس الجريمة التقليدية التي في الغالب تتم داخل الدولة، ويكون تأثيرها منحصرا في تلك الدولة فقط كما أنّ الجرائم المعلوماتية في جميع الأحوال يكون فيها الحاسب الآلي هو منبع ارتكاب هذه الجريمة بحيث يكون مرتكبها هو شخص ذو خبرة فائقة في مجال الحواسب الآلية[3].

---

[1] عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، ط أولى، دار المستقبل للنشر والتوزيع، عمان، الأردن، 2009 ص.107

[2] غانم مرضي الشمري، الجرائم المعلوماتية (ماهيتها، خصائصها، كيفية التصدي لها قانونيا)، ط أولى، الدار العلمية الدولية للنشر والتوزيع، عمان الأردن، 2016، ص24.

[3] علي جابر الحسيناوي، جرائم الحاسوب والانترنيت، د ط، دار اليازوري للنشر والتوزيع، عمان، الأردن، 2009، ص34.

فإذا كان هذا الشخص في هذا النمط من الجرائم يتجه للاعتداء على المعلومات بما تمثله من أسرار وبيانات وأموال، فإنّ تحديد أمر المال المعلوماتي يعد أيضا من الأمور التي تتطلب تحليلا وتأهيلا قانونيا خاصا، ذلك أنّ التطور المتسرع وظهور أنماط مستحدثة من الإجرام جعل من اللازم لوصف المال الذي يرد على شيء مادي أن يتغير وفقا للقانون والفقه الحديث، وبالتالي تصبح البيانات والتي هي جزء من معطيات الحاسب الآلي لها صفة المال، هذا الأخير الذي تغير وصفه وأصبح يرد على أي شيء له قيمة اقتصادية[1]، هذا المال المعلوماتي الذي يقع عليه الاعتداء تضاربت فيه الآراء حول طبيعته ما إن كانت مادية أو معنوية.

بل واختلفت حتى الأسباب والدوافع المؤدية إلى هذه الجريمة الخطيرة من شخص إلى آخر، ذلك أنّ الإرادة تلعب فيها دورا كبيرا في ارتكابها، هذه الإرادة التي يكون وراءها أسباب ودوافع عديدة مختلفة تساهم في تقويتها، لعل أبرزها تحقيق مكاسب مالية والشغف بالإلكترونيات وحب المغامرة والإثارة بالإضافة إلى الدوافع الشخصية كحب الظهور باستعراض القدرات الفنية على ارتكاب مثل هذه الجرائم أو الحقد والكراهية المؤدي غالبا للانتقام، وكذا الدوافع والمؤثرات الخارجية خاصة في نطاق التجسس والمنافسة والأعمال التجارية التي قد يُمارس الغش المعلوماتي فيها تحت تهديد أو ضغط.

هذه الأسباب والدوافع هي الطريق المؤدي للجرائم المعلوماتية وما ينتج عن هذه الأخيرة من مخاطر عدة، تجلت من خلال حس الشعور بمخاطر تقنية المعلوماتية وتهديدها للحياة الشخصية والخاصة بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية للأشخاص سواء الطبيعية والاعتبارية وما صاحبه من اتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة[2]؛ وتجلت كذلك من خلال تهديد الكمبيوتر بوضع برامج مغلوطة أو أخطاء مادية تلحق بالمعلومات والتي لا يمكن تفاديها أو

[1] محمود محمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص21.

[2] بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط أولى، منشورات الحبلى الحقوقية، بيروت، لبنان 2009، ص21

إتلاف البيانات والمعلومات التي يتم معالجتها آليا بواسطة الفيروسات أو الديدان؛ أو الإغراق بالرسائل وذلك حتى تفقد منفعة المال وصلاحيته في الاستعمال.

بل وأصبح امتلاك التكنولوجيا الحديثة وتوظيفها في شتى المجالات السياسية والعسكرية والاقتصادية أحد أهم أدوات إدارة العلاقات الدولية، بحيث ثمة تغيرات كبرى طرأت على مفهوم القوة وتحولاتها وتطبيقاتها والتي غيرت من موازين القوى العالمية، فإذا كان العدو في الحرب الباردة معروفاً وواضحاً ويمكن تعقبه والتنبؤ بسلوكه فإنّ الأمر مختلف تماماً في حالة الحرب المعلوماتية، ذلك أنّ العدو فيها ليس بالضرورة هو عبارة عن دولة، كما أنّ استهداف المناطق والخدمات الاستراتيجية[1] أصبح أقل تكلفة من الحرب التقليدية بل أكثر تدميراً في بعض الأحيان، خاصة إذا كان الأمر يتعلق بالسيطرة على البُنى التحتية والخدمات اللوجستية سواء كانت مدنية أو عسكرية.

كل هذه المخاطر دفعت معظم التشريعات العالمية كالتشريع الجزائري وبعض فقهاء القانون المختصين في هذا المجال إلى ضرورة مواكبة هذه الظاهرة الخطيرة المستحدثة من خلال تنظيمها وتقسيمها كل حسب نظرته إليها ووجهة رأيه فيها؛ وهو ما يفسر ظهور جهود دولية وأخرى فقهية كثيرة تبنت تقسيمها، ولعل أبرز هذه التقسيمات الفقهية والتشريعية للجرائم المعلوماتية، النموذج الفقهي الذي جاء به الفريق البحثي الأكاديمي الأمريكي والنموذج التشريعي والحماية الجنائية الذي جاء به المجلس الأوروبي للجرائم المعلوماتية.

فالحماية الجنائية تعتبر من الموضوعات الهامة التي بسطتها مختلف التشريعات من أجل ردع أشكال الجرائم والاعتداءات التي قد تمس بجوانب حياة الإنسان المتفاعل بشكل رهيب مع ما تخلفه تكنولوجيا الإعلام والاتصال، هذه الأخيرة ونظرا لنقائصها وما تخلفه من ثغرات فنية باتت عرضة للاستغلال ومهددة بالاعتداء عليها من طرف مجرمين معلوماتيين تختلف فئاتهم، وهو ما يفسر لزوم

[1] إيهاب خليفة، cyber defense أبعاد التحول في استراتيجية الدفاع الأمريكية، عن موقع https://futureuae.com/ar/Mainpage/Item/856/cyber-defense. تاريخ الاطلاع 2021/03/10.

بسط حماية جنائية في شقيها الموضوعي والإجرائي لسد النقص الذي خلفته هذه التكنولوجيا ولردع أشكال اعتداءات هؤلاء المجرمين.

خاصة من خلال الحماية الجزائية الإجرائية[1] للنظام المعلوماتي الذي يعتبر سلاحا مناسبا في مواجهة وكشف الجرائم المعلوماتية ذلك أنّها حماية عملية لهذا النظام، عكس الحماية الموضوعية الساكنة التي تكتفي فقط بتبيان أركان ونوع الجرائم المعلوماتية وتحديد العقوبة اللازمة لها، لكن ونظرا لما تتمتع به الجرائم المعلوماتية من تعقيدات واضحة جعلت المحققين في هذا المجال يصطدمون بعدة تحديات شخصية وأخرى متعلقة بطبيعة هذه الجرائم، حتمت عليهم مسايرتها من خلال تحديث معارفهم ومهاراتهم بصفة مستمرة ودورية.

لهذا فإذا ما وقعت جريمة معلوماتية ما ووصل العلم بها إلى ضباط الشرطة القضائية فإنّها تعلن ببدء مرحلة يطلق عليها في التشريع الجزائري اسم مرحلة جمع الاستدلالات أو مرحلة التحقيقات الأولية، والتي يكون الهدف منها تعقب المجرمين والبحث عنهم وجمع الاستدلالات اللازمة التي تثبت ارتكابهم لهذه الجريمة، فالدعوى العمومية قبل وضعها في ساحة القضاء لابد لها وأن تمر بهذه المرحلة الحساسة التي يلعب ضباط الشرطة القضائية الدور الرئيسي فيها[2]، والتي يمكن من خلالها جمع أكبر قدر من المعلومات عن هذه الجريمة وظروف ارتكابها وما سبقها من مقدمات.

هذا وقد حتمت الطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية على جل التشريعات المقارنة وكذا التشريع الجزائري، وجوب تحديد صفات مؤهلة للتحري والاستدلال على هذا النوع من الجرائم أين أعطيت لهم مهمة الضبط القضائي وهو ما أبرزه المشرع الجزائري ضمن نصوص خاصة، أين حدد

---

[1] الحماية الجزائية الإجرائية ترجمها المشرع الجزائري كأصل من خلال ق إ ج الأمر 66-155 الصادر ب 8 يونيو 1966، ج ر رقم 48 المؤرخة في 10 يونيو 1966، هذا القانون ما زالت تتوالى عليه بعض التعديلات إلى غاية يومنا هذا مسايرة للتطور الذي يشهده المجتمع في شتى المجالات وكذا بروز جرائم جديدة لم يشهدها العالم إلاّ حديثا كالجرائم المعلوماتية محل هذه الدراسة.

[2] سعيد ظافر ناجي القحطاني، الضوابط المهارية في محاضر جمع الاستدلالات وآثارها في توجيه مسار التحقيق (دراسة تطبيقية على قضايا متنوعة بمدينة الرياض)، عمل مقدم لنيل شهادة الماجستير في العلوم الشرطية التحقيق والبحث الجنائي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2004، ص31.

الصفات التي يخول لها مهام ضابط الشرطة القضائية في الجرائم المعلوماتية، وبين اختصاصهم الإقليمي الذي يباشرون فيه مهامهم والذي لا يجوز لهم تجاوزه تحت طائلة بطلان ما اتخذوه من إجراءات أثناءه وحتى تنظم مسؤوليتهم في حالات أخرى محددة قانونا.

هؤلاء الضباط يباشرون مجموعة من الإجراءات التمهيدية قبل البدء بجمع الأدلة حول نوع الجريمة المعلوماتية المرتكبة من خلال تلقي مختلف الشكاوى والتبليغات ثم القيام بالتحري والاستدلال حولها وعموما عندما يتجاوب ضباط الشرطة القضائية مع الجريمة المعلوماتية التي وقعت بالفعل نسميها ردة فعل فالغالبية العظمى من التحقيقات ذات طبيعة تفاعلية، على الرغم من أنّ بعض التشريعات المقارنة تركز على العمليات السرية المسبقة، كالتشريع الجزائري الذي يركز على مثل هذه العمليات كاعتماده على إجراء المراقبة بطريقة عادية وبطريقة إلكترونية في حالات معينة.

كما أنّه في أحيان قليلة ما يكتشف فيها المجرم المعلوماتي متلبسا بالجريمة المعلوماتية في حالات معينة، حالات التلبس هذه يجب أن تتوفر على بعض الشروط للعمل على أساسها[1] والمتمثلة في أن يكون هذا التلبس سابقا لإجراءات التحري والتحقيق الأوليين، وما يترتب عنه من قبض على المتهم أو تفتيشه أو تفتيش منزله أو ضبط لأشياء ذات علاقة بالجريمة المعلوماتية، كما يشترط وجوب اكتشاف هذه الجريمة من طرف ضابط الشرطة القضائية أو أن يكون هذا الأخير قد بلغ بها ببرهة قصيرة من ارتكابها، ويشترط كذلك أن تكتشف بطريق مشروع والذي قد يأتي أحيانا بطريقة عرضية ليس لضابط الشرطة القضائية دخل فيها[2].

هؤلاء الضباط بمجرد انتهائهم من هذه الإجراءات التمهيدية والتحضيرية يبدؤون بجمع الأدلة حول الجريمة المعلوماتية من خلال تطبيق إجراءات متعددة ومختلفة تجمع بها هذه الأدلة، والتي تبرز نسبة

---

[1] ذلك أنّ تحقق كل هذه الشروط يسمح لضباط الشرطة القضائية بممارسة سلطاتهم الاستدلالية ذات الطابع الاستدلالي وأخرى ذات طابع تحقيقي، هذه السلطات سيتم التطرق لها بشيء من التفصيل من خلال الفصل الثاني من هذا الباب.

[2] لويزة نجار، نظام المثول الفوري بديل للمحاكمة بإجراءات الجنح المتلبس بها، مجلة حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، المجلد 12، العدد 26، جامعة 08 ماي 1945 قالمة، الجزائر، فيفري 2019، ص322.

الضرر الذي تسببت فيه هذه النوعية من الجرائم والتي تكشف مقترفيها، هذه الإجراءات تنقسم بمجملها إلى قسمين الأول عبارة عن إجراءات عادية تشترك فيها مع بقية الجرائم التقليدية الأخرى من معاينة وتفتيش وضبط وخبرة، أمّا القسم الثاني عبارة عن إجراءات خاصة من تسرب واعتراض للمراسلات وتسجيل للأصوات والتقاط للصور وكذا مراقبة الاتصالات الإلكترونية، هذه الإجراءات الخاصة الأخيرة تشترك فيها مع جرائم أخرى محددة حصرا وذات خطورة كبيرة.

وكل هذه التحقيقات الأولية التي يقوم بها ضباط الشرطة القضائية من خلال جمعهم لمختلف الاستدلالات تتصرف النيابة العامة في نتائجها، ذلك أنّها صاحبة الاختصاص الأصيل وحدها دون ضباط الشرطة القضائية، فعندما تعرض المحاضر والتقارير التي أجراها هؤلاء الضباط على النيابة العامة قد ترى هذه الأخيرة بحفظ الأوراق إيذانا منها بعدم السير في الدعوى العمومية كما قد ترى على العكس تحريك تلك الدعوى سواء في الحالة العادية أو في حالة الجنح المتلبس بها[1].

خاصة إذا كانت الوقائع موضوع الاستدلالات لازالت بحاجة إلى أدلة أخرى تحدد مدى ثبوتها ومدى المسؤولية عنها كما هو الحال بالنسبة للجرائم المعلوماتية، فللنيابة العامة طلب افتتاح التحقيق من قاضي التحقيق عن طريق تقديم الطلبات أمامه، وذلك من أجل التحقيق مع المتهم ومع كافة أطراف الدعوى الآخرين إلى غاية إصدار الأحكام ومن ثم متابعتها أمام الجهات المختصة لحين الفصل فيها بحكم نهائي غير قابل لأي طريق من طرق الطعن.

هذه الخطورة والتعقيدات التي تخلفها الجرائم المعلوماتية تحتم على النيابة العامة الطلب من قاضي التحقيق بفتح تحقيق حولها، هذا الأخير الذي قد يضطر إلى استخدام وسائل وآليات مستحدثة في غاية الحساسية من اعتراض للمراسلات والتقاط للصور وتسجيل للأصوات، والتي يجب أن تفعل وفق

[1] أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، د ط، ديوان المطبوعات الجامعية الجزائر العاصمة، الجزائر، 1999، ص195.

ضوابط وشروط معينة حتى تكون ناجعة وتأتي بأكلها وحتى تكون بعيدة عن كل ما قد يعرضها للبطلان في المراحل اللاحقة من مراحل الدعوى.

وبفتح قاضي التحقيق تحقيقا حول جريمة معلوماتية ما، تبدأ مرحلة التحقيق الابتدائي أهم مرحلة من مراحل الدعوى العمومية المتعلقة بالجرائم المعلوماتية، ذلك أنّ هذه الجرائم تعتبر من القضايا الهامة والتي في كثير من الأحيان ما تحتاج إلى تمحيص وتثبت من طرف قاضي التحقيق قبل العمل على إحالتها وإحالة المتهمين إلى المحاكمة، هذا ونظرا لطبيعتها المتعدية الحدود جاءت فكرة تمديد الاختصاص المحلي لقضاة التحقيق وكذا العمل بإجراءات تسليم المجرمين على المستوى الإقليمي والدولي وذلك لتضييق الخناق على المجرمين المعلوماتيين وحتى لا يفلت الجناة من المتابعة الجزائية.

فيصبح قاضي التحقيق التابع لمحكمة جزائية ما له اختصاص إقليمي موسع يتجاوز اختصاصه العادي إلى محكمة أخرى أين يستطيع التنقل للقيام بمهام محددة متعلقة بالتحقيق الابتدائي في هذه النوعية من الجرائم المستحدثة، هذه المهام قد تكون عبارة عن إجراءات ذات طابع جزائي خاص نص عليها المشرع الجزائري، منها ما يطبق على كافة الجرائم كإجراءات المعاينة والخبرة والضبط وكذا التفتيش والحجز والتي قد تجرى هي الأخرى بطريقة خاصة على حسب خصوصية النظام المعلوماتي ومنها ما يطبق على جرائم محددة حصرا كالتي في شكل الجريمة المعلوماتية وهي إجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات والتسرب وكذا مراقبة الاتصالات الإلكترونية.

وقد تكون هذه المهام عبارة عن إجراءات تقليدية يقوم بها قاضي التحقيق، والتي يتم من خلالها استجواب المتهم بالجريمة المعلوماتية وأيضا مواجهته، كما تخول له سماع الشهود وكذا سماع الطرف المدني إن وجد، هذا ويبقى لقاضي التحقيق سلطة إعطاء عدة أوامر على حسب وضع وموقع المتهم من القضية كالأمر بإحضار المتهم والأمر بالقبض عليه وكذا الأمر بإيداع المتهم الحبس المؤقت أو الأمر بوضعه تحت الرقابة القضائية، هذه الأوامر تساعد وتساهم في عملية التحقيق الابتدائي من بدايته إلى

نهايته، هذا التحقيق تستدعي نتائجه إمّا إصدار أمر بانتفاء وجه الدعوى أو إصدار أمر بالإحالة إلى المحكمة المختصة.

وبما أنّ الجرائم المعلوماتية ذات طبيعة خاصة مميزة ومعقدة فإنّها تبقي قاضي التحقيق عالقا في دائرة الشك حول المتهم المعلوماتي، ذلك المجرم المعلوماتي في غالب الأحيان ما يكون محترفا في إخفائه لآثار وأدلة جريمته خاصة تلك الأدلة ذات الطبيعة المعنوية[1]، هذه النوعية من الأدلة تبقي قاضي التحقيق غارقا في شكه خاصة إذا لم يجد أدلة قوية تثبت براءة المتهم المعلوماتي، فيلجأ بذلك بل ويتعمد في كثير من الأحيان إلى إصدار الأمر بالإحالة إلى المحكمة المختصة بهذه الجريمة للتدقيق وتمحيص الأدلة المتوفرة ورغبة منه في الحصول على أدلة قوية أخرى أثناء المحاكمة وحتى بعدها.

وقبل البدء بمحاكمة المتهم بالجريمة المعلوماتية لابد في خطوة أولى النظر في الضمانات القانونية التي أعطاها القانون لهذا المتهم سواء كانت جوهرية أو عادية، وذلك أولا من خلال تحديد المحكمة المختصة بالنظر في هذا النوع من الجرائم وكذا علانية الجلسة وثانيا من خلال افتراض قرينة البراءة في هذا المتهم وحقه في الدفاع وعدم تحميله عبء إثبات هذه الجريمة المعلوماتية، هذه الأخيرة التي تبقى مسألة إثباتها على عاتق كل من المدعي وسلطة الاتهام، هذا مع بسط قاضي الحكم رقابته على الأدلة المستنبطة من مراحل الدعوى العمومية السابقة.

خاصة وأنّ هذه الأدلة أغلبها ذو طبيعة إلكترونية والتي جعلت من أمر التحقيق فيها وكذا رقابة قاضي الموضوع عليها يزداد صعوبة من خلال هذه المرحلة الفاصلة في الدعوى العمومية، ذلك أنّ هذه الطبيعة الخاصة التي تتميز بها هذه الأدلة تثير العديد من المشاكل سواء من الناحية الموضوعية ومن الناحية الإجرائية من جهة ومشكل إجراءات الحصول عليها من جهة أخرى فهي تتسع لتشمل إجراءات مستحدثة وكذا إجراءات تقليدية تطبق على أدلة جرائم عادية أخرى.

[1] الأدلة المعنوية (Soft Ware) هي البرمجيات التي توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة ويعرف لغة بأنها كلمة تستخدم للدلالة عن كل المكونات الغير مادية لنظام الحاسوب كنظم التشغيل وبرامج التطبيقات.

بل ومجرد الحصول على الدليل الإلكتروني من قبل قاضي الموضوع لا يكفي لاعتماده وحده كدليل إدانة، ذلك أنّه ذو طبيعة فنية خاصة تُمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، كما يثير الشك في مصداقيته كدليل إثبات جزائي لأنّ نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة[1]، إذن لابد على قاضي الموضوع أن يحصل على مزيد من الأدلة يعزز بها إثباته ويحسن بها إصدار حكمه كالاعتراف والأدلة الكتابية وكذا القرائن، وحتى إمكانية اتخاذ إجراءات خارج حدود الدولة المعنية إذا تطلب الأمر ذلك في شكل المساعدة القضائية الدولية.

هذا الحكم صدوره يعبر عن النتيجة التي آلت إليها التحقيقات في مراحل سير الدعوى العمومية وكذا مصير المتهم بالجريمة المعلوماتية إمّا بالبراءة أو الإدانة، لذلك على قاضي الموضوع قبل إصداره لهذا الحكم أن يحرص حرصا شديدا على تقدير أدلة الإثبات التي أتيحت له أثناء جلسة المحاكمة وأن يزنها جيدا وأن يستخلص منها قدر المستطاع قصد المتهم، وذلك حتى يكون حكمه الصادر صادرا عن قناعة قوية لا يهزها الشك وحتى يستطيع إحاطة حكمه هذا بأسباب مناسبة لا تخرج عن نطاق العلم والمنطق القانونين.

إذن هذا الحكم هو خاتمة المطاف في الخصومة ونقطة النهاية في سباق يترافع فيه أطراف الدعوى بأساليب وأدوات وحجج قانونية[2]، فهو يعتبر تتويجا لجهود كبيرة وجبارة وإجراءات طويلة يقوم بها أطراف الدعوى العمومية في هذه الجريمة المستحدثة، هذا الحكم يرتب آثار أولها من حيث تعرضه لموضوع الدعوى المتمثل في الجريمة المعلوماتية فقد يأتي حكما فاصلا فيها كما قد يأتي عكس ذلك

[1] خالد حسن أحمد لطفي، خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، د ط، دار الفكر الجامعي الإسكندرية، مصر، 2020، ص142.

[2] محمد سعيد عبد الرحمان، الحكم القضائي أركانه وقواعد إصداره، ط أولى، دار الفكر الجامعي، الإسكندرية، مصر، 2008 ص14

وثانيها من حيث قابليته للطعن فقد يأتي حكما ابتدائيا أو حكما نهائيا، وثالثها من حيث غياب وحضور المتهم في الجلسة فقد يأتي حكما غيابيا أو حكما حضوريا أو حكما حضوريا اعتباريا.

هذا ومن خلال ما سبق التطرق له بصفة عامة حول مختلف الإجراءات التي من الممكن تفعيلها في المراحل الثلاثة من سير الدعوى العمومية على الجرائم المعلوماتية، نفرض بأنّ الحماية الجنائية للنظام المعلوماتي في شقها الإجرائي هي السلاح الأمثل ذات الطابع القانوني في مواجهة وكشف هذه الجرائم المستحدثة ومعرفة مرتكبيها، بل وفي اكتشاف جرائم معلوماتية جديدة أخرى لم تكن السلطة المختصة بالتشريع على علم بها أصلا، بحيث تجعل هذه السلطة الأخيرة تنظمها وتضعها في قالبها المناسب انطلاقا من مبدأ شرعية النصوص الجزائية[1] الذي يحصر مصادر التجريم والعقاب في نطاق النصوص القانونية المكتوبة التي تضعها هذه السلطة[2].

وانطلاقا من هذه الفرضية فإنّ عملنا سيكون منصبا من أجل الوصول إليها كنتيجة، وعليه سيكون جهدنا محصورا في إطار الدراسة المفصلة لإجراءات سير الدعوى العمومية في هذه النوعية من الجرائم المستحدثة المتمثلة في الجرائم المعلوماتية، هذا وقبل التطرق بالتفصيل لهذه الدراسة وجب توضيح مسألتين في غاية الأهمية.

الأولى تكمن في سبب اختيارنا لهذا الموضوع، وهو أنّه يمس أحد الجرائم المستحدثة ألا وهي الجرائم المعلوماتية، ولأنّ هذه الأخيرة ذات طبيعة فنية في أغلبها جعلتنا نحس بثقل خطورتها، فهذه الخاصية من المؤكد أنّها تحمل تحت طياتها أسبابا وعوامل ستؤدي إلى حدوث الكثير من الكوارث الاقتصادية والمفاجآت غير السارة في المستقبل القريب، لأجل هذا سيكون موقعنا من هذه الدراسة هو اقتراح توصيات وحلول قانونية ذات طابع إجرائي تكون مساهمة في الصرح المتعلق بالوقاية من الجرائم المعلوماتية ومكافحتها مهما يكن نوعها ودرجة حداثتها.

---

[1] هذا المبدأ ترجمه المشرع الجزائري من خلال نص المادة 1 من ق ع بأنّه: " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون ".

[2] عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام)، د ط، المؤسسة الوطنية للفنون المطبعية، الرغاية، الجزائر 2015 ص99.

أمّا المسألة الثانية وهي سبب حصر دراستنا هذه في نطاق التشريع الجزائري ذلك أن المتطلع لعنوان هذه الدراسة والذي جاء ب " إجراءات سير الدعوى العمومية في الجرائم المعلوماتية"، يرى من الوهلة الأولى أنّه عنوان يتسع ليشمل في دراسته جميع ما جاء من إجراءات في التشريعات المقارنة ولكننا ولسبب بسيط والذي يكمن في مصطلح الدعوى العمومية نفسه والذي بُني عليه عنوان هذا البحث لاحظنا أنّها تُبنى فقط من طرف تشريعات عربية قليلة[1] تعد على الأصابع من أبرزها التشريع الجزائري هذا الأخير الذي غالبا ما يستعمل هذا المصطلح للتعبير عن الإجراءات الجزائية المتخذة في حالة ثبوت ارتكاب جريمة ما وذلك بهدف تطبيق العقوبات المقررة قانونا على الجاني.

هذا ولا يستطيع القارئ والمتمعن جيدا في هذا البحث تجاوز شعور التعقيدات التي كانت وما زالت تخلفه هذه الجرائم المعلوماتية من جهة وشعور الصعوبة في تفعيل مختلف الآليات الإجراءات عليها من جهة أخرى خاصة ما تعلق منها بالإجراءات الجديدة الخاصة التي حتمتها خصوصية هذه النوعية من الجرائم المستحدثة، كما لا أخفي عنكم استهانتي بهذا الدراسة من النظرة والوهلة الأولى هذه النظرة التي بدأت في التلاشي مع مرور الوقت ومن خلال السير في هذه البحث وفحص ما جاء حوله من قبل في كل من الفقه والتشريع سواء محليين كانا أو مقارنين.

ذلك أنّ هذا البحث ألقى ضمن جوانبه وفي جل مراحله عدة عقبات كان من اللازم علينا اجتيازها للوصول للهدف المطلوب والمنشود، هذه العقبات والصعوبات يكمن أبرزها في شح المادة العلمية من الناحية الإجرائية عبر مختلف مراحلها في الفقه والتشريع المحليين، وهذه المادة العلمية سواء العربية أو الأجنبية حتى وإن وجدت في التشريعات المقارنة إلاّ أنّها لم تغطي لب وجوهر مراحل هذه الدراسة خاصة من خلال مرحلتي التحقيق والمحاكمة في هذه النوعية من الجرائم المستحدثة والمتمثلة أساسا في الجرائم المعلوماتية.

---

[1] يستعمل المشرع الجزائري في الغالب مصطلح الدعوى العمومية – أنظر المواد 1، 2، 6، 7، 8 29، 35، 313، 314 من ق إ ج ويستعمل أحيانا مصطلح الدعوى العامة – أنظر الفقرة 1 من المادة 3 من ق إ ج واستعمل مصطلح الدعوى الجزائية – أنظر الفقرة 4 من المادة 3 من ق إ ج، هذا المصطلح تبناه كذلك كل من التشريعين التونسي والمغربي.

لذلك فإنّ هذه الدراسة استدعت منا الاعتماد على بعض مناهج البحث العلمي المتعارف عليها في نطاق العلوم الاجتماعية، وهو ما سيظهر جليا من خلال هذا البحث أين سنعتمد في غالبها على المنهج الوصفي نتطرق من خلاله لكل الإجراءات الممكن اعتمادها في نطاق الجرائم المعلوماتية، هذه الدراسة التي يتخللها كذلك في عناصر مختلفة كل من المنهجين التحليلي والمقارن لتوضيح مدى اللبس والغموض الذي يغطيها وموقف بعض التشريعات المقارنة حولها.

محاولين من كل ذلك الوصول إلى بيان مفهوم الجرائم المعلوماتية ورسم حدودها ومعرفة كيفية تعامل المشرع الجزائري مع خطرها من الناحية الوقائية والإجرائية وكيفية مواجهة التحديات والعقبات الإجرائية التي تثيرها، هذا مع الغوص في دراسة الطبيعة الفنية والقانونية لأدلتها الإلكترونية وتوضيح دور كل من ضباط الشرطة القضائية وقاضي التحقيق وقاضي الحكم في إثبات هذه الجرائم المستحدثة، وكذا تبيان طريقة تعاملهم مع شخص المتهم المعلوماتي لاستخراج أدلة مساعدة في إثبات نوع الجريمة المعلوماتية التي اقترفها هذا المتهم، على أن نحاول في الأخير إعطاء اقتراحات حول الكيفية التي يجب أن تكون بها ردة فعل سلطتي التحري والتحقيق مع هذا النوع من الإجرام المستمر والخطير.

فهذا الموضوع يثير الإشكالية الرئيسية التالية:

ماهي الآليات الإجرائية المستحدثة من طرف المشرع الجزائري التي تتناسب ومشكلة مكافحة الجرائم المعلوماتية؟

كما يثير الموضوع بعض التساؤلات الفرعية نذكر منها ما يلي:

هل ساهمت فعلا هذه الإجراءات المتخذة من طرف المشرع الجزائري في القضاء أو على الأقل في التخفيف من حدة هذه الجرائم المستحدثة؟

هل أسهمت الإجراءات الجديدة في تبني قواعد تسمح بوجود تعاون دولي في هذا المجال نظرا لخصوصية هذه الجرائم؟

ومن أجل حل هذه الإشكالية وكذا الإجابة على مختلف تساؤلاتها الفرعية عمدنا في الأول إلى خطة تتكون من بابين كأساس لها، أين سنتطرق في الباب الأول إلى ماهية الجرائم المعلوماتية في فصل أول من حيث مفهومها وأسبابها ومخاطرها وأهمية مواجهتها ومختلف تحدياتها من الناحية الإجرائية أمّا الفصل الثاني فسنتطرق لمختلف التحريات وإجراءات التحقيق الأولية سواء من حيث جمع الاستدلالات ومن حيث جمع الأدلة حول هذه الجرائم مع بيان مسألة تحريك الدعوى العمومية بشأنها.

مرورا إلى الباب الثاني الذي سنتطرق فيه إلى أهم مرحلتين في الدعوى العمومية، مرحلة التحقيق الابتدائي في فصل أول من حيث بيان الإجراءات الميدانية ومختلف السلطات التقليدية المخولة لقاضي التحقيق في هذه النوعية من الجرائم، أمّا الفصل الثاني فسنتركه لبيان مرحلة التحقيق النهائي أي المحاكمة عبر جميع مراحلها وأوقاتها، على أن نخرج في الأخير من خلال الخاتمة بمجموعة من النتائج التي ستخلفها هذه الدراسة مع إمكانية اقتراح بعض الحلول والتوصيات حول المشكلات الإجرائية التي قد تثيرها هذه الظاهرة الإجرامية المستحدثة.

الباب الأول: الجرائم المعلوماتية وإجراءات التحقيق الأولية فيها

لقد أصبح علم الإجرام المعلوماتي يتردد ويتبلور على ألسنة الكثير من الفقهاء لدرجة الإلحاح على مزيد من البحث والتقصي والدراسة حوله وهذا بغية الإحاطة بكافة جوانبه، ذلك أنّه يختلف اختلافا شاسعا عن الإجرام التقليدي، فالطبيعة الخاصة للجرائم المعلوماتية جعلتها تتمتع بعدة مميزات وخصائص تختلف بها عن غيرها من الجرائم بصفة عامة تقليدية كانت أم حديثة، حتى أنّ المجرم فيها يتمتع بالمهارة والمعرفة والذكاء في عملية ارتكابه لهذه النوعية من الجرائم.

فلا عجب إذن من التحدث عن ماهية الجرائم المعلوماتية من خلال معرفة مختلف التعريفات التي جاءت بها التشريعات ومختلف التعريفات التي جاء بها الفقهاء المختصون حولها، والتي تتمحور جلها في الجانب المعلوماتي محل وقوع الجريمة، هذه المعرفة تستوجب علينا لزوم معرفة الدوافع والأسباب التي تؤدي بالمجرم المعلوماتي لارتكابها، والتي من المنطق أن تختلف من مجرم لآخر كل حسب مركزه وظروفه داخل المجتمع هذا الاختلاف الذي أفرز عدة جرائم معلوماتية تباينت درجة خطورتها من جريمة لأخرى، لدرجة عجز الفقهاء وتشريعات الدول عن إيجاد تقسيم موحد لها عالميا.

هذه الجرائم من أجل كشفها ومتابعتها جزائيا لابد وأن تمر بمرحلة حساسة وهامة جدا، بحيث تُحدد وفق نتائجها مسألة البدء والسير بطريق الدعوى العمومية، ألا وهي مرحلة التحقيقات الأولية التي يكون صاحب الدور الرئيسي فيها ضباط الشرطة القضائية، الذين يقومون بالتحري وجمع الاستدلالات اللازمة من أجل كشف هذه الجرائم المستحدثة الجرائم المعلوماتية، هذه الأخيرة التي تضررت منها الكثير من الدول بل وزعزعت الأمانة والثقة لدى الكثير من الأشخاص الذين باتوا يتجنبون التعامل داخل العالم الافتراضي الذي أصبح بالنسبة إليهم لعبة في يد بعض المجرمين المحترفين يعبثون به كما يشاؤون.

لذلك تبقى مرحلة جمع الاستدلالات مرحلة حساسة جدا تجمع من خلالها مختلف الأدلة عن الجرائم المعلوماتية من قبل ضباط الشرطة القضائية، والذين يحيلون مختلف محاضرها وتقاريرها إلى النيابة العامة التي تبقى وحدها صاحبة الاختصاص في التصرف بنتائجها، فالدعوى العمومية قبل وضعها في

ساحة القضاء لابد لها وأن تمر بهذه المرحلة الحساسة التي يلعب فيها هؤلاء الضباط دور رئيسيا، والتي يمكن من خلالها جمع أكبر قدر من المعلومات عن هذه الجرائم المعلوماتية وظروف ارتكابها وما سبقها من مقدمات، لتعقب مرتكبيها والبحث عنهم وجمع الاستدلالات اللازمة التي تثبت ارتكابهم لها.

هذه المرحلة الهامة والحساسة سيتم التطرق له بشيء من التفصيل من خلال الفصل الثاني لهذا الباب، وهذا بعد التطرق أولا لماهية الجرائم المعلوماتية من خلال الفصل الآتي.

الفصل الأول: ماهية الجرائم المعلوماتية

لقد عنى الفقه الحديث عناية خاصة ونوعية بالجرائم المعلوماتية لدرجة أنّه أفرد لها علما جديدا متمثلا في علم الإجرام المعلوماتي، هذا الأخير أصبح يتردد ويتبلور على ألسنة الكثير من الفقهاء لدرجة الإلحاح على مزيد من البحث والتقصي والدراسة حوله وذلك بغية الإحاطة بكافة جوانب هذا النوع من الإجرام[1] الذي يختلف اختلافا شاسعا عن الجرائم التقليدية، وهو ما يلزمنا بالحديث عن ماهية الجريمة المعلوماتية والتي تقودنا لوجوب معرفة مختلف التعريفات التي جاءت بها التشريعات ومختلف التعريفات التي جاء بها الفقهاء المختصون، والتي تتمحور جلها في الجانب المعلوماتي محل وقوع الجريمة.

فطبيعة الجرائم المعلوماتية تحذوها خصوصية معينة كونها إحدى الجرائم المستحدثة التي تتمتع بعدة مميزات وخصائص تختلف بها عن غيرها من الجرائم بصفة عامة تقليدية كانت أم حديثة، كما أنّ المجرم فيها يتمتع بالمهارة والمعرفة والذكاء في عملية ارتكابه لهذه النوعية من الجرائم.

لذلك فإنّ عملية دراسة الجرائم المعلوماتية يقودنا كذلك للزوم معرفة الدوافع والأسباب التي تؤدي بالمجرم المعلوماتي لارتكابها، والتي من المنطق أن تختلف من مجرم لآخر كل حسب مركزه وظروفه داخل المجتمع هذا الاختلاف الذي أفرز عدة جرائم معلوماتية تباينت درجة خطورتها من جريمة لأخرى، لدرجة عجز الفقهاء وتشريعات الدول عن إيجاد تقسيم موحد لها.

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط ثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2014، ص23.

المبحث الأول: مفهوم الجريمة المعلوماتية

لا يزال هناك تباين أو عدم ثبات حول المصطلحات والتسميات التي تطلق على هذه الظاهرة الإجرامية الحديثة المتمثلة في الجرائم المعلوماتية والتي باتت تهدد الدول قبل الأفراد، ولا ربما يعود هذا التباين والاختلاف لنشأة وتطور وتمحور ظاهرة تكنولوجيا المعلومات من جهة، وإلى اختلاف وجهات النظر بين المختصين في مجال الإعلام وبين رجال القانون وعلماء الاجتماع وعلم النفس [1]من جهة أخرى.

وهو ما يفرض ضرورة النظر حول معرفة أولا مختلف التعريفات التي جاءت لشرح الجرائم المعلوماتية سواء كانت اصطلاحية أو فقهية وحتى تشريعية، وثانيا معرفة الطبيعة القانونية لهذه الجرائم والتي تتحدد بالنظر للطبيعة المعلوماتية، وثالثا وجوب معرفة الجاني والمجني عليه في إطارها وما يتمتعان به من مميزات وخصائص مع ذكر بعض الاعتداءات الشهيرة التي ألحقت ضررا كبيرة بالمنظومة المعلوماتية لعدة أشخاص كانوا ضحايا لها.

المطلب الأول: التعريفات المختلفة التي جاءت حول الجرائم المعلوماتية

إنّ غالبية التشريعات الحديثة ضمن نصوصها تتجه إلى عدم إيجاد تعريف جامع وشاف للجرائم المعلوماتية وهو ما لمسناه أيضا في جل النصوص القانونية الجنائية التي جاء بها المشرع الجزائري فالجرائم المعلوماتية أو ما يسميها البعض بالجرائم الإلكترونية أو جرائم الحاسب الآلي والإنترنيت رغم محاولة الكثير من الفقهاء وبذل الجهد في إيجاد ووضع تعريف جامع ومانع لها، لم يسفر إلى الوصول للنتيجة المطلوبة[2].

[1] عبد الحكيم رشيد توبة، المرجع السابق، ص107.

[2] غانم مرضي الشمري، المرجع السابق، ص24.

الفرع الأول: تعريف الجرائم المعلوماتية اصطلاحا

إنّ تعريف الجرائم المعلوماتية اصطلاحا يوجب معرفة ما يعني كل مصطلح أي معرفة الجريمة من جهة ومعرفة المعلوماتية من جهة أخرى وهو ما سيتم التطرق له في الآتي؛

أولا: تعريف الجريمة

إنّ الجريمة كظاهرة اجتماعية قد عرفتها المجتمعات البشرية منذ القديم وذلك بحسب تغير مضمونها ونطاقها بحسب الزمان والمكان، بحيث تتحكم فيها مجموعة من العوامل كالدين والحضارة والنظام السياسي والاقتصادي والقانوني، فمثلا الجريمة في الشريعة الإسلامية عرفت بأنّها محظورات شرعية زجر الله عنها بحد أو تعزيز، والمحظورات هي إتيان فعل منهي عنه أو ترك فعل مأمور به، فهي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه، فالجريمة في الشريعة هي إتيان فعل محرم معاقب على فعله أو ترك فعل معاقب على تركه والملاحظ أن الفعل أو الترك لا يعتبر جريمة إلاّ إذا صاحبه جزاء أي عقاب فإن لم يتواجد هذا الأخير فالفعل أو الترك ليس بجريمة[1].

هذا وينصرف تعريف فقهاء القانون للجريمة بأنّه: "كل مخالفة لقاعدة من قواعد القانون بمختلف فروعه المطبق والمعمول به في مجتمع من المجتمعات، سواء كانت تلك القواعد من قواعد القانون الجنائي أو غيرها من قواعد القوانين المختلفة كالقانون المدني والقانون التجاري والقانون الإداري والقانون المالي"[2]، إذن للجريمة مدلولين أحدهما واسع والآخر ضيق، الواسع ينصرف لكل مخالفة قاعدة قانونية مهما كان مصدرها شرعية أو جنائية أو إدارية أو مدنية إلى غيرها من المصادر أمّا المدلول الضيق فينحصر نطاقه في المخالفات التي تقع خرقا لأحكام قانون العقوبات والقوانين المكملة له.

---

[1] حسني عبد السميع إبراهيم، المرجع السابق، ص12.

[2] عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام) ، المرجع السابق، ص63.

ثانيا: تعريف المعلوماتية

المعلوماتية كلمة تقودنا إلى مصطلح المعلومات، هذا الأخير شاع استخدامه منذ الخمسينات من القرن الماضي في مجالات مختلفة لذلك اختلفت وتنوعت مفاهيمه وهو من حيث الأصل مشتق من كلمة علم، كما أنّ دلالته بوجه عام تدور حول المعرفة التي يمكن نقلها واكتسابها، لهذا ولأجل تعريف المعلوماتية يستلزم أولا معرفة المقصود بالمعلومات هذه الأخيرة المحيطة بنا من كل جانب ومتعلقة بشتى وجوانب مجالات الحياة فهناك المئات من التعريفات الاصطلاحية التي عرضها باحثون كثر من تخصصات وثقافات مختلفة حول هذا المصطلح.

فكانت إحدى تعريفاتهم بأنّها:"مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة"[1]، هذا المصطلح يشار إليه كذلك إلى المعلومات المعالجة والمبرمجة آليا والذي اختلف فيه الكثير من الباحثين من حيث مصدره ومنبعه.

فمنهم من نسب اقتراح مصطلح المعلوماتية إلى الأستاذ Drefus الذي استخدمه لتمييز المعالجة الآلية للمعطيات المعلوماتية وقال بأنّه مصطلح يتكون من مقطعين في اللغة الأجنبية الأول INFORMATIONوالثاني AUTOMATIQUE، كما تبنته بعد ذلك الأكاديمية الفرنسية في أبريل 1966، ومنهم من نسبه إلى الأستاذ A.I.Mikhailov مدير المعهد الاتحادي للمعلومات العلمية والتقنية (VINNTI) بالاتحاد السوفياتي سابقا والذي استعمله كوصف لعلم المعلومات العلمية.

بعد ذلك زاد استخدامه على نطاق واسع بمفاهيم متباينة لعدة باحثين في مناطق مختلفة[2] فمنهم من عرفها بأنّها: " علم يعنى بالمعالجة المنطقية للمعلومات التي تعد دعامة للمعارف الإنسانية والاتصالات

---

[1] محمد عبد الله أبو بكر، جرائم الكمبيوتر والإنترنيت موسوعة جرائم المعلوماتية، د ط، المكتب العربي الحديث، الإسكندرية مصر 2007، ص71.

[2] محمد عبد الله أبوبكر، المرجع السابق، ص73.

في المجالات الفنية والاقتصادية والاجتماعية وذلك باستخدام معدات آلية" فالمعلوماتية بمعناها الواسع هي كل وسيلة مخصصة لصناعة المعلومات أو لمعالجتها أو لتخزينها أو لعرضها أو لإتلافها أين يتطلب تشغيلها الاستعانة بالوسائل التقنية الإلكترونية[1].

الفرع الثاني: تعريف مختلف التشريعات والمنظمات الدولية للجرائم المعلوماتية

إن الانتشار الكبير للإنترنيت والحواسب الآلية في الحياة العملية أظهر معه ضرورة وضع حلول قانونية للمشاكل الناتجة عن استخدام المعلوماتية من قبل المشرع لسن قواعد خاصة لتنظيم استخدام الإنترنيت في بعض المجالات الحيوية واستخدام قواعد رئيسية إذا ما أراد المشرع أن يستهدي بها في تنظيم مجال أو أكثر من مجالات استخدام الإنترنيت، ووضع قواعد خاصة في مجال إثباتها وفي مجالاتها الأخرى[2]، ذلك أن العقبة الأولى هي عدم وجود تعريفا دقيقا وجامعا للجرائم المعلوماتية في كل التشريعات.

وهذا ما أشارت إليه الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة للجرائم المعلوماتية، وإن كانوا قد اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم إلاّ أنّهم لم يتوصلوا إلى تعريف متفق عليه دوليا لهذه المصطلحات، وربما ذلك بسبب محلها المتمثل في المعلومة هذه الأخيرة التي أشار إليها القانون الفرنسي الصادر في 29 يوليو 1982 الخاص بالاتصالات السمعية والبصرية بصفة عامة حيث عرفها بأنّها: " رنين أو صور أو وثائق أو بيانات أو رسائل من أي نوع ".

هذا وقد شهدت الجريمة المعلوماتية كذلك عدة تعريفات من منظمات وتنظيمات منها منظمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982 التي عرفتها بأنّها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "، وهذا التعريف فضلا عن تحديده لماهية السلوك الإجرامي للجريمة المعلوماتية التي قد

---

[1] علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، ط أولى، المؤسسة الحديثة للكتاب، طرابلس، لبنان 2006، ص301.

[2] عبد الصبور عبد القوى علي مصري، الجريمة الإلكترونية، ط أولى، دار العلوم للنشر والتوزيع، القاهرة، مصر، 2008 ص105.

تقع سواء بالفعل الإيجابي أو السلوك السلبي المتمثل في الامتناع[1] إلاّ أنّه جاء متسما بتوسيعه لنطاق الجرائم المعلوماتية، وكذلك بالنسبة لمكتب تقييم التقنية في الولايات المتحدة الأمريكية الذي عرفها بأنّها: " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[2].

أمّا عن الأمثلة التشريعية المقارنة التي أعطت تعريفا لها كان نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية[3]من خلال نص المادة الأولى منه أين عرفها بأنّها: " الجريمة المعلوماتية أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لهذا النظام"[4]، وكذلك المشرع الأمريكي عرفها بأنّها:" الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملف البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة"[5].

أمّا عن المشرع الجزائري فلقد جاء تعريفه لها من خلال القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[6] أين عرفها بأنّها: "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] خالد داودي، الجريمة المعلوماتية، ط أولى، دار الإعصار العلمي للنشر والتوزيع، عمان، الأردن، 2018، ص25.

[2] عبد العال الدربي، محمد صادق إسماعيل، الجرائم الإلكترونية، ط أولى، المركز القومي للإصدارات القانونية، القاهرة، مصر 2012 ص42.

[3] عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنيت في التشريعات العربية، ط أولى، القاهرة، مصر، 2009، ص6.

[4] هيئة الاتصالات وتقنية المعلومات، نظام مكافحة جرائم المعلوماتية، عن موقع https://www.citc.gov.sa/ar/ تاريخ الإطلاع 2020/03/23.

[5] أيمن عبد العال، الجرائم الإلكترونية في التشريع الفلسطيني، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية غزة فلسطين، 2013، ص7.

[6] قانون رقم 09- 04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

هذا وقد كانت السويد أول دولة سنت تشريعات خاصة بالجرائم المعلوماتية أين عالجت في قانون البيانات السويدي عام 1973 قضايا الاحتيال عن طريق الحاسب الآلي، هذا القانون الذي تميز بشموله على فقرات عامة بينت جريمة الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها، وتبعتها بعد ذلك الولايات المتحدة الأمريكية فبريطانيا فكندا ثم الدنمارك ففرنسا فهولندا، هذه الدول عدلت من قوانينها الجنائية ليتم إدخال الجرائم المعلوماتية في قالب وإطار قانونيين.

بحيث تم تجريم كل ما يشملها من عمليات احتيال ونصب وملكية فكرية واختراق أجهزة الآخرين إلى غيرها من الصور الأخرى، أمّا على المستوى العربي فمع الأسف لم تقم أي دولة عربية بسن قوانين خاصة تضم كل الجرائم المعلوماتية وإن وجد نص قريب من الفعل المرتكب فإنّ العقوبة المنصوص عليها تأتي لا تتلاءم وحجم الأضرار المترتبة على هذه الجريمة المعلوماتية[1].

وعليه ومن خلال التعريفات التشريعية التي ضُرب بها المثال سابقا، الملاحظ أنّها جاءت مختلفة فيما بينها ذلك أنّ كل مشرع إلاّ وأعطى تعريفا للجرائم المعلوماتية بحسب واقعه المعاش وبيئته وموقعه وبحسب الزاوية التي ينظر من خلالها لهذه الجرائم، وهو ما ترك المجال مفتوحا أمام الفقهاء من جهة وصعب من مهمتهم في إيجاد تعريف شامل وكامل وموحد لها من جهة أخرى بدليل اختلاف التعريفات الصادرة عنهم والتي سنبين بعضها من خلال العنصر الآتي.

الفرع الثالث: التعريف الفقهي للجرائم المعلوماتية

كنا قد أشرنا سابقا بأنّه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها فالبعض يطلق عليها جريمة الغش المعلوماتي والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي والاحتيال والجريمة الإلكترونية وآخرون يفضلون تسميتها بالجريمة المعلوماتية إلاّ أنّ الاتجاه الغالب يفضل اصطلاح الجرائم المعلوماتية على الجرائم المتعلقة بالحاسوب والانترنيت لأنّه

[1] عبد العال الدربيي، محمد صادق إسماعيل، المرجع السابق، ص172 – 174 .

عام، كما أنّه يتسع ليشمل التقنيات الحالية والمستقبلية كلها والمستخدمة في التعامل مع المعلومات أيا كان نوعها بما في ذلك الحاسوب وشبكة الانترنيت.

أمّا في إطار تعريف الفقه للجريمة المعلوماتية فالاتجاهات اختلفت في هذا الأمر ما بين موسع ومضيق لمفهوم الجريمة المعلوماتية.

من بين التعريفات الموسعة لمفهوم الجريمة المعلوماتية جاءت بأنّها: "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية والمعنوية" وبأنّها كذلك "كل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت "[1]، وبأنّها كذلك: "الجرائم المعلوماتية هي التهديدات الحقيقية التي تمارس بكميات كبيرة على أساس منتظم بأنواع مختلفة من الأنشطة الإجرامية والتي تثير القلق في حياة الكثير من الأشخاص في عصرنا الحالي الذي يتزايد فيه استخدام الكمبيوتر"[2].

وفي المقابل هناك بعض التعريفات التي ضيقت من مفهوم الجريمة المعلوماتية فجاءت بأنّها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى "[3]، وكذلك بأنّها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى "[4].

هذا ومن خلال التعريفات الفقهية السابقة الذكر نلاحظ بأنّ المشرع الجزائري تبنى الاتجاه الموسع عند تعريفه للجرائم المعلوماتية بدليل إدخاله في مجال هذه الجريمة أي شخص بفعله يرتكب أو يسهل ارتكابه الاعتداء على منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

---

[1] نهلا عبد القادر المومنى، الجرائم المعلوماتية، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص47.

[2] Chuck Easttom and Jeff Taylor, Computer crime, investigation, and the law revue routledge taylor& francis group, volume 13, numero 6, Royaume-Uni December 2012, p539.

[3] نهلا عبد القادر المومنى، المرجع السابق، ص49.

[4] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، د ط، الإسكندرية، مصر، 2008، ص42.

المطلب الثاني: الطبيعة القانونية للجرائم المعلوماتية ومختلف خصائصها

تختلف الجرائم المعلوماتية عن الجرائم التقليدية لكونها تتسم بطابع خاص في أنّها جريمة عابرة للحدود قد ترتكب في العديد من الدول ويكون تأثيرها ممتد ليصل إلى عدد غير محدود من الدول عكس الجرائم التقليدية التي في الغالب ما تتم داخل الدولة ويكون تأثيرها منحصرا في تلك الدولة فقط، كما أنّه وفي جميع الأحوال يكون فيها الحاسب الآلي هو منبع ارتكاب لهذه الجرائم المعلوماتية بحيث يكون مرتكبها غالبا هو شخص ذو خبرة فائقة في مجال الحاسب الآلي، وتكون فيه المعلومات محلا لهذه الجريمة إمّا بذاتها أو بما تمثله[1].

الفرع الأول: الطبيعة القانونية للجرائم المعلوماتية

تعد الجرائم المعلوماتية من الجرائم المستحدثة والتي ظهرت نتيجة التطور الهائل في مجال التقنية العالية وبالتالي فإن أمر تحديد هذا النمط من الإجرام يكتنفه صعوبات ترجع إلى الطبيعة الخاصة لهذا النوع من الجرائم والتي تطال المعلومات، فلا يخفى على أحد أنّ هناك اتجاهات فقهية متنافرة بخصوص تحديد مفهومها وطبيعتها ومع ذلك فإنّ أغلب الفقهاء متفق على إطلاق مصطلح الجرائم المعلوماتية على هذا النمط من الإجرام[2] وذلك كون أن المعلومات هي المحل الرئيسي التي تقع عليه مثل هذه الجرائم.

هذا ويرى جانب من الفقه[3]في إطار محاولة تحديد الطبيعة الخاصة للجرائم المعلوماتية بالقول: " يجب أن نعترف أنّنا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي ففي معظم حالات ارتكاب الجريمة ندخل في مجال المعالجة الإلكترونية للبيانات"، كما يشير أيضا إلى أنّ تحديد هذه الطبيعة تستلزم إضافة مجال معالجة الكلمات أو معالجة النصوص، والتعامل أيضا مع مفردات

---

[1] علي جبار الحسيناوي، المرجع السابق، ص34.

[2] محمود محمد عبابنة، المرجع السابق، ص20.

[3] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، د ط، دار النهضة العربية، مصر، 1992، ص5.

جديدة مثل البرنامج والبيانات ويضيف هذا الجانب من الفقه:" بأن القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه، وللتطور السريع المتلاحق في حقل المعلوماتية".

فيمكن القول بأنّه بينما تظهر الجرائم المعلوماتية في شكل جرائم ذوي الياقات البيضاء، يبقى بعضها لا يندرج ضمن هذه الفئة الأخيرة من الجرائم ذلك أنّه من غير الكافي التوقف عن استيعاب ومناداة المجرمين المعلوماتيين بذوي الياقات البيضاء، دون محاولة الحصول على الصورة الحقيقية لهؤلاء من خلال الدراسات الإجرامية[1] والأشكال الأخرى من الانحراف الإجرامي.

وإذا كان الجاني في هذا النمط من الجرائم يتجه للاعتداء على المعلومات بما تمثله من أسرار وبيانات وأموال فإنّ أمر تحديد المال المعلوماتي أيضا من الأمور التي تتطلب تحليلا وتأهيلا قانونيا خاصا فوفقا للتطور المتسرع وظهور أنماط مستحدثة من الإجرام كان من اللازم لوصف المال الذي يرد على شيء مادي أن يتغير وفقا للقانون والفقه الحديث، وبالتالي تصبح البيانات والتي هي جزء من معطيات الحاسب الآلي لها صفة المال الذي تغير وصفه وأصبح يرد على أي شيء له قيمة اقتصادية[2].

هذا ولقد اجتهد الفقه الغربي الحديث في محاولته لتحديد طبيعة المال المعلوماتي بوصفه ذو طبيعة معنوية، فهناك من قالوا بأنّ الأموال ليست ذات طبيعة معنوية ويستندون في ذلك أنّ المادة وفقا للتعريف العلمي هي كل ما يشغل فراغا في العالم الخارجي، وعلى ذلك فإنّ البيانات التي يتضمنها الحاسب الآلي هي من قبيل المواد وليست من قبيل المعنويات، ذلك لأنّها عبارة عن نبضات رقمية تشغل حيزا على ذاكرة التخزين، وهذا الرأي بالرغم من منطقه إلاّ أن الفكر القضائي والفقهي والتشريعي لم يتطور بعد بالشكل الذي يتقبل فكرة إدراجها في إطار المواد وبالشكل الذي يهجر فكرة وجوب إخراج المال من حيازة حائزه الشرعي وإزالة قدرته على التصرف فيه لتمام فعل السرقة.

---

[1] Mohamed CHAWKI, Essai sur la notion de cybercriminalité, IEHEI document provient du site iehei.org, Université Lyon III, France, juillet 2006, p30.

[2] محمود أحمد عبابنة، المرجع السابق، ص21.

الفرع الثاني: خصائص الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية جرائم ذات خصائص تتميز بها عن مختلف الجرائم التقليدية الأخرى سواء في أسلوبها أو في طريقة اقترافها[1]، وتتمثل مجمل هذه الخصائص في الآتي؛

أولا: الجرائم المعلوماتية جرائم مستحدثة

ذلك أنّها تعتبر من بين الجرائم الجديدة التي تهدد أمن الدولة وأمن مواطنيها وتشكل أخطارا جسيمة في ظل العولمة خاصة في ظل التقدم التكنولوجي الهائل الذي تحقق خلال السنوات القليلة الماضية، هذا التقدم الذي تجاوز بقدراته وإمكاناته أجهزة الدولة الرقابية فأضعف من قدراتها في تطبيق قوانينها.

ثانيا: عدم وجود مفهوم مشترك للجرائم المعلوماتية

لعل السبب في عدم وجود تعريف موحد للجرائم المعلوماتية يرجع لعدم وجود تنسيق دولي في مجال هذه الجرائم أو لاختلاف النظم القانونية، لذا الأمر يتطلب إيجاد الوسائل المناسبة لتشجيع جميع الدول لمواجهة الجرائم المعلوماتية والعمل على سن تشريعات خاصة تواجه هذا النوع من الإجرام وإبرام المعاهدات التي تحث على تبادل المعلومات والخبرات وتسليم وتبادل المجرمين[2].

ثالثا: الحاسب الآلي هو الأداة الرئيسية لارتكاب الجرائم المعلوماتية

يعتبر الحاسب الآلي الأداة التي تمكن الجاني من الدخول إلى شبكة الإنترنيت للقيام بأي جريمة أيا كان نوعها وهي خاصية متفردة عن أي جريمة أخرى.

رابعا: الجرائم المعلوماتية جلها ترتكب بمساعدة شبكة الانترنيت

تعد شبكة الانترنيت حلقة الوصل بين مختلف الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف الأخرى التي يستطيع المخترق الولوج إليها والتلاعب بها كيف شاء،

---

[1] منير محمد الجنبهي، ممدوح محمد الجنبهي، جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها، د ط، دار الفكر الجامعي الإسكندرية، مصر، 2004 ص13.

[2] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص47.

الأمر الذي دعا معظم تلك الأهداف إلى محاولة حماية نفسها من تلك الجرائم من خلال اللجوء إلى نظم الأمن الإلكترونية لتحد على الأقل من خسائرها عند وقوعها ضحية لتلك الجرائم.

خامسا: غالبا ما تقع الجرائم المعلوماتية أثناء المعالجة الآلية للمعطيات

قد تقع الجرائم المعلوماتية أثناء عملية المعالجة الآلية للمعطيات وفي أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال المعطيات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات.

سادسا: مرتكب الجرائم المعلوماتية هو شخص ذو خبرة فائقة في مجال الحاسب الآلي

غالبا ما يكون الجناة على دراية فائقة وذوي خبرة كبيرة في مجال استخدام الحاسب الآلي التي تمكنهم من تنفيذ جريمتهم والعمل على عدم اكتشافها، لذلك نجد أنّ من يرتكبون تلك الجرائم جلهم من بين الخبراء في مجال الحاسب الآلي[1].

سابعا: الجرائم المعلوماتية لا حدود جغرافية لها

لقد ألغت شبكة الإنترنيت أي حدود جغرافية فيما بين الدول فالأشخاص يمكنهم الآن التحدث والدردشة فيما بينهم من بلدان مختلفة وحتى بين قارات مختلفة، وعليه فإنّ أي جريمة ترتكب عبر شبكة الإنترنيت يمكنها أن تتجاوز حدود الدولة التي ارتكبت فيها لتتعدى آثارها مختلف البلدان على المستوى العالمي.

ثامنا: صعوبة إثبات الجرائم المعلوماتية

فهذه النوعية من الجرائم تتسم بالخفاء أي لا تترك آثار مادية لها بعد ارتكابها، فهي خطيرة وصعبة الاكتشاف وصعبة في تحديد مكان وقوعها بسبب اتساع نطاقها المكاني وضخامة البيانات لكونها تقع في بيئة إلكترونية يتم فيها نقل مختلف المعلومات وتداولها، فهي جرائم مستحدثة لا تترك في الغالب شهودا يمكن استجوابهم ولا أدلة مادية يمكن فحصها لذلك تلقى أجهزة الأمن المختلفة صعوبة

[1] منير محمد الجنبهي، ممدوح محمد الجنبهي، المرجع السابق، ص15.

كبيرة في الكشف عنها[1]، إذ يستطيع المجرم المعلوماتي في وقت وجيز جدا أن يمحو أو يحرف أو يغير في البيانات والمعلومات الموجودة في الحاسب الآلي.

ذلك أنّها تعتمد في أغلبها على الخداع والذكاء في ارتكابها والتضليل، فالجرائم المعلوماتية من النوعية التي يمكن وصفها بجرائم الذكاء التي ترتكب غالبا من قبل مجرمين ذوي مهارات تقنية عالية وإلماما بتكنولوجيا المعلومات، لذا فهي تحتاج إلى خبرة فنية لدى رجال القضاء والنيابة العامة ورجال الشرطة القضائية ممن لهم إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات من أجل التحقيق فيها وملاحقة مجرميها.

تاسعا: تردد المجني عليه أحيانا في الإبلاغ عن وقوع الجريمة المعلوماتية

ففي غالب الأحيان لا يتم الإبلاغ عن الجرائم المعلوماتية[2] إمّا لعدم اكتشاف الضحية لها وإمّا لخشيته من التشهير، لذا نجد أن عدد كبير من هذه الجرائم المرتكبة لم تكتشف كما أنّ معظمها الآخر تم اكتشافها بالمصادفة بل وبعد وقت طويل من ارتكابها.

المطلب الثالث: المجرم والمجني عليه في الجرائم المعلوماتية

الإنترنيت حسب بعض الفقهاء هو منطقة بدون قانون وبمجرد اتصال الحاسب الآلي الشخصي بهذه الشبكة يتم تداول مختلف المعلومات المتداولة وتصبح ذات صفة دولية، وبالتالي إذا بثت مادة معلوماتية في الجزائر يمكن لآخر في أي دولة من الاطلاع عليها، كما أنّ أي قرصان من بريطانيا يستطيع الولوج على موقع يُحتفظ فيه ببيانات شخصية تم معالجتها في اسبانيا وهكذا، وعليه فإن أي إجراء وأي معاملة كانت على أي نظام فهي معرضة للاختراق والتهديد من قبل مجرمين محترفين في هذا المجال[3]، فالمعادلة إذن تتطلب مجرم معلوماتي وضحية معلوماتي واعتداء الأول على الثاني معلوماتيا.

---

[1] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص45.

[2] نهلا عبد القادر المومنى، المرجع السابق، ص55.

[3] حسني عبد السميع إبراهيم، المرجع السابق، ص56.

الفرع الأول: المجرم المعلوماتي طوائفه وسماته وأنماطه

قد أشارت شركة GBM للحاسبات الآلية عن طريق الإعلانات في الجرائد الأمريكية ذات الشهرة الواسعة من أن الحاسبات الآلية ليس بإمكانها أن ترتكب بذاتها مختلف الجرائم المعلوماتية وإنّما تستخدم كوسيلة لارتكاب هذه الجرائم من طرف المجرم المعلوماتي الذي يعتبر جوهر المشكلة بشخصيته ودوافعه.

أولا: طوائف المجرم المعلوماتي

1- طائفة العاملين بمجال الحاسب الآلي

هم الذين يستغلون طبيعة عملهم لارتكاب جرائم مختلفة على المؤسسات التي يعملون بها أو على مؤسسات أخرى باستخدام المعلومات والبيانات والمهارات التي زودتهم بها وظائفهم، هذه المجموعة تمثل الغالبية العظمى من مرتكبي تلك الجرائم.

2- طائفة الموظفون الساخطون على مؤسساتهم

فقد يقومون باستخدام الكمبيوتر للتعدي على بعض المعلومات الخاصة بالشركة أو المعلومات الخاصة بالمؤسسة[1].

3- طائفة الهاكرز أو الكراكرز

الذين قد يستعملون الحاسب الآلي من أجل التسلية عن طريق استخدام شبكة الإنترنيت لتحقيق المزيد من الأرباح غير المشروعة، هذه الطائفة عرضة لاستغلال جماعة الجريمة المنظمة في عملياتهم المجرمة.

[1] جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، ط أولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2010 ص74.

ثانيا: سمات المجرم المعلوماتي

1- المجرم المعلوماتي إنسان ذكي

لا يتصور ولا يستنتج أن الإتلاف المعلوماتي دائما بحاجة إلى سلوك عنيف فمن الممكن أن ينشأ من تقنيات التدمير الناعمة كالتلاعب بالمعلومات أو الكيانات المنطقية هذه التقنيات لا يتم استعمالها غالبا إلاّ من ذوي الاختصاص وكذلك أصحاب الذكاء في هذا المجال، وهذا التدمير في الغالب ما يأتي بواسطة برامج تعرف بالفيروسات المعلوماتية يكون حجمها صغير يصعب اكتشافها وخلال فترة وجيزة من ولوجها تستطيع تحطيم جميع البطاقات، فالمجرم المعلوماتي دائما نجد شخصيته تتسم بالنشاط والمخاطرة والذهن المعقد الذي يسعى إلى خداع الآلة[1]، وبصفة عامة يتميز المجرم المعلوماتي بمجموعة من الخصائص[2] التي تميزه عن غيره من المجرمين ويرمز الأستاذ "parker"[3] إليها بكلمة[4] S .K.R.A.M.

2- المجرم المعلوماتي كإنسان اجتماعي

قد يلجأ بعض المجرمين المعلوماتيين أحيانا إلى ارتكاب مثل هذه الجرائم بدافع اللهو أو إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتية حتى أنّهم لأجل ذلك قد لا يحصلوا على أية منافع مالية، لكن لا يستخلص من ذلك انعدام أي خطر اجتماعي للإجرام المعلوماتي وذلك للسلوك غير الواعي من قبل هؤلاء المجرمين والذي يمكن أن يتسبب في أضرار جسيمة حتى ولو لم يكشف من جراء ذلك أي عداء للمجتمع أو أي نوايا آثمة.

---

[1] سامى علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنيت، د ط، دار الفكر الجامعي، الإسكندرية، مصر، 2007 ص50.

[2] هذه الخصائص أعطاها الأستاذ parker رمز S .K.R.A.M وهي Resources. Anthority. Motives Skills.Knowledge والتي تعني الباعث، السلطة، الوسيلة، المعرفة، المهارة.

[3] الأستاذ روبرت باركر هو باحث في تاريخ العصور الكلاسيكية ومؤرخ بريطاني ولد في 19 أكتوبر 1950.

[4] خالد داودي، المرجع السابق، ص32.

ثالثا: الأنماط المختلفة للمجرم المعلوماتي

1- صغار نوابغ المعلوماتية

وهم الشباب المولع بالمعلوماتية والحاسبات الآلية وجل أفعالهم تتمثل في الانتهاك غير المسموح به في ذاكرات الحاسبات الآلية فهم مفتونون بهذه الأنشطة غير المشروعة المبتكرة والمستحدثة، فهم لا يُقدرون أبدا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم هذه بالنسبة لنشاط المؤسسة أو الشركة وذلك كله بسبب ميلهم فقط للمغامرة والتحدي والرغبة في الاكتشاف، فالخطر الذي يواجه هذه الطائفة هو احتمال الانزلاق الذي من الممكن أن يحدث لهؤلاء أين يمكنهم أن يصبحوا من مجرد هواة صغار للأفعال غير المشروعة إلى محترفي لأعمال السلب، كما أنّهم معرضين للاستغلال من قبل منظمات أو أفراد غير شرفاء[1].

2- محترفو الجرائم المعلوماتية

وهم أفراد ذو خطورة خاصة بسبب تقنياتهم العالية وغموض شخصيتهم وتؤكد الدراسات والدعاوي التي تم تحريكها في هذا الشأن سواء في أمريكا أو في أوروبا أنّ الجيل الحديث هم الأكثر لمرتكبي أفعال الغش المعلوماتي بحيث تتراوح أعمارهم من 25 إلى 45 سنة.

الفرع الثاني: المجني عليه في الجرائم المعلوماتية

من المستحيل أن يتم تحديد على نحو دقيق نطاق وحدود الجرائم المعلوماتية وفقا لتقديرات بعض الخبراء من الصندوق الدولي للبنوك FBG، حتى أنّ بعض الضحايا لا يعلمون عنها شيئا إلاّ عندما تكون أنظمتهم المعلوماتية هدفا لتلك الأفعال المجرمة، كما تعتبر المعلومات أكثر هدف معرض للجرائم المعلوماتية وتكون إمّا بالحصول عليها أو تغييرها أو حذفها نهائيا، ولعل المجال الأكبر من هذه الجرائم

[1] سامي على حامد عياد، المرجع السابق، ص53.

يكون اقتصاديا بالدرجة الأولى أو بما يعرف بالجرائم الاقتصادية، وكلها لأجل الحصول على مزايا أو مكاسب اقتصادية[1].

هذا ويستخدم الحاسب الآلي في جميع الأنشطة التي تكون عرضة لخطر ظاهرة الغش المعلوماتي هذا الأخير الذي يستهدف البنوك في حدود 19 في المائة، ويستهدف خاصة المنشآت المالية أو التي تهيمن على القيم الرأس المالية وبعدها تأتي النقود[2]، إلاّ أنّ هناك سوق سوداء للمعلومات بجانب السوق الشرعي للمعلومات والتي تتم بمقتضاه مقايضة المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين.

ولعل معظم الجرائم المعلوماتية التي ترتكب عبر شبكة الإنترنيت تستهدف إمّا أشخاص أو جهات بعينها وغالبا ما تكون تلك الجرائم هي إمّا جرائم مباشرة ترتكب في صورة ابتزاز أو تهديد أو تشهير وإمّا جرائم غير مباشرة ترتكب في صورة الحصول على بيانات ومعلومات تخص تلك الجهات والأشخاص وتستخدم فيما بعد في ارتكاب جرائم مباشرة، وعليه فإنّ هذا النوع من الإجرام يستهدف في معظم اعتداءاته مختلف الأنشطة ذات الطابع الاقتصادي وذات الطابع الاجتماعي للدول والتي لا تخرج عن نطاق صور المعلومات الآتية؛

أولا: المعلومات ذات الطابع المالي

تستهدف المركز الحسابي والإداري وتنقلات الأموال والاستثمارات وفي المنشآت العامة والمنشآت الخاصة.

ثانيا: المعلومات ذات الطابع التجاري والصناعي

تستهدف الدراسات الخاصة بمختلف الأسواق وأيضا مشاريع الاستثمار وكذا التصنيع والإنتاج والتوزيع والتجارة والأسعار ومراكز البيع والقطاع الصناعي للإنتاج.

---

[1] منير محمد الجنبهي، ممدوح محمد الجنبهي، المرجع السابق، ص16.

[2] سامي على حامد عياد، المرجع السابق، ص61.

ثالثا: المعلومات ذات الطابع الشخصي

هي المعلومات المخزنة ضمن ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدى المستشفيات وبمختلف مراكز الأمن وكذلك الأحزاب ولدى المحامين.

رابعا: المعلومات ذات الطابع العسكري

تلك المتمثلة في أسرار الدولة والتصنيع الحديث للأسلحة والمشروعات النووية، هذه المعلومات هي الأكثر رواجا في سوق المعلومات السوداء.

الفرع الثالث: بعض الاعتداءات الشهيرة على نظام المعلوماتية

تعتبر الجرائم المعلوماتية أحد الجرائم المستحدثة والتي عُرفت بعد ظهور الحاسب الآلي، هذا الأخير الذي كان ضحية استغلال لنظامه المعلوماتي من طرف مجرمين معلوماتيين ارتكبوا الكثير من الاختراقات على هذا النظام، مسببين بذلك لخسائر فادحة لا تعد ولا تحصى ولاعتداءات لم يعرف مرتكبوها لحد الآن، ففي عام 2014 تم تسجيل 1290 انتهاكًا لحقوق الإنسان الناتجة عن معالجة الكمبيوتر تم اكتشافها من طرف الشرطة والدرك بفرنسا.

هذه الانتهاكات والجرائم ذات العلاقة بتكنولوجيا المعلومات والاتصالات شملت التجميع والمعالجة والكشف غير المصرح به لبيانات شخصية، وكذا مختلف الاختراقات للمراسلات الإلكترونية 778 حالة[1] والتي تمثل 60.3٪ من إجمالي انتهاكات حقوق الإنسان الناتجة عن معالجة الكمبيوتر.

ولعل أشهر الاعتداءات الشهيرة التي حصلت على المستوى الدولي تتمثل في الآتي؛

أولا: قضية مورس

تعد من بين أولى الهجمات الكبيرة والخطرة في بيئة الشبكات والتي من خلالها تمكن طالب يبلغ من العمر 23 عاما يدعى "روبرت مورس" من إطلاق فيروس عرف باسم (دورة مورس) في الإنترنيت

[1] Marine valzer, La cybercriminilaté et les infractions liées à l'utilisation frauduleuse d'internet élements de mesure et d'analyse pour l'année 2014, rapport annuel de l'observatoire national de la délinquance en cas réponses pénales France, 2015, P8.

والذي أدى إلى إصابة الآلاف من الأجهزة والتي يرتبط معها حوالي 60 ألف نظام عبر الإنترنيت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، بحيث قدرت تكاليف إعادة التصليح لهذه الأنظمة بحوالي مئة مليون دولار بالإضافة لمبالغ أخرى مثلت بدورها خسائر غير مباشرة والناجمة عن تعطل هذه الأنظمة، حكم على مورس بثلاث سنوات حبس وعشرة آلاف دولار غرامة[1].

ثانيا: قضية فيروس ميليسا

لقد تم إطلاق فيروس خطير عبر الإنترنيت والذي عرف بفيروس ميليسا "MELISSA" أين تم القبض والتمكن من اعتقال مبرمج الكمبيوتر في ولاية نيوجرسي الأمريكية في شهر نيسان عام 1999 بعدما انخرطت جهات تطبيق القانون وتنفيذه لعدة دول في تحقيق واسع حول هذا الفيروس ولقد اتهم الجاني باختراق اتصالات عامة والتآمر لسرقة خدمات الكمبيوتر؛ وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة ووصلت العقوبات في الاتهامات الموجهة له إلى السجن 40 عام[2].

ثالثا: قضية تيموثي ألن ليود

صاحب 35 عام مصمم ومبرمج والذي فُصل من عمله، فما كان منه إلاّ أن أطلق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي والتي تعمل لصالح وكالة الفضاء NASA والبحرية الأمريكية[3].

المبحث الثاني: أسباب ومخاطر الجرائم المعلوماتية ومختلف تقسيماتها

إنّ الجرائم المعلوماتية عبارة عن ظاهرة إجرامية والتي لازالت تقرع أجراس الخطر منبهة المجتمع الدولي عن الحجم الهائل للخسائر التي يمكن أن تنجم عنها على جميع المستويات الاقتصادية

[1] عبد الصبور عبد القوى علي مصري، المرجع السابق، ص32.

[2] عبد الصبور عبد القوى علي مصري، المرجع السابق، ص34.

[3] عبد العال الدربيي، محمد صادق إسماعيل، المرجع السابق، ص174.

والاجتماعية والثقافية والأمنية[1]، وإذا كانت المجتمعات العربية لم تتأثر بشكل كبير بمثل هذه المعضلة إلاّ أنّ هناك دولا كثيرة منها أصبحت تهتم بتلك الظاهرة لتقصي أسبابها ومخاطرها ومعرفة تصنيفاتها حتى تنجح في إيجاد طرق لمكافحتها.

المطلب الأول: أسباب ومخاطر الجرائم المعلوماتية

يوجد العديد من الأسباب والدوافع التي تؤدي بالشخص لكي يرتكب إحدى الجرائم المعلوماتية والتي تختلف من شخص لآخر كل حسب غايته وحسب تفكيره وحسب مركزه القانوني والاجتماعي، ولعل جل الأسباب والدوافع التي قد تؤدي بالشخص إلى سلك مسلك الجريمة المعلوماتية تكون من أجل تحقيق مكاسب مالية أو الولع في جمع المعلومات وتعلمها أو حب المغامرة والإثارة، إلى غيرها من الأسباب والمؤثرات الشخصية الأخرى التي تدفع بالمجرم الإلكتروني إلى اقتراف مختلف الاعتداءات داخل المنظومة المعلوماتية، مشكلا مخاطر جمة ومستعصية سواء على الأشخاص أو الحواسيب الآلية.

الفرع الأول: دوافع ارتكاب الجرائم المعلوماتية

عموما مهما كانت أسباب الظاهرة الإجرامية ومهما اختُلف في تفسيرها فلا يمكن أن تنبع إلاّ من إنسان، هذا الأخير ينقلها إلى المجتمع بطريق الاختيار وليس بطريق الجبر أو الآلية، فلابد أن يكون للإرادة نصيب في ظهور الجريمة[2]، خاصة وأنّ هناك جرائم ذات خصوصية جلية كالجرائم المعلوماتية والتي تلعب الإرادة فيها دورا كبيرا في ارتكابها، هذه الإرادة التي يكون وراءها أسبابا ودوافع عديدة تساهم في تقويتها، ولعل من أهم الأسباب والدوافع التي تؤدي إلى ارتكاب الجريمة المعلوماتية هي كالآتي؛

---

[1] عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنيت، د ط، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011، ص64.

[2] زيكو مصطفى، عوامل السلوك الإجرامي، مجلة الحوار الثقافي، المجلد 2، العدد 1، جامعة عبد الحميد ابن باديس، مستغانم الجزائر، فبراير 2013، ص192.

أولا: تحقيق مكاسب مالية

إنّ أبرز دافع وسبب من وراء ارتكاب الشخص أيّا كان للجرائم المعلوماتية هو الحصول على ربح مالي عن طريق المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسب الآلي أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية[1]، فالرغبة في تحقيق الثراء الشخصي تكون غالبا هي الدافع لارتكاب الجريمة المعلوماتية.

فقد تبين من خلال تحقيق قامت به إحدى المجلات المتخصصة بخصوص موضوع الأمن المعلوماتي أن غالبية حالات الغش المعلوماتي المعلن عنها قد بوشرت من أجل اختلاس أموال والتي كانت تهدر في تغطية الخسائر الضخمة لألعاب القمار أو نتيجة إدمان المخدرات[2]، ويعتبر هذا الدافع من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية نظرا لما يحققه لهؤلاء من ثراء فاحش مقارنة بالجرائم التقليدية الأخرى، كما تكون هذه الجرائم عموما والتي تستهدف الربح مدفوعة بالجشع[3].

ثانيا: الدوافع الشخصية والمؤثرات الخارجية

1- الدوافع الشخصية

هناك من الأشخاص الذين يرتكبون الجرائم المعلوماتية فقط من أجل الظهور أي تأكيد قدرتهم الفنية على ارتكاب أحد جرائم الحاسب الآلي نتيجة إحساسهم بالقوة والذات وبقدرتهم على اقتحام النظام، كما قد يكون الدافع من ارتكاب الجريمة الحقد والكراهية الأمر الذي يدفع للانتقام كما كان الحال بالنسبة لشاب تلاعب ببرامج الكمبيوتر الخاصة بالشركة التي يعمل بها[4] أين برمجها على أن تختفي

[1] محمد أمين الرومي، المرجع السابق،ط 2004، ص 24.

[2] سامي علي حامد عياد، المرجع السابق، ص57.

[3] Tamas Gaidosch, la filiere bien structuree de la cybercriminalite, revue finance &developement Washington, USA, juin 2018, p22.

[4] محمد أمين الرومي، المرجع السابق، ط 2004، ص 25.

كل البيانات الخاصة بديون الشركة بعد مضي ستة أشهر، وحدث بالفعل ما كان يصبو إليه أين اختفت بالفعل البيانات الخاصة بديون الشركة نهائيا من على جهاز الحاسب الآلي.

وقد يكون الدافع شخصيا عندما تكون المعلومات ذات قيمة مالية فكثيرا ما تسعى الشركات التجارية إلى الحصول على تلك البرامج والمعلومات بواسطة سرقتها من قبل القائمين على أجهزة الكمبيوتر[1]، كما قد يكون الدافع الشخصي لمرتكب الجرائم المعلوماتية هو دافع مذهبي ومن أمثلة ذلك ما قامت جماعات الألوية الحمراء بتدميرها لمراكز المعلومات الخاصة بها وكان هدفها مهاجمة الهيئات متعددة الجنسيات[2]التي ترمز للإمبريالية وإعادة توزيع الحركة الثورية بتنظيم الحزب الشيوعي المحارب.

2- المؤثرات الخارجية

فالمعلوم أن طبيعة الإنسان كمخلوق ضعيف سيكولوجيا ففي بعض الأحيان يتأثر بالضغوط الخارجية خاصة في نطاق المنافسة وكذا التجسس والأعمال التجارية، فمثلا ضمن نطاق أعمال الغش المعلوماتي فهي قد تمارس تحت تهديد أو ضغط من الغير وهذا ما يدفع بعض الدول وبعض الأشخاص إلى الاتصال بالأفراد الذين يشغلون مراكز حساسة، لكي يعملوا لصالحها أو لصالح مؤسسات أخرى للاطلاع على بعض المعلومات الأساسية عن طريق استعمال الخداع عند اللزوم أو الرشوة أو الإغراء بالإضافة إلى التهديد والإكراه، حتى أنّهم قد يزرعون جواسيس خاصين بهم.

ثالثا: الشغف بالإلكترونيات وحب المغامرة والإثارة

1- الشغف بالإلكترونيات

من الملاحظ أن بعض مرتكبي الأفعال المجرمة في نطاق المعلوماتية ليسوا على قدر كبير من الخطورة لأنّ كل ما يهمهم هو تحقيق انتصارات تقنية دون أن تكون لهم نوايا آثمة، وإن كان هذا لا

---

[1] عمرو عيسى الفقى، الجرائم المعلوماتية جرائم الحاسب الآلي في مصر والدول العربية، د ط، المكتب الجامعي الحديث الإسكندرية مصر، 2006، ص30.

[2] يقصد بالهيئات المتعددة الجنسيات تلك الموجودة في الولايات المتحدة الأمريكية والذين يعتبرون الكمبيوتر سلاح خطير ضد الإرهاب بفضل قدرته على حفظ المعلومات.

يمنع من أن تكون هناك دوافع أخرى آثمة وغير شريفة تؤدي إلى ارتكاب الجرائم المعلوماتية[1] فهناك من يقوم بارتكابها لأجل الحصول على الجديد من المعلومات لاعتبارهم أنّ الحصول على المعلومة يجب ألاّ يكون عليه قيد؛ ويفضل هؤلاء أن يكونوا مجهولين للتواجد باستمرار داخل الأنظمة لأطول فترة ممكنة فيكرسون كل جهدهم في تعلم كيفية اختراق المواقع الممنوعة، حتى أنّهم يتعاونون فيما بينهم في شكل مجموعات يكون الهدف منها تبادل المعلومات وتقاسم البرامج والأخبار.

2- حب المغامرة والإثارة

لقد جاء على لسان أحد القراصنة المعلوماتيين أنّ القرصنة كانت النداء الأخير الذي يبعثه دماغه، فقد كان يعود للمنزل بعد يوم ممل في المدرسة فيشغل جهاز الحاسب الآلي ويصبح عضوا في نخبة قراصنة الأنظمة أين كان يتبادل المعلومات مع الآخرين في جميع أنحاء العالم، وكان يتنقل من كمبيوتر إلى آخر محاولا العثور على هدفه وكان كل خطوة يخطوها إلاّ وتقربه من حافة التكنولوجيا واكتشاف ما وراءها واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض عليه أن يتواجد بها[2] ولقد جاء على لسانه أيضا؛ أنّ كل خطوة من هذه الخطوات كان بإمكانها إسقاطه بيد السلطات.

الفرع الثاني: المخاطر المتعلقة بالجرائم المعلوماتية

تختلف وتتعدد المخاطر المتعلقة بالجرائم المعلوماتية بحسب اختلاف المحل الذي وقعت عليه الجريمة، فمنها ما يقع على الأشخاص ومنها ما يقع على الحواسب الآلية كالقرصنة والتعرض لفيروسات خطيرة على مختلف هذه الأخيرة، فتقنية المعلومات الجديدة مكنت من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي حفظت في ملفات مؤتمتة أين يمكن نقلها عبر البلد في ثواني وبتكاليف منخفضة نسبيا، هذا ما يكشف صراحة أهمية المحل الذي يقع عليه التهديد والخطر.

[1] سامي علي حامد عياد، المرجع السابق، ص57.

[2] محمد أمين الرومي، المرجع السابق، ط 2003، ص 26.

أولا: مخاطر الجرائم المعلوماتية الواقعة على الأشخاص

إنّ الحديث عن المخاطر التي قد يتعرض لها الأشخاص من جراء الجرائم المعلوماتية يقودنا إلى الحديث على محلين الأول يتعلق بالأفراد في حياته الشخصية والثاني يتعلق بمختلف المؤسسات والدوائر الحكومية وكذلك الشركات الخاصة.

1- المخاطر التي يتعرض لها الأفراد من جراء الجرائم المعلوماتية

إنّ استخدام الحواسب الآلية وشبكة الانترنيت في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الشخصية للأفراد خلف آثارا إيجابية عريضة خاصة في مجال تنظيم الدولة لشؤون الأفراد، الأمر الذي أنشأ ما يعرف ببنك المعلومات[1]، وخلف أيضا وبالتوازي حس الشعور بمخاطر تقنية المعلوماتية وتهديدها للحياة الشخصية والخاصة، هذا الشعور زاد وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية للأفراد واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة[2] خاصة مع الاستعمال الواسع لشبكة الإنترنيت.

هذه الأخيرة خلقت سلسلة من التحديات الجديدة على الحياة الخاصة الشخصية، فهي تعد مصدرا غنيا للمعلومات كما أنّها تزيد من كمية البيانات المجمعة والمعالجة والتي يدخل في نطاقها المعلومات الشخصية للأفراد من عاداتهم وهواياتهم وآرائهم واتجاهاتهم، فهذه المعلومات الأخيرة أمست متوفرة في ظل هذه الشبكة العالمية والتي أصبحت تستخدم فيها العديد من الوسائل التقنية كرسائل الكوكيز[3]، وباتت تتدفق عبر الحدود دون أي اعتبار للجغرافيا والسيادة.

الأمر الذي يثير ويرتب مخاطر من جراء إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية الفنية والقانونية للبيانات الشخصية، كما أنّ هناك اعتداءات أخرى قد يتعرض

---

[1] يقصد ببنك المعلومات وفقا لمعجم المعاني: مركز للمعلومات يقوم بجمعها وتخزينها واسترجاعها لخدمة الذين يلجئون إليه.

[2] بولين أنطونيوس أيوب، المرجع السابق، ص21.

[3] رسائل الكوكيز" cookies" عبارة عن رسائل إلكترونية بمجرد انتقالها إلى نظام المستخدم ودخولها للموقع تتمكن من تسجيل بيانات تخص المستخدم والتي قد لا يرغب في الكشف عنها.

لها الأفراد وتطبق على المكونات غير المادية للكمبيوتر والتي قد تتطلب مجرد سلوك مادي في شكل الاطلاع البصري للمعلومات التي قد تظهر على شاشة الحاسب الآلي أو في شكل التصنت عليها إذا ما تجسدت في صورة سمعية.

2- المخاطر التي يتعرض لها الشخص الاعتباري من جراء الجرائم المعلوماتية

لا شك في أن الشخص الطبيعي يتمتع بالحق في الحياة الخاصة دون خلاف لأنّه من الحقوق اللصيقة بالشخصية والتي لا تثبت إلاّ للإنسان، المشكل يبقى فقط في الشخص الاعتباري هذا الأخير الذي تعددت حوله الآراء حول ما إذا كان يتمتع بهذا الحق أو لا، فالمعارضين لفكرة التمتع بهذا الحق يستندون لمجموعة من الأسباب من أهمها أن الحق في الخصوصية من الحقوق الدستورية اللصيقة بالشخصية الإنسانية[1]، أما المؤيدون لفكرة تمتع الشخص المعنوي بالحق في الخصوصية شأنه شأن الشخص الطبيعي استندوا إلى أنّ الخصوصية يمكن أن تشمل سرية الأعمال.

الأمر الذي يمكن معه القول بأن الحماية للحق في حرمة الحياة الخاصة في إطار المعلوماتية تمتد لتشمل سرية أعمال الشخص المعنوي، لأجل ذلك أقرت لجنة خبراء حقوق الإنسان للمجلس الأوروبي هذا، وقالت بأنّ الأشخاص القانونية والهيئات والجماعات تتمتع بمثل هذا الحق إذا ما كان الهدف من الاعتداء على الشخص الاعتباري حصول إضراره أو تحقيق منفعة ما، وعليه يمكن القول بأن الشخص الاعتباري مهدد بنفس المخاطر التي قد يتعرض لها الأفراد والتي تم توضيحها في العنصر السابق خاصة إذا ما تعلق الأمر بالبيانات والمعلومات الشاملة لسرية الأعمال.

ثانيا: مخاطر الجرائم المعلوماتية الواقعة على الحواسب الآلية

في عصر المعلوماتية أصبح هناك استغناء واضح عن تعلم الحساب والتذكر وأصبحت معه قدرة الإنسان على التفكير تنقص، فاللغة تقلصت والكتابة تمارس بالتلغراف والرموز، بالإضافة إلى تدني الروح التحليلية والنقد والقدرة على اتخاذ القرار، فأصبح الإنسان عبدا للماكينة وللعقل الإلكتروني

[1] علي أحمد عبد الزعبي، المرجع السابق، ص327.

المعرضين لعدة مخاطر والتي بدورها تهدد مصالح الأشخاص، وهذه المخاطر التي قد تأتي إمّا بواسطة شبكة الانترنيت وإمّا بدونها.

1- المخاطر الواقعة على الحواسب الآلية بطريقة عادية (بدون شبكة الإنترنيت)

والتي هي عبارة عن مخاطر تهدد الكمبيوتر والناجمة من وضع برامج مغلوطة كأن يقوم موظف مصرف بإجراء تحويل الأموال إلى الحساب المطلوب وتحويل تلك التي تقل مثلا عن الواحد الأورو (أي كسر الأورو) إلى حسابه الخاص، الأمر الذي يؤمن له مبالغ مالية طائلة كما حصل في سويسرا من قبل محتال لم ينكشف أمره إلاّ بمضي سنوات عدة[1]، وقد يكون الخطر ناجم عن أخطاء مادية والتي تلحق بالمعلومات والتي لا يمكن تفاديها، كأن يقوم أحد العمال في شركة ما من وضع رقم 1000 بدل رقم 100.

وبالتالي لا شيء يمكن أن يوقظ حفيظة الكمبيوتر للتصحيح وتتم جميع العمليات التالية بالاستناد إلى الرقم الخاطئ، هذا وهناك مخاطر أخرى قد تتجلى في شكل سرقة معلومات من قبل موظفين أو سرقة البرامج وإساءة الاستعمال، فعدم كتمان الموظفين وانتمائهم قد يسمح بتسرب المعلومات وإلحاق الضرر، فهذا ما سمح لمحتال أمريكي بعد حصوله على كلمة السر بإعطاء أمر لتسلم بضاعة إلى مشتري اعتاد أن يقوم بعمليات بواسطة الكمبيوتر بعدما استعمل اسم إحدى الشركات والاسم السري لمؤسسات أخرى.

2- المخاطر الواقعة على الحواسب الآلية بواسطة شبكة الانترنيت

وهي المخاطر التي تكمن في أي شيء من شأنه الإضرار بالحاسب الآلي من خلال محو وهدر للبيانات والمعلومات التي يتم معالجتها آليا وهو ما يسمى بالإتلاف، لأنّ جوهر عملية الإتلاف تعمل

[1] نعيم مغبغب، مخاطر المعلوماتية والانترنيت المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، ط ثانية، منشورات الحبلى الحقوقية، بيروت، لبنان، 2008، ص173.

على إفقاد منفعة المال وصلاحيته في الاستعمال وغالبا ما يتم ذلك بواسطة الفيروسات أو الديدان أو الإغراق بالرسائل الذي يؤدي بالجهاز إلى التوقف عن العمل؛

أ- الفيروسات

وهي مجموعة من التعليمات التي تتكاثر بصورة سريعة جدا وتصيب النظام المعلوماتي بالشلل وسميت بهذا الاسم نظرا للآلية العملية الشبيه بالفيروسات التي تصيب الكائنات الحية، فهذه الفيروسات تشبه الفيروس العضوي في جوانب عدة وتختلف معه في جوانب أخرى[1]، فالتشابه يكمن في ضررها للمصاب بها فقط بحيث لا تظهر الأعراض إلاّ بعد فترة حضانة، وبعد ذلك التكاثر بسرعة في جل الأعضاء الداخلية، أمّا الاختلاف فيتمثل في قدرة الفيروس على الوصول إلى أبعد نقطة ممكنة من الأرض عن طريق شبكة الحاسبات الآلية بشرط التواصل بينها وفتح قنوات الاتصال.

هذا ونظرا لاعتماد مختلف المؤسسات حاليا في عملها على نظام معلومات ضعيف الحماية فإنّه بذلك عرضة لهجوم الفيروسات والمتسللين مما قد يتسبب في خسائر كبيرة لهذه المؤسسات وعلى سمعتها وتسريب معلوماتها[2]، فهذه الفيروسات تساعد في ارتكاب الجرائم المعلوماتية والتي يمكن العثور عليها بشكل شائع في مجتمعات المخترقين، وغالبًا ما تكون متاحة مجانًا أو يتم تداولها داخل الأسواق السوداء.

هذا وتتمتع الفيروسات بمجموعة من الخصائص تجعلها في غاية الخطورة كالقدرة على الاختفاء حتى أنّ بعضها تقوم بإخفاء آثارها الدالة عليها فتضل البرامج المحتوية على هذه الفيروسات تعمل بكفاءة دون أخطاء لمدة طويلة وتنتشر بسرعة كبيرة تفوق سرعة الفيروس البيولوجي؛ كما لها القدرة

[1] محمد أمين الرومي، المرجع السابق، ط 2004، ص29.

[2] Tosal Bhalodia, Chandani Kathad and Keyur Zala, Comparative Study of Security Risk in Social Networking and Awareness to Individual, From a book of Bokhari Namrata Agrawal, Dharmendra Saini, Cyber Security Proceedings of CSI 2015 Springer Nature Singapore Pte Ltd, 2018, p216.

على الاختراق بعدة طرق كطريقة حصان طروادة[1] وكذلك القدرة على التدمير بمجرد الدخول إلى ذاكرة الحاسوب، وهناك عدت تصنيفات من الفيروسات[2]بحسب الضرر الذي تحدثه نخص بالذكر منها تلك التي تحدثه من ضرر على أجهزة الحواسب الآلية وهي كالآتي؛

– فيروسات تعمل على فقد ملفات من ذاكرة الحاسوب وذلك من خلال تكاثر الفيروس في ذاكرة الحاسوب، الأمر الذي يؤدي إلى زيادة هذا الأخير على حساب الملفات المخزنة مسببا مسحها وتدميرها وتدمير الذاكرة معها حتى أنّ صاحب الملفات لا يستطيع إرجاعها ولا استخدام البرامج.

– فيروسات تعمل على تحطيم الفهرس الرئيسي عن طريق مهاجمته بواسطة طرق متعددة كتغيير حرف واحد (byte) من الفهرس، والذي يؤدي بدوره إلى عدم الوصول لأي ملف على القرص بالرغم من وجوده فعليا.

– فيروسات تعمل على تغيير بيانات في ملفات أو برامج توقع المستخدم في مشاكل عديدة من خلال النتائج الخاطئة التي قدمتها المعالجة.

ب– برامج الدودة "Worm software"

الديدان[3] برامج تنتقل من شبكة إلى أخرى عبر الوصلات الرابطة بينها وهي أثناء عملية انتقالها تتكاثر كالبكتيريا عن طريق إنتاج نسخ منها، هدفها شغل أكبر مجال ممكن من سعة الشبكة لأجل تقليل أو خفض كفاءتها، كما يمكن أن تتعدى أهدافها لتبدأ في التكاثر والانتشار مخربة بذلك مختلف الملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال، هذا وتكمن خطورتها في استقلاليتها وعدم اعتمادها على أي برامج أخرى مما يعطيها حرية كاملة في الانتشار السريع، حتى أن بعضها خطير جدا

[1] حصان طروادة برنامج خطير يستخدم في عمليات اختراق أجهزة الحاسبات الآلي، يتمتع بعدة مميزات تجعل منه الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه، لذلك اكتسب هذا البرنامج شهرة كبيرة في مجال اختراق الحاسبات الآلية.

[2] مصطفى يوسف كافي، جرائم الفساد، غسيل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، د ط، الأردن 2014، ص 176.

[3] الديدان حسب تعريف الباحث محمد عبد الله أبو بكر عبارة عن برامج تستغل أي فجوات في نظم تشغيل الحاسب الآلي لتنتقل من حاسب إلى آخر مغطية شبكة بأكملها لتحدث في النهاية آثارها التخريبية.

كتلك الدودة التي ظهرت في أكتوبر عام 2002 والتي اشتهرت ب TANATOS أين انتشرت سريعا مخلفة وراءها آثارا تدميرية هائلة[1].

ومن بين أمثلة الاعتداء على نظم الحواسيب الآلية، برنامج دودة أعده طالب بجامعة Clausthal zellerfeld بألمانيا الغربية سابقا في شكل رسالة تهنئة وتحية أرسلها من خلال الحاسبات الآلية بمناسبة عيد الميلاد في ديسمبر 1987، ولقد صمم هذا البرنامج ليقرأ عناوين البريد الإلكتروني المخزنة في ذاكرة كل حاسب يصل إليه[2]، ليرسل بعد ذلك تهنئة إلى أصحاب تلك العناوين ثم ينتج نسخة من نفسه ويرسلها إلى جميع الحاسبات المتصلة بالحاسب المضيف.

وهكذا حتى أنّه وصل إلى شبكة VNET التابعة لشركة IBM والتي تربط بين حاسبات في 45 دولة آنذاك ودخل إليها وبدأ في التكاثر التسلسلي إلى أن غطى في غضون ساعتين أكثر من نصف مليون حاسب، الأمر الذي أدى إلى انهيار قدرة الشبكة على تحمل تدفق الخدمات المرسلة وتعطلها لمدة يومين تقريبا وتم خلالها استئصال البرنامج من النظام.

ج- الإغراق بالرسائل

يعتبر من الطرق الغريبة التي لم يتوانى المتسللين في إبراز وإثبات تفوقهم من خلالها والتي تعمل على إلحاق أضرار بأجهزة الحاسبات الآلية، وتكون ببعث كم هائل من الرسائل عبر البريد الإلكتروني لأجهزة الحاسبات الآلية المراد العمل على تعطيلها وتوقيفها عن الشغل، فهذه الرسائل قد تكون محملة بملفات كبيرة الحجم وذلك لهدف التأثير على الجهاز من خلال استغلال صغر المساحة المحددة للبريد الإلكتروني[3] غالبا، فتلك الرسائل تصل لجهاز الحاسب الآلي مرة واحدة في وقت واحد تقريبا فتعمل

---

[1] منير محمد الجنبهي، ممدوح محمد الجنبهي، المرجع السابق، ص63.

[2] محمد عبد الله أبو بكر، المرجع السابق، ص158.

[3] ممدوح محمد الجنبهي، منير محمد الجنبهي، أمن المعلومات الإلكترونية، د ط، دار الفكر الجامعي، الإسكندرية، مصر، 2005 ص46.

على إيقافه عن العمل في حينها نظرا لما تسببه من ملء منافذ الاتصال وكذلك ملء قوائم الانتظار وبالتالي انقطاع الخدمة التي تؤديها تلك الأجهزة.

ولهذا يجب شراء برنامج أمان جيدة للتعامل مع جميع أنواع الفيروسات والبرامج الضارة والتأكد من تحديثها متى توفر ذلك، لكنّ كيف تتعرف على البرنامج الجيدة لمكافحة الفيروسات والبرامج الضارة؟ للوهلة الأولى قد يبدو هذا السؤال بسيطا جدا، إلاّ أنّه ليس من السهل الإجابة عليه ذلك أنّ هناك متطلبات وظيفية لكل برنامج وكل مصنع له طرقه الخاصة في التعامل مع هؤلاء المتطلبات فقد يركز برنامجان متشابهان على جوانب أمنية مختلفة تمامًا وحتى بين الخبراء لا يوجد قناعة مطلقة بشأن من هم أفضل البرامج الأمنية[1].

لكن مع ذلك يمكنك الحصول على الأقل على فكرة جيدة عن الشركات المصنعة ذات الثقة والسمعة العالية من خلال معرفة البائعين الأعضاء في اختبار مكافحة البرامج الضارة، من منظمة المعايير (AMTSO) والتحقق من الاختبارات التي أجريت بواسطة مواقع موثوقة الاختبار مثل Virus Bulletin و AV-Comparatives و AV-TEST.

المطلب الثاني: تقسيمات الجرائم المعلوماتية

لقد تعددت الجهات التي عنت بتقسيم الجرائم المعلوماتية، منها ما هو دولي ومنها ما هو فقهي كل حسب نظرته إليها ووجهة رأيه فيها، لهذا ظهرت جهود دولية كثيرة لأجل تقسيمها إلى جانب تقسيم مختلف التشريعات وتقسيم الكثير من الفقهاء لهذه الأنواع من الجرائم، ومن بين نماذج التقسيمات الفقهية والتشريعية للجرائم المعلوماتية، النموذج الفقهي الذي جاء به الفريق البحثي الأكاديمي الأمريكي والنموذج التشريعي الذي جاء به المجلس الأوروبي للجرائم المعلوماتية.

[1] Eddy Willems, cyberdanger: undestanding and guarding against cybercrime company Springer Nature Switzerland AG, 2013, P124.

الفرع الأول: تقسيم الفريق البحثي الأكاديمي الأمريكي للجرائم المعلوماتية

يعد تقسيم الفريق البحثي الأكاديمي الأمريكي للجرائم المعلوماتية (M.S.C.C.C)[1] من بين التقسيمات الشائعة على مستوى الدراسات والأبحاث الأمريكية مع وجود فروق بينها من حيث مضمون التقسيم ومدى الانضباط، هذا ويعتبر هذا التقسيم المعيار المعتمد لتقسيم الجرائم المعلوماتية في مشروعات القوانين النموذجية الموضوعة من قبل جهات بحثية بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة الأمريكية المتصلة بهذا الموضوع، هذا ولقد جاء التقسيم الذي وضعه هذا الفريق البحثي على النحو التالي؛

أولا: طائفة الجرائم المعلوماتية التي تستهدف الأشخاص

تضم الطائفة فئتين رئيسيتين هما الجرائم الجنسية التي تستهدف الأشخاص والجرائم غير الجنسية التي تستهدف الأشخاص.

1- الجرائم المعلوماتية الجنسية التي تستهدف الأشخاص

تشمل حض وتحريض وإغواء أو محاولة إغواء القصر على ارتكاب أنشطة جنسية غير مشروعة وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية وتلقي أو نشر المعلومات عن القصر عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة والتحرش الجنسي بالقصر عبر الكمبيوتر والوسائل التقنية، بالإضافة إلى نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنيت بوجه عام وللقصر تحديدا وكذلك نشر الفحش والمساس بالحياء عبر الإنترنيت أو تصوير أو إظهار القصر ضمن أنشطة جنسية، واستخدام الإنترنيت لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم، والحصول على الصور بطريقة غير مشروعة لاستغلالها في أنشطة جنسية[2].

---

[1] M.S.C.C.C :Model State Computer Crimes Code.

[2] أيمن عبد الله فكري، المرجع السابق، ص154.

2- الجرائم المعلوماتية غير الجنسية التي تستهدف الأشخاص

تشمل القتل بالكمبيوتر وجرائم الإهمال المرتبط بالكمبيوتر والتحريض على الانتحار والتحريض عن قصد للقتل عبر الإنترنيت وكذلك التحرش والمضايقة والتهديد عبر وسائل الاتصال الحاسوبي والتعمد أو المشاركة في إلحاق الضرر المعنوي أو الملاحقة عبر الوسائل التقنية، كذلك اختلاس النظر أو الاطلاع على البيانات الشخصية وقنابل البريد الإلكتروني وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب فيها، إضافة إلى بث المعلومات المضللة أو الزائفة والدخول غير المصرح به لمعطيات الحاسب الآلي.

ثانيا: طائفة جرائم الأموال المتضمنة أنشطة الاختراق والإتلاف

والمتمثلة في الدخول غير المصرح به مع نظام الكمبيوتر أو الشبكة، تخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر والتعدي على الكمبيوتر واغتصاب الملكية وإنشاء البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، وكذلك استخدام اسم الغير أو اسم العلامة التجارية دون ترخيص بالإضافة إلى إدخال معطيات خاطئة أو مزورة إلى نظام الكمبيوتر، والتعديلات غير المصرح بها لأجهزة ومعدات الكمبيوتر والإتلاف غير المصرح به لنظم الكمبيوتر وأنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات وأنشطة الاعتداء على الخصوصية، وإفشاء كلمة سر الغير والحيازة غير المشروعة للمعلومات وإساءة استخدام المعلومات ونقل معلومات خاطئة.

ثالثا: جرائم الاحتيال والسرقة

تشمل جرائم الاحتيال والتلاعب بالمعطيات والنظم واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص والاختلاس عبر وبواسطة الكمبيوتر وكذلك سرقة معلومات الكمبيوتر وقرصنة البرامج وسرقة خدمات الكمبيوتر وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.

رابعا: جرائم التزوير

تشمل تزوير البريد الإلكتروني أو تزوير الوثائق والسجلات[1].

خامسا: جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب

تشمل تملك وإدارة مشروع مقامرة على الإنترنيت وتسهيل إدارة مشاريع القمار على الإنترنيت وتشجيع مشروع مقامرة عبر الإنترنيت واستخدام الإنترنيت لترويج الكحول ومواد الإدمان للقصر.

سادسا: جرائم الكمبيوتر ضد الحكومة

وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية والإخبار الخاطئ عن جرائم الكمبيوتر والعبث بالأدلة القضائية، وكذلك تهديد السلامة العامة وأيضا بث البيانات من مصادر مجهولة وتشمل الإرهاب الإلكتروني والأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات.

الفرع الثاني: تقسيم المجلس الأوروبي للجرائم المعلوماتية

لقد حرص المجلس الأوروبي على التصدي لمختلق الجرائم المعلوماتية وبذل الكثير من الجهود في سبيل ذلك منذ مطلع السبعينات من القرن الماضي، وكانت بداية العمل مهتمة بحماية البيانات الشخصية حتى لا تؤدي الرغبة في زيادة فعالية مختلف الحاسبات الآلية لخدمة المجتمع إلى تهديد حق الأفراد في الخصوصية، إلاّ أنّ أولى الاهتمامات بالجرائم المعلوماتية من قبل المجلس الأوروبي كانت بانعقاد المؤتمر الثاني عشر(12) لرؤساء معاهد العلوم الجنائية عام 1976، أين أسفر عن تشكيل لجنة لدراسة الجرائم الاقتصادية بصفة عامة[2].

هذه اللجنة أصدرت توصية رقم 81 (12) أقرتها لجنة الوزراء في المجلس الأوروبي في 25 يونيو 1981 عرفت من خلالها الجرائم الاقتصادية بصفة عامة، وضمنتها بعض الجرائم المعلوماتية كسرقة

[1] أيمن عبد الله فكري، المرجع السابق، ص156.

[2] محمد عبد الله أبوبكر، المرجع السابق، ص123.

المعلومات والتجسس المعلوماتي والتلاعب بالبيانات المعالجة إلكترونيا، وذهبت اللجنة إلى أنّ هذه الجرائم لتحققها لابد من توفر الشروط الآتية؛

– أن يتوافر لدى الفاعل معرفة خاصة بتكنولوجيا الحاسبات الآلية.

– أن يكون هناك صلة وثيقة تربط بين الفاعل وبين محل السلوك الإجرامي المتمثل في البيانات والمعلومات المعالجة إلكترونيا.

هذا ولقد أثير بعد ذلك مرة أخرى موضوع الجرائم المعلوماتية من قبل اللجنة الأوروبية لمشاكل الجريمة ضمن برنامج عملها لعامي 1985 -1986 أين قدمت للجنة الوزراء في الاتحاد الأوروبي تقريرا في صورة توصية تضمنت بعض الإرشادات الموجهة للمشرعين داخل الدول لغرض الوصول لسياسة جنائية موحدة في مواجهة جرائم الحاسب الآلي؛ ولقد تمثلت هذه الإرشادات في تقسيم الجرائم المعلوماتية واقتراح نصوص تشريعية في شأن كل منها، كما فرقت اللجنة في تقريرها بين طائفتين رئيسيتين للجرائم المعلوماتية.

أولا: تقسيم اللجنة الأوروبية للجرائم المعلوماتية

إنّ تقسيم اللجنة الأوروبية للجرائم المعلوماتية جاء وفق طائفتين، الأولى أساسية والأخرى اختيارية والتي جاءت كما يلي؛

1– الطائفة الأساسية للجرائم المعلوماتية

وتشتمل على ثمانية جرائم اتُفق على خطورتها وعلى انتشارها وهذه الجرائم هي: الاحتيال المعلوماتي، التزوير المعلوماتي، إتلاف المعلومات والبيانات وإتلاف برامج الحاسب الآلي، إعاقة نظام الحاسب الآلي عن أداء وظيفته الدخول غير المصرح به إلى نظام الحاسب الآلي، الاعتراض غير المصرح به لنظام الحاسب الآلي، النسخ غير المشروع لبرامج الحاسب الآلي وكذا النسخ غير المشروع للتصميمات الخاصة برقائق الحاسبات الآلية.

2- الطائفة الاختيارية للجرائم المعلوماتية

وتشتمل على العديد من الأفعال غير المشروعة بدأت في الظهور حديثا وتنذر بزيادة معدلها مستقبلا، بحيث لم تلقى إجماعا كالطائفة الأولى الأساسية بحيث ترك تجريمها على حساب تقدير كل دولة على حدة وتتمثل هذه الأفعال في: التعديل في البيانات المخزونة داخل نظام أو برامج الحاسب الآلي في الحالات التي لا يؤدي فيها هذا التعديل إلى إتلاف هذه البيانات أو البرامج، التجسس المعلوماتي، الاستعمال غير المصرح به لنظام الحاسب الآلي، الاستعمال غير المصرح به لبرامج الحاسب الآلي التي تشملها الحماية القانونية[1].

إنّ هذا التقسيم كذلك لم يلق إجماعا وتوافقا في قبوله، لأنّ الأفعال التي أدرجتها اللجنة ضمن الطائفة الاختيارية هي كذلك أفعال جديرة بالتجريم كالطائفة الأساسية، فكلا الطائفتان إلاّ وفيها اعتداء على حق أو مصلحة جديرة بالحماية الجنائية، وعلى إثر ذلك جاءت اتفاقية بودابست[2] المتعلقة بالإجرام المعلوماتي لتتدارك ذلك من خلال الاهتمام بكل هذه الأفعال المجرمة السالفة الذكر بعد أن آمن الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية والعولمة المستمرة للشبكات المعلوماتية[3].

ثانيا: تقسيم اتفاقية بودابيست للجرائم المعلوماتية

تعد اتفاقية بودابيست أهم اتفاقية دولية تتعلق بالأحكام الموضوعية والإجرائية للجرائم المعلوماتية هذه الاتفاقية وإن جاء توقيعها في نطاق قاري أوروبي إلاّ أن هدفها الأساسي كان تحسين وإصلاح وسائل مكافحة وقمع الإجرام المعلوماتي[4]، هذا ولقد قسمت هذه الاتفاقية الجرائم المعلوماتية إلى أربع

---

[1] محمد عبد الله أبوبكر، المرجع السابق، ص125.

[2] اتفاقية بودابيست 2001 التي تم التوقيع عليها في 23 نوفمبر 2001 والمتعلقة بالإجرام الكوني بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية (Convention Sur La cyber Criminalité, budapest).

[3] محمد عبد الله أبوبكر، المرجع السابق، ص126.

[4] نزار العنبكي، نحو قانون جنائي دولي لجرائم المعلوماتية والانترنيت ذات الصفة الدولية، مجلة العلوم القانونية والسياسية، المجلد 5، العدد 01، الجمعية العلمية للبحوث والدراسات الاستراتيجية، كلية الحقوق، أكاديمية البورك للعلوم، الدنمارك، 2013 ص55.

فئات رئيسية تشمل على تسع جرائم مختلفة حددتها تسع (09) مواد من هذه الاتفاقية[1] هذه الجرائم كما هي موضحة في الآتي؛

1- الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية

وتمثلت في الولوج غير القانوني الاعتراض غير القانوني، الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام، الاستخدام السيء لأجهزة الحاسب الآلي.

2- الجرائم المتصلة بالحاسب الآلي

وتتمثل هذه الجرائم في كل من التزوير المعلوماتي والغش المعلوماتي.

3- الجرائم المتصلة بالمحتوى

وهي الجرائم المتصلة في أغلبها بالمواد الإباحية للطفولة.

4- الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة

مختلف الأفعال التي تنتهك الملكية الفكرية[2] من مصنفات فنية وأدبية متعلقة بالحاسب الآلي وبرامجه.

المطلب الثالث: صور الجرائم المعلوماتية في التشريع الجزائري

جاءت الجرائم المعلوماتية في التشريع الجزائري بطريقة لا تتطابق مع تعريفها بدليل عدم صدور كل صورها وحتى أن هذه الصور جاءت في أغلبها ضمن نصوص وقوانين خاصة، الأمر الذي يفسر تناثرها في بحر التشريع الجزائري، وهذه الجرائم في مجملها عبارة عن اعتداءات قد تقع على النظام المعلوماتي أو تكون بواسطته وتتمثل في الآتي؛

[1] المواد من 2 إلى10 من اتفاقية بودابيست 2001 للجريمة المعلوماتية.

[2] جلال محمد الزغبي، أسامة أحمد المناعسة، المرجع السابق، ص94.

الفرع الأول: الجرائم المعلوماتية التي نُص عليها في قانون العقوبات

وهي مختلف الاعتداءات المعلوماتية التي جاء بذكرها المشرع الجزائري ونظمها من خلال ق ع وتتمثل مجملها في الآتي؛

أولا: جرائم المساس بأنظمة المعالجة الآلية للمعطيات

تمثل كل شروع أو اعتداء على نظام المعالجة الآلية للمعطيات من دخول وبقاء وإدخال للمعطيات بطريق غير المشروع أو تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة، وكل حيازة أو إفشاء أو نشر أو استعمال[1] لأي غرض كان المعطيات المتحصل عليها من إحدى هذه الجرائم أو إضرار بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، كل هذه الجرائم نص عليها المشرع الجزائري من خلال المواد من 394 مكرر إلى 394 مكرر7 من ق ع[2] الجزائري.

ثانيا: جرائم المساس بحرمة الحياة الخاصة

تتمثل في جرائم الالتقاط وكذا التسجيل والنقل لأحاديث أو صور خاصة وسرية في مكان خاص بأية تقنية كانت وبغير إذن صاحبها أو رضاه، جريمة الاحتفاظ أو الوضع في متناول الجمهور أو إفشاء أو النشر عن طريق الصحافة الوثائق أو الصور المتحصل عليها من الأفعال السالفة الذكر الشروع في ارتكاب إحدى هذه الجرائم، الشخص المعنوي باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام يساءل جزائيا في حالة ارتكابه لإحدى الجرائم السالفة الذكر، هذه الجرائم نظمتها المواد من 303 مكرر إلى 303 مكرر3 من ق ع[3] الجزائري.

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص (الجرائم ضد الأشخاص، الجرائم ضد الأموال، بعض الجرائم الخاصة)، ط السابعة عشر، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص494.

[2] قانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966 المتضمن ق ع الجزائري ج ر رقم 71، المؤرخة في 10 نوفمبر 2004.

[3] قانون رقم 06 – 23 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966 المتضمن ق ع الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

ثالثا:جرائم القذف أو السب أو الإهانة أو الإساءة أو الاستهزاء بأي وسيلة تقنية

تتمثل في جريمة الإساءة إلى رسول الله صلى الله عليه وسلم أو بقية الأنبياء بأي وسيلة كانت جريمة الاستهزاء بالمعلوم من الدين بالضرورة أو بأية شعيرة من شعائر الإسلام بأي وسيلة كانت[1] جريمة الإهانة أو سب أو قذف رئيس الجمهورية بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى جريمة الإهانة أو سب أو قذف ضد البرلمان أو ضد الجيش الوطني الشعبي أو أية هيأة نظامية أو عمومية أخرى بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى، هذه الجرائم نظمتها نصوص المواد 144 مكرر 144مكرر2، 146 من ق ع[2] الجزائري.

رابعا: الجرائم الجنسية المرتكبة ضد القصر بأية وسيلة

تتمثل في جريمة تصوير قاصر لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، جريمة تصوير الأعضاء الجنسية لقاصر ولأغراض جنسية أساسا، جريمة إنتاج أو توزيـــع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر، هذه الجرائم نظمتها المادة 333 مكرر1 من ق ع[3] الجزائري.

خامسا: الجرائم المرتكبة بالوسائل الإلكترونية والموجهة ضد أمن الدولة

تتمثل في جرائم التخابر وكذا إتلاف وإفساد أو إدخال عيوب على المنظومات المعلوماتية بقصد الإضرار بالدفاع الوطني أو التسبب في وقوع حادث، جريمة تسليم معلومات أو تصميمات يجب أن تحفظ بستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها

---

[1] قانون رقم 01 – 09، المؤرخ في 26 يونيو 2001، يتمم الأمر رقم 66 – 156، المؤرخ في 8 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 34، المؤرخة في 26 يونيو 2001.

[2] قانون رقم 11 – 14، المؤرخ في 2 غشت 2011، يعدل الأمر رقم 66 – 156، المؤرخ في 8 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 44، المؤرخة في 10 غشت 2011.

[3] قانون رقم 14 – 01، المؤرخ في 4 فبراير 2014، يعدل ويتمم الأمر رقم 66 – 156، المؤرخ في 8 يونيو 1966 المتضمن ق ع الجزائري، ج ر رقم 7، المؤرخة في 16 فبراير 2014.

وعلى كل فهي عبارة عن جرائم ترتكب بوسائل إلكترونية بغرض الإضرار بالدفاع أو الاقتصاد الوطني هذه الجرائم نص عليها من خلال المواد 61، 63، 64، 67 من ق ع الجزائري.

الفرع الثاني: الجرائم المعلوماتية التي نص عليها المشرع ضمن قوانين خاصة

وهي عبارة عن جرائم جاءت نتيجة تغير طبيعة المجتمع الجزائري من شتى النواحي الاجتماعية والثقافية والاقتصادية، هذه الجرائم جاءت ضمن قوانين خاصة والتي تمس في أغلبها نشاطات المجتمع ذات الطابع الاقتصادي وهي كالآتي؛

أولا: بالقانون المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية

وهي عبارة عن جرائم تنتهك بها سرية المراسلات بأي طريقة كانت سواء الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية واللاسلكية من قبل كل شخص وعامل مرخص له بتقديم خدمة مواصلات سلكية ولاسلكية، أو من خلال إنشاء أو استغلال أو إشهار شبكة عمومية أو شبكة مستقلة للمواصلات السلكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة، هذه الجرائم نصت عليها المواد 12، 131، 132، 133، 135 من القانون[1] المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

ثانيا: في القانون المتعلق بحقوق المؤلف والحقوق المجاورة

والمتمثلة في الاعتداء بطريق التقليد، الاستنساخ، الاستيراد، التصدير، البيع، التأجير، المساس بسلامة المصنفات[2]أو أداء الفنانين عن طريق أي منظومة معلوماتية، هذه الجرائم نصت عليها المواد 151 و152 من القانون[3]المتعلق بحقوق المؤلف والحقوق المجاورة.

---

[1] قانون رقم 2000 – 03 المؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية ج ر رقم 48، المؤرخة في 6 غشت 2000.

[2] يقصد بالمصنف كل شيء له علاقة بمنظومة معلوماتية أو يجرى بواسطة منظومة معلوماتية كبرامج الحاسوب مثلا.

[3] قانون رقم 03 – 05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر رقم 44، المؤرخة في 23 يوليو 2003.

ثالثا: في القانون المتعلق بالتأمينات الاجتماعية

وتتمثل في جرائم التسليم، الاستلام، تعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية، الإعداد، النسخ، الصناعة، الحيازة، التوزيع، بطريقة غير مشروعة للبطاقة الإلكترونية بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا ، هذه الجرائم نصت عليها المواد من 93 مكرر2 إلى 93 مكرر6 من القانون[1] المتعلق بالتأمينات الاجتماعية.

رابعا: في القانون العضوي المتعلق بالإعلام

وتتمثل في جرائم النشر، البث، بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي لأي خبر أو وثيقة تلحق ضررا بسر التحقيق الابتدائي سواء صورا أو رسومات أو أي بيانات توضيحية أخرى تعيد تمثيل كل أو جزء من ظروف الجنايات أو الجنح المذكورة في المواد 255 إلى 263مكرر ومن 333 إلى 342 من ق ع الجزائري، جريمة الإهانة بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي لرؤساء الدول الأجنبية وأعضاء البعثات الدبلوماسية المعتمدين لدى حكومة الجمهورية الجزائرية الديمقراطية الشعبية، هذه الجرائم نصت عليها المواد من 119 إلى 123 من هذا القانون[2]العضوي المتعلق بالإعلام.

خامسا: في القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين

تتمثل في الأفعال غير المشروعة التي من شأنها إعاقة والإضرار بعملية التوقيع والتصديق الإلكترونيين، وهي جرائم قد يرتكبها شخص عادي كجريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة أو يرتكبها مؤدي خدمات التصديق الإلكتروني كإخلاله بالتزامه

[1] قانون رقم 08 – 01 المؤرخ في 23 يناير 2008 يتمم القانون 83 – 11 المؤرخ في 2 يوليو 1983 والمتعلق بالتأمينات الاجتماعية، ج ر رقم 4، المؤرخة في 27 يناير 2008.

[2] قانون عضوي رقم 12 – 05 المؤرخ في 12 يناير 2012، يتعلق بالإعلام، ج ر رقم 2، المؤرخة في 15 يناير 2012.

بإعلام السلطة الاقتصادية بالتوقف عن نشاطه وعلى كل هي جرائم تجد تنظيمها من خلال نصوص المواد من 66 إلى 75 من القانون[1] المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

سادسا: في القانون المتعلق بالتجارة الإلكترونية

تتمثل في جرائم عرض للبيع وبيع واللعب أو مخالفة الشروط عن طريق منظومة معلوماتية لكل سلعة أو خدمة أو لعبة محظورة بمقتضى القانون[2]المتعلق بالتجارة الإلكترونية الجزائري، هذه الجرائم نصت عليها المواد من37 إلى 44 في هذا القانون الأخير.

سابعا: في القانون المتعلق بحماية الأشخاص الطبيعية في مجال المعطيات ذات الطابع الشخصي

تتمثل في كل الأفعال التي من خلالها يتم الاعتداء على كل ما هو متعلق بالمعطيات ذات الطابع الشخصي من دون الموافقة الصريحة للمعني وفي غير الحالات التي يسمح بها هذا القانون خصوصا إذا ما كانت تمس بالكرامة الإنسانية والحياة الخاصة والحريات العامة وبحقوق الأفراد وشرفهم وسمعتهم كجريمة معالجة أو أمر بمعالجة معطيات ذات طابع شخصي دون تصريح مسبق لدى السلطة الوطنية أو الترخيص منها طبقا للأحكام المنصوص عليها في هذا القانون[3]، وهذه الاعتداءات نصت عليها المواد من 54 إلى 69 في هذا القانون الأخير.

---

[1] قانون رقم 15 – 04 المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر رقم 6 المؤرخة بتاريخ 10 فبراير 2015.

[2] قانون رقم 18 – 05 المؤرخ في 10 مايو 2018 يتعلق بالتجارة الإلكترونية، ج ر رقم 28، المؤرخة في 16 مايو 2018.

[3] قانون رقم 18 – 07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر رقم 34، المؤرخة في في 10 يونيو 2018.

ثامنا: في القانون المتعلق بالوقاية من عصابات الأحياء ومكافحتها

تتمثل هذه الجرائم في الأفعال التي من شانها تشجيع أو تحريض عصابات الأحياء بوسيلة إلكترونية وكذا القيام بالأفعال المتعلقة بعصابات الأحياء عن طريق استعمال تكنولوجيا الإعلام والاتصال طبقا للأحكام المنصوص عليها من هذا القانون[1]، هذه الجرائم نصت عليها المواد 23 و29 و36.

تاسعا: في قانون الانتخاب

تتمثل هذه الجرائم في الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات الانتخابية أو محاولة المساس بها نصت عليها المادة 283 من هذا القانون[2].

المبحث الثالث: أهمية مواجهة الجرائم المعلوماتية ومختلف تحدياتها الإجرائية

إن الحماية الجنائية لنظام المعلوماتية لها ما يبررها ويعللها خاصة في ظل التطور السريع والهائل لمختلف التقنيات والبرامج، والذي جلب معه الكثير من الأساليب والطرق الجديدة المستعملة في اقتراف هذه الجرائم، هذه الحماية كأصل عام تكمن فائدتها في التقليل من هذه الجرائم وردع مختلف مجرمي المعلوماتية باختلاف أصنافهم وفئاتهم بالرغم من التحديات التي تواجه رجال التحري والتحقيق في كشف ومواجهة هذا النوع من الجرائم.

المطلب الأول: مبررات وفائدة الحماية الجنائية للنظام المعلوماتي

تعتبر الحماية الجنائية من أهم الحمايات ذات الطابع القانوني التي بسطتها مختلف التشريعات من أجل ردع أشكال الجرائم والاعتداءات التي تمس بجوانب حياة الإنسان، الذي أصبح الآن يتفاعل بشكل رهيب مع ما تخلفه تكنولوجيا الإعلام والاتصال، هذه الأخيرة ونظرا لنقائصها وما تخلفه من ثغرات فنية باتت عرضة للاستغلال ومهددة بالاعتداء عليها من طرف المجرمين المعلوماتيين بمختلف

[1] الأمر رقم 20-03، المؤرخ في 30 غشت 2020، يتعلق بالوقاية من عصابات الأحياء ومكافحتها، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[2] أمر رقم 21-01، المؤرخ في 10 مارس 2021، المتضمن القانون العضوي المتعلق بنظام الانتخابات، ج ر رقم 17 المؤرخة في 10 مارس 2021.

فئاتهم والمتطرق إليها سابقا، الأمر الذي يحتم بسط حماية جنائية فعالة تسد النقص الذي خلفته هذه التكنولوجيا وتردع أشكال أنواع اعتداءات هؤلاء المجرمين.

الفرع الأول: مبررات الحماية الجنائية للنظام المعلوماتي

إنّ غزو تقنيات وتكنولوجيا المعلومات للعالم بأسره والحاجة الملحة إليها تجلت من خلال الاعتماد عليها في جميع الميادين ومختلف الأنشطة الإنسانية بهدف تحقيق الرفاهية، وبالرغم من ضخامة مختلف الاستثمارات المالية والجهود البشرية من أجل تطويرها وتحديثها دوريا، إلاّ أن الهاجس الخطير الذي يهدد نجاحها يكمن في الاعتداء عليها من قبل مجرمين محترفين في هذا المجال، لذا كان من اللازم أن تتدخل مختلف التشريعات من أجل حمايتها جنائيا، هذه الحماية لها ما يبررها والتي تكمن في؛

أولا: عدم كفاية الوسائل التقنية المتوفرة

في أغلب الأحيان ما يعتمد منتجو البرامج على وسائل تقنية لحماية برامجهم من خطر النسخ والنقل كوضع كلمة معينة لا يتم تشغيل البرنامج دونها أو وضع رقم سري في بداية البرنامج يمنع نقله أو استنساخه من طرف الآخرين، إلاّ أنّ هذه التقنيات غير كافية لحماية النظام المعلوماتي كون أنّها قابلة للاختراق من قبل أشخاص محترفين مقارنة بالأشخاص العاديين، ففضلا عن صعوبتها عن هؤلاء الأخيرين فإنّها ليست بالصعوبة المعقدة بالنسبة للمتخصصين، فالقول بعدم كفاية الوسائل التقنية المتوفرة من أجل حماية النظام المعلوماتي[1] تؤيده شواهد كثيرة.

كان من بينها أحد البلدان المتطورة مفادها أنّ شركة أمريكية أعلنت عن توصلها إلى برنامج غير قابل للنسخ بفضل ما استخدمت فيه من تقنيات متقدمة من أجل تحصينه من السرقة، ففوجئت بعد ذلك بخطاب مرفق به نسخة من برنامجها الحصين، أين أكد صاحب الخطاب بأنّ عملية النسخ لم تستغرق أكثر من ستة ساعات فقط، من هنا يستنتج بأن مسألة النسخ غير المشروع للبرامج هي مسألة وقت فقط ولا شك في أنّ فعالية الوسائل التقنية للحماية الموضوعة من قبل منتجو البرامج مرهونة

[1] محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط ثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص153.

بحجم المال والوقت الذي ينفق لأجل الحماية، فكل ما كان المال والوقت كبير يرجى أن تكون الحماية على قدر عال والعكس كلما كانت البرامج أقل تكلفة وأقل وقت كلما كان احتمال الاختراق كبير ويسير.

ثانيا: ضخامة الاستثمارات المالية والجهود البشرية في إنتاج البرامج

معظم الصناعات تشهد نموا كبيرا في الاستثمار في تطبيقات تكنولوجيا المعلومات والاتصال لذلك زاد في معظم الدول الصناعية الاتفاق بشكل كبير على أجهزة ووسائل تكنولوجيا المعلومات والاتصال كجزء من الاتفاق الكلي على أدوات ووسائل قطاع الأعمال، فعلى سبيل المثال وفي الولايات المتحدة الأمريكية بالضبط ارتفع معدل الاستثمار في تكنولوجيا المعلومات والاتصال[1] من أقل من 5 % إلى 45% في المدة ما بين 1960 إلى 1996 وظل هذا المعدل في الزيادة حتى ارتفع إلى أكثر من 50 % في عام 2002 .

هذا وطبقا لتقديرات مكتب الإحصاء ومكتب التحليل الاقتصادي التابعين لوزارة التجارة الأمريكية، فإنّ الولايات المتحدة في الفترة ما بين 1990 – 1999 في صناعة تكنولوجيا المعلومات والاتصال أثمرت عائداتها 683 مليار وكان ذلك بالضبط في سنة 1998، لهذا فإنّ العلاقة بين التقنية والجرائم الاقتصادية تتمحور في استخدام التكنولوجيا والتقنيات المتطورة من أجل إجراء بعض العمليات الاقتصادية التي لا يجيزها النظام، فهذه التقنيات سهلت على المجرمين اختلاس أموال طائلة وتحويل الأرصدة النقدية بطرق غير مشروعة[2] .

كما وتعتبر شركة إدارة المنافع الدوائية المملوكة ل(eli_lily)، نموذجا مثاليا لذلك بحيث تستخدم هذه الأخيرة نظاما حاسوبيا مباشرا عبر الإنترنيت للربط بين حوالي خمسين ألف صيدلية وخمسين ألف طبيب، بحيث كلما قدم مريض وصفة طبية يقوم البرنامج بالبحث في سجل المريض ليرى ماهية الأدوية

[1] عواطف عبد الرحمان، الإعلام والعولمة البديلة، ط أولى، العربي للنشر والتوزيع، القاهرة، مصر، 2006، ص54.

[2] عبد الله عبد العزيز اليوسف، التقنية والجرائم المستحدثة، مؤلف جماعي بعنوان الظواهر الإجرامية المستحدثة وسبل مواجهتها ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2014، ص214.

الأخرى الموصوفة له في السابق من قبل أي طبيب في الشبكة بغض النظر عن المكان الذي تم فيه تعبئة السجل، ويبحث البرنامج كذلك على العقاقير المعروفة بخطورتها في حال تفاعلها مع الوصفة الحالية فإذا وجد أيا منها رفع الصيدلي علما أحمر ونبه المريض والطبيب على حد سواء[1].

وعليه فإذا كانت رؤوس الأموال المستثمرة في صناعة البرامج بمثل هذه الضخامة فلا شك بأنّ الاعتداء عليها يعد خطرا كبيرا على المستثمرين في مجال برامج الحاسب الآلي، لأنّه مرهون بعدد النسخ الأصلية المباعة من البرامج لذلك يعتبر السماح بنسخ البرامج بوجه غير رسمي وعدم ملاحقة قراصنة هذه البرامج مؤدي إلى خسارة كبيرة للمستثمرين، وبالتالي يعزفون عن الدخول في هذا المجال الحيوي والمهم من الاستثمار مما يهدد ويساهم في انهيار المجتمع، لاسيما وأنّ الحاسب الآلي ونظام المعلوماتية بصفة عامة بدأ يتدخل في أبسط الأمور فلم يبقي أي مجال إلاّ وغزاه هذا النظام[2].

ثالثا: خطورة الجرائم المعلوماتية

أصبحت تقنية المعلومات الجديدة قادرة على تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل الأفراد والمؤسسات والدوائر والأجهزة الحكومية ومن قبل الشركات الخاصة، وأكثر من ذلك يمكن مقارنة المعلومات المخزونة في ملف مؤتمن بمعلومات في قاعدة بيانات أخرى، أين يمكن نقلها داخل البلد الواحد أو من بلد لآخر في ثوان وبتكاليف منخفضة نسبيا[3]من هنا نخلص باتسام عامة الجرائم المعلوماتية بالخطورة فهي تقع على برامج ومعلومات ذات قيمة اقتصادية مسببة خسائر باهظة في الجهد والأموال كما تم تبيينه في الفرع السابق.

بل وقد تقضي على مؤسسة اقتصادية عملاقة بمجرد أن يعرف لص ذو دراية وخبرة في مجال المعلوماتية رقم حسابها أو الرقم السري الذي تحتفظ فيه بأسرارها الإدارية أو أسرارها الصناعية، فاللص

---

[1] ستان ديفيس، بناء الاقتصاد المبني على المعرفة، مؤلف جماعي بعنوان تنمية الموارد البشرية في اقتصاد مبني على المعرفة، ط أولى مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، الإمارات العربية المتحدة، 2004، ص48.

[2] محمد حماد الهيتي، المرجع السابق، ص154.

[3] بولين أنطونيوس أيوب، المرجع السابق، ص20.

المحترف يستطيع في خلال لحظات أن يدمر كل البيانات السرية لتلك المؤسسة أو أن يفشي سر صناعتها عن طريق وضعها على الشبكة المعلوماتية بحيث يكون في متناول الجميع[1]، فالحواسب الآلية لم يعد استخدامها مقتصرا على الشركات أو المؤسسات المالية والاقتصادية والتجارية بل أصبح في متناول الأفراد حتى في مدارسهم ومنازلهم مما يتيح للجميع الاتصال بالنظام المعلوماتي العالمي.

الفرع الثاني: فائدة الحماية الجنائية للنظام المعلوماتي

تنطوي الحماية الجزائية لبرامج الحاسب الآلي على ناحيتين، الأولى شخصية تحقق الحماية الجنائية لأسرار الأفراد والثانية موضوعية تنطوي على تأمين الاستثمارات المادية والبشرية المستخدمة في تكنولوجيا المعلومات الأمر الذي يؤدي إلى تحقيق أهداف التنمية الاقتصادية، ومع كل هذه الحماية فإنّها تعتبر قاصرة في مواجهة الكثير من الجرائم المعلوماتية التي كانت ولا زالت إلى يومنا هذا.

أولا: فائدة الحماية الجزائية الشخصية للنظام المعلوماتي

إنّ المعلومات المودعة بالخصوص في الحاسب الآلي والمتضمنة أسرار الحياة الخاصة معرضة للنشر والشيوع بما يسبب ضررا لصاحبها، الأمر الذي حتم إضفاء حماية جزائية لهذه المعلومات والبرامج للحلول دون تفاقم أخطار استعمال الحاسب الآلي ضد الحياة الخاصة للشخص[2]، كما أنّ بعض البرامج على قدرة بتغيير بعض البيانات المخزنة من قبل الحاسب الآلي وإحداث غش فيها أو إتلاف برنامج أو التجسس على ما تحتويه برامج أخرى من معلومات، لأجل ذلك قامت بعض النظم القانونية الغربية بإحداث تعديلات تشريعية فيها بغية حماية الحياة الخاصة لأفرادها والحيلولة دون الاعتداء عليها خاصة إذا ما تعلق الأمر بحقوق الملكية الأدبية لهؤلاء.

---

[1] محمد حماد الهيتي، المرجع السابق، ص156.

[2] محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، د ط، دار الجامعة الجديدة للنشر، الإسكندرية مصر، 2001 ص18.

هذا ولقد تأثرت الجزائر على غرار الدول الأخرى بما أفرزته الثورة المعلوماتية خاصة في مجال الحياة الخاصة من خلال القانون[1] 23/06 المعدل لقانون العقوبات الجزائري المواد 303 مكرر إلى 303 مكرر3 منه لكن دون حماية للمعطيات الشخصية في هذا الإطار؛ أين اعتبر ذلك قصورا في حق المشرع الجزائري إلى غاية أن تداركه بالقانون[2] 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، هذا القانون الذي أضفى حماية جزائية موضوعية وحماية جزائية إجرائية ذات طابعين إجرائية إدارية وإجرائية جزائية لأسرار الحياة الخاصة للفرد في نصوص المواد من 54 إلى 74 منه.

وعليه فإنّ الحماية الجزائية ضرورية ومهمة ويجب أن تكون فعالة من أجل حماية أسرار الأشخاص المحفوظة[3] داخل الحواسب الآلية، خاصة في ظل التوسع الهائل في استخدام هذه الحواسب لذلك لابد من إيجاد نصوص واضحة تجرم الانحراف بالمعلومات أو إفشائها إذا كان في ذلك مساس بسمعة الشخص أو حرمة حياته الخاصة سواء تم ذلك عمدا أو نتيجة إهمال.

ثانيا: فائدة الحماية الجزائية الموضوعية للنظام المعلوماتي

إنّ الحماية الجزائية لبرامج الحاسب الآلي من الناحية الموضوعية لها من الأهمية خاصة في مجال تشجيع الأشخاص على الابتكار في شتى المجالات، وفي مجال القضاء على القرصنة الدولية للبرامج وفي مجال التنمية الاقتصادية إلى غير ذلك من الأمور الأخرى؛

1- التشجيع على الابتكار

فالحماية الجزائية لبرامج الحاسب الآلي تعطي الأمان للمبتكر لأنّه سينال مقابلا عادلا لجهده يجعله يلج عالم تأليف البرامج، الأمر الذي يعود بالفائدة على تقدم الأمم علميا وتكنولوجيا، فمثلا

---

[1] القانون رقم 06- 23، يعدل ويتمم الأمر 66- 156، المتضمن ق ع الجزائري، القانون السابق.

[2] القانون رقم 18- 07، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر رقم34 المؤرخة في في 10 يونيو 2018.

[3] محمد محمد شتا، المرجع السابق، ص20.

الحجم الكبير للاستثمارات والميزانيات المستخدمة للإنفاق على إنتاج الأموال المعلوماتية والتي تمس مصالح كثير من الشركات والبنوك، فإذا لم يتم حماية برامج الحاسب الآلي تكون هذه الأموال والمصالح مهددة بالضياع مما يؤدي إلى إحباط شديد ينجم عنه قتل روح الابتكار عند الأشخاص، خاصة تلك التي تنفق بسخاء من أجل الارتفاع بمستوى حياة الناس اقتصاديا واجتماعيا وعلميا وخلقيا.

2- مكافحة القرصنة الدولية لمختلف البرامج

لقد دلت الإحصائيات الحديثة على أنّ القرصنة في بعض الدول بلغت حجما كبيرا بحيث أصبحت تهدد أنظمة المعلومات في العالم، ففي كندا وصلت نسبة تقليد البرامج إلى تسعين في المائة لذلك لا شك أنّ حماية البرامج الحواسب الآلية جزائيا سيفضي إلى تقليص مشكلة القرصنة الدولية لهذه البرامج، وسيقلل بالتالي من ارتكاب كافة الجرائم المعلوماتية لاسيما وأنّ هذه الأخيرة تتسم بصعوبة الإثبات لأن مرتكبيها في الغالب ممن يتميزون بمهارات ومعارف عالية[1] لذا يتعين على الدول أن تتعاون لإشاعة البرامج المبتكرة التي تخدم الإنسانية في مقابل مبالغ معقولة بدلا من انصراف الأفراد والدول إلى القرصنة.

3- تحقيق أهداف التنمية الاقتصادية

تعتبر تكنولوجيا المعلومات والاتصالات عنصرا هاما وفاعلا في زيادة الإنتاجية والنمو الاقتصادي، فالانتشار الواسع للحواسيب والإنترنت والهواتف المحمولة والشبكات عريضة النطاق يؤكّد مدى اختراق هذه التكنولوجيات لمختلف المجالات الاقتصادية وتأثيرها عليها، أيضا فقد أصبح ينظر لهذه التكنولوجيات على أنّها السبب في الزيادة الكبيرة في إنتاجية الاقتصاديات الحديثة[2].

---

[1] محمد محمد شتا، المرجع السابق، ص22.

[2] حسين العلمي، دور الاستثمار في تكنولوجيا المعلومات والاتصالات في تحقيق التنمية المستدامة دراسة مقارنة بين ماليزيا وتونس والجزائر، عمل مقدم لنيل شهادة الماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة فرحات عباس سطيف 1 الجزائر، السنة الدراسية 2012/ 2013 ص76.

فتكنولوجيا المعلومات والاتصالات تصنف ضمن التكنولوجيا المتعددة الأغراض، التي يمكن أن يدخل استخدامها ضمن العديد من القطاعات الاقتصادية، لذلك فالعقوبة من شأنها ردع مرتكب الجريمة المعلوماتية خاصة إذا غلب جانب العقوبة على جانب الفائدة التي سيجنيها من جريمته فالجاني في أغلب الحالات سيتجنب الإقدام على هذا الجرم خاصة إذا كان من أناس متكيفون اجتماعيا ويخشون من الفضيحة التي من الممكن أن تلحقها بهم العقوبة[1].

المطلب الثاني: التحديات الإجرائية التي تواجه مكافحة الجرائم المعلوماتية

تعتبر الحماية الإجرائية للنظام المعلوماتي السلاح الأمثل في مواجهة وكشف الجرائم المعلوماتية فهي عبارة عن حماية عملية لهذا النظام، عكس الحماية الموضوعية الساكنة التي تكتفي فقط بتبيان أركان ونوع الجريمة المعلوماتية وتحديد العقوبة اللازمة لها، هذا ونظرا لما تتمتع به الجرائم المعلوماتية من خصوصية واضحة جعلت المحققين في هذا المجال يصطدمون بعدة تحديات شخصية وأخرى متعلقة بطبيعة هذه الجرائم حتمت عليهم مسايرتها مع تحديث معارفهم دوريا في كل حين وفترة.

الفرع الأول: مبدأ الشرعية الإجرائية في الجرائم المعلوماتية

تعتبر الشرعية الإجرائية أحد الحلقات الهامة لمبدأ الشرعية الجنائية، هذه الأخيرة ظهرت لكي تحمي الإنسان من خطر التحكم في التجريم والعقاب فلا يكون بغير قانون[2]، حيث تلتزم الدولة أساسا بسلطة التجريم سلفا ثم سلطة المعاقبة خلفا في إطار المبدأ الأخير[3] الذي يطبق عمليا في إطار الدعوى

---

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د ط، دار الجامعة الحديثة، الإسكندرية مصر، 2007، ص31.

[2] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الكتاب الأول، ط عاشرة، دار النهضة العربية، القاهرة، مصر 2016 ص123.

[3] تنص المادة 1 من الأمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 49، المؤرخة في 11 يونيو 1966 بأنّه: " لا جريمة ولا عقوبة أو تدبير أمن إلاّ بقانون".

العمومية وفي إطار منظومة السياسة الجنائية المتبعة والتي يلعب فيها القاضي الجزائي دورا أساسيا[1] خاصة في الجرائم الخطيرة والمستحدثة كالجرائم المعلوماتية.

من هنا يبرز الدور الهام الذي يلعبه قانون الإجراءات الجزائية في تطبيق قانون العقوبات، ذلك أنّ الشرعية الجنائية غير كافية لوحدها لحماية حقوق الإنسان في مواجهة هذا التحكم، فما جدوى شرعية الجرائم والعقوبات إذا أمكن القبض على المتهم أو تفتيش شخصه أو مسكنه أو حبسه مؤقتا أو تعريضه لمحاكمة غير عادلة قائمة على افتراض الإدانة، فهذه الممارسات الإجرائية التعسفية التي لا يسمح بها القانون تؤدي إلى تطبيق معاكس لهذا الأخير، لذلك كان لابد من تدعيم مبدأ الشرعية الجنائية[2] بمبدأ آخر يحدد الإجراءات التي تتخذ في مواجهة المتهم وأن تنظم على نحو يحترم الحقوق والحريات[3]، هذا المبدأ يسمى بالشرعية الإجرائية الجنائية.

هذا المبدأ الأخير يكون تفعيله أمرا في غاية التعقيد والحساسية في مواجهة المتهم بالجرائم المعلوماتية، فهذه الأخيرة تعد من بين الجرائم ذات الطبيعة الفنية والتي تحتاج وتعتمد على الخبرة في مجال إثباتها بشكل كبير، أين يلعب الخبير المعلوماتي فيها دورا مهما من خلال تقديمه للمعلومات العلمية والمصطلحات التقنية، والتي يقوم بشرحها فيما بعد للقضاة لأنّها تشكل صعوبة بالغة لدى المحققين وأعضاء النيابة العامة لهذا تترك هذه المهمة في الغالب للخبراء، وهو الأمر الذي يفقد ويخرج القضية الجزائية من عناصرها القانونية فلا تتمكن المحكمة بذلك من الوقوف كلية على الحقائق المكونة لأركان الفعل الإجرامي والتيقن من الأدلة التي تثبت تلك الأركان[4].

---

[1] صالح جابر، خصخصة الدعوى العمومية في الفقه الإسلامي والتشريع الجزائي الجزائري، المجلة الدولية للبحوث القانونية والسياسية، المجلد 04، العدد 03، جامعة الوادي، الجزائر، ديسمبر 2020، ص94.

[2] مبدأ الشرعية كما أشرنا إليها سابقا من خلال ص 16 في المقدمة.

[3] أحمد فتحي سرور، المرجع السابق، ص124.

[4] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، ط أولى، الأكاديميون للنشر والتوزيع، عمان، الأردن، 2014 ص129.

الفرع الثاني: التحديات الإجرائية لشخص المحقق في مكافحة الجرائم المعلوماتية

تبقى التحديات الإجرائية التي تواجه شخص المحقق في مجال مكافحة الجريمة المعلوماتية مقتصرة على عاملين الأول داخلي شخصي والثاني خارجي متعلق بمجال التدريب على المستوى الدولي؛

أولا: العوامل الداخلية المؤثرة على شخص المحقق

يستوجب على المحققين من أجل كشف الجرائم المعلوماتية والتحقيق والفصل فيها بصورة جدية وفاعلة ضرورة تثقفهم، وكذا تأهلهم على جمع أدلتها مع تدربهم المستمر على تقنيات تكنولوجيا المعلومات ويجب أن يكتسبوا معرفة تشغيل نظام الكمبيوتر والتعامل معه بشكل صحيح والاطلاع على قواعد البيانات والمعلومات ومخرجات الكمبيوتر والاطلاع على مضمون الأسطوانات الممغنطة وسائر الوسائل المادية التي تحتوي على البيانات دون تسبب بالإضرار بها أو تلفا أو محوها.

هذا ويتطلب كذلك من المحقق في مجال الجرائم المعلوماتية اكتساب المعرفة لخرق الشفرة وكلمات السر للوصول إلى الدليل أو المعلومة موضوع الجريمة، كما يتطلب منه ضرورة معرفة الأساليب الفنية التي استعملها المجرم المعلوماتي وكشفها وفحصها وتأهيل القضاء في التعامل مع الأدلة المعلوماتية وتقدير قيمتها الثبوتية[1].

ثانيا: العوامل الخارجية المؤثرة على شخص المحقق

يتمثل مجمله في عدم رغبه القيادات الإدارية في بعض الدول تدريب المحققين لاعتقادهم بدوره السلبي في تطوير العمل، وما قد ينجم عنه من تهديد للتعاون الدولي في مجال التدريب في حالة تطبيق ما تعلمه وما اكسبه المتدربون من خبرات في الدورات التدريبية، وكذلك وجود فوارق فردية بين المتدربين تؤثر على عمليه اكتساب المهارات المستهدفة بصفة تامة ومتكافئة لدى مختلف الأفراد المتدربين لاسيما في مجال تكنولوجيا المعلومات وشبكات الاتصال.

---

[1] فريد منعم جبور، حماية المستهلك عبر الإنترنيت، ومكافحة الجرائم المعلوماتية دراسة مقارنة، ط ثانية، منشورات الحبلى الحقوقية بيروت، لبنان، 2012، ص212.

ذلك أنّه يوجد بعض الأفراد ممن لا يفقه شيئا في هذا المجال وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال، ومن الصعوبات أيضا والتي قد تؤثر على عمليه التدريب وعلى التعاون الدولي في مجالها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العلمي لبيئة العمل الطبيعية تمثيلا تاما من حيث ما يدور بها من وقائع وملابسات وإجراءات وما يتم فيها من نشاطات، لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية[1].

الفرع الثالث: التحديات الإجرائية في مواجهة الطبيعة الخاصة للجرائم المعلوماتية

يوجد الكثير من التحديات والمشكلات الإجرائية التي تنبع من الطبيعة الخاصة للجرائم المعلوماتية والتي امتدت إلى شبكة الإنترنيت بعد ما كانت تقتصر فقط على الحاسب الآلي وأنظمته هذه التحديات لا تخرج عن أحد النطاقين، الأول متعلق بالصعوبات والعقبات التي يفرضها التعاون الأمني الدولي والثاني متعلق بتعقيدات عملية إجراءات التحقيق في هذا النوع من الجرائم؛

أولا: التحديات المتعلقة بالتعاون الأمني والقضائي الدولي

تتميز الجرائم المعلوماتية بأنّها جرائم دولية عابرة للحدود، الأمر الذي يتطلب تعاون الدول من أجل كشف وإحباط مختلف الاعتداءات المعلوماتية وهو ما يعتبر تحديا كبيرا في وجه مختلف الأجهزة الأمنية والقضائية الداخلية والدولية، خاصة وأنّ هذه الجرائم غير موحدة المعالم بدليل اختلاف تعريفاتها من تشريع لآخر وتجريم بعض صورها في دول وإباحتها في دول أخرى، بالإضافة لعدم وجود قنوات اتصال تسمح للجهات القائمة على التحقيق بالاتصال بالجهات الأجنبية لجمع أدلة معينة أو الحصول على معلومات وبيانات متعلقة بالجريمة والمجرمين[2]، كما هو الحال في العديد من القضايا أين يتواجد

[1] غانم مرضي الشمري، المرجع السابق، ص128.

[2] عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية في مكافحة جرائم بطاقات الائتمان الإلكترونية والتعاون الأمني الدولي حيالها، د ط، دار الجامعة لجديدة، الإسكندرية، مصر، 2015، ص139.

الضحايا والجناة وناقل الاتصالات عبر مختلف البلدان خارج حدود الولاية القضائية[1] مما يوفر حواجز أمام تحديد هوية المجرمين المعلوماتيين وأمام التحقيق.

هذا مع بطء الإجراءات بين الدول بطريق المساعدات القضائية لدى بعض الجهات سواء في الرد على بعض الاستفسارات أو طلبات تنفيذ الإنابة القضائية والتأخر في الرد عليهما وما ينجر عن ذلك من ضياع أو فقدان لبعض الأدلة الهامة والضرورية، هذا وتؤدي قلة المعلومات الواردة من الجهات التي تطلب المتهم إلى تصعيب مهمة الجهات المختصة بالبحث عن المتهمين وإلقاء القبض عليهم والتأخر في إرسال ملف الجريمة والمعلومات المتعلقة بها، وكل هذا يفسر صعوبة عملية تعاون مختلف الأجهزة الأمنية والقضائية الدولية.

ثانيا: التحديات المرتبطة بإجراءات التحقيق

تتميز الجرائم المعلوماتية بطبيعتها الخاصة التي قد لا تسمح بترك أي أثر مادي في مسرح الجريمة فضلا عن أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة، وهو الأمر الذي يصعب من مهام رجال التحقيق فيها عندما يكونون بصدد القيام بأحد الإجراءات كالتفتيش أو الضبط أو المعاينة أو الخبرة، فمثلا الإجراء الأول الذي يتم عادة على شبكات المعلومات أين قد يتجاوز نظام المشتبه به ويمتد إلى أنظمة أخرى مرتبطة معه[2].

---

[1] Elisavet Charalambous, Dimitrios Kavallieros, Ben Brewster, George Leventakis Nikolaos Koutras and George Papalexandratos, Combatting Cybercrime and Sexual Exploitation of Children: An Open Source Toolkit, From a book of Babak Akhgar, Saskia Bayerl, Fraser Sampson, Open Source Intelligence Investigation- From Strategy to Implementation, Springer International Publishing, AG Switzerland, 2016, p237.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت (الجرائم الالكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنيت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط أولى، منشورات الحبلى الحقوقية، بيروت، لبنان 2007 ص46.

هذا الامتداد الذي يبقى محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش، وكذلك بالنسبة للإجراء الثاني المتعلق بالضبط والذي قد لا يتوقف على تحريز المكونات المادية للحاسب الآلي وما يتعلق به من أجزاء فقط بل قد يتعداه إلى ضبط وتحريز مختلف المعطيات والبيانات والبرامج المخزنة في هذا النظام أو النظم المرتبطة به أو أية أشياء ذات طبيعة معنوية أخرى، والتي تكون معرضة بسهوله للتغيير والإتلاف.

إذن هي كلها حقائق تثير تحديات متعددة تتعلق بمعايير التحريز والضبط المعلوماتي وتتعلق بمسألة مساسها بخصوصية صاحبها حتى وإن كان المشتبه فيه، خاصة عندما تشمل إجراءات الضبط كل محتويات النظام والتي تضم عادة معلومات وبيانات قد يحرص هذا الأخير على سريتها أو أن تكون محل حماية بحكم القانون أو بحكم طبيعتها أو بحكم تعلقها بجهات أخرى.

الفصل الثاني: إجراءات التحقيق الأولية في الجرائم المعلوماتية

تعتبر مرحلة التحقيقات الأولية من المراحل الحساسة والهامة، بحيث تُحدد وفق نتائجها مسألة البدء والسير بطريق الدعوى العمومية، هذه المرحلة يكون صاحب الدور الرئيسي فيها ضباط الشرطة القضائية، والذين يقومون بالتحري وجمع الاستدلالات اللازمة من أجل كشف الجرائم بصفة عامة التقليدية وكذا المستحدثة كالتي في شكل الجرائم المعلوماتية، هذه الأخيرة التي تضررت منها الكثير من الدول بل وزعزعت الأمانة والثقة لدى الكثير من الأشخاص الذين باتوا يتجنبون التعامل داخل العالم الافتراضي، فهذا العالم أصبح بالنسبة إليهم لعبة في يد بعض المجرمين المحترفين يجولون فيه كيف شائوا.

لهذا فإذا ما وقعت جريمة ما من الجرائم المعلوماتية ووصل العلم بها إلى ضباط الشرطة القضائية فإنّها تعلن ببدء مرحلة يطلق عليها في التشريع الجزائري اسم مرحلة جمع الاستدلالات أو مرحلة التحقيقات الأولية والتي يكون الهدف منها تعقب المجرمين والبحث عنهم وجمع الاستدلالات اللازمة التي تثبت ارتكابهم[1] لهذه الجريمة، فالدعوى العمومية قبل وضعها في ساحة القضاء لابد لها وأن تمر بهذه المرحلة الحساسة التي يلعب ضباط الشرطة القضائية الدور الرئيسي فيها، والتي يمكن من خلالها جمع أكبر قدر من المعلومات عن هذه الجريمة وظروف ارتكابها وما سبقها من مقدمات.

هذا ولقد حددت مختلف التشريعات صفات ضباط الشرطة القضائية ومختلف قواعد اختصاصاتهم للتحري والاستدلال عن الجرائم المعلوماتية، فهذا التشريع الجزائري مثلا قد حدد صفاتهم ومختلف قواعد اختصاصاتهم ضمن قوانينه الإجرائية الخاصة التي شهدت تعديلات كثيرة هذه التعديلات جاءت في بعضها نتيجة لتبني المشرع الجزائري لمفهوم جديد للجرائم المعلوماتية وكذا إنشائه لهيئات جديدة تعمل على الوقاية وعلى مكافحة وكشف هذه النوعية من الجرائم.

هؤلاء الضباط وفي الحالة العادية يختصون بتلقي الشكاوي والبلاغات عن الجرائم المعلوماتية والتي كثيرا ما يحجم فيها المجني عليهم عن الإبلاغ وتقديم شكوى عند ارتكابها بحقهم، بالرغم من أنّ هذه

[1] سعيد ظافر ناجي القحطاني، المرجع السابق، ص31.

الشكاوي والتبليغات تعتبر الخطوة الأولى لضباط الشرطة القضائية المختصون من أجل مباشرة التحري والاستدلال وكذا القيام بعملية المراقبة بشأن هذا النوع من الجرائم، هذه التحريات يمكن من خلالها استقصاء هذه الجرائم وفق ركنها الشرعي، أين يتحقق الضابط من أن الفعل المرتكب يشكل جريمة معلوماتية فيتحقق من ركنيها المادي والمعنوي وكذلك من ظروف ارتكاب هذه الجريمة وكذا البحث عن الفاعل من خلال تحديد هوية المشتبه فيهم.

أمّا في حالة التلبس بالجريمة المعلوماتية، فالمشرع الجزائري كان قد حدد حالات التلبس بالجريمة بصفة عامة بحيث أشملها على مختلف الجرائم العادية من جنايات وجنح، أما الجرائم المستحدثة كالتي في شكل الجريمة المعلوماتية فقد اجتهد الفقه أين أسقط بعض سلوكياتها وزمن وقوعها على حالات التلبس التي جيء بها في التشريع، هذا الأخير الذي أعطى لضباط الشرطة القضائية سلطات استدلالية وأخرى تحقيقية يقومون بها أثناء ثبوت حالة من حالات التلبس.

إنّ الهدف الأساسي من عملية التحري والاستدلال و ممارسة مختلف السلطات من قبل ضباط الشرطة القضائية في حالة التلبس هو جمع الأدلة عن الجرائم المعلوماتية، هذه الأخيرة وإن كانت تشترك مع الجرائم التقليدية الأخرى من حيث تطبيق الإجراءات العادية لجمع الأدلة حولها من خلال إجراءات المعاينة والتفتيش والضبط وكذا الخبرة فهي تحتاج أحيانا أخرى إلى تطبيق إجراءات خاصة من اعتراض للمراسلات والتقاط للصور وتسجيل للأصوات أو التسرب وكذا مراقبة الاتصالات الإلكترونية، هذه الإجراءات يجب أن تفعل وفق ضوابط وشروط أساسية تحت طائلة بطلانها.

هذا وتبقى مرحلة جمع الاستدلالات مرحلة أولية تجمع من خلالها مختلف الأدلة عن الجرائم المعلوماتية من قبل ضباط الشرطة القضائية الذين يحيلون مختلف محاضرها وتقاريرها إلى النيابة العامة التي تبقى وحدها صاحبة الاختصاص في التصرف بنتائجها.

المبحث الأول: مرحلة جمع الاستدلالات في الجرائم المعلوماتية

إنّ مرحلة جمع الاستدلالات تعتبر من بين أهم المراحل لكشف الجرائم وبالخصوص إذا ما تعلق الأمر بالجرائم المعلوماتية التي غالبا ما تقع في العالم الافتراضي، وهو الأمر الذي يزيد من صعوبة كشفها من طرف ضباط الشرطة القضائية المختصين، الذين من واجبهم اقتناص أي فرصة أو هفوة من قبل الجناة في هذا المجال حتى تسهل فيما بعد عملية قبضهم وتثبيت الحجة عليهم وتقديمهم أمام القضاء لمتابعتهم بالجرم المرتكب من قبلهم.

إنّ تنفيذ إجراءات التحقيق الأولية في الجرائم المعلوماتية يتطلب عمومًا الحد الأدنى من الأدلة الأولية أو بيان الإبلاغ عن هذه الجرائم، وتدابير كثيرة لجمع البيانات في وقتها المناسب أو الوصول إلى محتوى البيانات في أعلى مستوياتها[1]، هذه المرحلة الهامة الأولية للتحقيق سنتطرق لها بشيء من التفصيل من خلال المطالب الآتية.

المطلب الأول: ضباط الشرطة القضائية وقواعد اختصاصهم في الجرائم المعلوماتية

إنّ الجرائم المعلوماتية هي ذات طبيعة خاصة حتمت على جل التشريعات المقارنة كالتشريع الجزائري على وجوب تحديد صفات مؤهلة للتحري والاستدلال على هذا النوع من الجرائم، أين أعطيت لهم مهمة الضبط القضائي وهو ما أبرزه المشرع الجزائري ضمن نصوص خاصة أين حدد الصفات التي يخول لها مهام ضابط الشرطة القضائية في الجرائم المعلوماتية، وحدد كذلك لهذه الصفات اختصاصها الإقليمي الذي يباشرون فيه مهامهم والتي لا يجوز لهم تجاوزها تحت طائلة بطلان ما اتخذوه من إجراءات أثناءها وحتى ترتب مسؤوليتهم في حالات أخرى محددة قانونا.

[1] Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, rapport Délivré par Office des Nations unies contre les drogues et le crime Vienne, Autriche 25-28 février 2013, p9.

الفرع الأول: ضباط الشرطة القضائية المخول لهم البحث ومعاينة الجرائم المعلوماتية

لقد شهدت مهام الشرطة القضائية في الجزائر عدة تغيرات في السنوات الأخيرة نتيجة للتعديلات المتوالية التي جاء بها المشرع الجزائري في قانون الإجراءات الجزائية بدءا من قانون[1] 22/06 إلى الأمر[2] 02/15 وصولا للقانونين 07/17[3] ، 10/19 أين عدلت المواد 12 و15 و16 من هذا القانون والتي مست الصفات المخول لها مهمة ضابط الشرطة القضائية[4]، وكأصل عام فقد نص المشرع الجزائري ضمن هذا القانون على من يخول لهم هذه المهمة بنص المادة 12 من القانون 07/17 وهم القضاة والضباط والأعوان والموظفون المنوط بهم قانونا بعض مهام الضبط القضائي، وأمّا عن ضباط الشرطة القضائية الذين لهم صلاحية المتابعة والتحري عن الجرائم المعلوماتية فيجب التمييز بين قسمين؛

أولا: ضباط الشرطة القضائية المنصوص عليهم في ق إ ج

- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- الموظفون التابعون للأسلاك الخاصة للمراقبين ومحافظي وضباط الشرطة للأمن الوطني.
- ضباط الصف الذين أمضوا في سلك الدرك الوطني 3 سنوات على الأقل وتم تعينهم بموجب قرار مشترك صادر عن وزير العدل حافظ الأختام ووزير الدفاع الوطني بعد موافقة لجنة خاصة.

---

[1] قانون رقم 06- 22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] الأمر 15- 02 المؤرخ في 23 يوليو 2015 يعدل ويتمم الأمر رقم 66- 155 والمتضمن ق إ ج الجزائري ، ج ر رقم 41 المؤرخة في 29 يوليو 2015.

[3] قانون رقم 17- 07 المؤرخ في 27 مارس 2017 يعدل ويتمم الأمر رقم 66- 155 والمتضمن ق إ ج الجزائري ، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[4] قانون رقم 19- 10 المؤرخ في 11 ديسمبر 2019 المعدل والمتمم للأمر رقم 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 71، المؤرخة في 18 ديسمبر 2019.

– الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا 3 سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك عن وزير العدل ووزير الداخلية والجماعات المحلية بعد موافقة لجنة خاصة.

– الضباط وكذا ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل[1].

ثانيا: ضباط الشرطة القضائية المنصوص عليهم في المرسوم الرئاسي 261/15

– ضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني[2].

وعليه فإنّ هذه الصفات سواء من القسم الأول أو القسم الثاني هي المخول لها مهمة الشرطة القضائية حسب التعديلات الأخيرة التي شاهدها قانون الإجراءات الجزائية، والتي تقوم بعملية البحث والمعاينة عن الجرائم المعلوماتية أين يمتد اختصاصها إلى كامل الإقليم الوطني تحت إشراف النائب العام لدى المجلس القضائي المختص إقليما، كما يعلم وكيل الجمهورية المختص إقليما عن ذلك في جميع الحالات[3].

الفرع الثاني: قواعد اختصاص ضباط الشرطة القضائية في الجرائم المعلوماتية

إن مصطلح الاختصاص أوجدت له عدة تعريفات فكان من بينها أنّه: " ولاية قانونية مادية إقليمية، زمنية وشخصية، معترف بها لسلطة أو هيئة عامة للقيام بهذا العمل أو ذاك، ضمن شروط

[1] المادة 15 من قانون رقم 19- 10 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 71، المؤرخة في 18 ديسمبر 2019.

[2] مرسوم رئاسي 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 رقم 53، المؤرخة في 8 أكتوبر 2015.

[3] الفقرتان 7 و8 من المادة 16 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

محددة" وعرف كذلك بأنّه "الولاية التي يمنحها القانون لشخص أو هيئة للقيام بتصرفات معينة من حيث الموضوع، والأشخاص، والمكان"[1].

وكأصل عام وطبقا لقواعد ق إ ج الجزائري فإنّ ضباط الشرطة القضائية غير ضباط الشرطة التابعين لمصالح الأمن العسكري يوضعون بدائرة اختصاص كل مجلس قضائي تحت إشراف النائب العام الذي يحدد التوجيهات العامة اللازمة لهم من أجل تنفيذ السياسة الجزائية بدائرة اختصاص المجلس القضائي أين يتول وكيل الجمهورية إدارتهم على مستوى كل محكمة تحت رقابة غرفة الاتهام ويناط كذلك بضباط الشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي[2].

هذا ويبقى ضباط الشرطة القضائية في الحالات العادية يمارسون اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة أمّا في حالة البحث والتحري عن الجرائم المعلوماتية فيمتد اختصاصهم إلى كامل الإقليم الوطني وذلك حسب الحالات الآتية؛

أولا: حالة معاينة الجرائم المعلوماتية

المقصود بها الجرائم الماسة بأنظمة المعالجة الآلي للمعطيات المنصوص عليها في قانون العقوبات[3]ضمن نص المواد 394 مكرر إلى 394 مكرر7 في هذه الحالة إذا ما تعلق الأمر بالبحث ومعاينة هذه الجرائم يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني[4].

---

[1] أحمد غراب، ضرورة التمييز بين مصطلحي الاختصاص والصلاحية في المجال القانوني، مجلة العلوم الاجتماعية والإنسانية، المجلد 18، العدد 37، جامعة باتنة 1 الحاج لخضر، الجزائر، ديسمبر 2017، ص191.

[2] المادة 12 من قانون رقم 17- 07، المعدل والمتمم لق إ ج الجزائري ، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[3] قانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-156 المتضمن ق ع الجزائري، ج ر رقم 71 المؤرخة في 10 نوفمبر 2004.

[4] الفقرة 7 من المادة 16 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

ثانيا: حالة مراقبة الأشخاص المشتبه فيهم ارتكابهم للجرائم المعلوماتية

يجوز لضباط الشرطة القضائية ما لم يعترض وكيل الجمهورية المختص بعد إخباره أن يمددوا اختصاصهم عبر كامل الإقليم الوطني في عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم ارتكاب جريمة معلوماتية[1] أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجريمة أو قد تستعمل في ارتكابها.

ثالثا: حالة الاستعجال

فيجوز لضباط الشرطة القضائية أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به، ويجوز لهم أن يباشروا مهمتهم في كافة الإقليم الوطني بناء على طلب القاضي المختص قانونا ويساعدوهم في ذلك ضباط الشرطة القضائية الذين يمارسون وظائفهم في ذات الإقليم، على أن يخبروا مسبقا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة اختصاصه[2]، هذا وتدخل الجرائم المعلوماتية في إطار الاستعجال نظرا لطبيعتها الخاصة المتسمة بالسرعة والدقة في ارتكابها.

رابعا: حالة الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة

بحيث يجوز لضباط الشرطة القضائية تمديد إجراء التفتيش عن بعد في منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها إلى كامل الإقليم الوطني.

خامسا: حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية بشكل يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

أين يمتد الاختصاص بالنسبة لضباط الشرطة القضائية المنصوص عليهم ضمن قانون الإجراءات الجزائية، ولضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من أجل تفتيش المنظومات المعلوماتية عن بعد إلى كافة الإقليم الوطني.

---

[1] المادة 16 مكرر من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] الفقرة 3 المادة 16 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

سادسا: لمقتضيات التحريات والتحقيقات القضائية

يمتد الاختصاص بالنسبة لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ولضباط الشرطة القضائية المنصوص عليهم ضمن قانون الإجراءات الجزائية من أجل تفتيش المنظومات المعلوماتية عن بعد إلى كافة الإقليم الوطني وذلك عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية.

سابعا: حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

يجوز لضباط الشرطة القضائية كذلك في هذه الحالة تمديد إجراء التفتيش عن بعد في منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها[1] إلى كامل الإقليم الوطني.

المطلب الثاني: الإجراءات التمهيدية لضباط الشرطة القضائية في الجرائم المعلوماتية

تعتبر هذه المرحلة أحد المراحل الحساسة التي يباشرها ضباط الشرطة القضائية من أجل معرفة وكشف الجرائم المعلوماتية، أين يتلقون مختلف الشكاوى والتبليغات من قبل المجني عليهم وحتى من قبل أشخاص لا علاقة لهم بهذه الجرائم، هذه التبليغات والشكاوى تعتبر كخطوة أولى لحل غموض هذه الجرائم، وليس بمقدور أي شخص الإبلاغ عنها وإخبار السلطات المختصة بوقوعها ما لم تتوفر لديه القدرة على التعامل مع جهاز الحاسب الآلي ويستطيع إدراك الفعل غير المشروع.

بالرغم من ذلك فقد تم التشكيك في التصدي للجرائم المعلوماتية الواقعة بين الأشخاص خاصة من جانب نقص تفاعل واستجابة ضباط الشرطة القضائية والضحية وكذا مستوى الدعم المقدم لهذه الأخيرة، بل وفي كثير من الأحيان ما يقوم هؤلاء الضباط بدلاً من الاستجابة بالضغط على الضحايا للانسحاب من هذه المساحات الافتراضية عن طريق حذف الحسابات وتغيير هواتفهم، في هذه الحالة

[1] المادة 4 ولمادة 5 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

يكون الضحية هو المسؤول عن التعامل مع التهديد الافتراضي المعلوماتي من خلال إغلاق حساباته[1] وهو أمر لا يمكن تصوره بل وغير واقعي في ظل العصر الحديث والانتشار الرهيب لمواقع التواصل الاجتماعي.

وتأتي بعد هذه الخطوة مباشرة خطوة البدء بالتحري والاستدلال عن هذا النوع من الجرائم من قبل ضباط الشرطة القضائية المتطرق إليهم سابقا، هذا وتعتبر إجراءات التحري والاستدلال عملية مهمة من أجل جمع مختلف الأدلة التي لها علاقة بالجرائم المعلوماتية والبحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي ويكون ذلك بحماية مسرح الجريمة والحفاظ على الأدلة بمجموعة من ضباط شرطة قضائية أذكياء من الناحية الفنية وعلى دراية كافية في مجال التحقيقات القانونية.

الفرع الأول: تلقي الشكاوي والتبليغات عن الجرائم المعلوماتية

إنّ مصطلحي الشكوى والتبليغ نجد لهما ظهورا وبروزا في كتاب الله عز وجل في قوله تعالى: " قَدْ سَمِعَ ٱللَّهُ قَوْلَ ٱلَّتِى تُجَـٰدِلُكَ فِى زَوْجِهَا وَتَشْتَكِىٓ إِلَى ٱللَّهِ وَٱللَّهُ يَسْمَعُ تَحَاوُرَكُمَآ ۚ إِنَّ ٱللَّهَ سَمِيعٌۢ بَصِيرٌ " [2] وفي قوله تعالى: "يَـٰٓأَيُّهَا ٱلرَّسُولُ بَلِّغْ مَآ أُنزِلَ إِلَيْكَ مِن رَّبِّكَ ۖ وَإِن لَّمْ تَفْعَلْ فَمَا بَلَّغْتَ رِسَالَتَهُۥ ۚ وَٱللَّهُ يَعْصِمُكَ مِنَ ٱلنَّاسِ ۗ إِنَّ ٱللَّهَ لَا يَهْدِى ٱلْقَوْمَ ٱلْكَـٰفِرِينَ"[3]، والشكوى عُرفت بأنّها: " إفصاح المجني عليه أو من يمثله قانونا خلال مدة محددة إلى الجهات المختصة عن رغبته في تحريك الدعوى الجزائية قبل المتهم متظلما من جريمة وقعت عليه تكون خاضعة لقيد الشكوى"[4].

---

[1] Alex Black, Karen Lumsden and Lee Hadlington, Why Don't You Block Them Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime, From a book of, Karen Lumsden · Emily Harmer Online Othering Exploring Digital Violence and Discrimination on the Web This Palgrave Macmillan Springer Nature Switzerland AG, 2019, p360.

[2] سورة المجادلة الآية 1.

[3] سورة المائدة الآية 67.

[4] عبد القادر قائد سعيد المجيدي، شكوى المجني عليه كقيد من قيود تحريك الدعوى الجزائية في القانون اليمني والقانون الجزائري عمل مقدم لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 1، الجزائر، الموسم الجامعي 2014/2013 ص14.

أمّا التبليغ فعُرف بأنّه: "إخطار إلى السلطات العامة بوقوع جريمة من أي شخص معلوم كان أو مجهول وقد يكون مكتوبا أو شفهيا"[1]، وكنتيجة حتمية سواء بالنسبة للشكاوي أو التبليغات وصول معلومات لضباط لشرطة القضائية تفيد بوقوع جريمة أو جرائم معاقب عليها ضمن قانون العقوبات أو ضمن قوانين خاصة أخرى.

إنّ المشرع الجزائري عندما يستلزم في جريمة ما ضرورة التقدم بشكوى من المجني عليه فلابد وأن يترتب عنه أثر إجرائي معين، أنّه لا حرية للنيابة العامة في اتخاذ ما تشاء من إجراءات تتعلق بالجريمة موضوع الشكوى إلاّ بعد التقدم بها وإلاّ كانت إجراءاتها معرضة لجزاء البطلان، هذا الأثر لا يترتب على المرحلة السابقة على تحريك الدعوى العمومية مرحلة جمع الاستدلالات التي يقوم بها ضباط الشرطة القضائية أين يجوز لهم اتخاذ هذه الإجراءات حتى ولو لم يتقدم الشاكي بشكواه[2].

هذا بالنسبة للجرائم المقيد تحريك الدعوى العمومية بشأنها بقيد شكوى المجني عليه، فما بالك بالنسبة للجرائم الأخرى التي تحرك فيها الدعوى العمومية من غير قيد الشكوى كما هو الحال بالنسبة للجرائم المعلوماتية، لذلك فإنّ مسألة تلقي الشكاوي والتبليغات في هذه الجرائم تعتبر من قبيل الإجراءات المساعدة والموفرة للجهد من أجل كشف هذه الجرائم والقبض على مرتكبيها في أسرع وقت ممكن.

فالجرائم المعلوماتية بشتى ألوانها ليس بمقدور أي شخص الإبلاغ عنها وإخبار السلطات المختصة بوقوعها ما لم تتوفر لديه القدرة على التعامل مع جهاز الحاسب الآلي ويستطيع إدراك الفعل غير المشروع، لذلك فعلى ضباط الشرطة القضائية أن يعوا بأن عملية تلقي البلاغات لا تزيد عن كونها مجرد

---

[1] تميم بن عبد الله بن سيف التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص (قذف . سب . تشهير) وفقا للشريعة الإسلامية والنظام السعودي والقانون القطري، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، السعودية، 2016، ص 140.

[2] عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط ثانية منقحة ومعدلة، دار بلقيس للنشر، الدار البيضاء الجزائر، 2016 ص190.

عملية مبدئية، الغرض الأساسي منها هو تكوين صورة أولية عن نوع الجريمة المعلوماتية وكيفية وقوعها وتقدير مدى الخسائر والأضرار التي قد تسببها.

هذا ويجب على ضابط الشرطة القضائية أن يقتنع بأنّ المبلغ أو الشاكي لا يستطيع الإجابة عن كافة الأسئلة الدائرة في ذهنه وأنّ المعلومات التي يتلقاها الضابط هي في الغالب على قدر كبير من الاهتمام، كما ويتخذ التبليغ عدة أشكال فقد يأتي كتابيا أو شفهيا كما مر معنا في التعريف السابق للتبليغ وقد يأتي رقميا، هذا الأخير الذي يتم بطريق شبكة الإنترنيت بسبيل موقع إلكتروني محدد ومخصص لتلقي البلاغات المتعلقة بالجرائم المعلوماتية على أن يكون المبلغ على دراية كافية بالجوانب الفنية بالحاسب الآلي، وذلك ليتمكن من تقديم المعلومات المفيدة لضباط الشرطة القضائية للوقوف على طبيعة الجريمة المعلوماتية بطريقة صحيحة تمكنهم[1] من مباشرة التحري والاستدلال بشأنها.

هذا وتخضع مسألة تلقي البلاغات من طرف ضباط الشرطة القضائية في الجزائر لقانون الإجراءات الجزائية[2] ضمن نص[3]الفقرة 1 من المادة 17 منه، والملاحظ أنّها تبقى في تأخر بخصوص تطوير وسائل تلقي البلاغات خاصة فيما يتعلق بالجرائم المعلوماتية[4]، كما يبقى الإبلاغ عن هذه الجرائم في الوقت المناسب النقطة الفاصلة في الوصول لمقترفيها كما أنّ إحجام المجني عليهم بالإبلاغ وتقديم شكوى عن

---

[1] طاهر محمود أبو القاسم، الجرائم المعلوماتية صعوبات التحقيق فيها وكيفية مواجهتها، د ط، المنظمة العربية للتنمية الإدارية القاهرة، مصر، 2019 ، ص 107 - 108.

[2] قانون رقم 01- 08 المؤرخ في 26 يونيو 2001 يعدل ويتمم الأمر رقم 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001.

[3] تنص الفقرة 1 من المادة 17 من قانون رقم 01- 08 المعدل والمتمم لق إ ج الجزائري، القانون السابق، بأنّه: " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية " .

[4] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، د ط، النشر الجامعي الحديث، تلمسان، الجزائر، 2018، ص65.

ارتكاب جريمة معلوماتية بحقهم يؤدي بالضرورة لتزايد هذا النوع من الإجرام أين يشعر الجناة بثقة كبيرة في عدم قدرة الأجهزة الأمنية على الوصول إليهم وتقديمهم للقضاء[1].

وبما أنّ تقديم الشكاوى والتبليغات تعتبر الخطوة الأولى لضباط الشرطة القضائية المختصون من أجل مباشرة التحري والاستدلال بشأن هذا النوع من الجرائم ذات الطابع الدولي، فقد أنشأ مركزا عالميا للشكاوى الخاصة بجرائم الإنترنيت، هذا المركز يعتبر من بين أهم المؤسسات التي ظهرت إلى الوجود في مجال مواجهة جرائم الإنترنيت تأسس سنة 1999 وتمت هيكلته بشكل رسمي سنة 2000 بولاية وست فرجينيا في الولايات المتحدة الأمريكية، مهمته تلقي شكاوي الشاكين في إطار جرائم الإنترنيت عبر العالم عن طريق الشبكة المعلوماتية وموقعه هو (www.ic3.gov).

هذا الموقع الأخير يتلقى الشكاوي من أي شخص في أي بقعة تغطيها شبكة الإنترنيت في العالم كما يعمل على التعاون مع مختلف المنظمات الدولية المتخصصة والوكالات الدولية المنخرطة في محاربة الجرائم المعلوماتية بما في ذلك الوكالات والجهات الخاصة بتطبيق القانون[2] كالمنظمة الدولية للشرطة الجنائية (الإنتربول) من خلال التبليغ الذي تقوم به عن هذه النوعية من الجرائم وتعقب مجرميها.

الفرع الثاني: جهود الإنتربول في مكافحة الجرائم المعلوماتية

مع انتشار الحواسب الآلية بشكل رهيب في المجتمع الحديث أصبحت وظيفة الشرطة تتزايد وتصعب، وأصبح معه المجرمين المعلوماتيين يسجلون معلومات كثيرة أثناء ارتكابهم لجرائمهم على جهاز الحاسب الآلي، هذه المعلومات يمكن استخدامها أحيانًا كدليل في سياق الإجراءات الجزائية لهذا لابد من أن تكون عناصر الشرطة متمكنة من تكنولوجيا المعلومات قبل المثول أمام المحكمة الجزائية، هذه التكنولوجيا التي هي في تطور مستمر بحيث ظهرت في السوق أجهزة كمبيوتر جديدة وأنظمة مختلفة

[1] طاهر محمود أبو القاسم، المرجع السابق، ص108.

[2] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر 2011، ص110.

تعد مصدرا للمشاكل التي تواجهها الآن السلطات الأمنية والقضائية، ولحلها وجب النظر في الممارسات والأساليب التي سيتم اعتمادها في مجال هذه الجرائم المعلوماتية[1].

هذا وتبقى مسألة مكافحة أساليب الجرائم المعلوماتية العابرة للحدود الدولية غير كافية إلاّ إذا كان هناك تعاون دولي على المستوى الإجرائي الجنائي يسمح من خلاله بالاتصال المباشر بين أجهزة الشرطة في مختلف الدول وذلك بطريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية وتعميمها وتنسيق العمل فيما بينها لضبط هؤلاء المجرمين، وقد تبلور هذا النوع من التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية[2] (الإنتربول Interpol).

الإنتربول أو اللجنة الدولية للشرطة الجنائية كما كانت تسمى في ما مضى لتصبح الآن باسم المنظمة الدولية للشرطة الجنائية الدولية، والتي تضم في عضويتها الآن أكثر من 192 عضو وهدفها تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال وتقديم الدعم الفني والميداني بمختلف أشكاله[3]، خاصة في مكافحة الجرائم المعلوماتية من خلال تعقب المجرمين المعلوماتيين وكذا الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود للمكونات المنطقية للحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال، للبحث عما قد تحويه من أدلة[4]على ارتكاب الجرائم المعلوماتية.

هذه المعلومات ومختلف البيانات تعمل المنظمة على تبادلها بين الدول الأطراف، كما تتعاون على ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأعضاء من خلال مدها بالمعلومات المتوفرة الموجودة

---

[1] Liang Jiansheng, Criminalite informatique, Rapport de stage Travail soumis pour l'obtention d'un Diplome Professionnel superieur en Sciences de l' information et des Bibliotheques, Ecole Nationale Superieure des Sciences de 1'information et des Bibliotheques, lion, France, 1999, p57.

[2] طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، د ط، دار الجامعة الجديدة الإسكندرية، مصر، 2015، ص565.

[3] تعريف الإنتربول، عن الموقع الرسمي للإنتربول https://www.interpol.int/ar/3/3، بتاريخ 2021/03/15.

[4] غانم مرضي الشمري، المرجع السابق، ص 96.

على إقليمها، ذلك أنّ عضو الإنتربول من باب احترام السيادة الوطنية للدول[1] لا يستطيع القيام بنفسه بإجراء القبض على المجرمين المعلوماتيين لأنّه من اختصاص أجهزة الشرطة للدولة الطرف المتواجد على إقليمها هؤلاء المجرمين.

لكن هذا الدور المهم الذي تقوم به الإنتربول يلزمه تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على اتفاقيات فيما بينها، بحيث إذا ما اكتشفت شرطة دولة ما أنّ أحد الجرائم المعلوماتية قد تم ممارسته عبر شبكة الإنترنيت من خلال موقع موجود خارج حدودها فإنّها تقوم بالإبلاغ عنها إلى شرطة الدولة التي تم منها البث، هذه الأجهزة يجب أن يوكل إليها أيضا مهمة تلقي البلاغات التي يكون محورها متعلقا بالجرائم المعلوماتية وأن يكون من اختصاصها اتخاذ الإجراءات القانونية المناسبة[2] وتنفيذ التدابير الأمنية والوقائية مخافة استفحالها.

وهو الأمر الذي قامت به مجموعة الدول الثمانية (g8) أين أنشأت شبكة نقاط اتصال وطنية تضم متخصصين في مجال التحقيقات المتعلقة بمعالجة البيانات من أجل مكافحة الجرائم المعلوماتية وتعزيز التعاون بين أعضائها الذي يفوق عددهم الخمسين عضو على غرار نموذج الإنتربول[3]، هذا مع إمكانية تعاملها مع مختلف الجرائم المتعلقة بالتكنولوجيا الفائقة التطور بمستوى عالي من المهارة ولتوافر إمكانية المحافظة على الأدلة الموجودة في الوسائط الإلكترونية من الضياع أو التلف.

أمّا على المستويين العربي والإفريقي، فالأول من خلال مجلس وزراء الداخلية العرب أُنشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة للدول الأعضاء في مجال ملاحقة الجريمة ومجرميها في حدود القوانين والأنظمة المعمول بها في كل دولة عضو، مع تقديم المعونة في مجال

---

[1] محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2018، ص216.

[2] طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، المرجع السابق، ص566.

[3] محمد كمال شاهين، المرجع السابق، ص216.

دعم وتطوير أجهزة الشرطة في هذه الدول[1]، أمّا الثاني فقد اتخذ مكتب الممثل الخاص للإنتربول لدى الاتحاد الأفريقي من أديس أبابا (أثيوبيا) مقراً له، أين يتناول مع الاتحاد الإفريقي المسائل المتعلقة بالتحديات التي تواجهها إفريقيا في مجال تطبيق القانون، بحيث تتعاون المنظمتان على تمتين التعاون بين أجهزة الشرطة الإفريقية ومعالجة هذه التهديدات من خلال تبادل الموارد والخبرات بل ومحاولة تأمين استجابة مشتركة تترك أثراً أكبر[2].

لذلك فإنّ هذه الصورة من التعاون الأمني تعد من بين أهم الصور في مجال مكافحة الجرائم المعلوماتية خاصة وأنّ أجهزة العدالة الجزائية في جميع الدول ليست بنفس المستوى والإعداد من ناحية الإمكانيات البشرية والتقنية، ولأنّ هذه الجرائم يصعب تتبع مرتكبيها والتنقيب عن الأدلة الإلكترونية فيها، وكذلك يصعب القيام فيها بالتفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال، فإنّه يتطلب معه القيام ببعض العمليات الشرطية والأمنية والتقنية المشتركة لمواجهة ذلك ويؤدي بالضرورة إلى زيادة الخبرات والمهارات للقائمين على مكافحة هذه النوعية من الجرائم[3].

الفرع الثالث: القيام بالتحري والاستدلال عن الجرائم المعلوماتية

تاريخا قد كان العديد من العاملين في مجال العدالة الجنائية يكرهون تخصيص مواد خاصة لجرائم التكنولوجيا العالية، حتى أنّهم لم يبدوا رغبة كبيرة في إجراء التحقيقات المتعلقة بالحواسيب والتكنولوجيا، وربما يرجع ذلك لشعورهم أن جرائم التكنولوجيا المتقدمة لم تكن مشكلة في ولايتهم القضائية، لكن واقع الحال المتمثل في مدى خطورتها وحجم خسائرها جعل منها أمرا محسوما وألزم

[1] غانم مرضي الشمري، المرجع السابق، ص97.

[2] الإنتربول والإتحاد الإفريقي، عن الموقع الرسمي للإنتربول https://www.interpol.int/ar/5/3/3، بتاريخ 2021/03/15.

[3] أسامة العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، مجلة الحقوق، العدد 4، كلية الشريعة والدراسات الإسلامية جامعة الكويت، الكويت، 2015، ص126.

الأنظمة التشريعية بفرض الحماية القانونية لهذه التقنية[1]، فكل من التكنولوجيا الجديدة والتقدم التكنولوجي وتطوير الويب تم تحديدها الآن على أنّها تخلق مخاطر متزايدة على الضحايا المعلوماتيين هذه المخاطر لم يتم تصميم أدوات خاصة بها لمواجهتها، الأمر الذي يثير عدة تحديات تقابل عمليات التحقيق والملاحقة القضائية لهذه المخاطر.

لذلك فإنّ ضرورة معرفة ضباط الشرطة القضائية وفهمهم للتكنولوجيا التي يستخدمها المجرمون المعلوماتيين وكذا التشريعات وبروتوكولات سلامة الضحايا المعلوماتيين هي كلها تحديات في عملية التحقيقات الأولية[2]، هذا التحول المحتوم في مسار التشريعات العقابية والإجرائية من التقليدي المادي إلى المستحدث الرقمي لم يكن بالسلاسة المعتادة وذلك بفعل الطبيعة الخاصة للجرائم المعلوماتية التي تعتمد على أساليب ووسائل خاصة والتي تنتج عنها دلائل من نوع خاص، وكلها معطيات يستلزم أن تكون تحت مجهر رجال البحث و التحقيق في مجال متابعة مرتكبيها[3].

إنّ المتطلع للتحقيق في الجرائم المعلوماتية والتحقيق في الجرائم الأخرى يلاحظ وجود تشابه كبير بينها من حيث الإجراءات إلاّ أنّها تتفرق في العديد من النقاط التقنية، الأمر الذي يستدعي تطوير أساليب التحقيق الجنائية وإجراءاتها بصورة تتلاءم مع هذه الخصوصية، فالتحقيق في هذا النوع من الجرائم يتطلب السرعة والدقة وكذا الدراية الواسعة من قبل ضباط الشرطة القضائية لأنّ أغلب الإجراءات تتم في بيئة رقمية افتراضية سرعان ما تتغير ويضمحل معها الدليل[4] ويفلت معها الجاني من المتابعة

---

[1] Robert moore, Search and Seizure of Digital Evidence, LFB Scholarly Publishing, New York United States of America, 2005, p17.

[2] Brianna O'Shea, Roberta Julian, Jeremy Prichard and Sally Kelty, Challenges in Policing Cyberstalking: A Critique of the Stalking Risk Profile in the Context of Online Relationships, From a book of, Karen Lumsden · Emily Harmer, The previous reference, p340.

[3] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، عمل مقدم لنيل شهادة الدكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، الموسم الجامعي 2016/2015. ص108.

[4] ناني لحسن، المرجع السابق، ص52.

القضائية، هؤلاء الضباط وطبقا لنص المادة 12 من ق إ ج الجزائري[1] مختصين بإجراء التحريات والبحث اللازمة للكشف عن مثل هذا النوع من الجرائم وجمع الأدلة التي لها علاقة بها والبحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي.

هذا ويقصد بالتحريات التثبت من الوقائع التي تصل إلى علم ضباط الشرطة القضائية بجمع كافة القرائن الموصلة إلى الحقيقة نفيا أو إثباتا لواقعة معينة يفترض أنّها تشكل جريمة جزائية[2]، هذا ويعمل هؤلاء الضباط على استقصاء الجرائم والبحث عنها ويشمل ذلك البحث على الركن الشرعي أين يتحقق الضابط من أن الفعل المرتكب يشكل جريمة، فيتحقق من ركنيها المادي والمعنوي ويتحقق كذلك من ظروف ارتكاب الجريمة والبحث عن الفاعل من خلال تحديد هوية المشتبه فيهم[3].

فعموما عندما تتجاوب الشرطة القضائية مع الجرائم المعلوماتية التي وقعت بالفعل نسميها ردة فعل فالغالبية العظمى من التحقيقات ذات طبيعة تفاعلية، حتى أن تقرير الأمم المتحدة نفسه يقر بأنّ نسبة الجرائم المعلوماتية المكتشفة من خلال التحقيقات المسبقة كانت منخفضة، على الرغم من أنّ بعض البلدان تركز على العمليات السرية أو المسبقة[4].

وعليه يجب أن يبدأ التحري في الجرائم المعلوماتية مباشرة بعد الإبلاغ عن أي نشاط إجرامي مزعوم، كما يجب إنجاز العديد من العمليات الممثلة في مختلف التقارير والاحتواء وكذا التحليل والاستئصال في أقرب وقت ممكن بعد الهجوم، وتنظيم فريق الاستجابة للطوارئ الحاسوبية مع صياغة خطة الاستجابة للحوادث قبل الهجوم، هذه الخطة ستساعد في تحديد هدف التحقيق وستحدد كل

---

[1] الأمر رقم 66- 155 المؤرخ في 8 يونيو 1966 يتضمن ق إ ج الجزائري، ج ر السنة الثالثة، العدد 48، المؤرخة في 10 يونيو 1966.

[2] عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية في مكافحة جرائم بطاقات الائتمان الإلكترونية والتعاون الأمني الدولي حيالها، المرجع السابق، ص113.

[3] علي جبار الحسيناوي، المرجع السابق، ص119.

[4] Shipley todd, bowker art, investigating internet crimes : in introduction to solving crimes in cyberspace, Waltham, MA : Syngress. 2014, P253.

خطوة من خطوات عملية التحقيق، كما يجب أن تكون جزءًا من سياسة أمن الكمبيوتر الشاملة للشركات أين تحدد الخطة متطلبات الإبلاغ ومستويات الخطورة والمبادئ التوجيهية لحماية مسرح الجريمة والحفاظ على الأدلة.

لذلك فإنّ استخدام الشركات لفريق الاستجابة للطوارئ الحاسوبية لا يقدر بثمن، وذلك نظرًا للتعقيدات العديدة لأي جريمة معلوماتية[1]، ومن المفيد للغاية أن يكون هناك مجموعة واحدة على دراية تامة بخطة الاستجابة للحوادث للاتصال بها، على أن تكون هذه المجموعة ذكية من الناحية الفنية وعلى دراية في مجال التحقيقات القانونية وسياسة أمن الشركة (خاصة خطة الاستجابة للحوادث) ومستويات خطورة الهجمات المختلفة وعلى دراية من موقف الشركة أثناء نشر المعلومات والكشف عنها.

الفرع الرابع: القيام بإجراء المراقبة

يقصد بالمراقبة في الفقه القانوني عملية وضع شخص أو أماكن أو وسائل نقل أو مواد تحت رقابة سرية ودورية بهدف الوصول إلى معلومات لها علاقة بالشخص محل الاشتباه أو بأمواله أو بالنشاط الذي يقوم به[2]، هذه المراقبة تتنوع وسائلها وتتعدد صورها وهو ما يزيد من خطر المساس بخصوصية الإنسان وحياته وحرياته لذلك يتدخل المشرع من خلال نصوصه الآمرة ويحظر استخدام هذه الوسائل في بعض الأحيان وينظم استخدامها في أحيان أخرى بطريقة تكفل حماية الحق في الخصوصية[3].

---

[1] Welch Thomas, Computer crime investigation and computer forensics Information Systems Security, Vol. 6, Edition 2, Summer97, Texte intégral HTML.

[2] خلفي عبد الرحمان، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط ثالثة منقحة ومعدلة، دار بلقيس للنشر والتوزيع، الجزائر 2017، ص101.

[3] أشرف محمد إسماعيل، أثر المراقبة الإلكترونية على حق العامل في الخصوصية دراسة مقارنة، ط أولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2017، ص87.

هذا وقد تأتي المراقبة عادية أي مباشرة كتلك التي نص عليها المشرع الجزائري في ق إ ج أين يمارس فيها ضباط الشرطة القضائية اختصاصهم عبر كامل الإقليم الوطني وقد تأتي هذه المراقبة بشكل إلكتروني عن طريق وضع ترتيبات تقنية مسبقة في مكان يرتاده الشخص المشتبه فيه.

أولا: المراقبة العادية

لقد نص المشرع الجزائري على هذا الإجراء وجعله من اختصاص ضابط الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية عند إخباره، بحيث يجوز له وتحت سلطته أعوان الشرطة القضائية أن يقوم بعملية المراقبة عبر كامل الإقليم الوطني للأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب جرائم خطيرة حددت على سبيل الحصر، والتي كان من بينها نوع من أنواع الجرائم المعلوماتية والمتمثلة في جريمة المساس بالأنظمة المعالجة للمعطيات، لهذا يجوز لضابط الشرطة القضائية مراقبة أشخاصها ومراقبة نقل ووجهة الأشياء أو الأموال أو المتحصلات من ارتكاب هذه الجريمة أو التي قد تستعمل في ارتكابها[1].

ثانيا: مراقبة الاتصالات الإلكترونية

نص عليها المشرع ضمن القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر، بحيث يقوم ضابط الشرطة القضائية وبأمر من السلطات القضائية المختصة بمراقبة الاتصالات الإلكترونية لمجرد توفر معلومات تفيد بالاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني بل وحتى لمقتضيات التحريات لأي نوع من الجرائم المعلوماتية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء لهذا النوع من المراقبة[2]، هذا الإجراء يعتبر كأحد أساليب البحث والتحري الخاصة والذي سنتطرق له بشيء من التفصيل في العناصر اللاحقة.

---

[1] المادة 16 مكرر من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] المادة 4 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر رقم 47، المؤرخة في 16 أوت 2009.

المطلب الثالث: الإجراءات المتبعة في حالة التلبس بالجرائم المعلوماتية

بالرغم من أنّ القوانين المقارنة عددت حالات التلبس بالنّص عليها صراحة، إلاّ أنّها لم تستقم على ذات الطريقة في تحديدها، كما أنّ بعضها لم يحدد حالاتها كما هو الحال بالنسبة لقانون الإجراءات والمحاكمات الجزائية الكويتي رقم 17 لسنة 1960 الذي عالجها في إطار ما سماه بالجريمة المشهودة من خلال تنظيمه لإجرائي القبض والتفتيش[1]، على عكس المشرع الجزائري الذي حدد حالاتها، بحيث سمح لضابط الشرطة القضائية في حالة وقوع جريمة متلبس بها ويعاقب عليها القانون على الأقل بعقوبة الحبس بأن يخطر وكيل الجمهورية وينتقل على الفور بدون تمهل بحيث يتخذ جميع التحريات اللازمة[2].

حالة التلبس هذه بيّن المشرع الجزائري حالاتها وبيّن مختلف سلطات ضباط الشرطة القضائية فيها من خلال ق إ ج والتي سنرى إسقاطاتها على الجرائم المعلوماتية.

الفرع الأول: حالات التلبس وإسقاطاتها على الجرائم المعلوماتية

التلبس مصطلح قانوني يستخدم لوصف الحالة التي يتم فيها القبض على المجرم أثناء ارتكابه للجريمة أو الحالة التي يكون فيها الفعل المجرم قد حدث مؤخرا عندما تشهد الأدلة المقنعة على جرم صاحبه[3]، هذا ولقد اعتاد فقهاء القانون الجنائي على التفرقة كأصل عام بين حالتين من التلبس هما حالة التلبس الفعلي وهي حالة متصلة بظروف الزمان والمكان عندما يضبط الجاني حال قيامه بتنفيذ

---

[1] أشرف محمد عبد القادر سمحان، كفاية المظاهر الخارجية للتلبس للنهوض بدلائل الاتهام والآثار التي يرتبها القانون على توافرها مجلة دراسات علوم الشريعة والقانون، المجلد 46، العدد 3، كلية الشريعة والقانون، جامعة الجوف، السعودية، 2019 ص353.

[2] المادتين 42 و55 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] Flagrant délit- Définition, À propos d'un site https://droit-finances.commentcamarche.com/faq/4146-flagrant-delit-definition, Date de lecture27/06/2020.

الجريمة أمّا الثانية فهي حالة شبيهة بالتلبس وهي تعتمد على الوقت والحال والآثار المتصلة بالمكان الذي ارتكبت فيه الجريمة وظروفها[1].

أمّا التلبس بالجريمة في التشريع الجزائري فيعبر عنها بستة حالات بيّنها المشرع من خلال ق إ ج والتي تتمثل في مشاهدة الجريمة وقت ارتكابها أو عقب ارتكابها وفي متابعة ومطاردة العامة للمشتبه فيه بالصياح وفي وجود أشياء مع المشتبه فيه أو آثار تفيد بارتكاب الجريمة وكذا اكتشاف الجريمة في مسكن[2] هذا ويرى بعض الفقهاء أن الحالات السابقة الذكر يمكن إسقاطها بمختلف صورها في نطاق الجرائم المعلوماتية بحيث تكون على الشكل الآتي؛

أولا: مشاهدة الجريمة المعلوماتية وقت ارتكابها

تمثل هذه الحالة التلبس الحقيقي وذلك أنّ يشاهد ضابط الشرطة القضائية الجريمة حال ارتكابها أي أن يدرك الأفعال المادية للجريمة أو الشروع فيها وينصرف لفظ المشاهدة لجميع الحواس فلا يقتصر على المشاهدة بالعين فقط، وهي تنطبق على حالة اكتشاف ضابط الشرطة القضائية أو المجني عليه للجاني أثناء قيامه باختراق شبكة معينة أو نظام معلوماتي أو قاعدة بيانات على شرط وجود الإمكانات الفنية لتتبع ومطاردة الجاني للتعرف عليه.

ثانيا: مشاهدة الجريمة المعلوماتية عقب ارتكابها

يقصد المشرع بلفظ عقب ارتكابها أن تكون الجريمة قد وقعت منذ لحظات قليلة وآثارها لا تزال باقية تشير إلى وقوعها بعد برهة قصيرة جدا، وهي تنطبق على المثال التالي أين يقوم صاحب محل الإنترنيت أثناء مراجعته للحاسوب عقب استخدامه من طرف الزبون وقبل مغادرة هذا الأخير المحل باكتشاف ملفات تثير الاشتباه وعند فتحها تبين أنّها تحتوي على صور دعارة.

---

[1] عبد الرزاق مقران، ضمانات المشتبه فيه أثناء حالة التلبس، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق جامعة قسنطينة 1، الجزائر، الموسم الجامعي 2014/2013، ص28-29.

[2] المادة 41 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

ثالثا: متابعة ومطاردة العامة المشتبه فيه بالصياح

والذي قد يصدر من المجني عليه بالذات وما هو إلّا وسيلة لتنبيه المارة أو رجال الشرطة القضائية لتتبع الجاني، والصياح ما هو إلاّ عبارة عن اتهام مباشر للجاني من قبل الناس الذين شهدوا وقوع الجريمة للمساعدة في إلقاء القبض على الفاعل[1]، هذا الصياح غير متصور في الجرائم المعلوماتية بسبب حدوث التتبع في عالم افتراضي ومع ذلك من الآراء من لا يشترط وقوع الصياح أثناء التتبع فقد يكون المجني عليه أخرس أو لا يستطيع الصياح فيكتفي بالإشارة فقط.

رابعا: وجود أشياء مع المشتبه فيه

والتي تدل على مساهمة الجاني في الجريمة سواء كانت هذه الأشياء أداة جريمة أو تحصل عليها من الجريمة بحيث تعد قرينة قوية ضد المشتبه فيه ودالة على ارتكابه لها ومشاركته فيها، كما يشترط أن تكون ذات صلة وثيقة بين وجودها مع المشتبه فيه وبين الجريمة والتي يجب أن تكون في وقت قريب جدا من اللحظة التي ارتكبت فيه، كحالة ضبط أشياء تقنية لدى المشتبه فيه تفيد بارتكابه لأحد الجرائم المعلوماتية أو كانت حاصل ارتكابه لها.

خامسا: وجود آثار أو أدلة تفيد بارتكاب الجريمة المعلوماتية

فإذا ما وجدت مثلا برامج خاصة بالمشتبه فيه والتي تركها في جهاز الحاسوب قبل مغادرته تدل على مساهمته في ارتكاب أحد الجرائم المعلوماتية وفي وقت قريب جدا من وقوع هذه الجريمة.

الفرع الثاني: شروط صحة التلبس في الجرائم المعلوماتية

كنا قد ذكرنا الحالات الستة التي تعبر عن التلبس بالجريمة وضربنا لها أمثلة في الجرائم المعلوماتية لكن لصحة العمل على أساسها يجب أن تتوفر على بعض الشروط المتمثلة في أن يكون التلبس سابقا لإجراءات التحقيق وما يترتب عنه من قبض على المتهم أو تفتيشه أو تفتيش منزله أو ضبط لأشياء ذات علاقة بالجريمة، ويشترط وجوب اكتشاف هذه الجريمة من طرف ضابط الشرطة القضائية أو أن

[1] خلفي عبد الرحمان، المرجع السابق، ص77-78.

يكون هذا الأخير قد بلغ بها ببرهة قصيرة من ارتكابها، ويشترط كذلك أن تكتشف بطريق مشروع والذي قد يأتي أحيانا بطريقة عرضية ليس لضابط الشرطة القضائية دخل فيها[1].

هذا الشرط الأخير الذي أثار في مجال الجرائم المعلوماتية مسألة مشروعية التخفي عبر الإنترنيت من طرف ضابط الشرطة القضائية باستعمال أسماء وهمية في غرف المحادثات وحلقات النقاش قصد الكشف عن هذه الجرائم وعن مرتكبيها، هذه المسألة عالجها المشرع الجزائري من خلال مصطلح التسرب بدل مصطلح التخفي، وهو إجراء جديد نظمه المشرع الجزائري والذي يمكن أجهزة البحث والتحري من الكشف عن المجرم المعلوماتي في البيئة الافتراضية ذات الطبيعة الخاصة، فإذا ما شاهد ضابط الشرطة القضائية المكلف بعملية التسرب جريمة معلوماتية متلبس بها يتخذ الإجراءات الاستثنائية المخولة له قانونا لأنّه يعتبر في حالة مشروعة.

من ناحية أخرى تثار مشكلة تحديد الوقت اللازم لقيام حالة التلبس، والذي يترك تقدير مسألته في الجريمة التقليدية لضابط الشرطة القضائية ولقاضي الموضوع بحيث يكون على الأقل في وقت قريب جدا من وقت ارتكابها[2] بدليل استعمال المشرع الجزائري لمصطلحات "مرتكبة في الحال أو عقب ارتكابها" و "في وقت قريب جدا من وقت الجريمة"، وهذا بخلاف تقدير الزمن اللازم في الجرائم المعلوماتية الذي يصعب تحديده بسبب طبيعتها الخاصة إذا ما كانت فيه ملاحقة.

الفرع الثالث: سلطات ضباط الشرطة القضائية أثناء التلبس بالجرائم المعلوماتية

في حالة تحقق حالة التلبس بالجرائم المعلوماتية وبالرغم من صعوبة الأمر كما أشرنا إليه سابقا فإنّ القانون أتاح لضابط الشرطة القضائية سلطات معينة لا تتاح له في الحالة العادية من ارتكاب مثل هذا النوع من الجرائم، وهذه السلطات تنقسم بدورها إلى قسمين سلطات ذات طابع استدلالي وأخرى ذي طابع التحقيق.

---

[1] لويزة نجار، المرجع السابق، ص322.

[2] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص356.

أولا: سلطات ضابط الشرطة القضائية ذات الطابع الاستدلالي

1-إخطار وكيل الجمهورية بوقوع الجريمة

على ضابط الشرطة القضائية بمجرد تبليغه بوقوع جناية أو جنحة متلبس بها كما الحال بالنسبة للجرائم المعلوماتية أن يخطر وكيل الجمهورية التابع له إقليميا فورا مع تبيان قدر الإمكان زمان ومكان وقوعها وكل التفاصيل الأولية المتعلقة بها.

2-الانتقال فورا إلى مكان وقوع الجريمة المعلوماتية للقيام بالمعاينات

بحيث يتوجه فورا[1] وبدون تردد إلى مسرح الجريمة بمجرد تلقيه بلاغ بارتكابها دون اعتداد بالوقت الذي مضى بين الوصول وبين وقت ارتكاب الجريمة، وأول ما يقوم به الضابط عند وصوله لمسرح الجريمة هو إثبات حالتها أين يقوم بوصف مكانها والأشياء والوسائل التي استخدمت في ارتكابها وحالة المجني عليه، هذا الانتقال الذي قد يكون افتراضيا بواسطة شبكة الانترنيت وهو ما سنوضحه من خلال العناصر اللاحقة.

3- المحافظة على حالة مكان الجريمة المعلوماتية ومختلف آثارها

يستطيع ضابط الشرطة القضائية أن يمنع أي شخص لا علاقة له بالتحقيق من الاقتراب من المكان إذا ما خشي تغيير أماكن الجريمة ونقل الأشياء من المكان التي وجدت فيه[2] وفي سبيل ذلك له أن يعين عون يسهر على المحافظة على آثار الجريمة، كما يضع الأختام على الأماكن التي بها آثار أو أشياء تفيد التحقيق في الكشف عن الحقيقة.

---

[1] المادة 42 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] عمر خوري، سلطات الشرطة القضائية في مواجهة الجريمة المتلبس بها، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 51، العدد 3، كلية الحقوق، جامعة الجزائر، سبتمبر 2014، ص28.

4- ضبط الأشياء

على ضابط الشرطة القضائية ضبط كل شيء له علاقة بالجريمة المعلوماتية من مستندات وأدوات وتقنيات تفيد في عملية التحقيق وفي إظهار الحقيقة[1]، كما يجوز له عرضها على المشتبه فيهم للتعرف عليها ومعرفه ما إذا كانت لها صله بالجريمة أم لا.

5- تحرير محضر

يجب على ضابط الشرطة القضائية أن يحرر محضرا في الحال وفي نفس المكان الذي وقعت فيه الجريمة المعلوماتية والذي يجب أن يتضمن كل الإجراءات والأعمال التي قام بها، كما ترقم صفحاته ويؤشر على كل منها ويتم التوقيع على هذا المحضر في الأخير ليرسل بعد ذلك إلى وكيل الجمهورية[2].

ثانيا: سلطات ضابط الشرطة القضائية ذات طابع التحقيق

تعتبر الإجراءات ذات طابع التحقيق في الأصل من اختصاص قاضي التحقيق إلاّ أنّ القانون خول لضباط الشرطة القضائية عندما يكونون بصدد جناية أو جنحة متلبس بها، القيام ببعض هذه الإجراءات، وذلك لاعتبارات عملية بحتة متعلقة بالخشية من ضياع آثار الجريمة، وتتمثل مجمل هذه السلطات في؛

1- الأمر بضبط المشتبه فيه واقتياده إلى أقرب مركز

والذي يقصد منه تقييد المشتبه فيه واقتياده إلى أقرب مركز[3] للشرطة أو الدرك.

2- الأمر بعدم المبارحة أو عدم المغادرة

وهو الأمر الذي يوجهه ضابط الشرطة القضائية المتواجد بمكان ارتكاب جريمة متلبس بها إلى شخص أو عدة أشخاص يتواجدون في نفس المكان لغرض التعرف على هوية الشخص وسماع أقوال من حضر الجريمة وكذا جمع المعلومات اللازمة بشأن الجريمة المتلبس بها.

---

[1] المادة 45 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] عمر خوري، المرجع السابق، ص29.

[3] المادة 61 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

3- الاستعانة بالخبراء

يمكن لضباط الشرطة القضائية الاستعانة بهم من أجل المعاينات التي لا تقبل التأخير وذلك بغرض إظهار الحقيقة[1]، على أن يؤدي الخبراء اليمين قبل بدء عملهم كما أنّهم مطالبون بكتمان السر المهني.

4- إمكانية الاستعانة بوسائل الإعلام لتوجيه نداء للشهود

سواء بطريقة توجيه نداء للجمهور بقصد الحصول على معلومات أو شهادات قد تفيد التحريات الجارية، أو بطريقة نشر إشعارات أو أوصاف أو صور تخص شخصا يجري البحث عنه أو متابعته وذلك بعد إذن من وكيل الجمهورية[2].

5- التوقيف للنظر

والذي يهدف من ورائه منع المشتبه فيه من الهروب أو منعه من إتلاف الأدلة التي قد تظهر في مسرح الجريمة أو في مكان قريب منها، كما قد يمنع المشتبه فيه من الاتصال بالشهود والتأثير عليهم وغير ذلك من الإجراءات الاحترازية التي تساعد للوصول إلى الحقيقة[3].

هذا ويعتبر هذا الإجراء من أخطر الإجراءات الذي يقوم به ضباط الشرطة القضائية لذا فإنّ اللجوء إليه يكون مع إطلاع وكيل الجمهورية في حينه مع تقديم تقرير عن دواعي القيام بهذا الإجراء[4] والذي لا يكون إلاّ بمناسبة الجرائم المتلبس بها أو عند وجود قرائن قوية تعزز قيام الاشتباه لدى شخص محل الاحتجاز، هذا الإجراء الذي يمكن أن يمدد مرة واحدة بمناسبة الجرائم المعلوماتية[5] والذي يمكن

---

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص353.

[2] المادة 17 من أمر رقم 15-02، المؤرخ في 23 يوليو 2015، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري ج ر رقم 41، المؤرخة في 29 يوليو 2015.

[3] خلفي عبد الرحمان، المرجع السابق، ص84-85.

[4] الفقرة 01 من المادة 51 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[5] المادة 51 الفقرة 5 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

لوكيل الجمهورية من خلاله اللجوء للمحادثة المرئية عن بعد في حالة التمديد هذه، على أن يشار إلى ذلك في المحاضر المحررة[1].

6- القيام بتفتيش المساكن

وذلك في ما يتعلق بمساكن الأشخاص الذين ارتكبوا أو من المحتمل أنّهم قد ساهموا في ارتكاب إحدى الجرائم المعلوماتية، والذين قد يحوزون على أوراق أو أشياء لها صلة بالأفعال، ولما كان الأمر متعلق بالجرائم المعلوماتية فهناك بعض التشريعات المقارنة كالتشريع المصري وإن كانت في الأصل لا تسمح لضابط الشرطة القضائية بتفتيش منزل المتهم بناء على حالة التلبس بارتكاب الجريمة، فقد سمحت لهذا الأخير في أحوال التلبس بالجنايات والجنح المعلوماتية أن يأمر بالقبض على المتهم المعلوماتي الذي توجد دلائل كافية على اتهامه وهذا القبض يجيز التفتيش[2].

أما بالنسبة للتشريع الجزائري وبخصوص إحدى الجرائم المعلوماتية فقد أجاز لضابط الشرطة القضائية إجراء التفتيش في أي محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل[3] بناء على إذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق مع وجوب استظهار هذا الإذن قبل الدخول للمسكن أو الشروع في عملية التفتيش[4]، وعند الانتهاء من عملية التفتيش هناك بعض اللمسات الأخيرة التي يجب مراعاتها والتي تكمن في ضرورة كتابة بروتوكول يوصف فيه كيف كان هذا التحقيق وذكر نتائجه، بعد ذلك يجب على الفريق الذي يجري عملية التفتيش من ضباط شرطة قضائية

---

[1] الفقرة 04 من المادة 441 مكرر1 من الأمر رقم 20-04 المؤرخ في 30 غشت 2020، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[2] طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، المرجع السابق، ص414.

[3] المادة 47 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[4] المادة 44 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

وخبراء آخرين مناقشة كيفية إجراء هذه العملية من الناحية المثالية على أن يتم ذلك وفق منظور الخبير[1] المعلوماتي ووفق عملية مستحدثة خاصة بذلك.

المبحث الثاني: إجراءات جمع الأدلة وتحريك الدعوى العمومية في الجرائم المعلوماتية

لا تزال الجرائم المعلوماتية في تزايد وتطور مستمر خاصة مع ما تقذفه كل يوم التكنولوجيا الحديثة من تقنيات وبرامج متطورة وذكية، هذه الجرائم كما تطرقنا إليها سابقا ونظرا لما تتمتع به من خصائص والتي تميزها عن باقي الجرائم التقليدية الأخرى من حيث طبيعتها وطريقة ووسائل ارتكابها كان لابد على مختلف التشريعات من النص على إجراءات متعددة ومختلفة تجمع بها مختلف الأدلة المبرزة لنسبة الضرر الذي تسببت فيه هذه النوعية من الجرائم والكاشفة لمرتكبيها على أدق وجه؛ هذه الإجراءات تنقسم بمجملها إلى إجراءات عادية تشترك فيها مع بقية الجرائم التقليدية الأخرى وإلى إجراءات خاصة تشترك فيها مع جرائم أخرى محددة حصرا وذات خطورة كبيرة.

المطلب الأول: الإجراءات العادية لجمع الأدلة في الجرائم المعلوماتية

إنّ تحصيل وجمع أدلة الإثبات هي ما يشغل عمل وتفكير ضابط الشرطة القضائية أثناء قيامه بمختلف التحريات حول جريمة ما، ولا يتأتى له ذلك كأول خطوة سوى بتفعيل مجموعة من الإجراءات العادية في شكل المعاينة والتفتيش والضبط وحتى الاستعانة بالخبراء، والتي هي عبارة عن إجراءات مستعملة ومستخدمة بشكل روتيني في جميع وشتى أنواع الجرائم بما فيها الجرائم المعلوماتية بمختلف أصنافها، حتى وإن كانت هذه الإجراءات فيما يتعلق بهذه الجرائم الأخيرة من ناحية خصوصيتها تثير أحيانا بعض الصعوبات والإشكالات التي تحتم على المتحرين فيها ضرورة تفعيلها بطريقة خاصة ومتقنة توازي في ذلك خصوصية النظام المعلوماتي وطبيعة المعطيات الموجودة داخله.

[1] Joakim Kävrestad, Fundamentals of Digital Forensics, second edition, Springer Nature Switzerland AG 2018, 2020, p77.

الفرع الأول: إجراء المعاينة في مكان المنظومة المعلوماتية

يقصد بالمعاينة عموما رؤية أماكن ارتكاب الوقائع الجنائية لدرجة فحص جسم المجني عليه والمتهم وإثبات ما يوجد بها من أثار، وعرفها جانب من الفقه بأنّها عملية مشاهدة وإثبات للحالة في مكان الجريمة[1]، والمعاينة لمسرح الجريمة ومكان الحادث تختلف من جريمة لأخرى ومن مكان لآخر وذلك بحسب نوع مسرح الجريمة وبحسب نوع الجريمة المرتكبة، فمسرح جريمة القتل يختلف عن مسرح الجرائم المعلوماتية وهو ما يلزم ضابط الشرطة القضائية أن يتبع في معاينته طريقة تناسب مسرح الجريمة وتناسب نوع الجريمة المرتكبة[2].

الملاحظ أن المشرع الجزائري لم يقدم تعريفا لإجراء المعاينة وإنّما اكتفى بسرد كيفية وروده، وذلك عندما يُبلَغ ضابط الشرطة القضائية بجناية أو جنحة في حالة تلبس فيخطر بها وكيل الجمهورية في ذات الحين، وينتقل فورا إلى مكان الجناية أو الجنحة ويتخذ جميع التحريات اللازمة أين يسهر على المحافظة على الآثار التي يخشى أن تختفي ويضبط كل شيء يمكن أن يؤدي إلى كشف الحقيقة مع عرضها على الأشخاص المشتبه في مساهمتهم في تلك الجناية للتعرف عليهم[3]؛ هذا في حالة الانتقال العادي لضابط الشرطة القضائية إلى مسرح الجريمة أين يرى جانب من الفقه أن المعاينة فيها جوازية وأنّها لا تتمتع في مجال كشف غموض الجرائم المعلوماتية بنفس درجة الأهمية التي تلعبها في مجال الجرائم التقليدية.

ذلك أن هذه الجرائم قلما يترتب على ارتكابها آثار مادية كما قد يتردد عدد كبير من الأشخاص على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها، مما يجعل من الفرصة كبيرة في تغيير أو إتلاف أو العبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في

---

[1] محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنيت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنيت د ط، الدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2017، ص120.

[2] محمد علي أحمد الكواري، مسرح الجريمة ودوره في كشف غموض الجريمة، أطروحة تخرج، كلية علوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2007، ص44.

[3] المادة 42 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

الدليل المستمد من هذه المعاينة[1]، لذلك على ضباط الشرطة القضائية إذا ما أرادوا الاعتماد على هذا المعاينة العادية أن يراعوا كل القواعد والإرشادات الفنية[2] حتى يكون الدليل المستمد من هذه المعاينة مساعد في الكشف عن الحقيقة ومتمتع بقوة إثبات يغني في المراحل اللاحقة لسير الدعوى العمومية.

والانتقال للمعاينة لا يتم بالضرورة عبر العالم المادي كما شرحنا سابقا فقد يتم الانتقال لمعاينة مسرح الجريمة عبر العالم الافتراضي أين يستطيع ضابط الشرطة القضائية القيام بعملية المعاينة من خلال حاسوبه الموجود بمكتبه أو من خلال اللجوء لمقهى الإنترنيت، ويمكنه كذلك اللجوء لمزود خدمة الإنترنيت والذي يعتبر من أفضل الأمكنة التي يستطيع من خلالها إجراء المعاينة، هذه الأخيرة التي تختلف في الجرائم المعلوماتية بسبب طبيعة الدليل الإلكتروني غير المرئي والقابل للمحو[3]والتي تلزم وتجبر كذلك ضباط الشرطة القضائية قبل الانتقال الافتراضي لمسرح الجريمة القيام بالخطوات التالية؛

---

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنيت، د ط، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008 ص230.

[2] تتمثل أبرز القواعد والإرشادات الفنية في:

– تصوير الحاسب ككل وكل الأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة.

– العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع

الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

– التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة وغير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

– التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.

– إعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق.

[3] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص325.

– الحصول على معلومات مسبقة عن مكان الجريمة وعن نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها فنيا.

– التأكد من تأمين وصلاحية الأجهزة والمعدات المرجح استعمالها في عملية المعاينة مع إعداد خريطة للموقع المتوقع الإغارة عليه.

– إعداد فريق متخصص من الخبراء ورجال الأمن والضباط مع إعطائهم وقتا كافيا للاستعداد الفني بطريق وضع خطة فعالة من أجل ضبط أدلة الجريمة وقت معاينتها.

– يجب توفير الاحتياجات المساعدة من أجهزة وبرامج[1] للاستعانة بها في عملية الفحص والتشغيل.

– العمل على ضمان عدم انقطاع التيار الكهربائي المفاجئ وما يسببه من محو المعلومات في الذاكرة وبالتالي اضمحلال كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة[2].

وعليه فإنّ نجاح عملية المعاينة ككل مرهون بمدى اختصاص ومعرفة ضباط الشرطة القضائية بالمعلوماتية عموما وبنظمها خصوصا ناهيك عن كيفية تشغيلها ووسائلها وتقنيات إساءة استعمالها من قبل مستخدميها، وكل هذا لا يتأتى سوى بالتكوين والتدريب الدوري لهم وتحديد معارفهم حتى يتسنى لهم اكتساب مهارات عالية في مجال الكشف عن هذه الجرائم.

الفرع الثاني: إجراءات تفتيش مكونات المنظومة المعلوماتية

يقصد بالتفتيش من الناحية القانونية البحث عن شيء له علاقة بالجريمة محل البحث والذي يفيد في الوصول إلى الحقيقة وهذا ما قد يتطلب إجراء البحث في محل له حرمة خاصة[3]، والتفتيش كإجراء

---

[1] مثل برامج معالجة الملفات (xtree pro gold) وبرامج النسخ (lap link) وبرامج إنتاج صور مطابقة عن القرص الصلب (Encase) ومثل حقيبة الأدلة الرقمية الذي تستخدمه المباحث الفدرالية الأمريكية.

[2] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص326.

[3] أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، د ط، دار الجامعة الجديدة الإسكندرية، مصر 2019، ص287.

يكون بحسب السلطة المخول لها القيام به فهو إجراء تحقيق إذا ما قامت به النيابة العامة أو قاضي التحقيق وهو إجراء من إجراءات الاستدلالات إذا ما قام به ضابط الشرطة القضائية، هذا الأخير في حالة وقوع جريمة معلوماتية وطبقا لقواعد ق إ ج الجزائري يجوز له القيام بإجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل ويكون بناء على إذن مسبق من وكيل الجمهورية المختص[1]، وقد يكون هذا التفتيش عن بعد كما نص على ذلك القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أين يجوز لضابط الشرطة القضائية الدخول إلى المنظومتين الآتيتين؛

أولا: منظومة تخزين معلوماتية

هذه المنظومة تعبر عن مختلف المنظومات التقنية التي تسمح بتخزين مختلف المعلومات المراد استغلالها فيما بعد ولعل أبرز هذه الإمكانيات الذاكرة (Ram and Rom) أقراص التخزين (Storage Disks) سواء الصلبة (Hard Disks) أو المرنة (Floppy Disks) او المدمجة (Dvd-Rom /cd- Rom) وكذلك محركات الأشرطة (Tape Drives)[2].

[1] الفقرة 4 من المادة 47 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] عن موقع echhands.wordpress.com/2012/10/12/وحدات-التخزين-في-الكمبيوتر--computer-storage-components/ بتاريخ 2021/07/06.

ثانيا: منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها

هذه المنظومات التقنية تسمح لضابط الشرطة القضائية بأن يمدد التفتيش وبسرعة إلى منظومة معلوماتية[1] أخرى أو إلى جزء منها إذا كانت هناك أسباب تدعو للاعتقاد بأنّ المعطيات[2] المبحوث عنها مخزنة في المنظومة الأخيرة[3] وأنّ هذه المعطيات يمكن الدخول عليها انطلاقا من المنظومة الأولى وذلك بعد إعلام السلطة القضائية المختصة مسبقا بذلك؛ أمّا إذا ما تبين بأنّ المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ويمكن الدخول إليها من المنظومة الأولى، فالحصول عليها لا يكون إلاّ بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

إنّ الإذن الممنوح لضابط الشرطة القضائية من قبل السلطة القضائية المختصة يبقى خاضع لقواعد ق إ ج الجزائري إلاّ في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ففي هذه الحالة يختص النائب العام بمنح إذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها لمدة 06 أشهر قابلة للتجديد من أجل القيام بإجراءات التفتيش داخل منظومة معلوماتية وذلك على أساس تقرير يبين فيه طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[4].

---

[1] المنظومة المعلوماتية عرفها المشرع الجزائري ضمن الفقرة ب من المادة 2 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ".

[2] المعطيات المعلوماتية عرفها المشرع الجزائري ضمن الفقرة ج من المادة 2 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: " أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ".

[3] منظومة تخزين معلوماتية من خلال استقراء نص المادة 2 من القانون 09- 04، القانون السابق، لعل المشرع الجزائري يقصد بها أي نظام منفصل أو مجموعة من الأنظمة متصلة مع بعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بتخزين المعطيات المعلوماتية.

[4] المادة 04 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر رقم 47، المؤرخة في 16 أوت 2009.

هذا وإجراء التفتيش الذي يقع على المكونات المادية (Hard Ware) لا يثير أي إشكال في تنفيذه لإمكانيته وسهولته، وهذه السهولة لأنّها تقع على هذه المكونات المادية المنصوص عليها في أغلب القوانين الإجرائية، أمّا إجراء التفتيش الذي يقع على المكونات المعنوية (Soft Ware) فيثير إشكالا في إمكانية تفتيشه كالبرامج والنظم الخاصة بالتشغيل وقواعد البيانات، هذه الأخيرة التي يمكن أن تنظم جريمة ما أو تخزن طريقة ارتكاب جريمة ما بواسطة الحاسب الآلي[1].

الفرع الثالث: إجراءات ضبط مكونات المنظومة المعلوماتية

يقصد بالضبط في القانون وضع اليد على شيء له علاقة بجريمة وقعت، هذا الإجراء يساعد في عملية الكشف عن الحقيقة وعن مرتكبي هذه الجريمة، أمّا عن طبيعته القانونية فقد يكون إجراء استدلال أو إجراء تحقيق وذلك بحسب الطريقة التي يتم بها وضع اليد على الشيء المتصل بالجريمة فإذا ما كان هذا الشيء الذي ضُبط تم ضبطه دون الاعتداء على حيازة قائمة فإنّه يكون بمثابة إجراء استدلال، أمّا إذا كان هذا الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته أصبح الضبط بمثابة إجراء تحقيق[2]، وإجراء الضبط يأتي كأثر مباشر لإجراء التفتيش فغاية هذا الأخير هو ضبط الأدلة المادية التي تفيد في كشف الجريمة[3].

لذلك وبحسب الأصل فإنّ إجراء الضبط لا يرد إلاّ على الأشياء المادية وهو ما يسهل من عملية ضبط أدلة الجريمة الواقعة على المكونات المادية للحاسب الآلي كرفع البصمات وكضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في عملية نسخه غير المشروع، وتبقى الصعوبة في الاستثناء وهي ضبط المكونات غير المادية أي الوسائل الفنية المستخدمة في البرامج مثل الفيروسات وتبقى الصوبة

[1] علي جابر الحسيناوي، المرجع السابق، ص116.

[2] عبد العال الدريبي، محمد صادق إسماعيل، المرجع السابق، ص320.

[3] طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، المرجع السابق، ص418.

كذلك في ضبط بيانات الكمبيوتر (Data)[1] لعدم وجود أي دليل مرئي في هذه الحالات وكذا لسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات[2].

وبالرجوع للتشريع الجزائري وكأصل عام فقد نُص على هذا الإجراء ضمن ق إ ج بحيث أوجب على ضابط الشرطة القضائية في جميع الجرائم بما فيها الجرائم المعلوماتية أن يضبط كل ما يمكن أن يساعد في إظهار الحقيقة[3] ولعل الضبط المقصود به في هذه الحالة هو ضبط المكونات المادية (Hard Ware)، أمّا فيما يخص ضبط المكونات المعنوية (Soft Ware) فقد نُص عليها ضمن قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتكون بطريقة نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية من قبل ضابط الشرطة القضائية الذي يقوم بالتفتيش، أين تكون هذه المعطيات قابلة للضبط والوضع في أحراز وفقا للقواعد المقررة في ق إ ج.

هذا ويسهر ضابط الشرطة القضائية الذي يقوم بالتفتيش على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها عملية الضبط كما يجوز له استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات محل الضبط قصد جعلها قابلة للاستغلال لأغراض التحقيق بشرط أن لا تؤدي هذه التقنية إلى المساس بمحتوى المعطيات[4]، أمّا في حالة استحالة الضبط لأسباب تقنية يتعين على ضابط الشرطة القضائية استعمال التقنيات اللازمة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية

---

[1] Data مصطلح إنجليزي يستخدم في قطاع الاتصالات لوصف البيانات التي يمكن تداولها عبر شبكة هاتف أو شبكة كمبيوتر باستثناء البيانات الصوتية.

[2] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنيت، المرجع السابق، ص237.

[3] الفقرة 3 من المادة 42 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 6 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

ومنع نسخها[1]، ويمكنه أن يأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة بطريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[2].

الملاحظ أنّ عملية ضبط المكونات المعنوية ليست بالأمر الهين مقارنة مع ضبط المكونات المادية فالمسألة أكثر تعقيدا وتركيبا لأنّها تثير مشكلة لا مادية بيانات الحاسب الآلي كما ذكر في التقرير العام لمؤتمر (A I D P)[3]، هذا وقد تعددت الآراء حول إجراء الضبط إن كان يشمل المكونات المادية فقط أو يتعداه ليشمل كذلك المكونات المعنوية مثل ما تبناه المشرع الجزائري ضمن القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الرابع: إجراء الخبرة المعلوماتية

تعتبر الخبرة في مجال الجرائم المعلوماتية من بين طرق الإثبات المباشرة وذلك نظرا لاتصالها بالواقعة المراد إثباتها ونظرا للطبيعة الخاصة للجرائم المعلوماتية، وتقارير الخبراء هي وثائق شاملة للغاية والتي يجب أن تُفَصل بالدقة وبالتحليل من خلال التساؤل هل قام الخبير بإجراء الفحص والتحليل فمثلا في إجراء الخبرة بالنسبة للحاسب الآلي الذي ارتكبت به الجريمة المعلوماتية على الخبير أن يوضح الوسائل التي استخدمها ويبين النتائج وشروط الاختبارات التي أجريت من أجل إدلائه بهذه الخبرة[4].

---

[1] المادة 7 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] المادة 8 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر رقم 47، المؤرخة في 16 أوت 2009.

[3] المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات والذي عقد بريو دي جانيرو بالبرازيل، الفترة من 4 إلى 9 سبتمبر 1994.

[4] Easttom Chuck. Taylor Jeff, Computer Crime, Investigation, and the Law eBook Academic Collection Trial Boston, USA, 2011, p333.

هذا ولقد حدد المشرع الجزائري هدف الخبرة ضمن نص المادة 125 من قانون الإجراءات المدنية والإدارية[1] وقال بأنّ الخبرة تهدف إلى توضيح واقعة مادية تقنية أو واقعة علمية محضة للقاضي والخبرة في مجال المساعدة القضائية من أقوى مظاهر تعامل سلطات الاستدلال والتحقيق وسلطات المحاكمة مع الواقعة الإجرامية[2]، والخبرة المعلوماتية لها أهلها ويطلق عليهم اسم الخبراء المعلوماتيين، هذا ويعرف الخبير في المجال المعلوماتي بأنّه كل شخص تعمق في دراسة عمل من الأعمال المعلوماتية وتخصص في مجاله فترة زمنية طويلة، هذه المدة أكسبته خبرة عملية حتى أصبح ملما بتفصيلاته مما جعله متفوقا على الشخص العادي وجعله قادرا على إبداء الرأي الإلكتروني الرقمي في الأمور المتصلة بهذا المجال والتخصص.

إنّ إجراء الخبرة في مجال الجرائم المعلوماتية اعتمده المشرع الجزائري في هذه المرحلة (مرحلة جمع الاستدلالات) ضمن ق إ ج أين يستطيع ضابط الشرطة القضائية إذا اقتضى الأمر إجراء معاينات لا يمكن تأخيرها بأن يستعين بأشخاص مؤهلين لذلك، وهؤلاء الأشخاص عليهم أن يحلفوا اليمين كتابة على إبداء رأيهم بما يمليه الشرف والضمير[3]، واعتمده كذلك ضمن القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بحيث يجوز لضابط الشرطة القضائية أن يكلف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة من أجل اتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة[4].

---

[1] القانون رقم 08- 09 المؤرخ في 25 فيفري 2008 المتضمن قانون الإجراءات المدنية والإدارية، ج ر رقم 21، المؤرخة في 23 أبريل2008.

[2] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص329.

[3] المادة 49 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 8 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر رقم 47، المؤرخة في 16 أوت 2009.

كما يستطيع تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدته وتزويده بكل المعلومات الضرورية لإنجاز مهمته[1]، والمشرع لم يحدد طبيعة الشخص فقد يكون شخصا طبيعيا أو شخصا معنويا كما قد يكون خبيرا أو شخصا عاديا يملك مهارات وقدرات عالية في مجال تكنولوجيا الإعلام والاتصال كمترجم المكالمات التي تتم باللغة الأجنبية وكالأعوان المسخرين[2] لوضع الترتيبات التقنية من أجل التحريات الخاصة (اعتراض المراسلات وتسجيل الأصوات والتقاط الصور).

هذا ويركز مجال الخبرة أساسا على استكشاف الأدلة الرقمية كرسائل البريد الإلكتروني والصور الرقمية وتاريخ الرسائل الفورية والإنترنت المستعرض والفيديو الرقمي وملفات الصوت وما إلى ذلك بل ويهتم حتى بعملية تفسيرها[3]، لذلك يعتبر الخبراء المعلوماتيين من أهم المساعدين لضباط الشرطة القضائية في مجال الجرائم المعلوماتية نظرا لما يقدمونه من أعمال، هذه الخبرة تعتبر من بين أهم مصادر الأدلة الجزائية المعلوماتية التي تساعد كثيرا القضاة في المراحل اللاحقة من الدعوى العمومية سواء في مرحلة التحقيق أو مرحلة المحاكمة.

هذا ويلاحظ ارتفاع في أهمية الخبراء المعلوماتيين في عصرنا الحالي نتيجة لازدياد الأساليب الإجرامية المعلوماتية الأمر الذي يتطلب أنواع متخصصة منهم في مجالات معلوماتية معينة[4]، لأجل

---

[1] الفقرة 6 من المادة 5 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] الأعوان المسخرين لأجل وضع الترتيبات التقنية طبقا لنص المادة 65 مكرر8 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006هم الأعوان المؤهلون لدى مصلحة واحدة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية.

[3] Aamo Iorliam, Fundamental Computing Forensics for Africam : A Case Study of the Science in Nigeria, Springer International Publishing, AG Switzerland,2018,p17.

[4] مصطفى محمد موسى، التحقيق الجنائي في الجرائم المعلوماتية، الطبعة الأولى، دار الكتب القانونية، مصر، 2009، ص221.

ذلك نص المشرع الجزائري على إنشاء هيئات مؤهلة تقوم بإجراء الخبرة الرقمية سواء بمناسبة إجراء تحقيق أو المساعدة على إجرائه وتتمثل هذه الهيئات في؛

أولا – المعهد الوطني للبحث في علم التحقيق الجنائي

هذا المعهد[1] يضم أقساما ومصالحا ومخابر جهوية للبحث في علم التحقيق الجنائي من بينها مصلحة الخبرات الخاصة بالدلائل التكنولوجية والتي تقوم بطلب من السلطات القضائية المختصة بتحليل الدلائل المادية إثر المعاينة والتحريات في ميادين الدلائل المعلوماتية وجرائم الكمبيوتر والبصمات الصوتية ومعالجة الصورة والإشارة واستغلال الهواتف المحمولة وإعداد تقارير الخبرة[2].

ثانيا – قيادة الدرك الوطني للمركز الوطني لمكافحة الجريمة المعلوماتية

الموجودة في " بئر مراد رايس" بالجزائر العاصمة وظيفتها تحليل معطيات وبيانات الجرائم المعلوماتية وكشف هوية أصحابها والقيام بتأمين الأنظمة المعلوماتية[3].

ثالثا – المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

وهو مؤسسة عمومية ذات طابع إداري[4] تتمتع بالشخصية المعنوية والاستقلال المالي، تحت وصاية وزير الدفاع الوطني وخاضع للأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية[5] من بين مهامه إجراء الخبرات والفحوص العلمية بناء على طلب من القضاة أو المحققين أو السلطات

---

[1] المرسوم الرئاسي رقم 04- 432 المؤرخ في 29 ديسمبر 2004 المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي ج ر رقم 36، المؤرخة في 29 ديسمبر 2004.

[2] المادة 5 من القرار الوزاري المشترك المؤرخ في 14 أفريل 2007 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج ر رقم 36 الصادرة بتاريخ 3 يونيو 2007.

[3] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص338.

[4] المرسوم الرئاسي رقم 04- 183 المؤرخ في 26 جوان 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر رقم 41 المؤرخة في 27 جوان 2004.

[5] المادة 2 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر رقم 41 المؤرخة في 27 جوان 2004.

المؤهلة، هذه الخبرات تخضع لاختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية وذلك بغرض إقامة الأدلة[1] التي تسمح بالتعرف على مرتكبي الجرائم المعلوماتية مثلا.

رابعا – الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

هذه الهيئة[2] أسندت إليها مهمة إنجاز الخبرة الرقمية[3] وإجراء الخبرة القضائية[4] في مجال مكافحة الجرائم المعلوماتية.

المطلب الثاني: الإجراءات الخاصة لجمع الأدلة في الجرائم المعلوماتية

الجرائم المعلوماتية باعتبارها كأحد الجرائم المستحدثة ونظرا لتمتعها بطبيعة خاصة والتي ميزتها عن باقي الجرائم الأخرى ألزمت مختلف التشريعات كالتشريع الجزائري على ضرورة تبني أساليب تحري خاصة من أجل الإطاحة بأصناف المجرمين المعلوماتيين، والتي يجب أن تفعل وفق ضوابط وشروط معينة يتبعها ضابط الشرطة القضائية حتى تكون ناجعة وتأتي بأكلها وحتى تكون بعيدة عن كل ما قد يعرضها للبطلان في المراحل اللاحقة من التحقيق.

هذه الأساليب جاءت في شكل التسرب واعترض المراسلات وتسجيل الأصوات والتقاط الصور، وفي شكل مراقبة الاتصالات الإلكترونية بحيث نص عليها المشرع الجزائري على التوالي ضمن ق إ ج[5] في المواد من 65 مكرر5 إلى 65 مكرر18 وضمن القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 3 منه ولقد جاءت إجراءاتها كما يلي.

---

[1] المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر رقم 41 المؤرخة في 27 جوان 2004.

[2] مرسوم رئاسي رقم 15- 261، المرسوم السابق.

[3] الفقرة ب من المادة 14 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[4] الفقرة 5 من المادة 4 من مرسوم رئاسي رقم 15- 261 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر رقم 53، المؤرخة في 8 أكتوبر 2015.

[5] قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

الفرع الأول: إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

غالبا ما يكون من الصعب تحديد و تتبع المجرمين المعلوماتيين وتقييم مدى تأثيرهم في هذه الجرائم وكذا جمع وتحليل الأدلة الرقمية ذات الصلة[1]بها، لذا يعتبر اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراء يلجأ إليه ضابط الشرطة القضائية في الجرائم المستعصية الكشف في شكل الجرائم المعلوماتية، هذا الإجراء يطلق عليه اسم الترصد الإلكتروني وهو عبارة عن : " تسجيل المحادثات بأجهزة التسجيل ويمكن الاكتفاء بإحدى الوسائل التالية لعملية المراقبة فقد تتم بمجرد التصنت وقد يكتفي بالتسجيل الذي يسمع بعد ذلك تم يفرغ مضمونه في المحضر المعد لذلك "[2] هذا الترصد سنتطرق إليه بشيء من التفصيل من خلال الآتي؛

أولا: اعتراض المراسلات

إنّ المشرع الجزائري أجاز لضابط الشرطة القضائية اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية[3] بناء على إذن من وكيل الجمهورية أو قاضي التحقيق، إلاّ أنّ المشكل الذي أثير يكمن حول طبيعة هذه الوسائل إذا ما كانت عبارة عن اتصالات هاتفية فقط أم يمتد إلى المراسلات المتبادلة بالحاسب الآلي الخاص بالمتهم مع الغير مما يتبادلون معه تلك المراسلات[4].

والذي رجحه المشرع الجزائري أنّها تشمل حتى المراسلات المتبادلة بالحاسب الآلي أيا كان شكلها بدليل استعمال المشرع لمصطلحات واسعة كمصطلح المراسلات وعبارة وسائل الاتصال السلكية

---

[1] Hui kai lung . Kim seung hyun . Wang Qiu hong, Cyber crime deterrence and international legislation evidence from distributed denial of service attack Revues MIS Quarterly, Vol. 41, Issue 2, MIS Research Center (United States) Jun2017 p497.

[2] خلفي عبد الرحمان، المرجع السابق، ص143.

[3] الفقرة 2 من المادة 65 مكرر5 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[4] جميلة محلق، اعتراض المراسلات، تسجيل الأصوات، والتقاط الصور في ق إ ج الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون العدد 42، جامعة باجي مختار عنابة، الجزائر، جوان 2015، ص178.

واللاسلكية وبدليل التعريف الذي جاء به هذا المشرع في القانون رقم 09-04 السابق ذكره بحيث عرف المراسلات بأنّها : " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية "[1]، وبالرجوع مثلا للحاسب الآلي فهو يدخل في نطاق وسائل الاتصال وتتم بواسطته المراسلات على جميع أشكالها.

ثانيا: تسجيل الأصوات

هي عبارة عن تسجيل لأحاديث المتهم وشركائه، فبعدما أعطت جل التشريعات للمتهم الحق بالصمت فإنّه وبشكل غير مباشر، بات الآن يُأخذ اعتراف المتهم ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية، هذا الكلام عبارة عن حديث والذي قد يجري في مكان خاص أو في مكان عام ويكون شخصيا ويتضمن أدق الأسرار، أين يعبر الإنسان عن نفسه وينقل مكنوناتها إلى المتحدث إليه، وبغض النظر عن مكان التسجيل الذي قد يكون عاما كالشارع أو خاصا كالمسكن والأداة التي يتم بها، فالمهم في العملية هو الكلام المتفوه به والذي قد يشكل دليلا لإظهار الحقيقة[2].

وبالرجوع للمشرع الجزائري فقد أجاز لضابط الشرطة القضائية بالنسبة لجرائم حددها على سبيل الحصر كالجرائم المعلوماتية التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية لشخص أو عدة أشخاص في أي مكان بناء على إذن من وكيل الجمهورية أو قاضي التحقيق[3].

---

[1] الفقرة (و) من المادة 2 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، عدد 33، جامعة الإخوة منتوري قسنطينة، الجزائر، جوان 2010، ص237.

[3] الفقرة 4 من المادة 65 مكرر5 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

ثالثا: التقاط الصور

الصورة كأصل عام تعتبر وسيلة هامة تم استخدامها والاستعانة بها في تحقيق العديد من الأغراض والأهداف، وهي سلاح ذو حدين فقد يستعان بها من أجل تحقيق المصلحة العامة كما قد يتعدى بها على الحق في الخصوصية، والصورة قد تكون في شكلها العادي (الثابت) كما قد تكون في شكلها المرئي الذي يعد مرحلة متقدمة على التصوير العادي والذي بات له خصوصية واضحة حتى أنّ البعض قد أطلق على حضارة القرن العشرين بأنّها حضارة الصورة وذلك للأهمية والمكانة الواضحة التي نالتها هذه الأخيرة.

فقد أصبح يعتمد عليها في المجال الجنائي باعتبار الناتج عن عملية التصوير من الأدلة العلمية المهمة في الإثبات الجنائي نظرا لما تحتويه من تفاصيل معلوماتية بالغة الأهمية والتي تعد توثيقا لمواقع وشخصيات أو آثار وأحداث ومواقف[1]، وهذا ما دفع المشرع الجزائري على الأخذ بهذه الآلية ونظمها دون موافقة المعنيين بها وتكون بوضع ترتيبات تقنية من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص[2]، ولعل المشرع من خلال تفعيله لهذه الآلية وجعلها مقصورة على المكان الخاص فقط دون المكان العام كان لاعتبارات تقنية أو لاعتبارات تتعلق بحقوق الآخرين غير المعنيين بالجريمة أو لاعتبارات تتعلق بصعوبة إثبات وجود هؤلاء الأشخاص في تلك الأماكن.

وعليه ومن خلال ما تم التطرق له حول الآليات الثلاثة السالفة الذكر يلاحظ بأنّ المشرع الجزائري قد مكن ضابط الشرطة القضائية من اختصاصات بالغة الخطورة لما فيها من مساس بالحريات الفردية[3]، وهو المشكل الذي أثير في طبيعة الحق الأولى بالرعاية بين حق الدولة في كشف الجريمة والعقاب وحق

---

[1] كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي، عمل مقدم لنيل شهادة الدكتوراه في الحقوق كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 2016، صفحات261، 262، 266.

[2] الفقرة 4 من المادة 65 مكرر5 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[3] سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكادمية، العدد 9، كلية الحقوق والعلوم السياسية جامعة باتنة، الجزائر، جوان 2016، ص395.

الفرد في عدم المساس بحرمة حياته الخاصة، أين انقسم الفقه بين مؤيد ومعارض لاستخدام مثل هذه الآليات فكان معظمهم مرجح لمصلحة الدولة والمجتمع على مصلحة الفرد وقالوا بأنّ الحق في الحياة الخاصة ينتهي بمجرد حصول اعتداء أو ارتكاب جريمة[1].

وبالرجوع إلى المشرع الجزائري الملاحظ أنّه أخذ بالرأي المؤيد الذي يغلب المصلحة العامة على المصلحة الخاصة وأجاز استخدام مثل هذه الآليات لكن ليس في كل الجرائم وإنّما حصرها في جرائم معدودة كانت الجرائم المعلوماتية إحداها، أين أجاز لضابط الشرطة القضائية اعتراض كافة المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية وكذلك تسجيل الأصوات والتقاط الصور بمختلف أشكالها وكل هذه الآليات يجب أن تفعل وفق الشروط التالية تحت طائلة البطلان؛

– وجوب الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق[2]، وأن يتضمن هذا الإذن جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها ومختلف الأماكن المقصودة سكنية أو غيرها، وكذا نوع الجريمة التي تبرر اللجوء لمثل هذه الآليات والوقت المحدد واللازم لتفعيلها والذي لا يتجاوز أربعة (4) أشهر وتكون هذه المدة قابلة للتجديد حسب مقتضيات التحري والتحقيق[3].

– يجب أن تفعل هذه العمليات تحت المراقبة المباشرة لمصدر الإذن سواء وكيل الجمهورية قبل فتح تحقيق قضائي[4] أو قاضي التحقيق في حالة فتح تحقيق قضائي[5].

---

[1] عبد العالي حاحة، آمال يعيش تمام، الترصد الإلكتروني كآلية للتحري عن جرائم الفساد بين متطلبات حماية الحقوق والحريات وضرورات الكشف عن الجريمة، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس، ملحق خاص، العدد 3 الجزء الثاني، أكتوبر 2018، ص354.

[2] المادة 65 مكرر5 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[3] المادة 65 مكرر7 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[4] الفقرة 5 من المادة 65 مكرر5 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[5] الفقرة الأخيرة من المادة 65 مكرر5 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

– لزوم أخذ التدابير اللازمة لضمان احترام السر المهني لكل شخص ملزم قانونا بكتمانه عند القيام بمثل هذه العمليات[1].

بهذا وبعد تفعيل هذه الآليات ضمن الشروط السالفة الذكر يبقى على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص أن؛

– يحرر محضرا عن كل عملية اعتراض وتسجيل المراسلات وعن كل عملية للالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، وكذا عن العمليات التي توضع فيها مختلف الترتيبات التقنية هذا المحضر الذي يجب أن يذكر فيه تاريخ وساعة بداية وانتهاء هذه العمليات[2].

– يصف أو ينسخ ضمن محضر يودع بالملف جميع المحادثات المسجلة والمكالمات المترجمة أو المراسلات أو الصور التي تفيد في إظهار الحقيقة[3].

هذا ويجوز لضابط الشرطة القضائية المأذون له أو المناب من قبل قاضي التحقيق تسخير؛

– كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية من أجل تفعيل آليات التحري الخاصة[4].

– مترجم في حالة المكالمات التي تتم باللغات الأجنبية[5].

الفرع الثاني: إجراء التسرب

يعد التسرب إجراء أصيل من اختصاص ضابط الشرطة القضائية في التشريع الجزائري ويعتبر كأسلوب من بين أساليب التحري الخاصة التي نظمها المشرع من خلال الفصل الخامس من الباب

---

[1] الفقرة 1 من المادة 65 مكرر6 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] المادة 65 مكرر9 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[3] الفقرة 1 المادة 65 مكرر10 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[4] المادة 65 مكرر8 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[5] الفقرة 2 من المادة 65 مكرر10 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

الثاني من الكتاب الأول لق إ ج[1]، وهو إجراء في غاية الصعوبة على المتسرب كما قد يشكل في بعض الأحيان خطرا على حياته في بعض الجرائم التي يجري التسرب في شأنها كجرائم المخدرات والإرهاب وإجراء التسرب حسب المشرع الجزائري هو: " قيام ضابط عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك لهم أو خاف"[2].

هذا التعريف مستمد من تعريف ق إ ج الفرنسي للمتسرب، والذي قال عنه بأنّه ضابط عون شرطة قضائية مؤهل بوجه خاص ضمن الشروط المحددة بموجب مرسوم، ويعمل تحت مسؤولية ضابط شرطة قضائية مكلف بتنسيق العملية لمراقبة أشخاص مشبه بهم في ارتكاب جناية أو جنحة عن طريق التظاهر لدى هؤلاء الأشخاص كفاعل معهم أو شريك لهم أو خاف[3]، وبهذا يلاحظ بأن المتسرب قد يكون فاعلا أو شريكا أو خافيا لعائدات الجريمة أين يستعمل أثناء المراحل الإجرائية هوية مستعارة لذلك فهو مهدد في كل لحظة من لحظات عملية التسرب باكتشاف حقيقته كضابط عون شرطة قضائية، الأمر الذي يفسر بقاءه في دائرة الخطر أثناء وقبل الانتهاء من فترة التسرب ككل.

إنّ المشرع الجزائري من خلال تنظيمه لإجراء التسرب جعله يخضع لشروط معينة حتى يتم العمل به وحتى يتم الأخذ بشهادة ضابط الشرطة القضائية التي تجري عملية التسرب تحت مسؤوليته هذه الشروط تتمثل أولا في نوع الجريمة التي تقتضي ضرورات التحري حولها وهي عبارة عن جرائم[4] حددت على سبيل الحصر، والتي كان من بينها إحدى الجرائم المعلوماتية والمتمثلة في جريمة المساس بأنظمة

---

[1] قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] الفقرة 1 من المادة 65 مكرر12 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[3] يامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد 11 العدد 2، جامعة قاصدي مرباح ورقلة، الجزائر، جوان 2019، ص149.

[4] الجرائم هي جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.

المعالجة الآلية للمعطيات، أما الشرط الثاني فيتمثل في ضرورة حصول ضابط الشرطة القضائية على إذن مسبق من طرف وكيل الجمهورية أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية على أن يكون هذا الإذن مكتوبا ومسببا ومحددا لمدة التسرب التي لا يجب أن تتجاوز أربعة (4) أشهر، كما يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء مع ذكر هوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، وذلك كله تحت طائلة البطلان[1].

إنّ الجريمة المعلوماتية في صورة المساس بأنظمة المعالجة الآلية للمعطيات غالبا ما يصعب اكتشافها وإثباتها حتى وإن تم الاشتباه في مقترفها، فهي قد لا تترك آثار لها عند أو بعد القيام بها الأمر الذي يحتم اللجوء إلى آليات مغايرة حتى وإن كانت تقليدية كما هو الحال بالنسبة للتسرب وإن كان هذا الإجراء الأخير يعتبر كأسلوب تحري حديث بالنسبة للتشريع الجزائري، وذلك لما له من أهمية كبيرة في هذا النوع من الجرائم إذ من شأنه أن يحاصر النشاط الإجرامي ويقلص من الفوارق الموجودة بين مرتكب الجريمة ومكان البحث عنها، خاصة وأنّ هذا النوع من الجرائم غالبا ما يرتكب في عالم افتراضي.

لذا يجوز الأخذ بهذه الآلية في هذا النوع من الجرائم وهو ما قامت به المباحث الفدرالية الأمريكية لما دست أحد أعضائها للإطاحة بمجموعة من المجرمين تمتهن قرصنة البرمجيات والمتاجرة فيها بطريقة غير مشروعة[2]، فالملاحظ أنّ هذا الإجراء يأخذ به القانون الأمريكي في مثل هذا النوع من الجرائم ويطلق عليه مصطلح " العملية تحت التغطية "، ويعرف بأنّه كل تحقيق يتم من خلاله القيام بأعمال أو نشاطات تستدعي استخدام اسم مستعار أو هوية خيالية من طرف عون من المكتب الفدرالي للتحقيقات[3].

---

[1] المادة 65 مكرر15 من قانون رقم 06- 22، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] لخضر رابحي، عبد الحليم بوقرين، الإجراءات المستحدثة لمواجهة الجريمة في التشريع الجزائري، مجلة دراسات وأبحاث، مجلد 1، عدد 2، جامعة زيان عاشور بالجلفة، الجزائر، جوان 2019، ص569.

[3] رابح وهيبة، التسرب في التشريع الإجرائي الجزائري، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، مجلد 1، العدد 36 جامعة القدس المفتوحة فلسطين، حزيران 2015، ص301.

هذا وقد أثار التسرب شيئا من اللبس من حيث دقته كمصطلح لأنّ الراجح فقها يأتي بمسمى الاختراق والذي أخذ به المشرع الجزائري في القانون المتعلق بالوقاية من الفساد ومكافحته[1] من خلال نص المادة 56 أين اعتمده كإجراء في عملية جمع الأدلة المرتبطة بجرائم الفساد[2]، ويلاحظ أنّ المشرع الجزائري حصر هذا الإجراء في إطار الجرائم المعلوماتية على نوع واحد فقط وهي جريمة المساس بأنظمة المعالجة الآلية للمعطيات، فقد كان حريا به عند توسعته لمجال الأفعال التي تدخل في إطار الجرائم المعلوماتية أن يعدل من نص المادة 65 مكرر 11 ويجعل من عملية التسرب تشمل جميع الأفعال التي ترتكب على أو بواسطة منظومة معلوماتية.

الفرع الثالث: إجراء مراقبة الاتصالات الإلكترونية

يعتبر إجراء مراقبة الاتصالات الإلكترونية من بين أساليب التحري الخاصة التي جاءت بها ونظمتها مختلف التشريعات، ويعتبر التصنت الهاتفي هو أحد صور هذا الإجراء والشائع لدى الكثير من المجتمعات ويعتبر أحد الصور المستخدمة بكثرة من قبل السلطات الأمنية، فهو إحدى وسائل المعلومات التقنية المهمة وخاصة للتحقيق في أخطر الجرائم مثل الإرهاب أو الجريمة المنظمة أو الجريمة الاقتصادية، وذلك لأهميته الجلية في عملية الحصول على الأدلة التي قد يقدمها الأشخاص الذين لديهم معلومات ذات صلة بالجريمة المراد كشفها وذلك من خلال محادثتهم التلقائية والمعلومات غير المشوهة التي يشاركونها مع الغير، ومع ذلك يجب الأخذ في الاعتبار حقيقة أن هذا الإجراء مرتبط باختراق الحق في الخصوصية.

لهذا فإنّ استخدامه يحتاج إلى توازن مقبول بين المصلحة العامة للتحقيق في الجريمة وإثبات إدانة مرتكبها من جهة ومصلحة الجمهور في حماية الحق في خصوصية الأفراد، والذي يُحتمل أن يتعرض

---

[1] قانون رقم 06 – 01، المؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، ج ر رقم 14، المؤرخة في 8 مارس 2006.

[2] تنص الفقرة 1 من المادة 56 من قانون رقم 06 – 01 يتعلق بالوقاية من الفساد ومكافحته، ج ر رقم 14، المؤرخة في 8 مارس 2006 بأنّه:" من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب، أو اتباع أساليب تحرّي خاصة، كالترصد الالكتروني والاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة".

للاعتداء بنسبة كبيرة عليها من ناحية أخرى[1]، هذا ويعتبر التصنت كأحد صور إجراء مراقبة الاتصالات الإلكترونية في التشريع الجزائري، وهذا الإجراء ككل لم يعطى له تعريفا شافيا من قبل المشرع الجزائري، فلقد اكتفى هذا الأخير بتعريف الاتصالات الإلكترونية فقط وقال بأنّها: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[2].

إلاّ أنّه يمكن استنباط تعريف لهذه العملية كإجراء من خلال النصوص القانونية المنظمة له فنستطيع القول بأنّ إجراء مراقبة الاتصالات الإلكترونية طبقا للمشرع الجزائري هو قيام السلطات المختصة بإذن من السلطات القضائية المختصة بوضع ترتيبات تقنية خاصة يراقب من خلالها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية وذلك من أجل حالات خاصة متعلقة بموضوع الجريمة المراد كشفها.

هذا الإجراء نظمه المشرع الجزائري ضمن نص المادة 4 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وجعله يخضع لضوابط وشروط شكلية وموضوعية معينة والتي كان من أهمها حماية حق الحياة الخاصة للغير، هذا الحق الذي هو في الأصل مكفول دستوريا بنصي المادتين 46 و47 من التعديل الدستوري[3] لسنة 2016 بل وأفردت

---

[1] Milos Deset, European Standards and actual issues of the tapping in slovak criminal procedure law, Revues International Multidisciplinary Scientific Conference on Social Sciences & Arts SGEM, Vol 6 Sofia, Bulgaria, 2019,p 123.

[2] الفقرة (و) من المادة 2 من قانون رقم 09- 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[3] قانون رقم 16-01، المؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري الجزائري، ج ر رقم 14، المؤرخة في 7 مارس 2016 .

له حماية جنائية خاصة في قانون العقوبات[1] ضمن نصوص محددة[2]، وبعده في القانون المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخص[3]، وذلك نظرا لأهميته الكبيرة في اعتبار الأفراد.

لذا كان من اللازم على المشرع أثناء تنظيمه لإجراء مراقبة الاتصالات الإلكترونية أن يأخذ بعين الاعتبار الحياة الخاصة للغير وأن يحرص كل الحرص على تجنب المساس والاعتداء عليها مهما كانت الأوضاع، وذلك بدليل نص الفقرة الأخيرة من نص المادة 4 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي جاء في فحواها أنّ الترتيبات التقنية الموضوعة لمراقبة الاتصالات الإلكترونية من أجل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة؛ يجب أن تكون موجهة فقط لتجميع وتسجيل المعطيات ذات الصلة بالأفعال السابقة ودون المساس بالحياة الخاصة للغير تحت طائلة العقوبات المنصوص عليها في قانون العقوبات.

إنّ الملاحظ بالرغم من خطورة الأفعال والتي قد تصل إلى تهديد أمن الدولة إلاّ أنّ المشرع الجزائري جرم كل اعتداء يمس بمعطيات الحياة الخاصة للغير إذا ما كانت هذه المعطيات ليس لها أية صلة بالأفعال الإرهابية والاعتداءات على أمن الدولة، وعليه فإذا كان المشرع قد جرم الاعتداء على هذه المعطيات بالنسبة لهذه الجرائم الأكثر خطورة فما بالك بمن هي دونها في الخطورة كالجرائم المعلوماتية.

وكما أنّه بالرغم من مشكل اتساع نطاق الجرائم المعلوماتية الذي تعاني منه العديد من البلدان خاصة من خلال سن قوانين محددة لتمكين سلطات التحقيق من الوصول والاستيلاء على المعلومات

---

[1] قانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر 66-156 المتضمن ق ع الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] المواد من 303 مكرر إلى 303 مكرر 3 من القانون رقم 06- 23، يعدل ويتمم الأمر66-156 المتضمن ق ع الجزائري ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[3] المادة 2 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر رقم 34، المؤرخة في في 10 يونيو 2018.

والأدلة الرقمية، إلاّ أنّ هؤلاء المحققين منحوا صلاحيات واسعة من خلال مراقبة الاتصالات الإلكترونية تتجاوز التصورات العادية للخصوصية، والتي لاقت معارضة قوية خاصة مع تطور هذا المجال من التشريع والسوابق القضائية المرتبطة بها[1].

لذلك يبقى إجراء مراقبة الاتصالات الإلكترونية من أخطر أساليب التحريات الخاصة التي تستعمل من أجل جمع الأدلة ذات الصلة بالجرائم المعلوماتية، وذلك لما فيه من خرق صارخ لحرمة الحياة الخاصة للأفراد بدليل تفعيله كإجراء وقائي أي لمجرد شك الاعتداء على المنظومة المعلوماتية هذا الشك الذي لا يغني من الحقيقة شيئا إلاّ بعد تحققه وإقامة الدليل عليه، فكان حريا بالمشرع الجزائري أن يفعله على الأقل وفق الضوابط الشكلية والموضوعية التي فعل بها إجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات بدءا من شكل الإذن[2] المتحصل عليه، والذي يلزم تجميع وتسجيل المعطيات ذات الصلة فقط بهذه الجريمة لتجنب الاعتداء على الحياة الخاصة للغير.

المطلب الثالث: التصرف في نتائج التحقيقات الأولية للجرائم المعلوماتية

كأصل عام تعتبر النيابة العامة وحدها صاحبة الاختصاص في التصرف بنتائج التحقيقات الأولية دون ضباط الشرطة القضائية الذين يقومون بجمع مختلف الاستدلالات، فعندما تعرض المحاضر والتقارير التي أجراها هؤلاء الضباط على النيابة العامة قد ترى هذه الأخيرة بحفظ الأوراق إيذانا منها بعدم السير في الدعوى العمومية، كما قد ترى على العكس تحريك تلك الدعوى سواء في الحالة العادية أو في حالة الجنح المتلبس بها[3]، وأيا كانت وسيلة تحريكها فإنّ النيابة العامة تلتزم أولا بمراعاة ما قد يفرضه القانون

---

[1] Alison Lyle, Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism, From a book of, Babak Akhgar Saskia Bayerl, Fraser Sampson, The previous reference, p280.

[2] الإذن يبقى خاضع لنفس أحكام إجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات المنصوص عليها في ق إ ج والذي يعبر عن جميع العناصر التي تسمح بالتعرف على الاتصالات الإلكترونية المطلوب التقاطها ومختلف الأماكن المقصودة سكنية أو غيرها وكذا نوع الجريمة التي تبرر اللجوء لمثل هذه الآليات والوقت المحدد واللازم لتفعيلها والذي لا يتجاوز أربعة (4) أشهر وتكون هذه المدة قابلة للتجديد حسب مقتضيات التحري والتحقيق.

[3] أحمد شوقي الشلقاني، المرجع السابق، ص195.

في هذا الصدد بالنسبة لبعض الجرائم التي تتطلب الشكوى أو الطلب أو الإذن لتحريك الدعوى العمومية من أجلها.

الفرع الأول: التصرف بصورة الأمر بحفظ الأوراق

يعتبر الأمر بحفظ الأوراق أحد قرارات التصرف في نتائج التحقيقات الأولية والتي ليست لا من إجراءات الدعوى العمومية ولا من إجراءات التحقيق، هذا الأمر يعرف بأنّه: " قرار يصدر من النيابة العامة بوصفها سلطة اتهام، يعني أن الدعوى لا تتوفر لها المقومات القانونية أو الفعلية التي تحمل النيابة على السير فيها" أو بأنّه: " صرف النظر مؤقتا عن تحريك الدعوى الناشئة عن الجرم المثبت بمحضر الضابطة العدلية"[1].

وعموما يرجع أمر النيابة العامة بحفظ الأوراق لأسباب قانونية كانتفاء أركان الجريمة أو وجود سبب من أسباب الإباحة أو وجود سبب من أسباب انقضاء الدعوى كصدور حكم نهائي، وقد يرجع الحفظ لأسباب موضوعية كعدم كفاية الأدلة مثلا وكعدم معرفة الفاعل مثلا[2]، ولعل أبرز الحالات التي تأمر فيها النيابة العامة بحفظ الأوراق في نطاق الجرائم المعلوماتية خاصة عندما يكون الفعل المسند إلى المتهم لا يدخل تحت نص التجريم كانتفاء أركان الجريمة المعلوماتية وكتوفر مانع من موانع المسؤولية الجنائية بالنسبة للمجرم المعلوماتي أو لعدم معرفة الفاعل أو لعدم كفاية الأدلة حولها خاصة وأنّ الجرائم المعلوماتية في الكثير من الأحيان ما يصعب إثباتها وتتبع مرتكبيها.

هذا ويجمع الفقه والقضاء بأن تصرف النيابة العامة في ختام مرحلة التحريات الأولية بطريق الأمر بحفظ أوراق الدعوى العمومية يوقف السير بإجراءات الدعوى الجزائية مؤقتا دون أن يكون منهيا لها

---

[1] زايد بن عبد الرحمن الطويان، الأمر بحفظ الدعوى بعد التحقيق والقرار بأن لا وجه للسير فيها (دراسة مقارنة)، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية تخصص التشريع الجنائي الإسلامي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية الرياض، السعودية، 2004، ص61، ص63.

[2] عبد الله بن سعيد أبو داسر، الأمر بحفظ الأوراق والأمر بألا وجه للدعوى، عن مكتبة الألوكة، عن موقع alukah.net تاريخ الإطلاع 2020/08/01، ص4.

وحجتهم في ذلك أنّ هذا النوع من الأمر يقصد منه صرف النظر عن اتخاذ إجراءات المتابعة وذلك لانتفاء عناصر الاتهام التي تبرر المتابعة الجزائية أمام الجهات القضائية المختصة، وهو ما يفسر عدم إنهاء هذا الأمر للدعوى أو التسبب في انقضائها كالحكم النهائي وإنّما يعمل فقط على إيقاف السير فيها في ختام مرحلة التحريات الأولية[1].

خاصة إذا ما تعلق الأمر ببعض الجرائم ذات الطبيعة الخاصة والمبهمة في حل لغزها كالتي في شكل الجرائم المعلوماتية، هذه الجرائم التي تحتم في غالب الأحيان على النيابة العامة بعد أن تعرض عليها المحاضر والتقارير التي أجراها ضباط الشرطة القضائية عنها من ضرورة التثبت والتأكد الجيدين من عملية وكيفية اقترافها، والذي لا يتأتى سوى بفتح تحقيق حولها من خلال توجيه النيابة العامة لقاضي التحقيق أمرا بذلك، فيكون سببا في تحريك الدعوى العمومية.

الفرع الثاني: التصرف بطريق تحريك الدعوى العمومية

تعرف الدعوى العمومية بأنّها مطالبة الجماعة بواسطة النيابة العامة القضاء الجزائي توقيع العقوبة على مرتكب الجريمة، وتعتبر الوسيلة القانونية لتقرير مدى حق الدولة في العقاب توصلا لاستيفائه بمعرفة السلطة القضائية المختصة، أمّا إجراءات تحريكها والتي تقوم بها النيابة العامة فتكون من خلال تطبيق ق ع على من أخل بنظام الجماعة بمخالفة أوامر ونواهي القوانين العقابية[2].

هذه الإجراءات تفعل بطريق طلبات وكيل الجمهورية لقاضي التحقيق بفتح تحقيق[3]،كما قد تكون بإقامة الدعوى العمومية أمام محكمه الجنح أو المخالفات[4] بتكليف المتهم بالحضور أمامها[5] وكذا

---

[1] بلحو نسيم، سلطة النيابة العامة في حفظ أوراق الدعوى الجزائية (دراسة مقارنة)، عمل مقدم لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، الموسم الجامعي 2007/2006، ص 33.

[2] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، طبعة مزيدة ومنقحة، دار هومة للطباعة والنشر والتوزيع الجزائر العاصمة، الجزائر، 2018، ص 75.

[3] المادة 67 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادتين 333 و334 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادتين 394 و395 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

وفق إجراءات المثول الفوري أمام نفس المحكمة في الجنح المتلبس بها[1] وكذلك بإقامة المدعي المدني المتضرر من الجريمة دعواه المدنية أمام القضاء الجنائي تحقيقا[2]أو حكما[3]، وعموما فإذا ما قدّرت النيابة العامة كفاية الاستدلالات لإدانة المتهم فإنّها تلجأ إلى تحريك الدعوى العمومية مباشرة على محكمه الجنح والمخالفات وذلك بطريقة التكليف بالحضور وهو ما يطلق عليه الادعاء المباشر.

هذا ويعتبر الادعاء المباشر عبارة عن إجراء تقوم به النيابة العامة تطرح من خلالها الدعوى العمومية على المحكمة المختصة في حالة ما كانت الواقعة جنحة أو مخالفة، وبتبليغه تدخل الدعوى في حوزة المحكمة[4]، أمّا إذا كانت الوقائع موضوع الاستدلالات لازالت بحاجة إلى أدلة تحدد مدى ثبوتها ومدى المسؤولية عنها كما هو الحال بالنسبة لغالبية الجرائم المعلوماتية فللنيابة العامة طلب افتتاح التحقيق من قاضي التحقيق، وهو إجراء تقوم به النيابة العامة والذي يترتب عليه تحريك الدعوى العمومية أمام قاضي التحقيق.

إنّ الدعوى العمومية تبقى الأداة أو الوسيلة القانونية الأساسية للوصول إلى المضمون التقليدي لسلطة الدولة في العقاب بالرغم من انتهاج السياسة العقابية اتجاها إجرائيا يعمل على تيسير إجراءات الدعوى العمومية أو استحداث بدائل تتبع بها إجراءات الدعوى العمومية[5]، خاصة في ظل وجود جرائم معقدة كالتي على شاكلة الجرائم المعلوماتية التي تجبر النيابة العامة على سلك إجراءات الدعوى العمومية بمختلف مراحلها، ابتداء من تحريكها بتقديم الطلبات أمام قاضي التحقيق ثم التحقيق مع المتهم ومع

---

[1] المواد من 339 مكرر إلى 339 مكرر 7 من أمر رقم 15-02 المعدل والمتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41، المؤرخة في 29 يوليو 2015.

[2] المادة 2 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 72 من قانون رقم 06-22، يعدل ويتمم ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[4] أحمد شوقي الشلقاني، المرجع السابق، ص205.

[5] بلولهي مراد، بدائل إجراءات الدعوى العمومية، عمل مقدم لنيل شهادة الدكتوراه في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر، الموسم الجامعي 2019/2018، ص4.

كافة أطراف الدعوى الآخرين إلى غاية إصدار الأحكام ومن ثم متابعتها أمام الجهات المختصة لحين الفصل فيها بحكم نهائي غير قابل لأي طريق من طرق الطعن.

هذا الكلام الأخير يؤكده قرار صادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالحاسب الآلي، والذي أُكد أيضا من خلاله على ضرورة وضع الدول لأحكام وإجراءات متعلقة بالتحقيق والأدلة للتصدي للجرائم المعلوماتية مع ضمان أن تطبق القوانين الراهنة المتعلقة بسلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم مع إدخال تغييرات مناسبة إذا دعت الضرورة لذلك[1] بشرط الأخذ بعين الاعتبار المشاكل المتصلة بحماية الحياة الخاصة مع مراعاة حقوق الإنسان وحرياته الأساسية[2]، لذلك فإنّ أهم الأسئلة التي يجب الإجابة عليها تكمن في ما إذا كان بالإمكان تحقيق العدالة، لذلك غالبا ما يجب على النيابة العامة أن تقرر بأخذ القضية لأنّها نقطة أساسية لا ينبغي الاستخفاف بها[3].

فالخطورة والتعقيدات التي تخلفها الجرائم المعلوماتية تحتم على النيابة العامة الطلب من قاضي التحقيق بفتح تحقيق حولها، هذا الأخير الذي قد يضطر إلى استخدام وسائل وآليات مستحدثة في غاية الحساسية كالتي تطرقنا إليها سابقا من اعتراض للمراسلات والتقاط للصور وتسجيل للأصوات والتي يجب أن تفعل وفق ضوابط وشروط معينة حتى تكون ناجعة وتأتي بأكلها وحتى تكون بعيدة عن كل ما قد يعرضها للبطلان في المراحل اللاحقة من مراحل الدعوى.

---

[1] عماد مجدي عبد الملك، المرجع السابق، ص257.

[2] تقرير الأمين العام للمؤتمر، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك 18 – 25 أفريل 2005 ص8، عن موقع https://undocs.org/، تاريخ الإطلاع 2020/08/03.

[3] Greg Gogolin and James Jones, Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business, revue Information Security Journal: A Global Perspective, Copyright © Taylor & Francis Group, LLC, Royaume-Uni 2010, p116.

الباب الثاني: إجراءات الدعوى العمومية المتبعة في الجرائم المعلوماتية

كنا قد تطرقا بالقول سابقا بأنّ الدعوى العمومية تبقى هي الأداة والوسيلة القانونية الأساسية للوصول إلى المضمون التقليدي لسلطة الدولة في العقاب على الرغم من انتهاج السياسة العقابية اتجاها إجرائيا بطريق العمل على تبسيط إجراءات الدعوى العمومية خاصة في ظل وجود جرائم معقدة كالتي على شاكلة الجرائم المعلوماتية، هذه الأخيرة تجبر النيابة العامة على سلك طريق الدعوى العمومية بمختلف مراحلها ابتداء من تحريكها بتقديم الطلبات أمام قاضي التحقيق للتحقيق مع المتهم ومع كافة أطراف الدعوى الآخرين ومتابعتها إلى غاية إصدار الحكم الفاصل فيها بصفة نهائية.

الأمر الذي يفسر الأهمية الكبرى للتحقيق الابتدائي كمرحلة من الدعوى العمومية في الجرائم المعلوماتية، فهذه الأخيرة تعتبر من بين القضايا التي تحتاج إلى تمحص وتثبت كبيرين من طرف قاضي التحقيق قبل العمل على إحالتها وإحالة المتهمين إلى المحاكمة، ذلك أنّها ذات طبيعة خاصة والتي تفرض وجود قضاة تحقيق محترفين بالتحقيق في مثل هذا النوع من الجرائم، كما تفرض تدريبهم واضطلاعهم على ما يخفيه مجال المعلوماتية من برامج وتقنيات وتطبيقات مختلفة، هؤلاء القضاة الذين سهل القانون من تحركهم من خلال تمديد اختصاصهم المحلي وكذا العمل بإجراءات تسليم المجرمين على المستوى الإقليمي والدولي وذلك لتضييق الخناق على المجرمين المعلوماتيين.

بل وأعطاهم سلطات محددة والتي هي عبارة عن إجراءات ذات طابع حديث وأخرى ذات طابع تقليدي وكذا إصدار عدة أوامر على حسب وضع وموقع المتهم من القضية، هذه الأوامر تساعد وتساهم في عملية التحقيق الابتدائي من بدايته إلى نهايته، بحيث يتم إجراء تحليل وجمع الأدلة في موقعها وتحت رقابة سلطة التحقيق والتي على أساسها يتقرر المسار المستقبلي للقيام بعملية التحقيق، هذا التحليل والجمع للأدلة الإلكترونية يكون باستخدام أدوات وتقنيات مختلفة يقوم بها الخبراء بناءا على

طلبات سلطة التحقيق وذلك لعرض الأدلة أمام القضاء[1]، ذلك أنّ التحقيق تستدعي نتائجه من قضاة التحقيق إمّا إصدار الأمر بانتفاء وجه الدعوى أو أمر بالإحالة إلى المحكمة المختصة، هذا الأمر الأخير الذي غالبا ما يحصل في هذا النوع من الجرائم المعقدة الجرائم المعلوماتية.

ذلك أنّ ترجيح إدانة شخص كالمتهم المعلوماتي من قبل قاضي التحقيق ليس اقتناعا منه بملائمة إحالة الدعوى العمومية إلى المحكمة المختصة، هذه الأخيرة التي تعود إليها وحدها الحسم والحزم فيما إذا كان هذا الاقتناع يتطابق في نهاية الأمر مع حقيقة الواقع وصحيح القانون، فالطبيعة الخاصة والمعقدة للجرائم المعلوماتية تخلف وراءها أدلة تبقي قاضي التحقيق غارقا في شكه خاصة إن لم يجد أدلة قوية تثبت براءة المتهم المعلوماتي، فيتعمد في كثير من الأحيان إلى إصدار الأمر بالإحالة إلى المحكمة المختصة بهذه الجرائم للتدقيق في الأدلة المتوفرة ورغبة منه في إظهار أدلة قوية أخرى أثناء المحاكمة.

وكأصل عام فإنّ معظم المتهمين بالجريمة المعلوماتية تتم محاكمتهم أمام المحاكم الجزائية العادية، تبقى فقط مسألة تقديم المعلومات العلمية ومصطلحات التقنية العالية أمام هذه المحاكم ومهمة شرحها للقضاة هي التي تشكل صعوبة بالغة لدى المحققين وأعضاء النيابة العامة، لهذا تترك هذه المهمة في الغالب للخبراء وهو ما يفقد ويخرج القضية الجزائية من عناصرها القانونية، فلا تتمكن المحكمة بذلك من الوقوف كلية على الحقائق المكونة لأركان الفعل الإجرامي والتيقن من الأدلة التي تثبت تلك الأركان.

خاصة وأنّ الأدلة التي تثيرها في أغلبها ذات طبيعة إلكترونية، هذه الأدلة الإلكترونية جعلت من أمر التحقيق فيها ورقابة قاضي الموضوع عليها يزداد صعوبة من خلال هذه المرحلة الفاصلة في الدعوى العمومية، خاصة وأنّ هذا الدليل يثير عدة مشاكل سواء من الناحية الموضوعية أو الإجرائية حتى أنّ إجراءات الحصول عليه تتسع لتشمل كل من الإجراءات حديثة والإجراءات التقليدية المطبقة على الجرائم الأخرى العادية.

---

[1] Balsing Rajput, cyber Economic Crime in India : An Integrated Model for Prevention and Investigation, Springer Nature Switzerland AG, 2020, p166

هذه المرحلة الأخيرة من الدعوى العمومية والفاصلة تحمل في نهايتها ظرفا ووقتا حساسا جدا في الدعوى كلها، فخلالها يصدر قاضي الموضوع حكمه على المتهم بالجريمة المعلوماتية إمّا بالبراءة أو الإدانة، وذلك بعد تقديره لمختلف الأدلة المطروحة عليه في الجلسة وبناءا على اقتناعه الشخصي، كما أنّ هذا الحكم إلاّ ويرتب آثارا معينة أثناء وبعد إصداره، هذه الآثار تكفل القانون بترتيبها وتنظيمها ووضعها في قالبها وآجالها المحددة.

الفصل الأول: إجراءات التحقيق الابتدائي في الجرائم المعلوماتية

لا يمكن تصور حاليًا في عالم تغزوه التكنولوجيا الرقمية بشكل متزايد بإمكانية الاستغناء عن هذا المصدر المهم للمعلومات في سياق التحقيق القضائي بغض النظر عن مجاله، ذلك أنّ التجربة تظهر بأنّ العناصر الرئيسية للتحقيق قد تكمن في التفاصيل التي نسيها المجرم المعلوماتي في تنظيم براءته[1] المزعومة لذلك فإنّ استمرار العمليات الرقمية وكمية المعلومات التي تحتويها هذه التكنولوجيا هو مصدر وسيظل كذلك في المستقبل للتحقيق الابتدائي.

الذي يعد من أهم المراحل التي تمر بها الدعوى العمومية في الجرائم الخطيرة عامة والجرائم المعلوماتية خاصة، ذلك أنّ هذه الأخيرة تعتبر من القضايا التي في كثير من الأحيان ما تحتاج إلى تمحص وتثبت من طرف قاضي التحقيق قبل العمل على إحالتها وإحالة المتهمين إلى المحاكمة والتي قد يدان فيها هؤلاء كما قد يبرؤون، فالجرائم المعلوماتية كما هو واضح ذات طبيعة خاصة والتي تفرض وجود قضاة تحقيق محترفين بالتحقيق في مثل هذا النوع من الجرائم، كما تفرض تدريبهم واضطلاعهم على ما يخفيه مجال المعلوماتية من تقنيات وتطبيقات وبرامج مختلفة.

هذا وكما تطرقنا إليه سابقا بأنّ الجرائم المعلوماتية تعتبر ذات طبيعة متعدية الحدود، أي قد ترتكب من أي نقطة من العالم على أي نقطة أخرى منه كما أنّ المسافة بين النقطتين قد تبعد أو تقصر، من هنا جاءت فكرة تمديد الاختصاص المحلي لقضاة التحقيق وكذا العمل بإجراءات تسليم المجرمين على المستوى الإقليمي والدولي، وذلك لتضييق الخناق على المجرمين المعلوماتيين وحتى لا يفلت الجناة من المتابعة الجزائية، فيصبح قاضي التحقيق التابع لمحكمة جزائية ما له اختصاصا إقليميا موسعا يتجاوز اختصاصه العادي إلى محكمة أخرى أين يستطيع التنقل أو انتداب أي ضابط شرطة قضائية للقيام بمهام متعلقة بالتحقيق القضائي الابتدائي في الجرائم المعلوماتية.

---

[1] Daue Dominique, la criminalité informatique : l'informatique, ses risques et ses dangers, Atelier des fucam à Mons, expose upch, les professions comptables face au droit penal financier, Mons, Belgique, 2010 ,p7.

هذه المهام المتعلقة بالتحقيق القضائي الابتدائي في الجرائم المعلوماتية هي عبارة عن إجراءات ذات طابع جزائي خاص جاء بها المشرع الجزائري، منها ما يطبق على كافة الجرائم التي يستلزم المشرع التحقيق فيها وهي إجراءات المعاينة والخبرة والضبط وكذا التفتيش والحجز والتي قد تجرى هي الأخرى بطريقة خاصة على حسب خصوصية النظام المعلوماتي، ومنها ما يطبق على جرائم محددة حصرا كالتي في شكل الجرائم المعلوماتية كإجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات والتسرب وكذا مراقبة الاتصالات الإلكترونية.

هذا بالإضافة إلى الإجراءات التقليدية الأخرى التي جعلها المشرع من اختصاص قضاة التحقيق بحيث يتم من خلالها استجواب المتهم بالجريمة المعلوماتية وأيضا مواجهته وتخول لهم سماع الشهود وكذا سماع الطرف المدني إن وجد، هذا ويبقى لقضاة التحقيق سلطة إعطاء عدة أوامر على حسب وضع وموقع المتهم من القضية كالأمر بإحضار المتهم والأمر بالقبض عليه وكذا الأمر بإيداع المتهم الحبس المؤقت أو الأمر بوضعه تحت الرقابة القضائية، هذه الأوامر تساعد وتساهم في عملية التحقيق الابتدائي من بدايته إلى نهايته، هذا التحقيق الذي تستدعي نتائجه من قضاة التحقيق إمّا إصدار الأمر بانتفاء وجه الدعوى أو الأمر بالإحالة إلى المحكمة المختصة.

المبحث الأول: الإجراءات الميدانية للسلطة المخول لها التحقيق في الجرائم المعلوماتية

تختلف الإجراءات الجزائية باختلاف كل مرحلة من مراحل الدعوى العمومية، فالإجراءات المتبعة في مرحلة جمع الاستدلالات تختلف في مجملها عن الإجراءات المتبعة في مرحلة التحقيق الابتدائي وهكذا إلى مرحلة المحاكمة، ولا شك أنّ مرحلة التحقيق الابتدائي بالنسبة للجرائم الخطيرة كالتي في شكل الجرائم المعلوماتية يلعب قاضي التحقيق فيها دورا كبيرا، خاصة إذا ما كان مختصا ومحترفا في المجال المعلوماتي كما أنّه في الأصل مخول له قانونا استغلال سلطاته التي يقوم من خلالها بإجراءات تساعده على القيام بتحقيقه على أتم وجه.

وتتمثل مجمل هذه السلطات في إجراءات المعاينة والحجز والتفتيش مع ضبط مختلف الوسائل والمعلومات المساعدة في إثبات الجرائم المعلوماتية وكذا الاستعانة بالخبراء في المسائل التقنية المعقدة، هذه الإجراءات يستطيع قاضي التحقيق أن يقوم بها عن بعد إذا ما دعت ضرورات التحقيق الابتدائي ذلك خاصة وأن النظام المعلوماتي يمتلك كيانا معنويا مهدد بزوال آثار الاعتداء عليه في أية لحظة، الأمر الذي يحتم توفر عاملي السرعة والدقة من قبل المحقق والتي تفرضها الطبيعة الخاصة للجرائم المعلوماتية.

المطلب الأول: السلطة القضائية المختصة بالتحقيق الابتدائي في الجرائم المعلوماتية

قبل الاعتراف بضرورة وجود تشريعات خاصة بالجرائم المعلوماتية فإنّه يثور السؤال كذلك حول التشريع الضروري لتنظيم مكافحة الجرائم المعلوماتية، ذلك أنّ السلطات المخولة لجهات التحقيق الابتدائي[1] في هذا النوع الجرائم تنظمها الأحكام الجزائية المطبقة على الجرائم العادية، وهو ما سبب في حدوث مشاكل أكثر لا يمكن حلها، من هنا ظهرت ضرورة وجود قانون إجرائي خاص يواجه هذا النوع من الجرائم المستحدثة.

إنّ النيابة العامة وقاضي التحقيق وغرفة الاتهام هم من لديهم سلطة التحقيق الابتدائي في شتى الجرائم المختلفة على حسب درجة خطورتها من مخالفة أو جنحة أو جناية، فمثلا يعتبر قاضي التحقيق صاحب الاختصاص الأصيل بالتحقيق الابتدائي في الجرائم الخطيرة والمستحدثة كالتي في شكل الجرائم المعلوماتية، هذه الجرائم طبقا للتشريع الجزائري لابد وأن يحقق قاضي التحقيق فيها بشكل خاص وذلك بعد طلب من وكيل الجمهورية، هذا الأخير الذي يتمتع بسلطات واسعة خولت له الاتهام وكذا التدخل أثناء هذه المرحلة الحساسة من الدعوى العمومية مرحلة التحقيق الابتدائي.

وهو ما يفسر بأنّ الاستقلالية في التحقيق بالنسبة لقاضي التحقيق في التشريع الجزائري هي استقلالية نسبية، لأنّ المشرع خول للنيابة العامة سلطات واسعة وشاملة لكافة إجراءات التحقيق بحيث

[1] Qianyun Wang, A Comparative Study of Cybercrime in Criminal Law: China US England, Singapore and the Council of Europe, erasmus university rotterdam 2016 P269.

لا يكاد يخلو أي إجراء من تدخلها ورقابتها، بدءا من عملية اختيار قاضي التحقيق وتكليفه بإجراء التحقيق وكذا رقابتها أثناء سير التحقيق من خلال الاطلاع على مجرياته وحضورها بعض إجراءاته متى شأت، إلى غاية حقها بالطعن في جميع أوامره[1].

الفرع الأول: قاضي التحقيق كصاحب اختصاص أصيل للتحقيق في الجرائم المعلوماتية

تعود الملامح الأولى لنظام قاضي التحقيق إلى القانون الفرنسي، وبالنظر للروابط التاريخية بين الجزائر وفرنسا خاصة قبل سنة 1962 أين كان يحكم البلدين قانونا واحدا باستثناء بعض أوجه الاختلاف، لذا يمكن القول أنّه بعد سنة 1962 وإلى يومنا هذا وخصوصا فيما يتعلق ق إ ج فإنّ ما يجمعهما أكثر مما يفرقهما، وهذا الذي يدل بأنّ نظام قاضي التحقيق في الجزائر تعود جذوره التاريخية لنظام قاضي التحقيق في فرنسا[2].

هذا ويعتبر قاضي التحقيق في القانون الفرنسي هو القاضي المسؤول عن التحقيقات القضائية في القضايا الجنائية الأكثر خطورة أو المعقدة ولديه مهمة مزدوجة والمتمثلة في المضي قدما بكل نزاهة في إظهار الحقيقة واتخاذ قرارات قضائية معينة، ويتمتع كذلك بسلطات واسعة تسمح له بالعمل بفعالية في إظهار الحقيقة بحيث يمكنه التحرك على الفور وإجراء عمليات التفتيش والضبط وطلب آراء الخبراء والاستماع إلى الضحايا والشهود، إلاّ أنّه من الناحية العملية لا يمارس معظم هذه السلطات بصفة مباشرة لأنّه يفوضها إلى الشرطة القضائية في إطار ما يسمى بالإنابة القضائية[3].

وكما هو معلوم فإنّ الجرائم المعلوماتية تعتبر من بين الجرائم الخطيرة ذات الطبيعة الخاصة لذا تتطلب تحقيقا خاصا اتجاهها، وهو الأمر الذي يلزم قاضي التحقيق بأن يكون على دراية مقبولة بعلوم

---

[1] كعوان أحمد، مبدأ الفصل بين سلطتي الاتهام والتحقيق في قانون الإجراءات الجزائية الجزائري، مجلة صوت القانون، المجلد 5 العدد1، جامعة الجيلالي بونعامة بخميس مليانة، الجزائر، 2018، ص125.

[2] عمارة فوزي، قاضي التحقيق، عمل مقدم لنيل شهادة الدكتوراه علوم، كلية الحقوق، جامعة الإخوة منتوري قسنطينة، الجزائر الموسم الجامعي 2010/2009، ص5.

[3] vie publique au cœur du débat public , À quoi sert le juge d'instruction, À propos du site vie-publique, www.vie-publique.fr, Date de lecture 29/05/2020 .

الحاسبات الآلية تؤهله للخوض في مجال التحقيق المعلوماتية أو على الأقل يكون على دراية تامة بما يقوم به ضابط الشرطة القضائية من تقنيات أثناء تحرياته وكذا الخبير المعلوماتي المسخر لذلك، فخصوصية التحقيق في الجرائم المعلوماتية تستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع خصوصية الجرائم المتعلقة بالحاسب الآلي وتمكن قاضي التحقيق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين.

ولأجل تحقيق ذلك وفضلا عن تطوير الإجراءات الجزائية يجب تدريب كوادر التحقيق مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال، وكما أنّ الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي فهي أوجب وألزم في مجال الجرائم المعلوماتية، هذه الأخيرة التي تتعلق بمسائل فنية غاية في التعقيد ومحل الجريمة فيها غالبا ما يكون غير مادي، كما أنّها سريعة التطور في أساليب ارتكابها حتى أنّ غموضها لا يستطيع أن يكشفه سوى متخصص ومن على درجة كبيرة من التميز في مجال تخصصه، فإجرام الذكاء والفن لا يكشفه ولا يحله إلاّ ذكاء وفن متماثلين[1].

وبالرجوع للتشريع الجزائري فإنّ كل من النيابة العامة وقاضي التحقيق هما من يتوليان كأصل عام مهمة التحقيق الابتدائي بحيث لا يتم إحالة المتهم إلى المحاكمة إلاّ بعد عرضه على سلطة التحقيق للتأكد من ثبوت أدلة الاتهام عليه من عدمها[2] خاصة في الجرائم المتعلقة بالمعلوماتية، وهي المهمة والمرحلة الصعبة في الدعوى العمومية ككل، أين يجد قاضي التحقيق نفسه ملزما بحفظ أدلتها الكافية والتي على أساسها يحيل المتهم المعلوماتي إلى المحاكمة، وهو الأمر الذي يوفر الجهد والوقت على قضاء الموضوع فلا يمثل أمام القاضي الجزائي إلاّ من توافرت ضده أدلة كافية فلا تعرض عليه إلاّ القضايا المستندة على أسس قانونية وواقعية متينة، لذلك فإنّ مهمة النيابة العامة وقاضي التحقيق هي صعبة للغاية تتطلب الكثير من الجهد والتركيز والفن والذكاء في نفس الوقت.

---

[1] أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، د ط، دار النهضة العربية، القاهرة، مصر، 2015، ص259.

[2] قودة حنان، التصدي في مرحلتي التحقيق والمحاكمة، مجلة الباحث للدراسات الأكاديمية، المجلد 6، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة 1، الجزائر، 2019، ص894.

هذا ويستوجب التحقيق في الغالب القيام بإجراء عدة عمليات مادية والتي قد يكون لازما إجراؤها في نفس الوقت وفي أماكن مختلفة، وهكذا يجد قاضي التحقيق نفسه في العديد من الحالات ملزما باللجوء إلى غيره للاستعانة به في أداء مهمته في مثل هذه الحالات، وهو ما يعرف بإجراء الإنابة القضائية والتي يكلف بمقتضاها قاضي التحقيق أشخاصا وضعهم القانون تحت تصرفه بغرض إتمام بعض أعمال التحقيق استنادا للسلطات المفوضة لهم[1].

لذلك أجاز المشرع الجزائري لقاضي التحقيق الأخذ بهذا الإجراء بأن يكلف أي قاض من قضاة محكمته أو أي ضابط شرطة قضائية مختص بالعمل في تلك الدائرة أو أي قاض من قضاة التحقيق بالقيام بما يراه مناسبا من إجراءات التحقيق، على أن يذكر قاضي التحقيق في الإنابة نوع الجريمة موضوع المتابعة كما ليس له أن يعطي تفويضا عاما بطريق هذه الإنابة أين يقوم القضاة أو ضباط الشرطة القضائية المنتدبون بتنفيذ جميع السلطات المخولة لقاضي التحقيق لكن في حدود الإنابة القضائية، هذا ولا يجوز لضباط الشرطة القضائية استجواب المتهم أو القيام بمواجهته أو سماع أقوال المدعي المدني[2].

الفرع الثاني: الاختصاص المحلي لوكيل الجمهورية في الجرائم المعلوماتية

كنا قد تطرقا سابقا لتعريف الاختصاص المحلي بشكل عام والذي استنبطنا منه تعريف الاختصاص المحلي لقاضي التحقيق، هذا الاختصاص الأخير الذي يبقى خاضعا لأحكام نص المادة 40 من ق إ ج الجزائري، وقلنا أنّ هذه المادة أخذت بالمعايير المنصوص عليها في المادة 37 من نفس القانون والمتعلقة بالاختصاص المحلي لوكيل الجمهورية والذي يعرف بأنّه: " تلك الدائرة القضائية التي يستطيع فيها وكيل الجمهورية مباشرة وظيفته بصفة مباشرة طبقا لقانون الإجراءات الجزائية"[3].

---

[1] عبد المجيد زعلاني، الإنابات القضائية لقاضي التحقيق، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 35، العدد 4، كلية الحقوق جامعة الجزائر، ديسمبر 1998، ص10.

[2] المادة 138 من أمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] مولاي ملياني بغدادي، الإجراءات الجزائية في التشريع الجزائري، د ط، المؤسسة الوطنية للكتاب، الجزائر، 1992، ص139.

هذا الاختصاص يعتبر كأحد قواعد الاختصاص المحلي، ولما كانت هذه القواعد تعتبر من النظام العام أين يمكن إثارتها في أي مرحلة من مرحلة التقاضي سواء أمام المحكمة أو المجلس في حالة الاستئناف لأول مرة أو أمام المحكمة العليا، فيجب على القاضي إثارتها من تلقاء نفسه حتى ولو لم يثرها الأطراف وبالتالي وكأصل عام لا يجب أن يتعدى الاختصاص المحلي لوكيل الجمهورية إحدى الحالات المنصوص عليها في الفقرة 1 من المادة 37 من ق إ ج والمتمثلة في مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر[1].

وكاستثناء عن الأصل العام فإنّ الجرائم المعلوماتية باعتبارها وبطبيعتها من أبرز الجرائم العابرة للحدود بل وحتى للقارات، كان من اللازم على المشرع توسيع الاختصاص الإقليمي لوكيل الجمهورية عن طريق التنظيم ليشمل دائرة اختصاص محاكم أخرى[2] خلافا لما ورد في القواعد العامة، وهو ما ترجمه المرسوم التنفيذي 06 – 348 الذي مدد الاختصاص الإقليمي لوكلاء الجمهورية لمحكمة سيدي أمحمد ومحكمة قسنطينة ومحكمة وهران ومحكمة وورقلة إلى عدد من محاكم المجالس القضائية، ومدد معه بالموازاة اختصاص النائب العام المتبوع من طرف وكيل الجمهورية الذي مدد اختصاصه بموجب المرسوم الأخير.

فمن الطبيعي أن يشمل الاختصاص الإقليمي للنائب دائرة اختصاص كافة المجالس التي أحلقت باختصاص وكيل الجمهورية التابع له[3]، هذا الأخير يلزمه إذا ما كان مختصا لدى المحكمة الكائن بها مكان الجريمة المعلوماتية وإذا ما أخبر وأبلغ من طرف ضباط الشرطة القضائية بأصل وبنسختين من

---

[1] بن مكي نجاة، المرجع السابق، ص213.

[2] الفقرة 2 من المادة 37 من قانون رقم 04 – 14، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[3] قحموص نوال، قواعد الاختصاص القضائي بجرائم الفساد، مجلة دراسات في الوظيفة العامة، المجلد 2، العدد 1، المركز الجامعي بالبيض، الجزائر جوان 2015، ص3.

إجراءات التحقيق أن يرسل نسخة من إجراءات التحقيق إلى وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع[1].

هذا الأخير بعد أخذ رأي النائب العام يطالب بالإجراءات فورا إذا ما اعتبر أن الجريمة المعلوماتية موضوع التحقيق تدخل ضمن اختصاص المحكمة الأخيرة الذكر، ويتلقى بعد ذلك ضباط الشرطة القضائية العاملون بدائرة اختصاص المحكمة الكائن بها مكان الجريمة المعلوماتية التعليمات مباشرة من وكيل الجمهورية لدى هذه الجهة القضائية[2] ذات الاختصاص الإقليمي الموسع.

هذا وإذا تبين لهذا الأخير بأنّ هناك عناصر جديدة في ملف الإجراءات المتعلقة بالجريمة المعلوماتية من شأنها أن تؤدي إلى اختصاص وكيل جمهورية القطب الجزائي الاقتصادي والمالي فيمكنه أن يخبر هذا الأخير[3] الذي يستطيع أن يطالب بهذا الملف سواء من وكيل الجمهورية المخبر أثناء التحريات الأولية أو من قاضي التحقيق المخطر في حالة فتح تحقيق قضائي.

الفرع الثالث: الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية

بوجه عام فإنّ الاختصاص بمفهومه الإجرائي في المجال القضائي يمثل نصيب كل محكمة قضائية من الدعاوي التي تقررت لها ولاية الفصل فيها، فتكون لها الصلاحية في مباشرتها وبسط سلطانها للتصرف فيها[4]، أمّا الاختصاص المحلي فيعني ولاية الجهة القضائية بالنظر في الدعوى المعروضة أمامها استنادا إلى المعيار الجغرافي، بحيث ترمي قواعد الاختصاص الإقليمي إلى تعيين الدائرة الجغرافية للمحكمة

---

[1] المادة 40 مكرر1 من الأمر رقم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[2] المادة 40 مكرر2 من الأمر رقم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[3] الفقرة 03 من المادة 211 مكرر11 من الأمر قم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[4] بدر الدين شبل، الاختصاص الجنائي العالمي ودوره في تفعيل العدالة الدولية الجنائية، مجلة العلوم القانونية والسياسية، المجلد1 العدد 1، جامعة الوادي الجزائر، جوان 2010، ص109.

التي يؤول إليها الاختصاص في الفصل القضية من حيث موقعها[1]، وكقياس على ذلك فإن اختصاص قاضي التحقيق المحلي يمثل نصيبه من القضايا التي تقررت له ولاية الفصل فيها بحيث تكون له صلاحية مباشرتها وبسط سلطانه فيها شريطة عدم تجاوزه لإقليمه الذي حدده له المشرع.

هذا ويتحدد الاختصاص المحلي لقاضي التحقيق طبقا ل ق إ ج الجزائري[2] كأصل عام بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر[3]، أمّا إذا ما كان الأمر متعلق بجرائم خطيرة والتي حددها المشرع على سبيل الحصر كالجرائم المعلوماتية، فهنا المشرع وسع من اختصاص قاضي التحقيق ليشمل محاكم أخرى، لذلك يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى[4].

وعليه يصبح لقاضي التحقيق التابع لمحكمة جزائية ما اختصاصا إقليميا موسعا يتجاوز اختصاصه العادي أين يمكنه التنقل أو انتداب أي ضابط شرطة قضائية من أجل القيام بمهام متعلقة بالتحقيق القضائي في هذه الجرائم المعلوماتية، وهذا التوسيع من المشرع في الاختصاص المحلي لقاضي التحقيق وتطبيق هذه الإجراءات يكون عن طريق التنظيم[5].

هذا ويبقى الاختصاص المحلي لقاضي التحقيق في التشريع الجزائري خاضع ل ق إ ج وفقا لما نظمته المادة 40 التي أشرنا إليها سابقا، والتي أخذت بالمعايير المنصوص عليها في المادة 37 من ق إ

---

[1] مولاي عبد المالك، فنينخ عبد القادر، الدفع بعدم الاختصاص الإقليمي أمام القاضي العقاري، مجلة القانون العقاري والبيئة المجلد 7، العدد 1 جامعة بن باديس بمستغانم، الجزائر، جوان 2019، ص12.

[2] قانون رقم 04- 14، مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[3] الفقرة 1 من المادة 40 من قانون رقم 04- 14 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[4] الفقرة 2 من المادة 40 من قانون رقم 04- 14 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[5] بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، د ط، دار الخلدونية، الجزائر، القبة القديمة، الجزائر، 2017، ص215.

ج[1]، لذلك يبقى قاضي التحقيق تابعا وخاضعا لأحكام هذه المادة الأخيرة حتى أنّه وطبقا للفقرة 1 من نص المادة 67 من ق إ ج لا يجوز له أن يجري تحقيقا دون طلب ذلك من وكيل الجمهورية.

ولما كانت جريمة المساس بأنظمة المعالجة الآلية للمعطيات والتي هي أحد الجرائم المعلوماتية والتي قد ترتكب في مكان معين وتكون آثارها في مكان آخر[2] فإنّ المشرع الجزائري وبموجب نص المادة 40 الفقرة 2 أجاز تمديد الاختصاص المحلي لقاضي التحقيق بالقطب الجزائي المتخصص إلى دائرة اختصاص المحاكم الأخرى المحددة في التنظيم[3]، ونص على مختلف الإجراءات التي من الممكن أن تتخذ في هذا النوع من الجرائم من خلال تعديل الذي مس ق إ ج[4] الجزائري سنة 2020.

هذا وقد يكون قاضي التحقيق مطالبا بملف الإجراءات من طرف وكيل الجمهورية لدى المحكمة ذات الاختصاص الإقليمي الموسع بعد أن يأخذ هذا الأخير رأي النائب العام، وفي حالة فتح تحقيق قضائي مثلا حول جريمة معلوماتية يصدر قاضي التحقيق أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة ذات الاختصاص الموسع، أين يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة التعليمات مباشرة من هذا القاضي التحقيق الأخير[5].

---

[1] تنص المادة 37 من قانون رقم 04- 14 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004 بأنّه : " يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

[2] ناني لحسن، المرجع السابق، ص54.

[3] مرسوم تنفيذي رقم 06 – 348 المؤرخ في 5 أكتوبر 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر رقم 63، الصادرة بتاريخ 8 أكتوبر 2006.

[4] أمر رقم 20-04 المؤرخ في 30 غشت 2020، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[5] المادة 40 مكرر3 من الأمر قم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

هذا ويبقى الأمر بالقبض أو الأمر بالحبس المؤقت الذي صدر ضد المتهم من قاضي التحقيق الأول محتفظا بقوته التنفيذية حتى تفصل فيه المحكمة المختصة[1]، كما يجوز له أو بناء على طلب النيابة العامة أن يأمر باتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة المعلوماتية أو التي استعملت في ارتكابها وذلك طول مدة الإجراءات[2].

هذان القاضيان قد يصدرا أمرا بالتخلي عن ملف الإجراءات الخاص بالجريمة المعلوماتية لصالح قاضي التحقيق بالقطب الجزائي الاقتصادي والمالي إذا ما طالب به وكيل الجمهورية بالقطب الجزائي الاقتصادي والمالي عندما يرى بأنّ هناك عناصر جديدة في هذا الملف تغير في تكييف الجريمة من جريمة معلوماتية إلى جريمة ذات طابع اقتصادي ومالي[3]، هذا وتبقى أوامر القبض والحبس المؤقت منتجة لآثارها إلى غاية صدور أمر مخالف من قاضي التحقيق الأخير، كما لا تجدد إجراءات المتابعة والتحقيق وكذا الإجراءات الشكلية المتخذة[4].

الفرع الرابع: غرفة الاتهام كدرجة تحقيق ثانية حول بعض الجرائم المعلوماتية

إنّ الحاجة إلى جهاز قضائي يكون بمثابة المصفاة بين التحقيق وجهة الحكم أين يقدر قيمة الأدلة ويكون كذلك ضمانا لحرية قرار القضاة ويحافظ على استقلالية القاضي من الضغوطات الخارجية كما يكون القرار الصادر عنه لا يتعلق بقاض فرد، هي كلها أسباب مقنعة أدت إلى خلق المشرع لما يسمى بغرفة الاتهام، هذه الأخيرة تتصل بالدعوى عندما يتنحى قاضي التحقيق عن نظر ملف الدعوى عند خروجه من يده ووصوله بالطرق القانونية إلى هذه الغرفة.

---

[1] المادة 40 مكرر4 من قانون رقم 04- 14 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[2] المادة 40 مكرر5 من قانون رقم 04- 14 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71 الصادرة بتاريخ 10 نوفمبر 2004.

[3] المادة 211 مكرر10 من الأمر رقم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[4] المادة 213 مكرر10 من الأمر قم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

وهو الأمر الذي جعلها صاحبة السلطة عليه أين تتكفل برقابة العناصر المادية والقانونية لكل قضية تعرض عليها، وغرفة الاتهام ليست مقيدة بوقائع الدعوي كما رفعت إليها فالقانون لم يقيدها بذلك بحيث خول لها سلطة كاملة في تقدير الوقائع واستكمال عناصرها المادية والقانونية، وكذلك خول لها تكييف الواقعة التي نتجت عنها الجريمة وإعطائها التكييف القانوني الصحيح الذي ترى أنّه الأكثر انطباقا عليها من الوصف الأول الوارد في طلبات النيابة وفي أوامر قاضي التحقيق[1].

إنّ اتصال غرفة الاتهام بملف الدعوى في التشريع الجزائري يكون بطلب ومن تقديم النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة، وذلك بعد ما يصل هذا الأخير من قاضي التحقيق ملف الدعوى وقائمة بأدلة الإثبات تفيد بأنّ الوقائع تكون جريمة وصفها القانوني جناية، هذا ويبقى أمر الإيداع أو القبض الصادر من جهة التحقيق ضد المتهم منتجا لآثاره إلى حين الفصل في القضية من طرف الجهة المحال إليها أو إلى حين القضاء بانتفاء وجه الدعوى من طرف غرفة الاتهام ما لم يفرج على المتهم قبل ذلك[2].

ولما كان الأمر متعلق بالجرائم المعلوماتية ذات الطبيعة المتميزة وبالخصوص في التشريع الجزائري فمن الممكن أن يكون لها قابلية للإحالة إلى غرفة الاتهام من أجل إكمال التحقيق فيها، ذلك أنّ الجرائم المعلوماتية لم يعد نطاقها محصورا في جنحة المساس بأنظمة المعالجة الآلية للمعطيات أو جنحة المساس بحقوق المؤلف والحقوق المجاورة في البيئة الرقمية، بل أصبح نطاقها موسعا مع صدور القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها أين أصبحت موضوعاتها كثيرة ومتعددة وأصبح وصفها يدور بين الجنحة والجناية.

---

[1] فوزي عمارة، غرفة الاتهام بين الاتهام والتحقيق، مجلة العلوم الإنسانية، المجلد 19، العدد 2، جامعة الإخوة منتوري قسنطينة الجزائر ديسمبر 2008، ص204- ص207.

[2] المادة 166 من قانون رقم 17 – 07، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20، المؤرخة في 29 مارس 2017.

فالمشرع الجزائري أراد من خلال توسيعه لنطاق الجرائم المعلوماتية مواكبة التطور السريع والهائل لتكنولوجيا الإعلام والاتصال فأصبح لدينا من خلال تعريفه[1] لهذه الجرائم عالما طبيعيا يقابله عالما افتراضيا تمارس فيه شتى الجرائم الموجودة في العالم الأول من قذف وسب وتشهير وسرقة واحتيال وإرهاب، يبقى المشكل في تكييفها بالمعنى التطبيقي للقانون المنظم لبعض هذه الجرائم ذلك أنّ المشرع نفسه نص على جرائم ترتكب بواسطة تكنولوجيا الإعلام والاتصال أعطاها وصف الجرائم الاقتصادية والمالية الأكثر تعقيدا[2].

وإسقاطا على الذي مضى فإنّ احتمال الاعتداء على منظومة معلوماتية بشكل يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني المتطرق له في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها والتي تعتبر صورة من صور الجرائم المعلوماتية[3] فهي تعد من بين أبرز الجرائم التي يمكن إعطاؤها الوصف الذي أتت به في قانون العقوبات والتي جاءت في أغلبها بوصف جنايات كجريمة التخابر[4] مع دولة أجنبية المنصوص في قانون العقوبات، والتي قد ترتكب بواسطة الاعتداء على منظومة معلوماتية.

---

[1] الفقرة أ من المادة 2 من القانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] الفقرة 02 من المادة 211 مكرر3 من الأمر قم 20- 04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[3] الفقرة ب من المادة 4 من قانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[4] تنص المادة 61 من قانون رقم 06 – 23 المعدل والمتمم للأمر66-156 المتضمن ق ع الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006 بأنّه : " يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم بأحد الأفعال التالية:

1 - .....

2 – القيام بالتخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى"

وهو الأمر الذي يلزم إحالتها بعد التحقيق فيها إلى غرفة الاتهام وفقا للإجراءات المنصوص عليها في المادة السابقة الذكر 166 من ق إ ج الجزائري، لكن يبقى الإشكال يثور حول الجريمة الأخيرة أنّها تبقى داخلة في نطاق جرائم الخيانة والتجسس المنصوص عليها في قانون العقوبات[1]، ولا يمكن إدخالها في نطاق الجرائم المعلوماتية خاصة وأنّ القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها لم يعطي أي عقوبات لهذه الاعتداءات الخطيرة، لذلك يبقى على عاتق المشرع الجزائري أن يعيد النظر في عقوبات هذه الجريمة بحيث تكون أشد من التي جاء بها قانون العقوبات، ذلك أنّها ترتكب بوسيلة تسرع من عملية ارتكابها كما أنّها غالبا ما تحدث في بيئة رقمية صعبة الكشف والإثبات.

المطلب الثاني: السلطات العملية لقاضي التحقيق في الجرائم المعلوماتية

إنّ الهدف الأساسي من وراء وضع قانون إجرائي يشمل مكافحة الجرائم المعلوماتية خاصة من خلال القدرة على اعتراض الاتصالات الإلكترونية للمجرمين المعلوماتيين، سوى لأنّ مختلف الأنظمة القانونية الدولية رأت فيه بأنّه الحل الأمثل وبأنّ مختلف القوى الاقتصادية الكبرى قد تبنته من قبل والتي قدمت ضمانات مختلفة ضد انتهاكات سلطات تطبيق القانون، فعلى سبيل المثال يتضمن قانون ماليزيا المتطلبات التي تسمح لقوات الشرطة اعتراض الاتصالات لكن بموافقة المدعي العام[2].

علاوة على ذلك اتبعت نيوزيلندا نهجًا محايدًا فيما يتعلق بالتكنولوجيا من خلال تطبيق نفس القواعد والضمانات لسلطة اعتراض الاتصالات الإلكترونية بالضبط مثل التي كانت لديها من قبل في سلطة اعتراض الاتصالات الصوتية، لهذا يبدو واضحا أن الطبيعة الدقيقة للقيود على استخدام سلطة الاعتراض قد تختلف على أساس النظام القانوني للاقتصاد، وتاريخ الشرطة القوي وبيئتها السياسية ومفهوم ونطاق وطبيعة مشكلة الجريمة المعلوماتية.

---

[1] جرائم الخيانة والتجسس نص عليها في القسم الأول من الفصل الأول من الباب الأول من الكتاب الثالث ضمن المواد 61 62 63، 64 من الأمر رقم 66-156، المتضمن ق ع الجزائري، ج ر رقم 49 المؤرخة في 11 يونيو 1966.

[2] I-WAYS, Cybercrime Laws Prevention and Enforcement Capacity Builds Digest of Electronic Commerce Policy and Regulation, IOS Press, 2003, p119.

هذا وكنا قد تطرقنا من خلال الفروع السابقة إلى السلطة الأصيلة المخول لها التحقيق الابتدائي في الجرائم المعلوماتية داخل صرح التشريع الجزائري، هذه السلطة تمثلت في شخص قاضي التحقيق الذي منحه ق إ ج عدة سلطات عملية أولية لابد وأن يقوم بها على وجه السرعة والتي حتمتها الطبيعة الخاصة للجرائم المعلوماتية، فقاضي التحقيق قبل قيامه بمهامه التقليدية[1] التي يطبقها على أنواع الجرائم الأخرى لابد له وأن يقوم بنفس الإجراءات والسلطات المتطرق لها سابقا في الباب الأول والتي يأذن بقيامها من قبل ضباط الشرطة القضائية من إجراءات المعاينة والتفتيش والضبط والخبرة وإشرافه على إجراءات التسرب وكذا أسلوب الترصد الإلكتروني بمختلف أشكاله لكشف مختلف الجرائم المعلوماتية.

الفرع الأول: القيام بإجرائي المعاينة والخبرة في المنظومات المعلوماتية

إنّ عمليات التحقيق إذا ما تمت قبل تحريك الدعوى العمومية فهي تعد من قبيل أعمال الاستدلال وهي الأعمال التي غالبا ما يقوم بها ضباط الشرطة القضائية، أمّا في حالة ما إذا تمت بعد تحريك الدعوى العمومية فهي من قبيل أعمال التحقيق الابتدائي والتي غالبا ما يقوم بها قاضي التحقيق كصاحب اختصاص أصيل، وعليه فإذا ما قام قاضي التحقيق بإجراء المعاينة والخبرة للمنظومات المعلوماتية فإن هذه المعاينة والخبرة تعد عملا من عمل التحقيق[2].

هذا وتعتبر المعاينة والخبرة من أكبر العقبات التي قد تواجه الإثبات في الجرائم المعلوماتية وذلك نظرا لحداثة هذه الأخيرة وحاجتها الماسة لخبراء ومختصين في مجال تكنولوجيا الإعلام والاتصال مع ضرورة مواكبتهم للتطورات الهائلة في مجال الاتصالات وتكنولوجيا المعلومات بالشكل الذي يُمَكن من الاعتماد عليهم لغرض التوصل إلى مختلف الأدلة التي من شأنها أن تساهم في إثبات هذا النوع من الجرائم المستحدثة.

---

[1] نقصد بالمهام التقليدية هنا تلك المهام التي يقوم بها قاضي التحقيق والمتعلقة بالاستجواب والسماع والمواجهة والتي سنتطرق لها من خلال العناصر الآتية.

[2] علي جبار الحسيناوي، المرجع السابق، ص115.

أولا: إجراء المعاينة

المعاينة عموما إجراء ينتقل بموجبه المحقق إلى مكان وقوع الجريمة ليشاهد وليقوم بعملية فحص دقيقة للأدلة المادية للجريمة ولآثارها ومكان وقوعها مع الأخذ بالإجراءات الضرورية للحفاظ على أدلة الجريمة[1]، والمحقق في التشريع الجزائري ضمن هذه المرحلة من سير الدعوى العمومية ممثل في شخص قاضي التحقيق، يجوز له القيام بإجراء المعاينات اللازمة في هذه المرحلة أين يمكنه الانتقال إلى مكان وقوع الجريمة والقيام بها بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته، ويجب عليه أن يستعين دائما بكاتب التحقيق لتحرير كل ما يقوم به من إجراءات ضمن محضر مُعد لذلك[2].

هذا وتبقى المعاينة التي يقوم بها قاضي التحقيق في الجرائم المعلوماتية من حيث إجراءات العمل بها مثل التي تطرقنا لها من خلال الباب الأول عند حديثنا عن إجراء المعاينة التي يقوم بها ضابط الشرطة القضائية، فإذا ما أراد قاضي التحقيق الانتقال للمعاينة والاعتماد عليها كإجراء، فعليه أن يراعي كل القواعد والإرشادات الفنية حتى يكون الدليل المستمد من هذه المعاينة مساعد في الكشف عن الحقيقة ومتمتع بقوة إثبات يغني في مرحلة المحاكمة.

هذا الانتقال كما تم توضيحه سابقا قد لا يكون بالضرورة عبر العالم المادي فقد يتم بطريق العالم الافتراضي أين يستطيع قاضي التحقيق القيام بعملية المعاينة من خلال حاسوبه الموجود بمكتبه أو من خلال اللجوء لمقهى الإنترنيت، كما يمكنه كذلك اللجوء لمزود خدمة الإنترنيت والذي يعتبر من أفضل الأمكنة التي يستطيع من خلالها إجراء المعاينة، فهذه الأخيرة تختلف في الجرائم المعلوماتية بسبب طبيعة الدليل الإلكتروني غير المرئي والقابل للمحو، والتي تلزم وتجبر قاضي التحقيق قبل الانتقال الافتراضي لمسرح الجريمة القيام بنفس الخطوات التي يجب أن يقوم بها ضباط الشرطة القضائية والتي تطرقنا لها سابقا.

---

[1] أشرف على قوقزة، الوسائل الإلكترونية لارتكاب جرائم الذم والقدح والتحقير في التشريع الأردني والاتفاقيات الدولية دراسة تحليلية مقارنة، د ط، دار المناهج للنشر والتوزيع، عمان، الأردن، 2017، ص121.

[2] المادة 79 من الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

خاصة من خلال حسن توظيف الخبرة، ذلك أنّ الخبير يمكنه البحث عن الأدلة الرقمية وتوقع العثور عليها في الجرائم المعلوماتية وملاحظة المعلومات التي يكون من الصعب للغاية أو حتى المستحيل الحصول عليها[1]، هذا ويبقى نجاح أية عملية معاينة بطريق العالم الافتراضي مرهون بمدى اختصاص ومعرفة قاضي التحقيق بالمعلوماتية عموما وبنظمها خصوصا ناهيك عن كيفية تشغيلها ووسائلها وتقنيات إساءة استعمالها من قبل مستخدميها، ولا يتأتى ذلك سوى بالتكوين والتدريب الدوري لقضاة التحقيق وتجديد معارفهم حتى يتسنى لهم اكتساب مهارات عالية تؤهلهم للكشف عن مثل هذه الجرائم.

ثانيا: إجراء الخبرة

الغرض من الخبرة هو استرجاع المعلومات ذات قيمة في الإثبات من خلال تقنيات تعمل على نسخ "شيئًا فشيئًا" المعلومات المخزنة والممحاة، وحل تشفير الملفات أو التوقيعات الرقمية، التي يمكن أن تبرز وتجلب عدة تغييرات[2]، فالعاملين في مجال القضاء والمتعاملين معه يعلمون علم اليقين بأنّ القضايا الجزائية تُبنى في البداية على التصريحات التي قد يدلي بها المتهم والضحية إن وجد والشهود عن الوقائع وهؤلاء جميعا قد يتراجعون عن أقوالهم في أي مرحلة من مراحل الدعوى، لذلك يكتسي التحقيق أهمية بالغة في تحقيق العدالة من حيث إثبات الوقائع الجنائية إلى فاعليها أو نفيها، هذا الإثبات الذي يصعب أمره في الجرائم ذات الطبيعة التقنية مثل الجرائم المعلوماتية أو الجرائم التي تحتاج إلى أمور تقنية للكشف عنها، من هنا يتضح دور الخبرة الجنائية في توضيح الغموض عن مثل هذه الجرائم[3].

---

[1] Joakim Kävrestad, the previous reference, p61.

[2] Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité La référence précédente, p10.

[3] فروحات سعيد، السلطة التقديرية للقاضي الجنائي في التعامل مع الخبرة الجنائية، مجلة الواحات للبحوث والدراسات، المجلد 9 العدد 2، جامعة غرداية، الجزائر، ديسمبر 2016، ص121.

فالخبرة طريق من طرق التحقيق يُؤخذ بها كذلك في مرحلة التحقيق الابتدائي، وهي في المسائل الجزائية تبدأ من مرحلة ملاحظة الجريمة إلى إنزال العقوبة بالفاعل[1]، لذلك فإنّ أمر القاضي بندب خبير يعتبر دليل على أنّ هذا الأخير تنقصه المعرفة اللازمة في الأمور الفنية والتقنية، فلا مبرر لتدخله في تلك النواحي ولا يحق له أن يقيد الخبير بإتباع وسيلة فنية معينة[2]، هذا وتعتبر الجرائم المعلوماتية من المسائل الجزائية التي تفرض على قاضي التحقيق أن يندب لها خبيرا في مجال المعلوماتية، لديه من المهارات الفنية التي تؤهله لكشف مختلف الاعتداءات والاختراقات على المنظومة المعلوماتية للمجني عليه.

وبالرجوع إلى التشريع الجزائري نلاحظ أنّه فصل في مسألة الخبرة الجزائية أين أشار لها في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها عندما أجاز لقاضي التحقيق بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو له دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدته وتزويده بكل المعلومات الضرورية لإنجاز مهمته[3] وكذلك نظمها ضمن ق إ ج، فإذا ما عرضت لقاضي التحقيق مسألة ذات طابع فني كالجرائم المعلوماتية مثلا، فله أن يأمر بندب خبير من تلقاء نفسه أو بطلب من النيابة العامة وحتى بطلب من الخصوم.

هذا الخبير يقوم بأداء مهمته تحت رقابة هذا القاضي[4]، هذه المهمة التي يجب أن تحدد في قرار الندب والتي لا يجوز أن تهدف إلاّ إلى فحص مسائل ذات طابع فني[5]، ويقوم الخبراء بمهمتهم وهم على اتصال مع قاضي التحقيق الذي يجب أن يحيطوه علما بتطورات الأعمال التي يقومون بها، ويمكنوه في

---

[1] زروقي عاسية، الخبرة الجزائية ومدى سلطة القاضي الجزائي في تقديرها، مجلة معالم للدراسات القانونية والسياسية، المجلد 3، العدد1 المركز الجامعي بتندوف، الجزائر، جوان 2019، ص100.

[2] مسعودان فتيحة، الدور الإيجابي للقاضي في الخبرة القضائية، مجلة الدراسات القانونية، المجلد 3، العدد 2، جامعة يحي فارس بالمدية الجزائر، جوان 2017، ص477.

[3] الفقرة 4 من المادة 5 من قانون 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[4] المادة 143 من قانون رقم 06 – 22 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[5] المادة 146 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

كل حين من أي شيء يجعله قادرا على اتخاذ الإجراءات اللازمة[1]، هذا ويجوز لقاضي التحقيق في حالة ما إذا طلب الخبراء الاستنارة في مسألة خارجة عن دائرة تخصصهم أن يصرح لهم بضم فنيين مختارين لتخصصهم[2]، كما يجوز له أثناء القيام بإجراءاته أن يستعين بالخبراء إذا رأى لزوما لذلك[3].

هذا ويبقى كل قرار صادر من قاضي التحقيق بندب خبير أو خبراء خاضع لشكليات وشروط معينة تلزم الخبير على التقيد بها تحت طائلة استبدالهم بغيرهم من الخبراء وحتى اتخاذ ضدهم تدابير تأديبية قد تصل إلى شطب أسمائهم من جدول الخبراء، وفي حالة استبدالهم بغيرهم من الخبراء فعليهم أن يقدموا النتائج التي جادت بها أبحاثهم وأن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق والوثائق التي عُهد بها إليهم على ذمة إنجاز مهمتهم[4].

إنّ الملاحظ من خلال القانونين السابقين أنّ الخبراء في مجال الجرائم المعلوماتية ما بين مقيد وغير مقيد ضمن الجدول الخاص بالمجلس القضائي صاحب الاختصاص، فالقانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها أعطى الحق لقاضي التحقيق أن يندب أي شخص مهما كانت صفته وفي أي وقت من فترة قيامه بالتحقيق[5]، أمّا ق إ ج فجعل ضرورة أن يكون الخبير مقيد في الجدول الخاص بالمجلس القضائي حتى ينتدبه قاضي التحقيق إلاّ في الحالات الاستثنائية أين يستطيع هذا الأخير انتداب خبير غير مقيد ضمن الجدول ويكون ذلك بقرار مسبب[6].

---

[1] الفقرة 2 من المادة 148 من الأمر رقم 69 – 76 المؤرخ في 16 سبتمبر 1969 يعدل ويتمم الأمر رقم 66 – 155 يتضمن ق إ ج الجزائري، ج ر رقم 60، المؤرخة في 19 سبتمبر 1969.

[2] الفقرة 1 من المادة 149 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] الفقرة 3 من المادة 148 من الأمر رقم 69 – 76 المعدل والمتمم للأمر رقم 66 – 155 المتضمن ق إ ج الجزائري، ج ر رقم 60، المؤرخة في 19 سبتمبر 1969.

[4] الفقرة 1 من المادة 148 من الأمر رقم 69 – 76 المعدل والمتمم للأمر رقم 66 – 155 المتضمن ق إ ج الجزائري، ج ر رقم 60، المؤرخة في 19 سبتمبر 1969.

[5] الفقرة 4 من المادة 5 من قانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[6] المادة 144 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

ونلاحظ بأنّ المشرع الجزائري أحسن ضمن القانون الأول عندما ألغى كل القيود الشكلية لانتداب الخبراء في مجال الجرائم المعلوماتية، وذلك لما تتمتع به هذه الجريمة من سرعة في ارتكابها وصعوبة في كشفها وفي الحفاظ على أدلتها، والتي قد تضمحل أثناء وقت الاستعانة بالخبير بطريق ق إ ج، هذا وتجدر الإشارة مرة أخرى إلى أنّ الجرائم المعلوماتية مفهومها حديث لذلك فإنّ الخبراء المعنيين بهذا المجال لديهم خبرة محدودة، وبالرغم من ذلك فإنّهم يلعبون دورًا رئيسيًا في تحليل هذه الظاهرة الناشئة وأكثر إستراتيجية في فكها[1].

الفرع الثاني: القيام بإجراء تفتيش المنظومات المعلوماتية

يعتبر التفتيش بمعناه القانوني إجراء من إجراءات التحقيق ووظيفته البحث عن أدلة الجريمة، وبالرغم من أنّه يعد وسيلة للحصول على دليل إلاّ أنّ أغلب التشريعات لم تعطي تعريفا له وهو ما ترك المجال مفتوحا للفقه من أجل إيجاد تعريفا مفصلا له، لذا جاء إحداها على النحو التالي أين اعتُبر بأنّه:" إجراء من إجراءات التحقيق فهو ليس عملا إداريا من أعمال الضبط الإداري وإنّما هو عمل من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين "[2]، وقد يتطلب التحقيق تفتيش شخص المتهم أو منزله قصد ضبط الأشياء المحصلة من الجريمة، لذا فإنّ إجراء التفتيش يعتبر من اختصاص سلطة التحقيق والذي يهتم بالبحث في مستودع السر عن أدلة الجريمة[3].

---

[1] Franck Guarnieri et Éric Przyswa, Cybercriminalité et expertise: enjeux et défis revues Sécurité et stratégie, Club des Directeurs de Sécurité des Entreprises, Paris France, 2012, p50.

[2] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، المجلد 3، العدد 2، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، جوان 2012، ص159، ص160.

[3] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون المجلد 22، العدد 2، جامعة باجي مختار عنابة، الجزائر، ديسمبر2016، ص84.

هذا ولقد تطرقنا لهذا الإجراء في حديثنا السابق ضمن الباب الأول بمناسبة التحريات والتحقيقات التي يقوم بها ضباط الشرطة القضائية وقلنا بأنّ هذا التفتيش يمس المكونات المادية[1] (Hard Ware) والمكونات المعنوية[2] (Soft Ware) لمختلف المنظومات المعلوماتية، وإذا كان التفتيش الذي يمس المكونات المادية لا يثير أي صعوبة فإنّ تفتيش المكونات المعنوية هو التي يثير الكثير من المشاكل كتفتيش منظومة معلوماتية، سواء كانت ضمن حاسوب واحد أو متصلة عن طريق شبكة سلكية أو لا سلكية كالإنترنيت.

هذا الاتصال الذي قد يكون متواجدا مع حاسوب آخر داخل الوطن أو خارجه، لذا سيكون من الصعب الكشف عن مختلف الاعتداءات نظرا للطبيعة المعنوية الخاصة لهذه المعطيات التي يقع عليها التفتيش والمخزنة إلكترونيا، ناهيك أنّها تتم في بيئة افتراضية تتطلب وسائل تقنية وبشرية خاصة لحل مختلف التعقيدات كنظام التشفير أو نظام ترميز البيانات وذلك للولوج إلى مختلف الملفات من أجل تقديمها كدليل ضد المتهم[3]، وللإشارة فإنّ المشرع الجزائري أجاز لقاضي التحقيق أن يباشر التفتيش والقيام بهذا الإجراء في جميع الأماكن التي يمكن العثور فيها على أشياء تفيد في إظهار الحقيقة[4] خاصة إذا ما تعلق الأمر بجريمة من الجرائم المعلوماتية التي غالبا ما يتم ارتكابها ضمن عالم افتراضي.

ومع هذه الطبيعة الخاصة التي تتمتع بها الجرائم المعلوماتية فقد أجاز المشرع الجزائري من خلال ق إ ج لقاضي التحقيق أن يباشر بنفسه أو يأمر ضباط الشرطة القضائية القيام بعملية التفتيش في أي

---

[1] المكونات المادية (Hard Ware) هي كل الأشياء الملموسة من أجزاء وأدوات الحاسوب والتي تعمل بشكل متكامل من أجل أداء مهمة في معالجة البيانات آليا وهذه الأجزاء ممثلة في شكل وحدات الإدخال كلوحة المفاتيح وشاشات اللمس ووحدة الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والبرامج وكذا وحدات الإظهار كالشاشة والطابعة.

[2] المكونات المعنوية (Soft Ware) هي البرمجيات التي توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة ويعرف لغة بأنها كلمة تستخدم للدلالة عن كل المكونات غير المادية لنظام الحاسوب كنظم التشغيل وبرامج التطبيقات.

[3] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، المرجع السابق، ص85.

[4] المادة 81 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

وقت ليلا ونهارا وفي أي محل سكني أو غير سكني على امتداد التراب الوطني[1]، مع لزوم أن يراعي ما تضمنته أحكام المادتين 45 و47 بخصوص الشروط التي يجب أن يتم وفقها التفتيش وأن يتخذ مقدما جميع التدابير اللازمة لضمان احترام السر المهني وحقوق الدفاع[2] تحت طائلة بطلان الإجراءات[3] ذلك أنّه في حالة قيام قاضي التحقيق بتفتيش مسكن غير مسكن المتهم فعليه استدعاء صاحب المسكن حتى يكون حاضرا أثناء تفتيش منزله، وإذا ما كان غائبا أو رفض الحضور يجري القاضي التفتيش بحضور اثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش، فإن لم يوجد فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية[4].

إنّ الملاحظ من خلال الفقرة السابقة ومن خلال استقراء المواد المتعلقة بإجراء التفتيش نقول لعل المشرع الجزائري ما كان يقصده من الانتقال هو الانتقال المادي لمسرح الجريمة والقيام بعملية التفتيش الذي يقع على المكونات المادية للحاسوب، وهو ما فسره وأكده صدور القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها، الذي أجاز لقاضي التحقيق دون انتقال مادي إلى مسرح الجريمة أن يفتش عن بعد منظومة تخزين معلوماتية أو منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة بها، وله أن يمدد التفتيش إلى منظومة أخرى انطلاقا من المنظومة الأولى إذا ما اعتقد أن المعطيات المبحوث عنها مخزنة فيها[5]، وإذا تبين بأن المعطيات المخزنة في المنظومة الأخرى وهذه الأخيرة تقع في الخارج فلا يمكن الحصول على هذه المعطيات إلاّ بمساعدة السلطات الأجنبية المختصة وذالك طبقا للاتفاقيات الدولية ذات الصفة ووفقا لمبدأ المعاملة بالمثل.

---

[1] المادة 47 من القانون رقم 06 – 23 المعدل والمتمم للأمر 66-156 المتضمن ق ع الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[2] الفقرة 2 من المادة 83 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 48 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] الفقرة 1 من المادة 83 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادة 5 من قانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

الفرع الثاني: القيام بإجراء ضبط وحجز المعطيات المعلوماتية

كنا قد تطرقنا ضمن الفرع السابق لأهم إجراء يقوم به قاضي التحقيق في مرحلة التحقيق الابتدائي ألا وهو إجراء التفتيش والذي قلنا أنّه ينصب سواء على المكونات المادية وعلى المكونات المعنوية للحاسب الآلي، وعلى ذلك فإن ضبط الأشياء المتعلقة بالجريمة المعلوماتية هو الأثر المباشر للتفتيش والضبط كإجراء من إجراءات التحقيق هو وضع اليد على الشيء وحبسه والمحافظة عليه لمصلحه التحقيق، فهو يمثل الضبط القضائي الذي يهدف إلى الحصول على دليل وذلك لمصلحة التحقيق عن طريق إثبات واقعه معينه.

هذا وقد تم الإشارة سابقا إلى أن الحاسب الآلي كمحتوى للمعلوماتية يتكون من مكونات مادية ومكونات منطقية أي معنوية[1]، هذه الأخيرة التي يثار حولها التساؤل أيضا في مدى صلاحيتها لأن تكون محلا للضبط، وهو الأمر الذي انقسم الفقه لأجله ما بين مؤيد ومعارض لضبط المكونات المعنوية للحواسب الآلية.

الرأي المعارض: ذهب إلى أن بيانات الحاسب لا تصلح لأن تكون محلا للضبط وبرر ذلك بانتفاء الكيان المادي عنها وأنّه لا سبيل لضبطها إلاّ بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي أو بنقلها على دعامة أو غيرها من الوسائل المادية، وكذلك استند على أنّ النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة.

الرأي المؤيد: ذهب إلى أنّ البيانات المعالجة إلكترونيا عبارة عن ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية والتي بالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها فلهذا قال أصحاب هذا الرأي بأنه لا يمكن إنكار وجودها المادي؛ هذا ويستند كذلك أنصار هذا الاتجاه إلى بعض النصوص التشريعية كاتفاقية بودابست لمكافحة الجرائم

[1] طارق إبراهيم الدسوقى عطيه، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية مصر 2009، ص441.

المعلوماتية 2001 والتي حسمت هذه المسالة بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الإلكترونية لأن تكون محلا للضبط[1]، هذه الاتفاقية خولت لأطرافها تبني إجراءات تشريعية تمنح للهيئات المتخصصة سلطة الضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وذلك وفق طريقتين؛

- طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة مادية بحيث تكون قابله للضبط والوضع في أحرز[2] مختومة حسب ما هو في مختلف القوانين الإجراءات الجنائية.
- طريق يتضمن تدابير جديدة مستحدثة خاصة بضبط مختلف الأدلة الجنائية الرقمية[3].

لهذا حتمت الطبيعة الخاصة للجرائم المعلوماتية وصعوبة إثباتها على بعض الدول تطوير نصوصها التشريعية المتعلقة بمحل التفتيش والضبط متبعين في ذلك للرأي الأخير، ليشمل الضبط فضلا عن الأشياء المادية المحسوسة الأشياء المعنوية الممثلة في البيانات المعالجة إلكترونيا، فأصدرت بذلك هذه الدول تشريعات خاصة بجرائم الحاسب الآلي والتي تتضمن القواعد الإجرائية المناسبة لهذه الصورة التي تتيح ضبط وحجز البيانات[4].

وهو الاتجاه الذي تبناه المشرع الجزائري من خلال إصداره للقانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات والاتصال ومكافحتها، أين أجاز لقاضي التحقيق أثناء مرحلة التحقيق الابتدائي أن ينسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وذلك وفقا للقواعد المقررة في ق إ ج.

---

[1] خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية مصر 2019، ص74.

[2] الحرز طبقا لمعجم المعاني هو الموضع الحصين، عن موقع https://www.almaany.com/ar/dict/ar-، بتاريخ 2021/03/19.

[3] المادة 19 من اتفاقية بودابست 23 نوفمبر 2001، الاتفاقية المتعلقة بالجريمة الإلكترونية.

[4] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، عمل مقدم من أجل متطلبات نيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد، تلمسان، الجزائر، الموسم الجامعي 2018/2017، ص293.

لذلك تناول المشرع الجزائري وفق للقانون الأخير[1] قواعد تسمح بضبط وحجز الأشياء والوثائق التي لها علاقة بالجريمة المراد كشفها كالجريمة المعلوماتية، بحيث ألزم قاضي التحقيق بإحصاء الأشياء والوثائق المطلوبة على الفور ووضعها في أحراز مختومة، كما يجب عليه أن يضبط الأشياء والوثائق النافعة في إظهار الحقيقة فقط أو التي قد يضر إفشاؤها بسير التحقيق، هذا ولا يجوز فتح هذه الأحراز والوثائق إلاّ بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا كما يُستدعى أيضا من ضبطت لديه هذه الأشياء لحضور هذا الإجراء، هذا ويستطيع كل من يعنيه الأمر في أقصر وقت وعلى نفقته الخاصة أن يحصل على نسخة أو صوره فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تَحل دون ذلك مقتضيات التحقيق[2].

الفرع الرابع: إعطاء إذن القيام بإجرائي الترصد الإلكتروني والتسرب

تطرقنا من خلال الفصل السابق لإجراءات التسرب وصور الترصد الإلكتروني من اعتراض للمراسلات والتقاط للصور وتسجيل للأصوات وكذا مراقبة الاتصالات الالكترونية والتي يقوم بإجرائهما ضابط الشرطة القضائية بإذن من السلطة القضائية المختصة سواء من طرف وكيل الجمهورية أو النائب العام أو قاضي التحقيق، هذا الأخير صاحب الإذن الأصيل في هذه المرحلة المسماة مرحلة التحقيق الابتدائي، وذلك عندما يكون بصدد التحقيق في جرائم خطيرة وجرائم ذات طبيعة خاصة كالتي على شاكلة الجرائم المعلوماتية.

أولا: إذن قاضي التحقيق بإجراء الترصد الإلكتروني

الترصد الإلكتروني مصطلح أشار إليه المشرع الجزائري فقط في موضوع جرائم الفساد، والملاحظ بأنّه مصطلح واسع ويحوي كل أشكال الآليات والإجراءات ذات الطابع التقني الإلكتروني التي نظمها المشرع الجزائري ضمن ق إ ج في صور إجراءات اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

---

[1] المادة 6 من قانون رقم 09 – 04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] المادة 84 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

وكذا إجراء مراقبة الاتصالات الإلكترونية المستحدث بالقانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

فالترصد الإلكتروني مصطلح عام يشير إلى أشكال المراقبة الإلكترونية التي يمكن من خلالها رصد مكان وحركة الأشخاص وسلوكهم المحدد في إطار الإجراءات الجزائية، كتتبع موجات الراديو أو المقاييس الحيوية أو الأقمار الصناعية، وعادة ما تشتمل على جهاز متصل بشخص ما ويتم مراقبته عن بعد[1] هذا الإجراء عمل به المشرع البلجيكي قبل المشرع الجزائري من خلال قانون التحقيق الجنائي البلجيكي واعتمد عليه بشكل رئيسي في بعض الجرائم الخطيرة والتي كانت الجرائم المعلوماتية إحداها، بل وحتى مؤسسات القطاع العام الاقتصادي التي أُلزمت بتسجيل وتخزين بيانات الاتصال وبيانات التعريف لمستخدمي الخدمة[2].

هذا وإن كانت الصور الثلاث الأولى من الترصد الإلكتروني لا تثير إشكالات كبيرة طالما أنّها لا تمس بحرمة الحياة الخاصة إلاّ في حالات معينة حددها المشرع الجزائري حصرا وبضوابط وشروط معينة فإنّ الصورة الأخيرة المتمثلة في مراقبة الاتصالات الإلكترونية التي جاء بها القانون رقم 09-04 السابق الذكر هي التي تثير إشكالا كبيرا وتضاربا كبيرا بين أغلب الفقهاء القانونين ما بين مؤيد ومعارض لها ذلك أنّ هذه الآلية في التشريع الجزائري أُنشأت لها هيئة خاصة بها تقوم بمراقبة مختلف الاتصالات الإلكترونية في أي وقت، الأمر الذي اعتبر بالنسبة لطائفة كبيرة من الفقهاء اعتداء صارخا لحق وحرمة

[1] MIke Nellis and Dominik Lehner, scope and definitions electronic monitoring Council for Penological Cooperation, european committee on crime problems council of europe, Strasbourg, France, October 2012, p2.

[2] Florence de Villenfagne, Séverine Dusollier, La Belgique sort enfin ses armes contre la cybercriminalité :A propos de la loi du 28 novembre 2000 sur la criminalité informatique , Contribution à un journal/une revue, Faculte de droit, Centre de recherche information, droit et societe, Belgique, 2002, p30.

الحياة الخاصة لكثير من الأشخاص ممن ليس لهم أية علاقة بالجرائم محل الوقاية كالتي في شكل الجرائم المعلوماتية.

حاليا نؤيد الاتجاه المعارض لهذه الآلية وإن كانت هذه الأخيرة لها دور مهم في كشف العديد من الجرائم الخطيرة لكن على حساب حرمة الحياة الخاصة لكثير من الأشخاص وهو أمر غير منطقي وغير مقبول ونقول بأنّ المشرع الجزائري بإمكانه الاستغناء عنها خاصة فيما يتعلق بالجرائم المعلوماتية، فالجزائر تملك الكثير من الأدمغة والمؤهلات بل وتستطيع جلب الإمكانيات المختلفة التي تسمح لها بالتصدي لجل وأشكال الجرائم الخطيرة كالتي في شكل الجرائم المعلوماتية، يكفي فقط أن تحسن توظيفها وجعلها في محلها وموقعها المناسبين.

ثانيا: إذن قاضي التحقيق بإجراء التسرب

كنا قد تطرقنا بشيء من التفصيل لهذا الإجراء ضمن الفصل الثاني من الباب الأول وخلصنا في الأخير بأنّ المشرع الجزائري حصر هذا الإجراء في إطار الجرائم المعلوماتية على نوع واحد فقط منها وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقلنا بأنّه كان حريا به عند توسعته لمجال الأفعال التي تدخل في إطار الجرائم المعلوماتية أن يعدل من نص المادة 65 مكرر 11 ويجعل من عملية التسرب تشمل جميع الأفعال التي ترتكب على أو بواسطة منظومة معلوماتية.

ويبقى هذا الإجراء في هذه المرحلة من الدعوى العمومية وطبقا لق إ ج الجزائري خاضعا لإذن وسلطة قاضي التحقيق، فهذا الأخير أثناء تحقيقه حول وقوع هذا النوع من الجريمة المعلوماتية قد يأذن[1] به لضابط الشرطة القضائية وذلك بعد إخطاره لوكيل الجمهورية، على أن يكون هذا الإذن مكتوبا ومسببا وألاّ يتجاوز مدة أربعة (4) أشهر وذلك تحت طائلة بطلانه ويجب أن يذكر في هذا الإذن نوع الجريمة

[1] المادة 65 مرر11 من قانون رقم 06-22 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

المعلوماتية التي تبرر اللجوء لعملية التسرب وكذا هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته[1].

هذا ويستطيع قاضي التحقيق أثناء هذه المرحلة من الدعوى وبعد انتهاء المهلة الأولى من عملية التسرب أن يجدد ويكرر هذه العملية إذا ما استدعت ذلك مقتضيات التحقيق في الجريمة المعلوماتية وله السلطة كذلك في أن يوقفها في أي وقت قبل انقضاء المدة القانونية لها[2]؛ على أن يمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، بحيث يستطيع القاضي في سبيل ذلك أن يرخص بتمديد هذه العملية لمدة أربعة أشهر أخرى[3]، وبعد انتهاء هذه العملية يجوز لقاضي التحقيق سماع ضابط الشرطة القضائية الذي جرت العملية تحت مسؤوليته دون سواه كشاهد عن الأحداث التي جرت أثناء العملية[4].

إنّ إجراء التسرب يعد من بين أبرز وأنجع الآليات التي يمكن لقاضي التحقيق أن يعتمد عليها إذا ما استدعت ضرورات التحقيق ذلك، خاصة في ظل ظهور شبكة الويب المظلمة والعالية التشفير أين أصبحت طرق تحديد الجاني مثل تتبع الموقع الجغرافي وعناوين "IP" طرقا تقليدية وغير فعالة على الإطلاق في بعض الجرائم كالتحرش الجنسي بالأطفال، الأمر الذي يتطلب معه ضرورة وجود عملاء سريين مدعمين بأساليب بديلة لمتابعة وتحديد وملاحقة الجناة[5]، هذا الإجراء الذي يستطيع من خلاله

---

[1] الفقرات 1 و2 و3 من المادة 65 مكرر15 من قانون رقم 06-22 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[2] الفقرات 4 و5 و6 من المادة 65 مكرر15 من قانون رقم 06-22 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[3] المادة 65 مرر17 من قانون رقم 06-22 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[4] المادة 65 مرر18 من قانون رقم 06-22 المعدل والمتمم لق إ ج الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006.

[5] Nicci MacLeod and Tim Grant, Assuming Identities Online: How Linguistics Is Helping the Policing of Online Grooming and the Distribution of Abusive Images fom books of, Tim owen-jessica marshall, The previous reference, p88.

العون المحترف من الاختراق والتسرب داخل الشبكة الإجرامية المعلوماتية بطريقة إلكترونية عن بعد بحيث تضمن أمنه من جل أشكال ما قد يهدد حياته وسلامته وكذا حياة وسلامة عائلته.

المبحث الثاني: السلطات التقليدية المخولة لقاضي التحقيق في الجرائم المعلوماتية

نقصد بالإجراءات التقليدية المخلولة لقاضي التحقيق في هذه المرحلة من الدعوى العمومية تلك السلطات التي يمارسها في وجه المتهم بالجريمة المعلوماتية على عكس الإجراءات العملية المتطرق إليها من خلال المبحث السابق التي لا يكون للمتهم دور أساسي فيها، وهذه السلطات الممارسة في وجه هذا الأخير تتمثل في استجوابه ومواجهته بالجريمة المعلوماتية المنسوبة إليه وكذا سماع الشهود والطرف المدني إن وجدوا، هذا ويستطيع قاضي التحقيق ممارسة عدة سلطات أخرى تساعده في إكمال والسير في تحقيقه والتي يستطيع من خلالها إحضار أو القبض على المتهم وكذا إيداعه الحبس المؤقت أو وضعه تحت الرقابة القضائية.

المطلب الأول: السلطات التقليدية الأساسية المطبقة ضد المتهم بالجريمة المعلوماتية

لقد منحت جل القوانين المقارنة أثناء مرحلة التحقيق الابتدائي لقضاة التحقيق عدة سلطات تمارس ضد المتهم في شتى الجرائم على حسب درجة خطورتها، فهذا التشريع الجزائري أعطى من خلال ق إ ج لقاضي التحقيق عدة سلطات يمارسها على المتهم بالجريمة المعلوماتية، والتي يمكنه من خلالها القيام باستجواب ومواجهة المتهم وكذا سماع شهود الجريمة والطرف المدني إن وجدوا، هذه السلطات سنتطرق إليها بشيء من التفصيل من خلال الفروع القادمة.

الفرع الأول: القيام باستجواب المتهم بالجريمة المعلوماتية

لقد تعددت التعريفات الفقهية القانونية حول هذا الإجراء بحيث جاءت إحداها على أنّ الاستجواب الجزائي يعتبر مناقشة للمتهم بشكل مفصل في الأدلة القائمة ضده في الدعوى إثباتا ونفيا

كما عرف بأنّه مواجهة المتهم بالتهمة المنسوبة إليه ومطالبته بإبداء رأيه فيها ومن ثم مناقشته مناقشة تفصيلية في أدلة الدعوى إثباتا ونفيا وذلك لمحاولة كشف الحقيقة[1].

لذلك فإنّ قيام قاضي التحقيق باستجواب المتهم يعبر عن مدى مناقشة هذا الأخير مناقشة تفصيلية حول مدى علاقته بالجريمة ومواجهته بالأدلة القائمة ضده وكذا مطالبته بالرد عليها إثباتا أو نفيا، فإجراء الاستجواب هو ذو طبيعة مزدوجة فهو من ناحية وسيلة للتحقيق في يد المستجوب تمكنه من الحصول على دليل ينير له مجريات التهمة، ومن ناحية أخرى يتيح الفرصة للمتهم لينفي التهم المنسوبة إليه وإثبات براءته إن كان كذلك أو تخفيف مسؤوليته عن طريق توضيح اقتراف الجريمة إن كان مذنبا[2]، ولعل الغرض الأساسي من استجواب المتهم بالجريمة المعلوماتية هو الحصول على اعتراف هذا المتهم.

هذا الاعتراف الذي يشكل أهمية كبرى في الجرائم المعلوماتية بل ويعتبر من بين أهم وأقوى الأدلة في مثل هذا النوع من الجرائم، ذلك أنّه يساعد في التعامل مع بعض الجرائم المعلوماتية وأيضا مع بعضها الآخر التي تحتاج لاستخدام سبل علمية حديثة لإيجاد دليل عليها، حتى أنّ بعض الفقه ذهب بالقول بأنّ الاعتراف في مرحلة سابقة كان هو الأساس في مثل هذه النوعية من الجرائم[3]، هذا الدليل يساعد ويسهل كذلك على قاضي التحقيق في الحصول على أدلة أخرى تثبت وتؤكد بها طبيعة ونوعية الجريمة المعلوماتية المرتكبة من قبل هذا المتهم.

لكن بشرط أن يكون هذا الاعتراف نابع من إجراءات وظروف صحيحة وطبيعية تنفي تعرض المتهم من جميع أشكال الإكراه، فقد تنتهك حقوق المتهم من طرف سلطة التحقيق إذا لم تأخذ هذه

---

[1] خالد بن محمد المهوس، الاستجواب الجنائي وتطبيقاته في النظام الإجرائي السعودي، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2003، ص24.

[2] زروقي عاسية، سلطة القاضي في تقدير القيمة الإثباتية لإجراءات الاستجواب، مجلة الحقوق والحريات، العدد 5، جامعة محمد خيضر بسكرة، الجزائر، 2018، ص124.

[3] أحمد سعد محمد الحسيني، المرجع السابق، ص197.

الأخيرة بعين الاعتبار الشروط والضمانات القانونية لإجراء الاستجواب[1]، خاصة إذا ما تعلق الأمر بجرائم ذات طبيعة مميزة كالتي في شكل الجرائم المعلوماتية والتي تستوجب كل الحرص والحذر أثناء تفعيل هذا الإجراء من قبل قاضي التحقيق حتى لا تضيع منه مختلف الأدلة وحتى لا يخطئ في مرتكب هذه النوعية من الجرائم، لأنّه بخطئه سيفوت على نفسه بنسبة كبيرة ضبط وحجز الأدلة وكذا اللحاق بمرتكب الجريمة المعلوماتية وبالتالي إيقاف مختلف اعتداءاته.

هذا ويبقى الاستجواب كأصل عام إجراء قضائي من اختصاص قاضي التحقيق ولا يجوز له أن ينيبه إلى ضابط الشرطة القضائية للقيام به[2]، هذا القاضي يقوم من خلاله بجميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وكذا التحري عن أدلة الاتهام وأدلة النفي[3] إن وجدت، والابتعاد عن أي وسيلة غير مشروعة من شأنها التأثير على إرادة المتهم، كالإكراه والوعد اللّذيْن يفقد من خلالهما إجراء الاستجواب معناه كإجراء للدفاع بل وقد يصبح أداة من أدوات الاتهام[4]، لذلك فإذا ما خولفت القواعد المتعلقة بتحديد اختصاص السلطة التي تباشر الاستجواب أو القواعد المخالفة للاختصاص

---

[1] الفحلة مديحة، حقوق المتهم أثناء الاستجواب في الشريعة الإسلامية والقانون الجزائري، مجلة لبدر، المجلد 8، العدد 2، جامعة بشار، الجزائر، فبراير 2016، ص58.

[2] تنص المادة 139 من القانون رقم 82-03 المؤرخ في 13 فيفري 1982 المعدل والمتمم للأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 7، المؤرخة في 16 فيفري 1982بأنّه: " يقوم القضاة أو ضباط الشرطة القضائية المنتدبون للتنفيذ بجميع السلطات المخولة لقاضي التحقيق ضمن حدود الإنابة القضائية غير أنّه ليس لقاضي التحقيق أن يعطي بطريق الإنابة القضائية تفويضا عاما.

ولا يجوز لضباط الشرطة القضائية استجواب المتهم أو القيام بمواجهته أو سماع أقوال المدعي المدني".

[3] تنص المادة 68 الفقرة 1 من قانون رقم 01-08 المؤرخ في 26 يونيو 2001 يعدل ويتمم الأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001 بأنّه: " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي".

[4] سعيد بن عبد الله بن بدوي الكناني الزهراني، الاستجواب والمواجهة في نظام الإجراءات الجزائية السعودي، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008، ص95.

الشخصي أو النوعي أو المكاني فإنّه يترتب عن ذلك البطلان المطلق[1]، وهو الأمر الذي يجب على السلطة القضائية تجنبه خاصة في الجرائم المعلوماتية المتميزة بالسرعة في ارتكابها وسرعة اندثار أدلتها.

الفرع الثاني: القيام بإجراء مواجهة للمتهم بالجريمة المعلوماتية

يأتي إجراء مواجهة المتهم تلقائيا بعد إجراء الاستجواب بل وقد لا يتم ولا يكتمل هذا الأخير إلاّ بالاستعانة بالإجراء الأول فيبدأ تفعيلهما في وقت مختلف وقد ينتهي تفعيلهما في آن واحد، هذا وبعد تطرقنا إلى إجراء الاستجواب في الجرائم المعلوماتية بشيء من التفصيل من خلال الفرع السابق فلابد من توضيح إجراء المواجهة الذي يستعمله قاضي التحقيق لإثبات وكشف نوع الجريمة المعلوماتية المرتكبة.

هذا الإجراء يتم من خلاله جمع المتهم مع متهم آخر أو جمع المتهم مع شاهد في حالة ما إذا كان هناك تناقض في الأقوال لكلا طرفي المواجهة المتهم بالمتهم أو المتهم بالشاهد، وذلك لإجراء مناقشة بينهما لرفع هذا التناقض وللوقوف على صحة دليل أو واقعة، هذا وتلتقي المواجهة مع الاستجواب في النقطة التي يتم من خلالها مجابهة المتهم بالأدلة القائمة ضده، هذه المجابهة تختلف فقط في شخص المقابل أين يكون المجابه في الاستجواب هو قاضي التحقيق نفسه[2] أمّا المواجهة فتكون بين المتهم والشخص الذي يوجه أقوالا ضده سواء كان شاهدا أو متهما آخر.

وكأصل عام فقد نظم المشرع الجزائري إجراء المواجهة ضمن المواد 101 و105 و106 و108من ق إ ج[3]، ونظر لسرعة ارتكاب الجرائم المعلوماتية وطبيعتها الخاصة فقد سمح هذا القانون

---

[1] دايخ سامية، ضمانات المتهم أثناء الاستجواب أمام قاضي التحقيق في ظل قانون الإجراءات الجزائية الجزائري، مجلة العلوم الإنسانية المجلد 6، العدد 1، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1، الجزائر، جوان 2016، ص297.

[2] مزهر جعفر عبيد، شرح قانون الإجراءات الجزائية العماني، الجزء الأول، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن 2009، ص435.

[3] المواد 101 و106 و108 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966. المادة 105 من القانون رقم 01-08 المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001.

لقاضي التحقيق بإجراء مواجهات مع استجوابات تقتضيها هذه الحالة المستعجلة لوجود أمارات على وشك الاختفاء على أن تحرر فيما بعد في المحضر دواعي الاستعجال[1] والمتمثلة في غالب الظن في السرعة والطبيعة الخاصة التي تتميز بها هذه النوعية من الجرائم، أمّا فيما يخص مواجهة المتهم مع المدعي المدني فلا يجوز أن يتم هذا الإجراء دون حضور محامي المتهم ما لم يتنازل هذا الأخير صراحة عن ذلك[2].

هذا ونظرا لطبيعة المواجهة والاستجواب وما تثيره من معلومات حساسة وحركات معينة يبديها المواجه فقد أحسن المشرع الجزائري حين أجاز لوكيل الجمهورية إمكانية حضور إجراء المواجهة[3] وذلك ربما لزيادة فرص الوصول لهدف القيام بهذا الإجراء، بل ويكون حضوره ضروري في الجرائم كالتي على شاكلة الجرائم المعلوماتية، أين يستطيع توجيه ما يراه مناسبا من أسئلة على أن تحرر مع معلومات إجراء المواجهة في محاضر وفقا لما أشارت إليه المادة 108 من ق إ ج[4].

---

[1] المادة 101 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966بنصها: " يجوز لقاضي التحقيق على الرغم من مقتضيات الأحكام المنصوص عليها في المادة 100 أن يقوم في الحال بإجراء استجوابات أو مواجهات تقتضيها حالة استعجال ناجمة عن وجود شاهد في خطر الموت أو وجود إمارات على وشك الاختفاء
ويجب أن تذكر في المحضر دواعي الاستعجال".

[2] الفقرة 1 من المادة 105 من القانون رقم 01-08، المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001 بنصها: " لا يجوز سماع المتهم أو المدعي المدني أو إجراء مواجهة بينهما إلاّ بحضور محاميه أو بعد دعوته قانونا ما لم يتنازل صراحة عن ذلك".

[3] الفقرة 1 من المادة 106 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966بنصها:
" يجوز لوكيل الجمهورية حضور استجواب المتهمين ومواجهتهم وسماع أقوال المدعي المدني
ويجوز له أن يوجه مباشرة ما يراه لازما من الأسئلة".

[4] الفقرة 1 من المادة 108 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966بنصها:
" تحرر محاضر الاستجواب والمواجهات وفق الأوضاع المنصوص عليها في المادتين 94 و95 وتطبق أحكام المادتين 91 و 92 في حالة استدعاء مترجم".

الفرع الثالث: القيام بسماع شهود الجريمة المعلوماتية

الشاهد عند الفقه القانوني هو الحاضر وقت ارتكاب الواقعة، أو من يمكن الحصول منه على إيضاحات بشأن هذه الواقعة و فاعلها أو من يرى المحقق فائدة من سماع شهادته أو من يرى لزوم سماع شهادته عن الوقائع التي تثبت ارتكاب الجريمة و إسنادها للمتهم أو براءة ساحته منها بحيث يتوصل بها إلى إثبات ذلك؛ والمشرع الجزائري على غرار معظم التشريعات لم يبين ويوضح من هو الشاهد وإنّما اكتفى بإعطاء تلميحات حوله[1] ويستشف ذلك من خلال نص المادة 88 من ق إ ج الجزائري[2] بقوله: "يستدعي قاضي التحقيق أمامه بواسطة أعوان القوة العمومية كل شخص يرى فائدة من سماع شهادته".

وبطبيعة الحال يختلف الشاهد في الجرائم المعلوماتية عن الشاهد في الجرائم التقليدية ذلك أنّ الشاهد في هذه الأخيرة هو من عاين بعض أو كل تفاصيل الواقعة بأحد حواسه، بينما يكون الشاهد في الجرائم المعلوماتية ملم أو متخصص في تقنيات الحاسوب، ولم يعاين تفاصيل الجريمة عند وقوعها بأحد حواسه، وإنّما استعملت تجربته وخبرته في الولوج إلى الحاسب الآلي والانترنت بحثا عن أدلة الجريمة التي سيدلي فيها فيما بعد بشهادته حول ما توصل إليه من نتائج[3]ضرورية ومساعدة في مرحلة التحقيق الابتدائي.

هذا الشاهد المعلوماتي الذي تتعدد أوصافه، فهناك أشخاصا آخرين يعدون بمثابة شهود في الجرائم المعلوماتية والمتمثلين في مقدمي الخدمات الوسيطة في مجال المعلوماتية والإنترنيت وهم على التوالي متعهدي الوصول ومتعهدي الإيواء ومسئولي المنتج المعلوماتي ومسئولي ناقل المعلومات ومسئولي متعهد

---

[1] نبيلة أحمد بومعزة، الحماية الجزائية للشاهد في القانون الجزائري، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 2، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، سبتمبر 2019، ص80.

[2] الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] شرف الدين وردة ، الإثبات الجنائي بالأدلة الإلكترونية دراسة مقارنة، عمل مقدم لنيل شهادة الدكتوراه، تخصص قانون جنائي كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، الموسم الجامعي 2017/2016، ص248.

الخدمات وكذا مورد المعلومات ومؤلف الرسالة؛ وهؤلاء كلهم بحكم دورهم يقومون بتوصيل طالب الخدمة أو المستهلك مع شبكة الإنترنيت[1].

ويتعين على الشاهد المعلوماتي في ظاهر الأمر أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للوصول إلى الأدلة الإجرامية من خلال ولوجه إلى أنظمة تشغيل الحواسيب أو الشبكات إلاّ أنّ الخلاف يبقى حول دور الشاهد في إمكانية مده ليد العون و المساهمة بشكل أكبر في التحقيق أم يبقى ملتزم بقول الحقيقة فقط، لأنّ هناك اتجاه يرى أنصاره بأنّ الشاهد المعلوماتي يستطيع القيام بطبع المعلومات وتحليل البيانات والكشف عن كلمات السر، أمّا اتجاه آخر فيرى أنصاره أنّ الشاهد المعلوماتي ليس من التزاماته أن يقوم بطباعة البيانات المخزنة في ذاكرة الحاسوب لا بتحليل ذاكرة النظام المعلوماتي[2] لأنّ هذا من عمل الخبير.

وبالرجوع للتشريع الجزائري ومن خلال استقراء النصوص المنظمة للشهادة[3]كدليل إثبات نلاحظ بأنّ المشرع سابقا ومن خلال ق إ ج لم يكن يتطرق لهذا الأمر، ويتجلى ذلك من خلال عدم وضعه لشروط يجب توفرها في الشاهد المعلوماتي وكذا مدى مساعدة هذا الأخير في التحقيق حول الجرائم المعلوماتية، وهو ما كان يلزم قاضي التحقيق بأن يأخذ بشهادة هذا الشاهد بما يتعين عليه في ظاهر الأمر، بحيث يلتزم الشاهد بقول الحقيقة فقط دون المساعدة في التحقيق الذي هو متروك من اختصاص قاضي التحقيق الذي يستعين فيه بالخبير المعلوماتي، هذا الأخير الذي رأينا في الفروع السابقة كيف تساعد خبرته في التحقيق ومدى اعتمادها فيما بعد كدليل إثبات.

لكن بعد صدور القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نلاحظ أنّ المشرع الجزائري أجاز لنوع واحد من الشهود وهم مقدمي الخدمات أن يقدموا المساعدة لقاضي التحقيق وذلك بجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في

---

[1] طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، المرجع السابق، ص343.

[2] ربيعي حسين، المرجع السابق، ص257.

[3] أنظر المواد من 220 إلى 238 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

حينها التي يتعين عليهم حفظها وتقديمها لقاضي التحقيق فيما بعد[1]، هذا وقد أضاف المشرع لمقدمي خدمات الإنترنيت التزامات تجعلهم يسحبون فوريا المحتويات المتاح الاطلاع عليها مع تخزينها وجعل الدخول إليها غير ممكن بمجرد علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين[2].

هذا و قد ظهرت في الآونة الأخيرة طريقة جديدة تدلى بها الشهادة عن بعد بطريقة إلكترونية دون حضور الشاهد عن طريق النقل المباشر أو البث الحي المباشر عبر وسائل إلكترونية من خلال شبكة الإنترنيت أو عبر الأقمار الصناعية من دون أن يكون حاضرا في التحقيق وحتى المحاكمة، وهذه الطريقة أصبحت مقبولة في السنوات الأخيرة لدى أغلب الفقهاء على اعتبار أنّ الشاهد المعلوماتي[3] بشهادته على هذا النحو سيظهر كما لو كان حاضرا بكامل هيئته أمام سلطة التحقيق، بل وحتى أنّها مناسبة في ظل الخطورة الكبيرة للجرائم المعلوماتية وكذا تعقيدات اكتشافها وسرعة ارتكابها وسهولة اندثار آثارها.

هذا الإجراء ذا الطبيعة السريعة نجد له تنظيما في التشريع الجزائري من خلال التعديل الأخير لق إ ج، أين يمكن لقاضي التحقيق ولمقتضيات حسن سير العدالة أو الحفاظ على الأمن أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي احترام مبدأ الآجال المعقولة استعمال تقنية المحادثة المرئية عن بعد في الشهادة بل وفي جميع الإجراءات القضائية المخولة له؛ على أن تضمن الوسائل المستعملة سرية الإرسال وأمانته وكذا التقاط وعرض كامل وواضح لمجريات الإجراء المتخذ بهذه التقنية[4]، بحيث يتم تسجيلها على دعامة إلكترونية تضمن سلامتها وترفق بملف الإجراءات فيما بعد.

---

[1] الفقرة 1 من المادة 10 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] المادة 12 من القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[3] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، ط أولى، المكتب الجامعي الحديث الإسكندرية، مصر، 2018، ص150.

[4] المادة 441 مكرر من الأمر رقم 20-04، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

الفرع الرابع: القيام بسماع الطرف المدني

كأصل عام فإنّ قواعد الاختصاص تفرض أن يكون نظر الدعوى العمومية أمام القضاء الجزائي وأن يكون نظر الدعوى المدنية أمام القضاء المدني، وكاستثناء عن القاعدة العامة فقد خول المشرع بالنسبة للدعوى المدنية المتعلقة بالدعوى العمومية أن تنظر أمام القضاء الجزائي، وذلك عندما يكون منشؤها هو ذات الفعل الإجرامي الذي نشأت من خلاله الدعوى العمومية، لهذا أعطي المتضرر من الجريمة الحق في أن يدعي بحقه المدني أمام جهة التحقيق الابتدائي[1] عامة وقاضي التحقيق خاصة وعليه فإنّ المتضرر من الجرائم المعلوماتية له حق الادعاء المدني أمام قاضي التحقيق كما يجوز لهذا الأخير إجراء سماع أقوال هذا الطرف المدني إذا ما رأى ضرورة لذلك.

وسماع الطرف المدني الأصل في إجرائه أن يكون بحضور محاميه ما لم يتنازل صراحة عن ذلك وإلاّ لا يجوز لقاضي التحقيق سماع أقواله أو إجراء مواجهة بينه وبين المتهم، كما يجب أن يوضع ملف الدعوى تحت تصرف محاميه أربع وعشرين ساعة على الأقل قبل سماعه أو مواجهته بحيث يتم سماعه في محضر يمضي فيه كل من قاضي التحقيق والطرف المدني وحتى الكاتب[2]، هذا الإجراء يعتبر أحد الإجراءات الهامة التي يمكن أن يستعين بها هذا القاضي في هذه المرحلة الحساسة من الدعوى العمومية وخاصة إذا ما كان يحقق في جرائم خطيرة كالتي على شاكلة الجرائم المعلوماتية مسرح ونواة هذا البحث والدراسة.

فقد يتدخل الطرف المدني المتضرر من الجريمة المعلوماتية في الخصومة في مرحلة التحقيق الابتدائي أمام قاضي التحقيق، هذا الطرف سواء من قبله أو من قبل محاميه بإمكانه في أي وقت من هذه المرحلة أن يتقدم بطلب كتابي إلى هذا القاضي من أجل تلقي تصريحاته، وإذا رأى قاضي التحقيق أنّه لا موجب من اتخاذ الإجراء المطلوب منه فيتعين عليه أن يصدر أمرا مسببا خلال 20 يوم التالية من

---

[1] مزهر جعفر عبيد، المرجع السابق، ص286.

[2] المادة 105 من قانون رقم 01-08 المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001.

الطلب[1] وإلاّ جاز للطرف المدني أن يرفع طلبه خلال 10 أيام إلى غرفة الاتهام التي يجب أن تبث فيه خلال أجل 30 يوم من تاريخ إخطارها بقرار غير قابل للطعن[2].

هذا وقد أجاز المشرع الجزائري للمجني عليه في الجرائم المعلوماتية تحريك الدعوى العمومية[3] كما أقر له حق الادعاء مدنيا أمام قضاء التحقيق عن طريق تقديم شكوى إلى قاضي التحقيق المختص يدّعي فيها بالحقوق المدنية، وهذا الحق الممنوح للمجني عليه ما هو إلاّ وسيلة تخوله تحريك الدعوى العمومية حتى يتمكن من طرح دعواه المدنية أمام القضاء الجزائي في حالة جهل أو تقاعس النيابة العامة عن الجريمة المعلوماتية المرتكبة وتحريك الدعوى العمومية بشأنها[4]، حيث يقوم قاضي التحقيق بعرض الشكوى المصحوبة بالادعاء المدني على وكيل الجمهورية، هذا الأخير الذي يملك سلطة الموافقة على إجراء التحقيق حتى يستقل قاضي التحقيق بتكييف الوقائع و توجيه الاتهام بعد ذلك[5].

هذا القاضي الأخير يدرك مسبقا بأنّه ليس بالضرورة أنّ كل مدعي مدني هو فعلا ضحية لجريمة معلوماتية، الأمر الذي يجعل هذا الأخير موضع شك إلى حين إثبات صدق نواياه بعد سماعه من قبل قاضي التحقيق المختص، الذي يُقتضى منه استخراج كل معلومة من هذا المدعي والتي من شأنها أن تؤدي إلى كشف الحقيقة، كما أنّ استدعاء قاضي التحقيق للمدعي المدني في الجرائم المعلوماتية يعد

---

[1] المادة 69مكرر من قانون رقم 06-22 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[2] عبد الرحمان خلفي، المرجع السابق، ص262.

[3] المادة 1 مكرر من القانون رقم 17-07، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[4] محمد الأخضر مالكي، حقوق المجني عليه في الدعوى العمومية، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق جامعة الإخوة منتوري قسنطينة، الجزائر، الموسم الجامعي 2009/2008، ص26.

[5] المادة 73 من القانون رقم 82-03 المعدل والمتمم للأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 7، المؤرخة في 16 فيفري 1982.

أحد الأسباب الفعالة التي جعلت المشرع الجزائري يخول لهذا القاضي استدعاء هذا الطرف من أجل الحصول منه على توضيحات لازمة بشأن الواقعة محل الدعوى[1].

المطلب الثاني: السلطات التقليدية الاحتياطية المطبقة ضد المتهم بالجريمة المعلوماتية

لقد وضعت مختلف التشريعات منها التشريع الجزائري عدة سلطات وإجراءات في يد قاضي التحقيق تخوله إجراء عمله على أكمل وجه، خاصة في نطاق الجرائم الخطيرة والسريعة مثل الجرائم المعلوماتية، هذه السلطات التي تفعل في نطاق الجرائم المعلوماتية اعتبرناها تقليدية واحتياطية مقارنة مع حداثة الطرق التي ترتكب فيها هذه الجريمة الأخيرة، وهذه الإجراءات مهمة للغاية بحيث تخول قاضي التحقيق ضبط تحركات المتهم وتضمن بنسبة كبيرة مثول هذا الأخير أمامه في أي وقت شاء من فترات التحقيق القانونية، هذه السلطات تتمثل مجملها في الآتي.

الفرع الأول: الأمر بإحضار المتهم بالجريمة المعلوماتية

يعتبر الأمر بإحضار المتهم بالجريمة المعلوماتية أحد أوامر التحقيق، التي يستطيع قاضي التحقيق من خلالها أن يكلف هذا المتهم بالحضور أمامه في مكان معين وفي التاريخ والوقت المبين بالمذكرة وذلك للتحقيق معه من خلال استجوابه أو مواجهته بغيره من الشهود أو المتهمين، هذا الإجراء يُقتضى فيه حضور المتهم المعلوماتي كراهة، لذلك يجوز لقاضي التحقيق اللجوء إلى الإكراه أو القوة لتنفيذ هذا الأمر خاصة إذا رفض هذا المتهم الحضور أمامه[2]، وبالرجوع للتشريع الجزائري نجد أنّ هذا الإجراء قد نص عليه المشرع[3] وعرفه بأنّه ذلك الأمر الذي يصدره قاضي التحقيق إلى القوة العمومية لاقتياد المتهم ومثوله أمامه على الفور[4].

---

[1] عمارة فوزي، المرجع السابق، ص120.

[2] سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، الطبعة الثانية، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، 1999، ص560.

[3] أمر رقم 66-155،المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 101 من أمر رقم 66-155،المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

إنّ هذا الأمر يخصص كذلك للمتهم المعلوماتي الذي يرفض المثول لأول مرة أمام قاضي التحقيق والذي يصدر عادة في بداية إجراءات التحقيق، هذا المتهم الذي قد يبلغ بذلك ويتخلف عن الحضور الأولي الطوعي، هنا يتدخل قاضي التحقيق عن طريق القوة العمومية من أجل إحضاره أمامه وحتى يتسنى له سؤاله عما هو منسوب إليه ومواجهته بغيره من المتهمين أو الشهود، هذا ونظرا لعمومية النص فهو أمر جائز في جميع الجرائم[1] بما في ذلك الجرائم المعلوماتية، وفي مواجهة أي شخص سواء كان له موطن معروف أو مجهول وأي شخص يحتمل هروبه أو لا يولي العناية اللازمة لأوامر قاضي التحقيق.

ولعل ما يهم في هذا المقام الطبيعة الخاصة السريعة للجرائم المعلوماتية، والتي من المؤكد أنّها ستجبر قاضي التحقيق في بعض الحالات المتعلقة بهذه الجريمة أن يستعجل في إصدار أمر الإحضار من خلال اللجوء إلى جميع الوسائل الإعلامية بحيث يبين فيه مختلف البيانات الجوهرية المبينة في أصل هذا الأمر على أن يُتبَع هذا الأخير بتوجيه أصل أمر الإحضار وذلك في أقرب وقت ممكن[2] إلى العون أو الضابط المكلف بتنفيذه.

يبقى إشكال فقط وهو حول إمكانية دخول العون أو الضابط المكلف بالتنفيذ إلى مسكن المتهم فالمشرع الجزائري لم ينصص صراحة على ذلك عندما التزم الصمت حول هذا الأمر الخطير والذي يدل في ظاهره على عدم إجازة هذا الدخول؛ وعدم الإجازة هذه وإن كان ولابد وأن يُأخذ بها في الجرائم العادية فالوضع سيكون معقدا عندما يتعلق الأمر بالجرائم الخطيرة كالتي على شاكلة الجرائم المعلوماتية الأمر الذي جعل بعض الفقه ينادي بضرورة إجراء المشرع لتعديل على ق إ ج يجري من خلاله مسحا على كافة النصوص المتعلقة بمثل هذه الإجراءات الحساسة ويحدث تنسيقا بينها وبين

[1] بوشليق كمال، أوامر قاضي التحقيق المقيدة للحرية، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 02، جامعة عمار ثليجي الأغواط، الجزائر، جوان 2020، ص272 وص273.

[2] المادة 111 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

النصوص الجديدة بحيث تتماشى مع تنفيذ هذه النصوص الأخيرة على الجرائم الخطيرة والمستحدثة في أرض الواقع[1].

هذا وتعتبر الجرائم المعلوماتية كما قلنا سابقا إحدى هذه الجرائم الخطيرة والمستحدثة والتي قد يتركب فيها المجرم المعلوماتي اعتداءاته في مكان وتظهر نتائجها في مكان آخر، والتي قد يكون فيها قاضي التحقيق مختصا في القضية وأصدر أمر بالإحضار، ففي هذه الحالة خول المشرع الجزائري لوكيل الجمهورية المختص بمكان تواجد المتهم المعلوماتي أن يساق إليه هذا الأخير حتى يستجوبه على أن يحيله بعد ذلك إلى قاضي التحقيق المختص بالقضية، وإذا ما أبدى هذا المتهم حججا قوية أمام وكيل الجمهورية تفيد بعدم ارتكابه للجريمة المعلوماتية مثلا وقرر أن يعارض إجراء إحالته، فإنّه بذلك يقتاد إلى مؤسسة إعادة التربية على أن يبلغ قاضي التحقيق المختص في الحال وبأسرع وقت حتى ينظر فيما إذا ما كان ثمة محل للأمر بنقل المتهم[2].

أما في حالة التلبس بالجريمة المعلوماتية هنا على ضابط الشرطة القضائية توقيف المشتبه فيه لمدة 48 ساعة قابلة للتمديد مرة واحدة بإذن من وكيل الجمهورية لضرورات التحقيق[3] بحيث يقع عبأ حماية هذا المشتبه فيه على عاتق هذا الضابط ويكون توقيف المشتبه فيه إما بإحضاره أو إلقاء القبض عليه مع مراعاة الشروط الخاصة بالأمر بالإحضار أو الأمر بالقبض[4]، هذا الأمر الأخير الذي سنتطرق إليه بشيء من التفصيل من خلال الفرع الآتي.

---

[1] عمارة فوزي، المرجع السابق، ص264.

[2] المادة 114 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 51 من القانون رقم 06-22 المعدل والمتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

[4] لخذاري عبد الحق، حقوق المتهم أثناء مرحلتي التحقيق والمحاكمة في الفقه الإسلامي والقانون الجنائي الجزائري، مجلة الحقيقة المجلد 12، العدد 26، جامعة أدرار، الجزائر، ديسمبر 2013، ص268.

الفرع الثاني: الأمر بالقبض على المتهم بالجريمة المعلوماتية

الأمر بالقبض في التشريع الجزائري هو عبارة عن إجراء يصدر عن السلطة القضائية المختصة بحيث تأمر من خلاله القوة العمومية بالبحث عن المتهم وسوقه إلى المؤسسة العقابية المنوه عنها في الأمر أين يجرى تسليمه وحبسه[1]، وهو يعد من بين الإجراءات الاحتياطية التي وضعها المشرع بيد السلطة القضائية المختصة، والذي يساهم ويساعد في عملية التحقيق مع المتهمين بالجرائم المعلوماتية من خلال استجوابهم ومواجهتهم مع غيرهم من الشهود والمجني عليهم المعلوماتيين، إذن هو باب للوصول لكثير من إجراءات التحقيق اللاحقة اللازمة والهامة.

هذا الأمر يعتبر أحد الأوامر الهامة الصادرة عن سلطة التحقيق والذي يصدر إلى القوة العمومية من أجل البحث مثلا عن المتهم المعلوماتي وسوقه إلى المؤسسة العقابية المنوه عنها في ذات الأمر والذي له ذات آثار الأمر بالإحضار السابق الذكر لذلك قيده القانون الجزائري ببعض الشروط[2] الاختيارية منها والمقيدة، فيجوز لقاضي التحقيق إذا كان المتهم هاربا أو مقيما خارج الجمهورية بعد استطلاع رأي وكيل الجمهورية أن يصدر ضد المتهم المعلوماتي أمرا بالقبض على أن ينفذ وفقا للأوضاع[3] السابق ذكرها في الفرع السابق.

هذه الأوضاع تتمثل مجملها أولا في تنفيذ هذا الأمر بالقبض من قبل أحد الضباط أو أعوان الضبط القضائي أو أحد أعوان القوة العمومية[4]، ثانيا إذاعة الأمر بالقبض في حالة الاستعجال بجميع الوسائل بحيث يوجه أصل الأمر الذي يحتوي على كافة البيانات المتعلقة بالقبض في أقرب وقت ممكن إلى الضابط المكلف بتنفيذه[5]، ثالثا إذا رفض المتهم المعلوماتي الامتثال لهذا الأمر أو حاول الهرب يتم

---

[1] الفقرة 1 من المادة 119 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] أحمد شوقي الشلقاني، المرجع السابق، ص276.

[3] المادة 119 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 110 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادة 111 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

إحضاره لقاضي التحقيق جبرا عنه أي بطريق القوة[1]، على أن يتم إحاطة هذا المتهم المعلوماتي بالتهمة المنسوبة إليه من خلال هذا الأمر الذي يتضمن هويته ونوع التهمة والمواد القانونية المطبقة عليها[2].

هذا وتبقى مسألة الشروط المقيدة لقاضي التحقيق أي الواجبة لتطبيق هذا الأمر منها استجواب المتهم المعلوماتي خلال 48 ساعة بعد القبض عليه، وإلاّ يقتاد مباشرة بعد انتهاء هذه المدة إلى وكيل الجمهورية بطلب من قاضي التحقيق في حالة غيابه وإلاّ إلى أي قاض من قضاة الحكم الذي يستجوبه وإلاّ أخلي سبيل هذا المتهم، أو اعتبر الحبس متعسفا فيه بعد مرور هذه المدة ولم يخلى سبيله[3]، أمّا فيما يخص الشرط الآخر المهم فيتعلق بميقات تنفيذ الأمر بالقبض فلا يجوز للمكلف بتنفيذ هذا الأمر الدخول إلى مسكن المتهم قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا[4].

هذا وكما قلنا سابقا بعد القبض على المتهم المعلوماتي فإنّه بذلك يساق إلى المؤسسة العقابية المنوه عنها في أمر القبض على أن يستجوب خلال 48 ساعة التي تعقب ساعة القبض عليه، هذا الاستجواب الذي من خلاله قد يأمر قاضي التحقيق بإيداع المتهم المعلوماتي الحبس المؤقت أو وضعه تحت الرقابة القضائية وإلاّ الإفراج عنه وهو ما سنوضحه من خلال الفروع الآتية.

الفرع الثالث: الأمر بإيداع المتهم بالجريمة المعلوماتية الحبس المؤقت

كما أشرنا إليه سابقا فإنّ الجرائم المعلوماتية تختلف عن الجرائم التقليدية سواء من ناحية عالميتها وسهولة إخفائها وكذلك من ناحية تعقيداتها، حتى التقييم الكمي حولها أثبت بأنّها صعبة المكافحة بل وأصبحت عبئًا كبيرًا على كثير من المؤسسات والشركات بسبب صعوبات الكشف عنها وصعوبة

---

[1] المادة 116 من أمر رقم 66-155،المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] مهديد هجيرة، حق المتهم في الإحاطة بالتهمة في قانون الإجراءات الجزائية الجزائري، مجلة الدراسات القانونية، المجلد 3، العدد 2، جامعة يحي فارس بالمدية، الجزائر، جوان 2017، ص501.

[3] المادة 121 من قانون رقم 06-22، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006..

[4] الفقرة 1 من المادة 122 من القانون رقم 82-03 المعدل والمتمم للأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 7 المؤرخة في 16 فيفري 1982.

التحقيق حولها كما أنّ الجاني فيها قد يفلت من الإدانة، هذا الأخير الذي لا يجوز حبسه[1] ولو مؤقتا إذا لم تتوفر في حقه أدلة تكفي لإدانته.

فالحبس المؤقت يعد من بين مظاهر الصراع بين سلطة الدولة وحق المتهم في احترام حريته وإنسانيته على اعتبار أن هذا الإجراء من إجراءات التحقيق فيه سلب لحرية المتهم وهذا الإجراء الأصل فيه أنّه جزاء جنائي لا يجوز توقيعه إلاّ بحكم قضائي صادر بالإدانة[2]؛ هذا الإجراء لم يعرفه المشرع الجزائري وحتى الفقه اختلف في تعريفه فجاءت إحدى تعريفاته بأنّه إيداع المتهم الحبس خلال مرحلة التحقيق القضائي بل وجعله المشرع الجزائري[3] إجراءا استثنائيا وقرر له شروطا لاتخاذه وأيضا حدد مدته[4].

فالمشرع وضع عدة ضوابط لهذا الإجراء الخطير فلا يُلجأ إليه إلاّ بشروط بحيث نظمه لحماية حقوق الإنسان و كرامته، فليس كل جناية أو جنحة معاقبا عليها بالحبس يكون صاحبها فيها عرضة للحبس المؤقت، كما يستثنى الحدث الذي لم يتجاوز سنه 13 سنة[5]، إضافة أنّه لا يجوز إصدار الأمر بالحبس المؤقت في المخالفات أو الجنح المعاقب عليها بالغرامة المالية، وكذلك كاستثناء الذي يحول دون إمكانية إصدار الحبس المؤقت للصحافيين و السياسيين أمام وكيل الجمهورية فهذا الامتياز قد سحبه المشرع أيضا أمام قاضي التحقيق[6].

---

[1] Xingan Li, Crucial Elements in Law Enforcement against Cybercrime international journal of information security science, volume *7,* Numero3 international institute for innovation society, helsinki, finland, septembre 2018 p154.

[2] فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، مصر، 1999، ص825.

[3] المادة 123 من الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41، المؤرخة في 29 يوليو 2015 تنص: " يبقى المتهم حرا أثناء إجراءات التحقيق القضائي

غير أنّه إذا اقتضت الضرورة اتخاذ إجراءات لضمان مثوله أمام القضاء يمكن إخضاعه لالتزامات الرقابة القضائية

إذا تبين أن هذه التدابير غير كافية يمكن بصفة استثنائية أن يؤمر بالحبس المؤقت"

[4] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، د ط، دار هومة للطباعة، الجزائر، 2008، ص127.

[5] المادة 58 من القانون رقم 15-12 مؤرخ في 15 يوليو 2015، يتعلق بق ح ط، ج ر رقم 39، المؤرخة في 19 يوليو 2015.

[6] عبد الله أوهايبية، محاضرات في قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، الجزائر،2011، ص388.

هذا وتعتبر الجرائم المعلوماتية كما قلنا سابقا إحدى الجرائم المستحدثة والخطيرة والتي لا تقل عقوبتها عن الحبس، وطبقا لما أثرناه من بعض الشروط حول مدى تطبيق إجراء الحبس المؤقت في حق المتهم بصفة عامة فالملاحظ بالنسبة للمتهم بهذه النوعية من الجرائم أنّه سيكون معرضا لهذا الإجراء بنسبة كبيرة جدا، على الرغم من القفزة النوعية لحماية حق حرية المتهم التي جاء بها تعديل المادة 123 من ق إ ج[1] الجزائري خاصة إذا ما توافرت شروط تفعيل إجراء الحبس المؤقت[2] لدى المتهم بالجريمة المعلوماتية لاسيما فيما يتعلق بعدم كفاية التزامات الرقابة القضائية التي تضمن حضور المتهم لإجراءات التحقيق[3].

إن التعديل الذي جاء به المشرع الجزائري من خلال الأمر 15-02 فيما يخص إجراء إيداع المتهم الحبس المؤقت استطاع إلى حد كبير ضبط لُب ما يتعلق بهذا الإجراء الخطير سواء من حيث مدته والأسباب المؤدية إلى تفعيله ومرات وإجراءات تمديده[4] التي قد تصل إلى تمديده مرة واحدة وبأربع

---

[1] تنص الفقرة 1 من المادة 123 من الأمر رقم 15-02، المعدل والمتمم لق إ ج الجزائري، القانون السابق، بأنّه: " يبقى المتهم حرا أثناء إجراءات التحقيق القضائي ".

[2] تنص المادة 123 مكرر من الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41 المؤرخة في 29 يوليو 2015 بأنّه: "يجب أن يؤسس أمر الوضع في الحبس المؤقت على معطيات مستخرجة من ملف القضية تفيد:

1- انعدام موطن مستقر للمتهم أو عدم تقديمه ضمانات كافية للمثول أمام القضاء أو كانت الأفعال جد خطيرة.

2- أن الحبس ا لمؤقت هو الإجراء الوحيد للحفاظ على الحجج أو الأدلة ا لمادية أو لمنع الضغوط على الشهود أو الضحايا، أو لتفادي تواطؤ بين المتهم ين والشركاء قد يؤدي إلى عرقلة الكشف عن الحقيقة.،

3- أن الحبس ضروري لحماية ا لمتهم أو وضع حد للجريمة،أو الوقاية من حدوثها من جديد،

4- عدم تقيد ا لمتهم بالالتزامات ا لمترتبة على إجراءات الرقابة القضائية دون مبرر جدي".

[3] رمضاني ابتسام، تافرونت عبد الكريم، تطبيق نظام المراقبة الإلكترونية في التشريع الجزائي الجزائري، مجلة الباحث للدراسات الأكاديمية، المجلد 07، العدد 02، كلية الحقوق والعلوم السياسية، جامعة باتنة الحاج لخضر، الجزائر، 2020، ص 861.

[4] بحرية أسيا، دراسة تحليلية للحبس المؤقت في ظل الأمر 15-02 المعدل لقانون الإجراءات الجزائية، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 3، العدد 2، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت، الجزائر ديسمبر 2018، ص106.

أشهر للمرة الواحدة[1] في الجرائم المعلوماتية التي لا يتجاوز وصفها لحد الساعة وصف الجنحة في التشريع الجزائري؛ فيبقى بذلك لقاضي التحقيق فيما يخص هذه الجريمة المستحدثة تفعيل إجراء الحبس المؤقت من عدمه وذلك كله مرهون بطبيعة المعطيات المتاحة لديه وبنوع الجريمة المعلوماتية الموجودة أمامه.

هذا ويمكن لقاضي التحقيق في حالة عدم تفعيله لإجراء الحبس المؤقت بالنسبة للمتهم بالجريمة المعلوماتية أن يفعل إجراء هاما آخر والمتمثل في إجراء الرقابة القضائية والذي سنتطرق له بشيء من التفصيل من الخلال الفرع الآتي.

الفرع الرابع: الأمر بوضع المتهم بالجريمة المعلوماتية تحت الرقابة القضائية

نظراً لكثرة المنادين بقرينة البراءة الأصلية والتزايد المستمر والمطالبة بالتضييق في استعمال الحبس المؤقت، جاء المشرع بنظام الرقابة القضائية التي تعد بحق نقلة نوعية وتدبير بديل للحبس المؤقت بحيث يهدف من وراء تنفيذها إلى الحد من اللجوء المفرط للحبس المؤقت، فهي تبدوا كإجراء وسط بين الحبس المؤقت والإفراج، إذ يمكن تكييفها على أنها تدابير احتياطية وأمنية الغرض منها إبقاء المتهم تحت تصرف القضاء وإلزامه ببعض الالتزامات[2].

أمّا تعريفها قانونا فليس هناك نص قانوني يعرف نظام الرقابة القضائية لا في التشريع الجزائري ولا حتى في التشريع الفرنسي، أمّا فقها فقد عرفه البعض بأنّه نظام إجرائي بديل للحبس المؤقت يفرض بموجبه قاضي التحقيق التزاما أو أكثر على المتهم ضمانا لمصلحة التحقيق أو المتهم والتي يجب على هذا الأخير أن يلتزم بها[3]، هذا وقد استحدث المشرع الجزائري نظام الرقابة القضائية وكان في بدايته كبديل للحبس المؤقت بموجب القانون رقم 86-05، ليعود الفضل لهذا القانون الأخير الذي وضع

[1] المادة 124 و125 من الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41 المؤرخة في 29 يوليو 2015.

[2] أحسن بوسقيعة، التحقيق القضائي. دار هومة، ط الحادية عشر، 2014، ص1.

[3] محمد حزيط، المرجع السابق، ص140.

إلى جانب الحبس المؤقت وسيلة قسرية تدعى الرقابة القضائية والذي نظم أحكامها بمقتضى المادة125مكرر1[1].

وإذا كان القانون رقم 86-05 قد أدخل تعديلات على ق إ ج التي بموجبها أوجد نظام الرقابة القضائية كبديل للحبس المؤقت ووسيلة للحد من اللجوء إلى الحبس المؤقت استثناءاً فقط[2]، وإذا كان المسلم به أن نظام الرقابة القضائية هو بديل للحبس المؤقت فقد ذهب جانب آخر من الفقه بقوله أنّ الحقيقة ليست كذلك لأن هذا النظام منطقيا يعتبر بديلا للحرية وليس للحبس ما دام أنّه يطبق على أشخاص كانوا قبل فرضه يتمتعون بحرية مطلقة[3].

وأمّا فيما يخص شروط تطبيق الرقابة القضائية فلم يضع المشرع الجزائري قيوداً خاصة على تطبيقها سوى ما تعلق بطبيعة الجريمة التي يجب أن تكون معاقب عليها بالحبس[4] أو أشد عقوبة، لذلك يستطيع قاضي التحقيق تفعيلها فيما يخص موضوع الدعوى العمومية لهذه الدراسة المتمثلة في الجرائم المعلوماتية بحيث يخضع المتهم فيها لواحد أو أكثر من الالتزامات المنصوص عليها في نص المادة 125 مكرر 1 من ق إ ج الجزائري[5]، والتي تخول كذلك لقاضي التحقيق أن يأمر بوضع ترتيبات تقنية يستطيع من خلالها مراقبة المتهم إلكترونيا في الحالات المتعلقة بالتزامات مكان تواجد المتهم[6].

---

[1] عبد الرحمان خلفي، المرجع السابق، ص375.

[2] القانون رقم 86- 05 المؤرخ في 04 مارس 1986 يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 10 المؤرخة في 05 مارس 1986.

[3] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، ط سادسة، 2006، ص399.

[4] نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي. دار هومه، ط ثانية، 2016، ص258.

[5] أمر رقم 15-02 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41، المؤرخة في 29 يوليو 2015.

[6] الفقرة 3 من المادة 125 مكرر1 من الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري ج ر رقم 41، المؤرخة في 29 يوليو 2015.

هذا الإجراء المستحدث الأخير[1] الذي بموجبه يستطيع قاضي التحقيق أن يأمر ضباط الشرطة القضائية بمراقبة المتهم الخاضع لأحد التزامات الرقابة القضائية بطريقة إلكترونية للتحقق من مدى التزام هذا المتهم بالتدابير المفروضة عليه، بل وسيكون حسبا رأينا ذا فعالية بالنسبة للمتهم بالجريمة المعلوماتية خاصة إذا ما كان قاضي التحقيق أو ضابط الشرطة القضائية متمكنا ومحترفا في مجال تكنولوجيا المعلومات والاتصال، فيكون بذلك جزاء من جنس العمل الضار بالنسبة لمجرمي الجرائم المعلوماتية، كما أن تفعيل إجراء المراقبة الإلكترونية قد يحول دون ارتكاب المجرم المعلوماتي لاعتداءات أخرى أو ضبطه متلبسا أثناء ارتكابه لهذه الاعتداءات مرة أخرى إذا ما كانت هذه التقنية ذات مستوى عال من التطور والذكاء.

وتجدر الإشارة كذلك أنّ المشرع الجزائري لما جاء بتقنية السوار الإلكتروني كتقنية تكنولوجية جديدة ترك لقاضي التحقيق السلطة التقديرية كي يفرض التزاماته على واضع السوار[2]، بحيث يتم من خلاله مراقبة المتهم عن طريق سوار معدني مخصص لهذا الغرض يثبت في أسفل القدم بواسطة مفتاح يحتفظ به قاضي التحقيق، هذا الأخير يكلف ضباط الشرطة القضائية بمراقبة المتهم عن طريق تطبيق إعلامي وآلي يحدد المواقع حتى يتم مراقبة تحركات المتهم ضمن الإقليم المحدد من طرف قاضي التحقيق[3].

هذا المشرع أحسن كذلك لما أجاز لجهة التحقيق[4] استعمال المحادثة المرئية عن بعد، لذلك تستطيع الآن جهة التحقيق في الجرائم المعلوماتية الاعتماد بدرجة كبيرة عليها خاصة من خلال إجراءات استجواب المتهم بالجريمة المعلوماتية أو بسماع شخص وفي إجراء المواجهة بين الأشخاص، حتى وإن

---

[1] استحدث نظام المراقبة الإلكترونية بموجب الأمر رقم 15-02 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري ج ر رقم 41، المؤرخة في 29 يوليو 2015.

[2] قتال جمال، عقابوي سلمى، بدائل العقوبة السالبة للحرية – السوار الإلكتروني-، مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 02، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، جانفي 2020، ص186.

[3] نجيمي جمال، المرجع السابق، ص259.

[4] جهة التحقيق في التشريع الجزائري يمثلها كل من قاضي التحقيق وغرفة الاتهام وقاضي الحكم في حالة إجراء تحقيق تكميلي طبقا لنص المادة 356 من ق إ ج.

كان هذا الشخص مقيما بدائرة اختصاص محكمة أخرى أو محبوسا في مؤسسة عقابية، بل وحتى في التبليغات التي يستوجب ق إ ج الجزائري تحرير محاضر بشأنها أو محاضر سماع هذا الشخص فإنّها ترسل بالطريق الإلكتروني لصاحبها حتى يوقع عليها[1]، وكذلك إذا ما أمر قاضي التحقيق بوضع هذا المتهم المعلوماتي رهن الحبس المؤقت فيكون عبر هذه الوسيلة بإعلامه شفاهة أين يبين له مختلف حقوقه، هذا وترسل نسخة من الأمر بالإيداع للتنفيذ عن طريق إحدى وسائل الاتصال حسب الحالة إلى وكيل الجمهورية أو مدير المؤسسة العقابية[2].

الفرع الخامس: استعانة قاضي التحقيق بآلية تسليم المجرمين

تجدر الإشارة بأنّه في كثير من الأحيان ما تعتبر الجرائم المعلوماتية مجرد تهديد أو مشكل صغير بالنسبة للكثير من السلطات الحكومية العالمية حيث يتم وضعها عادة في نهاية القائمة في دورات البرلمان على العكس تماما مقارنة بما تطرقنا إليه بالدراسة سابقا، خاصة عندما نرى بأنّ مختلف هذه الحكومات تعتمد على أساليب غير مبررة في محاربة وتتبع ومكافحة هذه الهجمات الإلكترونية لا تتناسب والتهديدات التي يشكلها المجرمين المعلوماتيين، لذلك يجب على مختلف الحكومات أن تعتمد بشكل أكبر على محاربة هذا الإجرام المستحدث بل ويجب حتى على مختلف المنظمات أن تأخذ هذه الجرائم على محمل الجد[3]، خاصة من خلال التعاون الدولي في مكافحة هذه الجرائم العابرة للحدود الإقليمية.

هذا وتعتبر آلية تسليم المجرمين صورة من صور التعاون الدولي أين تقوم الدولة المطلوب منها التسليم بعملية تسليم شخص يوجد داخل إقليمها إلى دولة أخرى من أجل متابعته قضائيا، بل وحتى

---

[1] المواد 441 مكرر2 و441 مكرر3 و441 مكرر4 من الأمر رقم 20- 04، المعدل والمتمم لق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[2] المادة 441 مكرر 6 من الأمر رقم 20- 04، المعدل والمتمم ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[3] Anil Kumar - Jaini Shah, The Threat of Advancing Cyber Crimes in Organizations: Awareness and Preventions, International Journal of Advanced Research in Computer Science, Volume 5, numero 8, Udaipur , India, Nov-Dec 2014, p89.

تقديمه إلى جهة قضائية دولية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكم جنائي صادر ضده[1]، هذه الآلية جاءت نتيجة للتطورات التي حدثت في كافة المجالات كمجال الاتصالات وتقنيات المعلومات بحيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، فنشاطهم الإجرامي لم يعد قاصرا على إقليم معين وإنّما امتد وتعدى مختلف الحدود الدولية،[2] فأصبح المجرم يشرع في التحضير لارتكاب جريمته في بلد معين ثم ينفذها في بلد آخر على أن يفر لبلد ثالث.

هذه الآلية تختلف طبيعتها القانونية من دولة لأخرى وذلك حسب الجهة المختصة بإصدارها فهناك دول تعتبرها عملا سياديا تباشر من طرف السلطة التنفيذية دون رقيب وهناك دول أخرى تعتبرها عملا قضائيا صادر عن جهة قضائية مختصة وفقا لإجراءات معينة، ويوجد دولا تتبنى نظاما مختلطا لآلية تسليم المجرمين يجمع بين الطابع السيادي والطابع القضائي في آن واحد[3]، كما هو الحال في الجزائر والذي تبنته وفق الشروط والإجراءات الآتية؛

أولا: شروط تسليم المجرمين في مجال مكافحة الجرائم المعلوماتية

قبل ذكر هذه الشروط التي تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم، لابد من المعرفة في الأول بأنّ طبيعة الجريمة لها دور كبير في تحديد ما إذا كان بالإمكان أن يسلم المجرم من أجلها فلا يجوز تطبيق هذا الإجراء على جميع الجرائم، لهذا وفيما يخص موضوع الدعوى المتمثل في الجرائم المعلوماتية فإنّ إجراءات تسليم المجرمين[4] في التشريع الجزائري تطبق عليها وذلك من خلال الشروط التالية؛

---

[1] سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين دراسة مقارنة. د ط، دار الجامعة الجديدة، الإسكندرية مصر، 2007، ص76.

[2] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، ط أولى، مكتبة الوفاء القانونية، الإسكندرية مصر 2016، ص481.

[3] أمل لطفي حسن جاب الله، نطاق السلطة التقديرية للإدارة في مجال تسليم المجرمين دراسة مقارنة. ط أولى، دار الفكر الجامعي الإسكندرية، مصر، 2013، ص29.

[4] تنص الفقرة 1 و 2 من المادة 697 من ق إ ج الجزائري بأنّه:" الأفعال التي تجيز التسليم سواء كان مطلوبا أو مقبولا هي الآتية:
- جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جناية

1- التجريم المزدوج

أن تكون نوع الجريمة المعلوماتية المطلوب التسليم من أجلها مجرمة ومعاقبا عليها في تشريع كلا الدولتين الطالبة والمطلوب إليها التسليم حتى ولو اختلف في وصف الجريمة في تلك الدولتين[1].

2- عدم جواز تسليم الرعايا

يعتبر أحد المبادئ السائدة التي استقر عليها المجتمع الدولي أيّا كانت نوع الجريمة المعلوماتية المرتكبة من قبل أحدهم في أي إقليم خارج دولته، هذا الإجراء يقاس عليه حتى طالبي حق اللجوء السياسي والذين كذلك لا يجوز تسليمهم هم الآخرين[2].

3- عدم جواز تسليم من تم محاكمته عن ذات الجريمة المطلوب تسليمهم لأجلها

يعتبر أحد الضمانات الأساسية للمتهم بالجريمة المعلوماتية فهو يهدف إلى تحقيق أكبر قدر من الحماية القضائية للشخص المطلوب تسليمه، مع ذلك لا يحول دون إمكان إرسال الأجنبي مؤقتا للمثول أمام محاكم الدولة الطالبة على شرط أن يعاد بمجرد الانتهاء من الفصل في الجريمة من طرف القضاء الأجنبي، هذا الشرط يطبق حتى ولو كان الأجنبي خاضعا لإكراه بدني طبقا للقانون الجزائري[3].

ثانيا: إجراءات تسليم المجرمين في مجال مكافحة الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية أحد الجرائم الحديثة والخطيرة والتي تتطلب السرعة في تفعيل إجراءات متابعتها أمام الجهات القضائية المختصة وهو الأمر الذي حذا بالمشرع الجزائري وفق شروط معينة إلى تبسيط إجراءات آلية تسليم المجرمين استعجالا منه لملاحقة المتهمين بهذا النوع من الإجرام، هذه الشروط

ـ الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة المطبقة طبقا لنصوص ذلك القانون سنتين أو أقل أو إذا تعلق الأمر بمتهم قضي عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تجاوز الحبس لمدة شهرين".

[1] الفقرة 4 من المادة 697 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] الفقرة 1 من المادة 698 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 701 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

في حالة عدم توفرها في وقتها المحدد فإنّ حالة الاستعجال تنتفي، ويلاحق المتهمين بطريق عادي غير استعجالي.

1- الحالة الاستعجالية

يستطيع وكيل الجمهورية لدى المجلس القضائي المختص أن يأمر بالقبض المؤقت على الأجنبي المتهم بالجريمة المعلوماتية بناء على طلب مباشر من السلطات القضائية للدولة الطالبة، هذا الطلب المرسل بمجرد إخطار سواء بالبريد أو بأي طريق من طرق الإرسال الأكثر سرعة التي يكون لها أثر مادي مكتوب يدل على وجود أحد المستندات[1] الواردة في نص المادة 702 من ق إ ج الجزائري؛ على أن يرسل في الوقت ذاته إخطارا قانونيا عن هذا الطلب بالطريق الدبلوماسي إلى وزارة الخارجية أو بطريق البريد أو البرق أو بأي طريق من طرق الإرسال التي يكون لها أثر مكتوب، كما يجب على النائب العام المختص أن يحيط كل من الناب العام لدى المحكمة العليا ووزير العدل عن هذا الأمر بالقبض[2].

في حالة لم تتلقى الحكومة الجزائري أي من المستندات السابق ذكرها خلال الخمس والأربعين يوما من تاريخ إلقاء القبض على هذا المتهم يجوز الإفراج عن هذا الأخير بناءا على عريضة توجه إلى المحكمة العليا التي تفصل فيها خلال ثمانية أيام بقرار غير قابل للطعن، أمّا في حالة وصول هذه المستندات بعد المدة القانونية هنا تستأنف الإجراءات[3] كما لو كانت حالة عادية.

---

[1] المستندات وفقا للمادة 702 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966 تعبر عن أصول أو نسخ رسمية من الحكم الصادر بالعقوبة حتى ولو كان غيابيا أو أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا بإحالة المتهم بالجريمة المعلوماتية إلى جهة القضاء الجزائي أو عن الأمر بالقبض أو أية ورقة صادرة من السلطة القضائية ذات قوة قانونية على أن تتضمن بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل بالإضافة لنسخة من النصوص القانونية المطبقة على الفعل المكون للجريمة المعلوماتية وأن ترفق كذلك ببيان لوقائع الدعوى.

[2] المادة 712 الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 713 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

2- الحالة العادية

وجوب طلب التسليم من طرف حكومة الدولة الطالبة إلى الحكومة المطلوب منها بالطريق الدبلوماسي، بواسطة وزير الخارجية الذي يحيله بعد فحصه للمستندات والملف إلى وزير العدل للنظر فيه وتقرير مدى أحقيته، كما يجب أن يرفق مع طلب التسليم بيان الأفعال المطلوب التسليم من أجلها وزمان ومكان ارتكابها، وتكييفها القانوني والنصوص الواجبة التطبيق[1]، وبعد ذلك ما لم يتنازل الأجنبي المتهم بالجريمة المعلوماتية في حق عدم تسليمه للدولة الطالبة[2] يتولى النائب العام وخلال الأربع والعشرين ساعة التالية على قبض الأجنبي المتهم بالجريمة المعلوماتية باستجوابه، بهدف التحقق من هويته ويبلغه بالمستند الذي بموجبه قبض عليه[3]، ويُنقل في أقصر وقت ممكن ليُحبس في سجن العاصمة[4].

في نفس الوقت تحول المستندات المقدمة والمؤيدة لطلب التسليم إلى النائب العام لدى المحكمة العليا الذي يقوم باستجواب هذا المتهم ويحرر بذلك محضرا خلال أربع وعشرين ساعة[5]، هذه المحاضر والمستندات ترفع إلى الغرفة الجنائية بالمحكمة العليا بحيث يمثل الأجنبي المتهم بالجريمة المعلوماتية وفق الآجال المحددة أمامها في جلسة علنية ما لم يتقرر خلاف ذلك بناء على طلب النيابة أو صاحب الشأن اللذيْن يُسمع لقوليهما، كما يجوز لهذا المتهم بأن يستعين بمترجم وحتى بمحام مقبول أمام هذه الغرفة وعلى ذلك يجرى استجوابه ويحرر محضرا بهذا الاستجواب[6].

بعد كل هذه الإجراءات قد تصدر المحكمة العليا رأيا نهائيا مسببا يُرفض من خلاله طلب التسليم أمّا إذا قبلت التسليم هنا يعرض وزير العدل مرسوما بالإذن بالتسليم نافذا لمدة شهر من تاريخ تبليغه

---

[1] المادتان 702 و703 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] المادة 708 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 704 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 705 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادة 706 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[6] المادة 707 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

للدولة الطالبة للمتهم بالجريمة المعلوماتية وإلاّ أفرج عن هذا الأخير بعد انقضاء هذه المدة دون استلامه بحيث لا يجوز المطالبة به مرة أخرى لنفس السبب[1].

إنّ تحقق شروط وإجراءات آلية تسليم المجرمين يحقق مصلحة الدولة الطالبة في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها، ويحقق في نفس الوقت مصلحة الدولة المطلوب منها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون يهدد أمنها واستقرارها[2]، خاصة إذا ما كان موضوع الدعوى العمومية هو الجرائم المعلوماتية ذات الطبيعة المتعدية للحدود، لذلك يجد قاضي التحقيق نفسه أحيانا ملزما بالاستعانة بهذه الآلية الدولية للقيام ببعض تحقيقاته، يكفي أن تكون هناك اتفاقية بين الدولة الطالبة الجزائر والدولة المطلوب منها التسليم أيّا كانت، وأن تكون هذه الاتفاقية تُعنى بعملية تسليم المجرمين ووضع قوانين خاصة بها داخل أطراف الاتفاقية.

المطلب الثالث: تصرف قاضي التحقيق في نتائج التحقيق في الجرائم المعلوماتية

كنا قد تطرقنا من خلال هذا الفصل لعدة سلطات وإجراءات مخولة لقاضي التحقيق يبحث ويكشف عن المجرمين المعلوماتيين ويحقق من خلالها معهم، هذه الإجراءات تساعده في استقصاء مختلف الأدلة المهمة والمساعدة في إظهار نوع الجريمة المعلوماتية المرتكبة وكذا كشف المخططات اللاحقة لهؤلاء المجرمين، أمّا عن نتائج هذا البحث والاستقصاء فهي من تحدد في نهاية هذه المرحلة من الدعوى طبيعة الأوامر التي يجب على قاضي التحقيق إصدارها، هذه الأوامر التي لا تخرج عن أحد الأمرين إمّا تصرف القاضي بالأمر بأن لا وجه لمتابعة المتهمين المعلوماتيين، وإمّا التصرف بالأمر بإحالة القضية إلى المحكمة المختصة بنظر هذه القضية.

[1] المادة 711 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، المرجع السابق، ص482.

الفرع الأول: الأمر بأن لا وجه للمتابعة في الجريمة المعلوماتية

الجدير بالذكر أنّ صلاحيات قاضي التحقيق القضائية تبرز أكثر في مرحلة غلق التحقيق الابتدائي خاصة عند إصداره لأمر بأن لا وجه للمتابعة في الدعوى العمومية، هذا الأمر الذي يصدره قاضي التحقيق بإنهاء التحقيق القضائي الذي يجريه بناء على أسباب قانونية أو أسباب موضوعية، فتتوقف عنده الدعوى العمومية في مرحلة التحقيق الابتدائي، لذا لا تتخذ بعد هذه المرحلة أي إجراءات تحقيقية أخرى وبطبيعة الحال مع عدم الإحالة[1]، هذا وتجدر الإشارة أنّه من الناحية العملية في الجزائر لا يجوز لقاضي التحقيق أن يصدر أي أمر من أوامر التصرف إلاّ بعد إبلاغه لوكيل الجمهورية[2].

وعليه إذا تبين لقاضي التحقيق على ضوء النتائج التي توصل إليها أن الوقائع المتابع من أجلها المتهم لا تكون جريمة معلوماتية أو أنّه لا توجد دلائل كافية ضد هذا المتهم أو كان مقترف مثل هذه الجريمة الأخيرة ما زال مجهولا، يصدر قاضي التحقيق أمر بألاّ وجه للمتابعة ضد هذا المتهم الذي يجب أن يخلى سبيله إذا كان محبوسا مؤقتا فور صدور الأمر حتى وإن استأنفت النيابة العامة في هذا الأمر أمام غرفة الاتهام[3]، فصدور أمر بألاّ وجه للمتابعة من قبل قاضي التحقيق في الأصل يعبر عن عدم مواصلة الدعوى العمومية في الجريمة المعلوماتية والتوقف بها عند مرحلة التحقيق الابتدائي فحسب.

فبغض النظر عما يستلزمه التحقيق فهناك أوقات تأتي يجب أن يغلق فيها ملف كل قضية بمجرد انتهاء التحقيق فيها بحيث يجب تقبل نتائجها والمضي قدما للتحقيق في قضايا أخرى[4]، هذا ويكون صدور هذا الأمر تعبيرا عن النتائج المذكورة آنفا التي توصل إليها هذا القاضي، والتي يترتب عنها خروج

---

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، ط مزيدة ومنقحة، دار هومة للطباعة والنشر والتوزيع الجزائر العاصمة، الجزائر، 2018، ص587.

[2] معمري كمال، الأمر بألا وجه للمتابعة، مجلة البحوث والدراسات القانونية والسياسية، المجلد 3، العدد 2، كلية الحقوق والعلوم السياسية، جامعة البليدة 2، العفرون، البليدة، الجزائر، جوان 2013، ص248.

[3] المادة 163 من الأمر رقم 15-02 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41، المؤرخة في 29 يوليو 2015.

[4] Michael cross, scene of the cybercrime, second edition, syngress publishing INC 2008, P239.

الدعوى الجزائية من حوزة سلطة التحقيق نهائيا، فلا تملك الرجوع عن قراراها إلاّ إذا ظهرت دلائل جديدة تبرر العودة إلى التحقيق[1]، هذه الدلائل التي اشترط فيها المشرع الجزائري أن تكون جديدة لم تعرض على قاضي التحقيق من قبل لتمحيصها والتي من شأنها أن تعزز الأدلة الضعيفة الأولى أو من شأنها أن تعطي الوقائع تطورات نافعة لإظهار الحقيقة، كما اشترط في هذه الأدلة أن يكون للنيابة العامة وحدها سلطة تقرير إعادة التحقيق بناءا عليها[2].

هذا ويعتبر عدول قاضي التحقيق بعد إصداره الأمر بأن لا وجه للمتابعة بطلبه من النيابة العامة إعادة التحقيق بناء على أدلة جديدة ضروري ومهم في الجرائم المعلوماتية موضوع دراستنا وبحثنا هذا فهذه الجريمة كما أشرنا إليها سابقا تتميز بصعوبة اكتشافها من جهة وصعوبة إثابتها من جهة أخرى كما أنّها قد تلقي بآثارها بعد فترة طويلة من ارتكابها تتجاوز فترة التحقيق الابتدائي حولها، هذه الآثار التي قد تولد أدلة جديدة قوية في الإثبات تساعد في إظهار الحقيقة، يبقى فقط كما أشرنا سابقا على عاتق النيابة فيما بعد وحدها تقرير إعادة التحقيق في هذه القضية بناء على هذه الأدلة الجديدة.

الفرع الثاني: الأمر بالإحالة إلى المحكمة المختصة بالنظر في الجريمة المعلوماتية

الإحالة كأصل عام إجراء يستهدف من ورائه الحيلولة دون حدوث تنازع محتمل في الاختصاص سواء كان تنازع إيجابي أو سلبي[3]، أمّا الأمر بالإحالة في جانبه الجزائي يعتبر أمرا ناقل للدعوى العمومية من مرحلة التحقيق الابتدائي إلى مرحلة المحاكمة وهو أمر تصرف ومنهي للتحقيق بحيث يتضمن رجحان إدانة المتهم نتيجة اقتناع سلطة التحقيق بملائمة إحالة الدعوى إلى المحكمة المختصة[4].

لذلك إذا رأى قاضي التحقيق أن الواقعة تعد جريمة معاقبا عليها كإحدى الجرائم المعلوماتية أصدر أمر بالإحالة للمحكمة المختصة بنظرها، أين يقوم بإرسال ملف الإجراءات كاملا مرفقا بأمر

---

[1] سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المرجع السابق، ص569.

[2] المادة 175 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] سامية نوري، محمد الأمين نوري، نظام الإحالة على محكمة التنازع في التشريع الجزائري، مجلة طبنة للدراسات العلمية الأكادمية المجلد 3، العدد 1، المركز الجامعي سي الحواس بريكة، باتنة، الجزائر، جوان 2020، ص301.

[4] نظير فرج مينا، الموجز في الإجراءات الجزائية، ط ثانية، ديوان المطبوعات الجامعية، الجزائر، 1992، ص101.

الإحالة إلى وكيل الجمهورية الذي يقوم بدوره بغير تمهل بإرساله إلى قلم كتاب الجهة القضائية، وتحديد ميعاد الجلسة لنظر الدعوى أمام المحكمة المختصة، كما يقوم بتكليف المتهم بالحضور للجلسة التي يكون قد حددها له أمام تلك المحكمة لنظر الدعوى[1].

كما أنّ ترجيح إدانة شخص كالمتهم المعلوماتي من قبل قاضي التحقيق ليس اقتناعا منه بملائمة إحالة الدعوى العمومية إلى المحكمة المختصة، هذه الأخيرة التي تعود إليها فقط الحسم والحزم ما إذا كان هذا الاقتناع يتطابق في نهاية الأمر مع حقيقة الواقع وصحيح القانون[2]، فهناك اختلاف بين درجة الاقتناع الكافي للأمر بالإحالة ودرجة الاقتناع التي تصل إلى حد اليقين والحزم بالنسبة لأحكام المحاكم ولئن كان الشك أمام جهات الحكم يفسر لمصلحة المتهم، فهو عند التصرف في التحقيق يفسر ضد مصلحة المتهم[3]، خاصة في مثل جرائم معقدة كالجرائم المعلوماتية التي تزيد من صعوبة التحقيق فيها.

فالطبيعة الخاصة والمعقدة للجرائم المعلوماتية تجعل من قاضي التحقيق كثير الشك حول المتهم المعلوماتي، ذلك أنّ المجرم المعلوماتي في غالب الأحيان ما يكون محترفا في إخفائه لآثار وأدلة جريمته خاصة تلك الأدلة ذات الطبيعة المعنوية[4]، هذه النوعية من الأدلة تبقي قاضي التحقيق غارقا في شكه إن لم يجد أدلة قوية تثبت براءة المتهم المعلوماتي، فيلجأ بذلك بل ويتعمد في كثير من الأحيان إلى إصدار الأمر بالإحالة إلى المحكمة المختصة بهذه الجريمة للتدقيق وتمحيص الأدلة المتوفرة ورغبة منه في الحصول على أدلة قوية أخرى أثناء المحاكمة وحتى بعدها.

---

[1] المادة 165 من قانون رقم 90-24، المؤرخ في 18 أوت 1990، المعدل والمتمم للأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 36، المؤرخة في 22 أوت 1990.

[2] نظير فرج مينا، المرجع السابق، ص 102.

[3] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، المرجع السابق، ص 214.

[4] الأدلة ذات الطبيعة المعنوية كما تطرقنا إليها سابقا من خلال العناصر السابقة.

الفصل الثاني: إجراءات المحاكمة في الجرائم المعلوماتية

كأصل عام فإنّ معظم المتهمين بالجريمة المعلوماتية تتم محاكمتهم أمام المحاكم الجزائية العادية، تبقى مسألة تقديم المعلومات العلمية ومصطلحات التقنية العالية أمام هذه المحاكم ومهمة شرحها للقضاة هي التي تشكل صعوبة بالغة لدى المحققين وأعضاء النيابة العامة، فتترك هذه المهمة في الغالب للخبراء وهو الأمر الذي يفقد ويخرج القضية الجزائية من عناصرها القانونية، فلا تتمكن المحكمة بذلك من الوقوف كلية على الحقائق المكونة لأركان الفعل الإجرامي والتيقن من الأدلة التي تثبت تلك الأركان.

من هنا يرى بعض الفقه والذي بدوري والذي بدوري أؤيده، بضرورة التحضير لإجراءات المحاكمة وإلزامية القيام به من طرف المحقق وممثل النيابة العامة، فالمحقق في خطوة أولى يجب عليه أن يلخص القضية تلخيصا كافيا شافيا يحصر فيه جميع التهم ويبين فيه سيناريو الجريمة المعلوماتية كما كشفتها التحريات والتحقيقات والأدلة المتوفرة، وفي خطوة ثانية يجب عليه أن ينسق مع الخبير المعلوماتي الذي ساهم في هذه القضية بحيث يشرح له الجوانب القانونية الخاصة بها، ويقوم بعد ذلك بحصر جميع الأدلة المتوفرة وأن يرتبها وفقا لأهميتها وقوتها[1].

أمّا الخطوة الثالثة فيجب عليه أن يلتقي بممثل النيابة العامة الذي يتولى مهمة الادعاء في القضية ويشرح له أبعاد الفعل الإجرامي حتى يتمكن هذا الأخير من صياغة التهمة المناسبة ويتفقان حول العناصر والأركان التي تقوم عليها الجريمة المعلوماتية وكذا على ترتيب الأدلة حسب كل ركن وعنصر من عناصر الجريمة، وفي خطوة رابعة يجب أن يتم اللقاء بين المحقق وممثل النيابة العامة والخبير المعتمد عليه في هذه القضية من أجل ترتيب المصطلحات الفنية المستخدمة أثناء إجراءات المحاكمة وتعريف استخدامها ومرادفاتها التي قد ترد أثناء الاستجواب وذلك حتى لا يستطيع المتهم التلاعب بها وإثارة الشك من خلالها.

[1] محمد الأمين البشرى، المرجع السابق، ص130.

تبقى آخر خطوة مهمة وتكمن في ضرورة وضع سيناريو للمحاكمة سواء من قبل المحقق أو ممثل النيابة العامة، بحيث يقوم من خلاله بترتيب الأحداث والوقائع ومجمل العمليات الفنية التي تشكل الجريمة المعلوماتية مع إظهار القصد الجنائي ومبررات علاقة المتهم المعلوماتي مع الفعل الإجرامي موضوع الاتهام هذا السيناريو الذي يجب أن يشمل أسلوب الإخراج القانوني للأدلة الجزائية بطريقة تتناسب معها الحقائق المؤكدة في عقل قاضي الحكم، وهنا يحدد واضع السيناريو النهج الذي يتبعه في تقديم أدلة الإثبات المختلفة.

هذا ونشيد كذلك بالمشرع الجزائري بالرغم من تأخره، ونقول بأنّه أحسن لما نظم من خلال التعديل الأخير لق إ ج[1] بأن سمح للمحكمة الناظرة في موضوع الدعوى العمومية باستعمال المحادثة المرئية عن بعد[2] من تلقاء نفسها إن هي رأت ضرورة لذلك، هذه الضرورة التي تفرضها أحيانا الطبيعة الخاصة للجريمة موضوع المتابعة كالجرائم المعلوماتية التي تعتبر محورا لتفعيل مختلف الإجراءات الجزائية المتطرق إليها من خلال هذه الدراسة، وهذه المرحلة الهامة من سير الدعوى العمومية في الجرائم المعلوماتية والمتمثلة في إجراءات المحاكمة، رأينا من الأحسن أن نقسمها إلى ثلاثة مراحل مرتبطة ومتصلة مع بعضها البعض والتي لا يمكن الاستغناء عن أي واحدة منها، هذه المحاكمة وإجراءاتها الأكيد أنّها سترتب آثارا قانونية بحيث قد يبرأ أو يدان من خلالها المتهم بالجريمة المعلوماتية.

[1] أمر رقم 20-04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.
[2] المادة 441 مكرر7 والمادة 441 مكرر8 من أمر رقم 20-04، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري ج ر رقم 51، المؤرخة في 31 غشت 2020.

المبحث الأول: المرحلة الأولى من محاكمة المتهم بالجريمة المعلوماتية

قبل البدء بإجراء محاكمة المتهم بالجريمة المعلوماتية لابد في خطوة أولى النظر في الضمانات القانونية التي أعطاها القانون لهذا المتهم سواء كانت جوهرية أو عادية، وذلك من خلال تحديد المحكمة المختصة بالنظر في هذا النوع من الجرائم وعلانية الجلسة أولا وكذا افتراض قرينة البراءة في هذا المتهم وحقه في الدفاع وعدم تحميله عبء إثبات هذه الجريمة المعلوماتية، هذه الأخيرة التي تبقى مسألة إثباتها على عاتق كل من المدعي وسلطة الاتهام.

كل هذه العناصر سنأتي على تفصيلها وشرحها وإيضاحها من خلال المطالب والفروع الآتية.

المطلب الأول: الضمانات الجوهرية للمتهم المعلوماتي أمام المحكمة المختصة

لقد نصت مختلف التشريعات المقارنة منها التشريع الجزائري على ضمانات أساسية يجب أن يحوزها المتهم قبل وأثناء جلسة المحاكمة، هذه الضمانات تبعث في نفسيته الطمأنينة، هذا الشعور الذي يعزز من جودة وقوة الدفاع لهذا المتهم عن نفسه في مواجهة التهم الموجهة إليه خاصة إن كان متهما بجريمة يغلب عليها الطابع الفني الذي لا يلم به معظم المحققين كالجريمة المعلوماتية التي هي موضوع بحثنا ودراستنا.

الفرع الأول: المحكمة المختصة بالنظر في الجريمة المعلوماتية

إنّ جميع الإجراءات سواء الدولية أو الإقليمية المطبقة على الجرائم تعترف بشرط الاختصاص الإقليمي الذي يتطلب من الدول الأطراف ممارسة ولايتها القضائية على أي جريمة منصوص عليها وفقًا لقانونها الجزائي، والتي ترتكب في المنطقة الجغرافية للدولة بل وحتى الأفعال الإجرامية التي ترتكب على السفن والطائرات، فطبقا لهذا المبدأ أنّه ليس من الضروري أن يكون جميع أركان الجريمة المعلوماتية واقعة في الإقليم لكي تكون الولاية القضائية الإقليمية قابلة للتطبيق، من هنا أقر التقرير التفسيري لاتفاقية

الجرائم المعلوماتية لمجلس أوروبا بمبدأ الإقليمية[1] وأكده لأحد أطراف الولاية القضائية الإقليمية إذا ما هاجم شخص نظام كمبيوتر في منطقة ما ونظام الضحية موجود في منطقة أخرى.

فمتى كانت الجرائم المعلوماتية وأيا كان نوعها فإنّ المحاكم المحلية هي مختصة بالنظر فيها دون غيرها على شرط أن يكون القانون المحلي صالحا للتطبيق عليها، والاختصاص الإقليمي يتحدد كما هو معلوم بثلاثة ضوابط في مكان ارتكاب الجريمة أو مكان إقامة المتهم أو مكان ضبطه، هذه الأماكن الثلاثة للاختصاص الإقليمي متساوية لا تمييز بينها، والمحكمة التي ترفع إليها الدعوى تكون هي المختصة الأولى ولأنّ السلوك الإجرامي والنتيجة يمثلان شطري الفعل المادي للجريمة المعلوماتية فإنّ محاكم مكان السلوك أو مكان النتيجة تكون مختصة هي الأخرى بذلك[2].

فيتحدد الاختصاص المحلي للمحكمة الناظرة في الجرائم المعلوماتية في التشريع الجزائري طبقا لنص المادة 329 من ق إ ج[3] بمكان وقوع الجريمة المعلوماتية أو بمحل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر، بل وقد وسع المشرع من خلال المرسوم[4] التنفيذي رقم 06-348 في الاختصاص المحلي لأربعة محاكم تنظر في هذا النوع من الجرائم والذي كان بهدف وضع إطار إجرائي متماسك يمكنه التحقيق والفصل في هذا النوع من الجرائم بكل مهنية[5] ويجب على المحاكم أن تكون معززة بقضاة متخصصين في شتى المجالات كمجال المعلوماتية.

---

[1] Ebauche de Office des nation unies contre la drogue et le crime Vienne, Étude détaillée sur la Cybercriminalité, United nations, New York, usa, 2013, p191.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، مصر، 2006، ص51.

[3] القانون رقم 04-14، المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71، المؤرخة في 10 نوفمبر 2004.

[4] المرسوم التنفيذي 06-348، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر رقم 63 المؤرخة في 8 أكتوبر 2006.

[5] بن مكي نجاة، المرجع السابق، ص2016.

فهذا المشرع المصري مثلا قد أخرج جانبا كبيرا من الجرائم المعلوماتية من اختصاص المحاكم العادية أو كل الاختصاص بنظر الدعاوي الجزائية الناشئة عنها إلى المحاكم الاقتصادية، فقد جعل لهذه الأخيرة الولاية بنظر دعاوي المسؤولية الجزائية الناشئة عن مخالفة كل من قانون تنظيم الاتصالات وقانون تنظيم التوقيع الإلكتروني وحافظ على توزيع هذه الدعاوي نوعيا ومكانيا على الدوائر الابتدائية والاستئنافية داخل المحاكم الاقتصادية أين حافظ بذلك على مبدأ التقاضي على درجتين[1].

هذا وتعتبر الجرائم المعلوماتية من أبرز الجرائم التي تثير مشكلات الاختصاص على المستوى المحلي والدولي وذلك كله بسبب التداخل والترابط القوي بين شبكات المعلومات، فالفعل غير المشروع للجريمة المعلوماتية قد يقع في مكان معين وتنتج آثاره في مناطق أخرى داخل أو خارج الدولة فتنشأ بذلك مشكلتين أساسيتين، مشكلة البحث عن الأدلة الجزائية خارج دائرة الاختصاص التي سجلت فيها الشكوى وتم تحريك الدعوى العمومية فيها، وكذا مشكلة فحص البيانات في مراكز معلومات التي قد تكون تابعة لدول أخرى وما ينجر عنه من خضوع إجراءات التحقيق للقوانين الجزائية السارية في تلك الدول[2].

وبالرجوع إلى المشرع الجزائري نجده قد أحدث مؤخرا من خلال الأمر[3] رقم 20-04 المتمم والمعدل لق إ ج قطب جزائي ذا اختصاص وطني موسع ينظر حتى في الجرائم المعلوماتية[4]، ذلك أنّ هذه الأخيرة التي ليس لها حدود معينة خاصة في ظل الانفتاح على الأسواق العالمية وارتباطها دوليا، فقد بات التعامل التجاري بما يعرف بالتجارة الإلكترونية وانتشار أنظمة الدفع الإلكتروني المالية ينجر

---

[1] طارق عفيفي صادق أحمد، الجرائم الإلكترونية جرائم الهاتف المحمول، ط أولى، المركز القومي للإصدارات القانونية، القاهرة مصر 2015، ص235.

[2] محمد الأمين البشرى، المرجع السابق، ص127.

[3] أمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[4] مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، نشرة القضاة، العدد 66، مديرية الدراسات القانونية والوثائق، المديرية العامة للشؤون القضائية والقانونية، وزارة العدل، الجزائر، السنة القضائية 2011/2010 ص61.

عنها جرائم معلوماتية خطيرة كالتي في شكل تبييض الأموال وإخفاء مصادرها غير المشروعة[1]، وهو ما جعل المشرع من خلال إصداره لهذا الأمر محاولة إيجاد حل لهذا الخطر على غرار التدابير التي أوردها في المرسوم التنفيذي[2] 06-348 والقانون رقم 09-04 السابق الذكر.

بحيث يعتبر المرسوم التنفيذي رقم 06-348 ترجمة لأحكام المواد 37 و40 و329 من ق إ ج الجزائري، هذا المرسوم مدد الاختصاص المحلي لأربع محاكم إلى دوائر اختصاص محاكم أخرى مست كامل الإقليم المحلي الجزائري شرقا وغربا، وسطا وجنوبا في جرائم حددت على سبيل الحصر[3] منها الجرائم المعلوماتية خاصة في صورة جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

بل ومن خلال صدور الأمر السابق الذكر المتمثل في الأمر رقم 20-04، نلاحظ أنّ المشرع وعلى مستوى محكمة مقر مجلس الجزائر قد أحدث قطبا جزائيا وطنيا متخصص في متابعة قضايا التي لها علاقة بالجريمة الاقتصادية والمالية وقضايا الجرائم المرتبطة بها كالتي في صور الجرائم المعلوماتية موضوع هذه الدراسة، بل وحتى الجرائم الاقتصادية والمالية الأكثر تعقيدا[4]، هذا القانون الأخير أعطى لهذا القطب السالف الذكر اختصاصا موسعا يشمل كامل الإقليم الوطني الجزائري تنظر من خلاله لبعض الجرائم المعلوماتية المرتبطة بالجرائم الاقتصادية والمالية، والتي قد ترتكب في أية نقطة من الإقليم الجزائري[5].

---

[1] زيبحة زيدان، المرجع السابق، ص175.

[2] المرسوم التنفيذي 06-348، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر رقم 63 المؤرخة في 8 أكتوبر 2006.

[3] المواد 1 و2 و3 و4 من المرسوم التنفيذي رقم 06-348، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر رقم 63 المؤرخة في 8 أكتوبر 2006.

[4] طبقا لنص المادة 211 مكرر3 من الأمر رقم 20-04 يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020 فإنّه يقصد بالجريمة الاقتصادية والمالية الأكثر تعقيدا تلك : " الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة الأضرار المترتبة عليها أو لصبغتها المنظمة أو العابرة للحدود الوطنية أو لاستعمال تكنولوجيات الإعلام والاتصال في ارتكابها، تتطلب اللجوء إلى وسائل تحرّ خاصة أو خبرة فنية متخصصة أو تعاون قضائي دولي ".

[5] المادتين 211 مكرر1 و211 مكرر2 من الأمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

هذا وخروجا عن هذه المبادئ العامة للاختصاص المحلي المتطرق إليها سابقا وبعدما كان الأصل أنّ المحاكم الجزائرية لها إقليم يشمل إقليم الدولة وفقط، أصبحت المحاكم الجزائية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، وذلك على شرط ارتكابها من طرف أجنبي وشرط استهدافها لمؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[1].

الفرع الثاني: مشاكل الاختصاص القضائي المتعلقة بالجرائم المعلوماتية

تعد مسألة الاختصاص القضائي المتعلقة بالجرائم المعلوماتية أحد العقبات التي واجهت الفقه الإجرائي وأحد المشاكل المعاصرة التي فرضها العالم الافتراضي، ذلك أنّ هذه الجريمة لا تعرف حدودا جغرافية حتى الإنترنيت ليست حكرا أو خاضعة لسيطرة دولة معينة، الأمر الذي يفسر تعدد القوانين الجزائية التي يمكن أن تحكم الجرائم المعلوماتية، ولعل الاتجاه الغالب لحل هذه المشكلة كان من خلال تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي الدولي[2] والمحلي في الجرائم التقليدية.

أولا: إشكالية الاختصاص المحلي في الجرائم الواقعة خارج الإقليم الوطني

تولي القوانين الوطنية الجزائية للسلطة القضائية صلاحية النظر في الجرائم من حيث النطاق الإقليمي أو النوعي خاصة في الجرائم الهامة والخطرة التي ترتكب من قبل مواطنيها أو التي تقع على مواطنيها خارج نطاق إقليمها، وكذلك الأمر بالنسبة للجرائم التي تمس بهيبتها أو بعملتها الوطنية وهو ما يطرح بعض التساؤلات عن المعيار الذي يجب اعتماده فيما يخص الجرائم المعلوماتية، خاصة وأنّها ذات طبيعة

[1] المادة 15 من قانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[2] محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنيت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011 ص198.

متعدية للحدود الوطنية كما أن الفضاء الإلكتروني الذي ترتكب فيه أو ترتكب بواسطته معظمها ليس لها جنسية محددة ولا تخضع لنفوذ دولة دون غيرها أو جهة معينة ما[1].

فلا تخلو العولمة من التأثير على تطبيق سيادة القانون الجنائي ذلك أنّها تعطل بشكل خاص على مبدأ الإقليمية للقانون الجنائي، الذي يميل إلى المفهوم التقليدي للقانون الجنائي الذي يعبر عن سيادة الدول، وهو ما يؤدي إلى التساؤل عما إذا يستطيع القانون الجزائي إيجاد الآلية المناسبة ضد تطور الجرائم الدولية خاصة تلك المتعلقة بالجرائم المعلوماتية، خاصة وأنّ الدول تشعر بالغيرة على سيادتها أكثر من أي مكان آخر[2] حتى وإن كانت تدرك حقًا حاجتها إلى التعاون لإحباط الجرائم المعلوماتية.

فكأصل عام تخضع قواعد القانون الجزائي في تطبيقها من حيث المكان لمبدأ الإقليمية، ذلك أن معظم الجرائم عناصر الركن المادي فيها تكتمل في مكان واحد فيتحدد القانون الواجب التطبيق وبالتبعية تتحدد المحكمة المختصة بنظر الدعوى، لكن أحيانا بعض الجرائم ما يتعدى مداها حدود الدولة الواحدة وقد يتجزأ الركن المادي فيها ويتوزع على أكثر من مكان كما هو الحال بالنسبة للجرائم المعلوماتية التي يمكن أن يقع سلوكها في مكان وتتحقق النتيجة الإجرامية فيها في مكان آخر قد يكون في نطاق إقليم دولة أخرى، على هذا الأساس يثور التساؤل حول المحكمة المختصة إقليميا للنظر في هذه الجريمة هل بمكان وقوع السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة[3].

فهذا القانون الأمريكي مثلا يمتد نطاق تطبيقه إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية، وهذا القانون الإنجليزي أجاز الاختصاص في النظر في الدعاوي الناشئة عن إساءة استخدام الحاسب الآلي متى كان هناك ارتباط بين الواقعة المرتكبة وبريطانيا، بل

---

[1] عادل مشموشي، جرائم المعلوماتية وتحديات مسارحها الافتراضية أدواتها الإلكترونية أساليبها التقنية مقتضياتها التشريعية، ط أولى المؤسسة الحديثة للكتاب، بيروت، لبنان، 2019، ص584.

[2] Romain Boos, La lutte contre la cybercriminalité au regard de l'action des États Doctorat de droit privé et sciences criminelles, faculté de droit sciences économique gestion, Université de Lorraine Nancy, France, 2017, p181.

[3] ناني لحسن، المرجع السابق، ص59.

لا نكاد نرى ممن وسع هذا النطاق أكثر من المشرع الفرنسي الذي جعل من اختصاص قضائه بالجرائم المعلوماتية يمتد إلى الخارج متى كانت ظروف الواقعة الإجرامية تهدد مصالح فرنسا[1].

وبالرجوع إلى التشريع الجزائري فقد نص المشرع صراحة على هذا الأمر وفصل فيه من خلال القانون رقم 09-04 السابق الذكر، أين أعطى للمحاكم الجزائية اختصاص النظر في الجرائم المعلوماتية المرتكبة خارج الإقليم الوطني الجزائري وذلك فقط عندما يكون مرتكبها أجنبي وتستهدف اعتداءاته المعلوماتية مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[2] فالملاحظ بأنّ المشرع الجزائري في هذا الأمر ضيق كثيرا من نطاق الاختصاص سواء نوعيا أو مكانيا لهذه المحاكم على عكس التشريعات المقارنة السابقة الذكر.

ثانيا: إشكالية الإجراءات أمام الأقطاب القضائية المتخصصة

بالرجوع لنصوص المواد 40 مكرر1 و40 مكرر2 و40 مكرر2 من ق إ ج[3]الجزائري الملاحظ أنّها أبقت على العلاقة التقليدية المنظمة للعلاقة التدريجية بين مختلف السلطات القضائية المختصة في مجال التحري والتحقيق عن الجرائم المعلوماتية وهو الأمر الذي يثير التعقيدات الآتية؛

1- بقاء كل من النائب العام لدى الجهة القضائية المختصة إقليميا والنائب العام لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع بعيدان عن مجال التحقيق الابتدائي وعن تطوراته وهو ما يؤثر من فعالية حقهما في المطالبة بالملف في الوقت المناسب[4].

---

[1] ناني لحسن، المرجع السابق، ص60.

[2] المادة 15 من قانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

[3] الأمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[4] ناني لحسن، المرجع السابق، ص61.

2- إنّ مطالبة وكيل الجمهورية التابع للجهة القضائية ذات الاختصاص الموسع وبعد أخذ رأي النائب العام لدى هذه الجهة القضائية لملف الإجراءات فورا[1]، يجعل من دور النائب العام لدى الجهة القضائية العادية يكاد ينعدم في العلاقة الجديدة التي تنشأ بين وكيل الجمهورية لدى الجهة القضائية العادية ووكيل لجمهورية لدى الجهة القضائية المتخصصة، فحتى وإن كانت هذه التدابير الجديدة لم تغير من طبيعة العلاقة الموجودة بين وكيل الجمهورية والنيابة العامة إلاّ أنّه يجب احترام مبدأ التدرج.

3- حالة ما إذا كان وكيل الجمهورية التابع للجهة القضائية المتخصصة ووكيل الجمهورية التابع للجهة القضائية العادية ينتميان إلى مجلسين مختلفين، قد يؤدي ذلك إلى إثارة تنازع بين النائب العام لدى الجهة القضائية المتخصصة والنائب العام لدى الجهة القضائية العادية مما يستلزم تدخل وزارة العدل.

4- في حالة فتح تحقيق قضائي[2] هنا يثور الإشكال لدى قاضي التحقيق التابع للجهة القضائية ذات الاختصاص الموسع، حول طبيعة الإخطار من حيث مدى ضرورة طلب افتتاحي جديد ومن حيث صاحب الممضي على هذا الطلب ومن حيث محتوى هذا الطلب لاسيما في حالة تقدم قاضي التحقيق الأول في الإجراءات.

5- مدى إلزامية قاضي التحقيق الجديد بالتحقيق فلا وضوح لإمكانية رفضه للتحقيق أو التصريح بعدم الاختصاص، فقد يرى هذا القاضي أن الطلب جاء سابقا لأوانه بسبب عدم اتضاح معالم الجريمة المعلوماتية بعد[3].

---

[1] المادة 40 مكرر2 من الأمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[2] الفقرة 2 من المادة 40 مكرر3 من الأمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[3] ناني لحسن، المرجع السابق، ص63.

هذه الإشكالات في الحالة التي تكون فيها الجرائم المعلوماتية تأخذ وصف الجنحة فما بالك في الحالة التي تأخذ هذه الجريمة وصف الجناية أين قد يتغير اسمها مثلا من جريمة معلوماتية إلى جريمة اقتصادية ومالية الأكثر تعقيدا[1]، هذه الأخيرة تدخل في اختصاص القطب الجزائي الوطني المتخصص فقط والموجود بمحكمة مقر مجلس قضاء الجزائر العاصمة أين يمارس فيه كل من رئيس القطب وكذا وكيل الجمهورية وقاضي التحقيق التابعين له صلاحياتهم في كامل الإقليم لوطني.

الفرع الثالث: افتراض قرينة البراءة في المتهم المعلوماتي

هناك ضمانات عدة يفرضها أصل البراءة للمتهم المعلوماتي ذلك أنّه غير مكلف قانونا بإثبات براءته، هذا المبدأ بدوره يرتب ضمانات وحقوقا إجرائية يلزم إتباعها في المحاكمة وحين الاستجواب ذلك أن قرينة البراءة تقتضي ألاّ يدان أحدا إلاّ بعد إثبات مسؤوليته عن الأفعال المسندة إليه إثباتا يقينيا لا شبهة فيه، كما تقتضي أن لا يشكك أحد في قوتها الدستورية فيجب أن يكون هناك نظاما للأدلة الجزائية يقوم على احترام الطبيعة والكرامة الإنسانية للمتهم بصفة عامة والمتهم المعلوماتي بصفة خاصة بل ويجب الابتعاد عن استخدام الوسائل التي من شأنها أن تؤثر على إرادة المتهم أو تلغيها[2].

إنّ قرينة البراءة تعتبر من بين أهم المبادئ التي نصت عليها الكثير من الدساتير كان من بينها الدستور الجزائري[3]والذي اعتبر أن المتهم بريء حتى تثبت جهة قضائية مختصة إدانته[4]، بل وأكدت عليه سابقا المواثيق الدولية كالإعلان العالمي لحقوق الإنسان الصادر عام 1948 والاتفاقية الأوروبية لحماية حقوق الإنسان الأساسية الصادر عام 1950 وكذا الاتفاقية الدولية للحقوق المدنية والسياسية لعام 1966، لذلك بات من الطبيعي وفي جميع مراحل الدعوى كمرحلة محاكمة المتهم المعلوماتي التي نحن

---

[1] الفقرة 02 من المادة 211 مكرر3 من الأمر رقم 20-04، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

[2] صابر غلاب، أصول الإثبات والمحاكمات الجنائية، د ط، دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2017 ص117.

[3] الدستور الجزائري 2020، الصادر وفق مرسوم رئاسي رقم 20-442، الصادر بتاريخ 30 ديسمبر 2020، ج ر رقم 82 المؤرخة في 30 ديسمبر 2020.

[4] المادة 41 من الدستور الجزائري 2020، ج ر رقم 82، المؤرخة في 30 ديسمبر 2020.

بصدد دراستها الآن أن يتفرع عن ذلك وأثناء استجوابه بأن يعامل على أنّه غير مذنب حتى يُثبت عكس ذلك ولعل أحد أبرز صور ذلك هو حق المتهم في الصمت وعدم جواز إجباره على الخروج عن ذلك الصمت[1].

فعلى الرغم من التطور الهائل الذي يشهده الدليل العلمي في مجال الإثبات الجنائي والذي يجعله مقبولا لدى المحكمة إلاّ أن هناك في الدعوى ما يجعل القاضي يشك في شخص آخر يكون قد ارتكب الجريمة، الأمر الذي يدعو القاضي أن يقتنع اقتناعا يقينيا بارتكاب المتهم للجريمة وإلاّ وجب عليه أن يقضي ببراءة المتهم إعمالا لمبدأ الشك يفسر في كل الأحوال لصالح المتهم، فالمعروف قانونا ومن أجل سلامة الحكم القاضي بالبراءة على المتهم يكفي أن يشكك قاضي الموضوع في مرحلة إسناد التهمة إلى المتهم[2].

أمّا إذا نظرنا إلى محكمة النقض الفرنسية فنجد بأنّها تأخذ بهذا المبدأ في نطاق ضيق، ومبرر ذلك أنّ الشك في الأدلة لا يكفي وحده لتبرئة المتهم بل يجب أن يستند هذا الشك على أدلة قاطعة، على عكس محكمة النقض المصرية التي أخذت بمبدأ قرينة البراءة على نطاق واسع وأكدت عليه من خلال أحد أحكامها وقالت بأنّ الشرعية الإجرائية سواء ما اتصل بحياد المحقق أو بكفالة الحرية الشخصية والكرامة البشرية للمتهم وكذا مراعاة حقوق الدفاع تعتبر ثوابت قانونية أعلاها الدستور والقانون وحرص على حمايتها القضاء[3]؛ وذلك ليس فقط حماية لمصلحة المتهم بل أنّها تستهدف في المقام الأول مصلحة أهم وهي حماية قرينة البراءة مع تعزيز ثقة الناس بعدالة القضاء.

---

[1] عمار عباس الحسيني، ضياء عبد الله الجابر، حق المتهم في الصمت أثناء الاستجواب، مقال ضمن كتاب أبحاث في القانون العام د ط، منشورات زين الحقوقية، بيروت، لبنان، 2013، ص97.

[2] بن لاغة عقيلة، حجية أدلة الإثبات الجنائية الحديثة، عمل مقدم لنيل شهادة الماجستير، تخصص قانون جنائي وعلوم جنائية كلية الحقوق، جامعة الجزائر1، الجزائر، السنة الجامعية 2012/2011، ص70.

[3] ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2012 ص169.

وبالرجوع إلى التشريع الجزائري نجد أنّ المشرع أنّه نص على هذا المبدأ وأكد عليه ضمن مختلف دساتيره خاصة في الدستور الأخير[1] من خلال المادة[2] **41**، بل نص على أحد تطبيقاته أين فسر الشك في كل الأحوال لصالح المتهم ضمن ق إ ج[3]، إلاّ أنه لم يأتي على كيفية تطبيقه تاركا المجال لقضاء المحكمة العليا التي استقرت في أحد تطبيقاتها على أنّ: " القرارات القاضية بالبراءة مثلها مثل القرارات الصادرة بالإدانة يجب أن تعلل تعليلا كافيا حتى تتمكن المحكمة العليا من مراقبة صحة تطبيق القانون فالقرار الذي يكتفي بالحكم بالبراءة بقوله أنّه يوجد في الدعوى شك لصالح المتهم يعتبر ناقص التسبيب ويستوجب النقض "[4].

المطلب الثاني: الضمانات العادية للمتهم المعلوماتي أمام المحكمة المختصة

هناك ضمانات أخرى يحوزها المتهم بالجريمة المعلوماتية اعتبرناها في رأينا بأنّها عادية لكون بعضها قد ترد عليها استثناءات قانونية تعدم وجودها كحق اختيار المحامي وكذا علانية الجلسة ولكون بعضها الآخر يفرضها المنطق القانوني والتي تأتي آليا أثناء مجريات جلسة المحاكمة كتحمل عبء الإثبات من طرف سلطة التحقيق والاتهام وكذا رقابة قاضي الحكم على الأدلة المادية المستنبطة من مرحلتي التحري والتحقيق الابتدائي.

---

[1] الدستور الجزائري 2020، الصادر وفق مرسوم رئاسي رقم 20-442، الصادر بتاريخ 30 ديسمبر 2020، ج ر رقم 82 المؤرخة في 30 ديسمبر 2020.

[2] تنص المادة 41 من الدستور الجزائري 2020، ج ر رقم 82 المؤرخة في 30 ديسمبر 2020بأنّه: "كل شخص يُعتبر بريئا حتّى تثبِت جهة قضائيّة نظاميّة إدانته، في إطار محاكمة عادلة ".

[3] المادة 01 من القانون رقم 17-07، المعدل والمتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20، المؤرخة في 29 مارس 2017.

[4] مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الأول، د ط، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2013 ص617.

الفرع الأول: حق المتهم المعلوماتي في الدفاع والعلانية أثناء جلسة المحاكمة

يعتبر حق الدفاع وكذا العلانية في جلسة المحاكمة من بين أكثر الضمانات المعروفة لدى الجمهور هاذين الحقين أقرتهما مختلف التشريعات المقارنة وكذا التشريع الجزائري الذي نظمهما ووضعهما في قالبهما القانوني وهما بالتفصيل على التوالي من خلال الآتي.

أولا: حق المتهم المعلوماتي في الدفاع واختار المحامي

يعتبر حق الدفاع في المواد الجزائية من بين أكثر الحقوق الدستورية صلة بمبدأ أصل البراءة وأكثرها ارتباطا بالحق في المساواة أمام القضاء الجزائي، بل وضمانا أساسيا للعدالة الجزائية التي لا يتصور إحقاقها مع هدر حق الدفاع، من هذا المنطلق يتبين للناظر والمتأمل في فكرة حق الدفاع في المادة الجزائية أنّ هذا الحق لا يعبر عن مصلحة خاصة بل أنّه يتعدى ذلك ليعبر عن مصلحة عامة جماعية متعلقة بالنظام العام في المجتمع الإنساني، فإظهار متانة مقومات العدالة وتحقيق حماية للمراكز الإجرائية في الدعوى العمومية وضمان إقامة العدالة الفعلية والحقيقية[1] لا تقوم إلاّ بوجود مثل هذا الحق وضمان استيفائه وتوفير حماية كاملة له.

لهذا يمنح القانون للخصوم الحق في استصحاب وكلائهم أثناء التحقيق نظرا للدور الرئيسي الذي صار المدافع يلعبه في الإجراءات الجزائية خاصة مدافع المتهم، فحضور المحامي لإجراءات التحقيق الابتدائية والنهائية يمثل نوعا من الرقابة على المحقق بما يحول بينه وبين التورط في مخالفة القانون كما يمد المتهم بشعور الطمأنينة التي تتيح له أن يحسن عرض وجهة نظره[2] وفي هذا مصلحة للتحقيق ككل فحق المتهم المعلوماتي في الاستعانة بمحامي يعتبر من بين أهم الضمانات، ذلك أنّ حضور هذا الأخير مع موكله أثناء التحقيق فيه ضمان لسلامة الإجراءات.

---

[1] حاليمية سفيان، بوالقمح يوسف، حصانة الدفاع في املواد الجزائية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 10، كلية الحقوق والعلوم السياسية، جامة محمد بوضياف المسيلة، الجزائر، جوان 2018، ص378.

[2] أحمد سعد محمد الحسيني، المرجع السابق، ص124.

هذا وتبعا للأهمية التي يحتلها الدفاع في العملية الإجرائية، كان من الضروري تعزيزه بالوسائل القانونية التي تمكن المتهم ومحاميه من تقديم ما لديهما من أدلة نفي لرد أدلة الاتهام ودحضها، هذه الوسائل تحقق مبدأ التكافؤ وإقامة التوازن بين الأطراف لكل من النيابة العامة والأطراف الأخرى للدعوى الجزائية، ذلك أنّ كل طرف في المحاكمة ينبغي أن يكون قادرا على عرض قضيته، لأنّه بمجرد السير في الدعوى العمومية ينشأ إخلال غير معقول في التوازن بين الأطراف[1] قد يغيب من تكافؤ وسائل الدفاع ولا يمكن عندها وصف المحاكمة بالعادلة.

ثانيا: حق المتهم المعلوماتي في علانية جلسة المحاكمة

إنّ مناط العلانية يكمن في تمكين الجمهور من حضور جلسات المحاكمة وذلك من خلال الإعلان عن موعدها ومكان إجرائها وتوفير التسهيلات اللازمة لذلك، فلا يكفي مجرد حضور الخصوم ومحاميهم للقول بالعلانية فلابد وأن يسمح للجمهور بحضورها[2]، هذا وتظهر أهمية هذا الإجراء من خلال تحقق مصلحة العدالة ومصلحة المجتمع وتحقق مصلحة المتقاضي، كما أنّ إتاحة الفرصة أمام الجمهور لحضور الجلسات يبدد الشكوك ويولد الاطمئنان لديهم اتجاه حسن سير العدالة وينشر الوعي لديهم مع تحقيق ما يسمى في علم العقاب بالردع العام.

إنّ علانية جلسة المحاكمة كأصل عام مبدأ كرسته مختلف التشريعات المقارنة وكذا التشريع الجزائري خاصة في التعديل الدستوري 2020 الأخير من خلال نص المادة 169 منه[3]، هذا المبدأ يضمن رقابة شعبية على عمل القضاة ويدعم حيادهم عن طريق شعورهم بهذه الرقابة مما يبعد عن أحكامهم ما قد يحوم حولها من شكوك، كما يعتبر ضمانة للمتهم المعلوماتي من خلال حقه في الوصول للحقيقة

---

[1] حاليمية سفيان، بوالقمح يوسف، المرجع السابق، ص 380.

[2] زينب بوسعيد، علانية المحاكمة الجزائية بين القاعدة والاستثناء، مجلة الحقيقة، المجلد 14، العدد 3، جامعة أحمد دراية – أدرار الجزائر، سبتمبر 2015، ص250.

[3] تنص الفقرة 2 من المادة 169 من الدستور الجزائري 2020، ج ر رقم 82 المؤرخة في 30 ديسمبر 2020 : " ينطق بالأحكام القضائية في جلسات علنية ".

بإجراءات سليمة وتحقيق محاكمة عادلة[1]، لكن يجب المعرفة بأنّ تفعيل هذا المبدأ ليس على إطلاقه فلا يجب الأخذ به في الحالة التي يكون فيها هذا المتهم المعلوماتي قاصرا[2] وفي الحالة التي يكون في علانية الجلسة خطرا على النظام العام أو الآداب[3].

الفرع الثاني: عبء إثبات الجرائم المعلوماتية كضمانة للمتهم المعلوماتي

تطرقنا سابقا بالقول أنّ الأصل في كل إنسان البراءة ويكون ذلك سواء البراءة من الجريمة أو التحرر من الالتزام لذلك من يدعي خلاف هذا الأصل فعليه أن يثبت ادعاءه من خلال إقامة الدليل لدى السلطات المختصة بالإجراءات الجزائية، فلا يقتصر إقامته أمام قاضي الموضوع فقط بل يتسع لإقامته أمام سلطة التحقيق أو سلطات الاستدلال[4]، عبء الإثبات هذا كان في العصور القديمة يقع على عاتق المتهم أين كان يخضع لمجموعة من الإجراءات الغيبية القاسية لإظهار براءته حتى مع بداية النصف الثاني من العصور الوسطى[5] تحققت ثورة حقيقية في أوروبا في مجال الإثبات الجزائي أصبح فيها عبء الإثبات يقع على عاتق سلطة الاتهام[6].

إذن من هذا المنطلق عبء إثبات العناصر المكونة للجرائم المعلوماتية يقع على عاتق سلطة الاتهام خاصة إذا ما رفعت الدعوى من طرفها، كما يجب عليها أن تهتم بإثبات براءة البريء كما تهتم بإدانة المتهم المعلوماتي[7]، لكن عموما يبقى عبئ إثبات الجرائم المعلوماتية على كل من المدعي وسلطة الاتهام

---

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، المرجع السابق، ص26.

[2] تنص الفقرة 1 من المادة 82 من قانون رقم 15-12، يتعلق بح ط، ج ر رقم 39 المؤرخة في 19 يوليو 2015: بأنّه:" تتم المرافعات أمام قسم الأحداث في جلسة سرية ".

[3] تنص الفقرة 1 من المادة 285 من أمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966 بأنّه : " المرافعات علنية ما لم يكن في علانيتها خطر على النظام العام والآداب في هذه الحالة تصدر المحكمة حكمها القاضي بعد الجلسة سرية ..... وإذا تقررت سرية الجلسة تعين صدور الحكم في الموضوع في جلسة علنية " .

[4] طاهر محمود أبو القاسم، المرجع السابق، ص132.

[5] النصف الثاني من العصور الوسطى يبدأ حسابه من القرن الثاني عشر حتى القرن الرابع عشر.

[6] لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي، ط أولى، مركز الدراسات العربية، الجيزة، مصر، 2018 ص43.

[7] طاهر محمود أبو القاسم، المرجع السابق، ص133.

وفي حالة عجزهما عن إثبات الادعاء وإتيان الدليل على ذلك أو عدم كفاية هذا الأخير فإنّه يجب تبرئة ساحة المتهم.

بل ويستطيع هذا المتهم أن يمارس في دعواه دورا إيجابيا، ذلك أنّ القانون اعترف له بالوسائل التي تساعده على إعداد وتنظيم وسائل دفاعه وكذا البحث عن شهود نفي وتكليفهم بالحضور للإدلاء بشهادتهم في صالحه بل وحقه في مناقشة الأدلة القائمة ضده وتفنيدها[1]، هذا ويبقى عبء إثبات الجرائم المعلوماتية أحد أهم عناصر قرينة البراءة والذي يمشي بالتوازي مع عنصر كنت قد وضحته في فرع سابق والمتمثل في الشك الذي يجب أن يفسر لمصلحة هذا المتهم المعلوماتي.

الفرع الثالث: رقابة قاضي الحكم على الأدلة المستنبطة من المراحل السابقة للدعوى

كأصل عام فإنّ المشرع يتدخل في سلطة القاضي الجزائي من حيث تنظيم وسائل الحصول على الأدلة وكذا طريقة تقديمها إليه، هذا القاضي الذي بدوره يجب أن يقوم بالتحقق من مدى قانونية هذه الأدلة واستنادها إلى إجراءات صحيحة بل ويعمل من خلال سلطته التقديرية على تحديد وتقدير قوتها في الإثبات، كما أنّه هو من يقرر قبول الدليل من عدمه على شرط أن يكون استنتاجه للحقيقة وما كشف عنها من أدلة أخرى لا يخرج عن مقتضيات العقل والمنطق[2]، وإذا كان مبدأ حرية القاضي الجزائي في الاقتناع يتعلق بنطاق سلطته في تقدير وتقييم الدليل فعليه أن يختار وسائل الإثبات الملائمة لذلك.

هذا وتعتبر حرية قاضي الموضوع في تقدير الأدلة المعروضة عليه من المراحل السابقة في الدعوى العمومية نتيجة منطقية لمبدأ الاقتناع الشخصي، وهو غير ملزم بإصدار حكم بالإدانة أو بالبراءة لتوافر

[1] صابر غلاب، المرجع السابق، ص119.

[2] محمد عبد الرحمان عنانزه، القصد الجرمي في الجرائم الإلكترونية، ط أولى، دار الأيام للنشر والتوزيع، عمان، الأردن، 2017 ص229.

دليل معين طالما أنّه لم يقتنع به[1]، والدليل لا يكون مشروعا ومقبولا في عملية الإثبات إلاّ إذا كانت عملية البحث عنه أو الحصول عليه قد تمت بالطرق التي حددها القانون، وهذا ما أكدت عليه توصيات[2] المؤتمر الدولي الثاني عشر للجمعية الدولية لقانون العقوبات المنعقد من 16 إلى 22 سبتمبر 1979 في هامبورج بجمهورية ألمانيا الاتحادية.

فمهمة القاضي الجزائي أن يستقي قناعته في الحكم من خلال أدلة مشروعة، أمّا الأدلة التي تأتي وليدة لإجراءات غير قانونية، فيجب على قاضي الموضوع أن يطرحها ولا يجوز الاعتماد عليها لأنّه لا يجوز اقتضاء حق الدولة في العقاب من خلال ممارسة إجراءات غير قانونية[3]، حتى وإن كان الأصل فيه أنّه حر في أن يستمد قناعته من أي دليل يطمئن إليه فإنّه ترد على هذا الأصل بعض الضوابط يتعين على القاضي الالتزام بها وهو بصدد اختيار الأدلة التي يستمد منها اقتناعه فلا يستمد قناعته إلاّ من الأدلة التي تتوافر فيها الشروط أو الضوابط التي حددها القانون، والمتمثلة أساسا في مشروعية هذه الأدلة وأن تطرح هذه الأدلة في الجلسة وتحصل المناقشة فيها[4].

المبحث الثاني: المرحلة الثانية من محاكمة المتهم بالجريمة المعلوماتية

كلما تعمقنا في موضوع الجرائم المعلوماتية إلا ووجدناها ذات طبيعة خاصة ومتميزة حتى من خلال آثارها وكذا الأدلة التي تثيرها والتي في أغلبها ذات طبيعة إلكترونية، هذه الأدلة الإلكترونية جعلت من أمر التحقيق فيها ورقابة قاضي الموضوع عليها يزداد صعوبة من خلال هذه المرحلة الفاصلة في الدعوى العمومية، خاصة وأنّ هذا الدليل يثير عدة مشاكل سواء من الناحية الموضوعية وحتى من

---

[1] بلولهي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، ، عمل مقدم لنيل شهادة الماجستير في العلوم الجنائية كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر، 2011، ص40.

[2] كانت أحد توصياته هي: " أنّ قبول الدليل في الدعاوى الجزائية يجب أن يأخذ بعين الاعتبار كمال النظام القضائي وحقوق الدفاع ومصالح المجني عليه ومصالح المتهم".

[3] بن لاغة عقيلة، المرجع السابق، ص46.

[4] بلولهي مراد، المرجع السابق، ص103.

الناحية الإجرائية، بل وتتسع إجراءات الحصول عليه من إجراءات حديثة وحتى إجراءات تقليدية تطبق على جرائم عادية أخرى، هذا ما سيتم تفصيله في هذا المبحث من خلال المطالب والفروع الآتية.

المطلب الأول: الدليل الإلكتروني وحجيته أمام القاضي الجزائي في الجرائم المعلوماتية

لقد أثرت الثورة التكنولوجية على أنوع الجرائم التي صاحبتها وظهور أنماط مستحدثة من الجرائم والمتمثلة في الجرائم المعلوماتية، والتي أثرت بدورها على أدلة إثباتها أين أصبحت الأدلة التقليدية غير قادرة بمفردها على إثبات هذا النوع من الجرائم، هذه الأخيرة تحتاج إلى طرق تقنية تتناسب مع طبيعة هذه الجرائم بحيث يمكن فك رموزها وترجمة الشفرات والأرقام إلى كلمات وبيانات محسومة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعملية الخاصة[1]، هذه الأدلة يطلق عليها اسم الأدلة الإلكترونية.

الفرع الأول: طبيعة الدليل الإلكتروني المستخرج من الجرائم المعلوماتية

يعتبر الدليل الإلكتروني كما عرفه بعض الفقه بأنّه: " معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"[2]، وعرفه بعض الفقه كذلك بأنّه: " الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون"[3].

---

[1] أشرف على قوقزة، المرجع السابق، ص96.

[2] محمد الأمين البشرى، المرجع السابق، ص234.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دون طبعة، دار الكتب القانونية، مصر 2006، ص81.

ونظرا للطبيعة الخاصة التي تتمتع بها الجرائم المعلوماتية فهو يعتبر من أبرز أدلة إثباتها ذلك أنّه يتميز عن الدليل الجزائي التقليدي بعدة خصائص هي كالآتي؛

أولا: خصائص الدليل الإلكتروني في الجرائم المعلوماتية

1- الدليل الإلكتروني ذو طبيعة تقنية فنية

لا يتم إدراكه إلاّ بالاستعانة بالحاسب الآلي والأجهزة الإلكترونية من خلال استخدام برامج إلكترونية خاصة بذلك، هذه الخاصية تترتب عنها عدد من الإيجابيات والسلبيات، فمن بين الإيجابيات صعوبة التخلص من هذا الدليل[1] بخلاف الدليل التقليدي أمّا السلبيات فمن أبرزها أنّه يصعب الوصول إليه ولا يتم كشفه إلاّ من خلال الاستعانة بأشخاص يتوفر فيهم نوع من الثقافة والمعرفة التقنية[2] (الخبراء المعلوماتيين).

2- الدليل الإلكتروني ليس أقل مادية من الدليل المادي

فهو مستمدة من الأجهزة بالرغم من أنّه يعتبر من قبيل الأدلة الفنية والعلمية غير ملموسة.

3- الدليل الإلكتروني عبارة عن مجالات مغناطيسية أو كهربائية

وترجمته وإخراجه في شكل مادي ملموس لا يعتبر هو الدليل وإنّما هي عبارة عن عملية نقل لتلك المجالات من طبيعتها الإلكترونية إلى شكل يمكن الاستدلال بها على معلومة معينة.

4- إمكانية استخراج نسخ من الدليل الإلكتروني على عكس الدليل العادي

وهذه النسخ لها نفس القيمة العلمية والحجة الثبوتية، بل ويصعب التخلص من هذا الدليل مما يمكن استرجاعه بعد محوه وحتى إصلاحه بعد إتلافه وإظهاره بعد إخفائه.

---

[1] Eoghan casey, digital evidence and forensic science, computer and the internet computer crime, 1st ed Academic press, USA, UK, 2000, p8.

[2] طارق عفيفي صادق أحمد، المرجع السابق، ص 277.

5- الدليل الإلكتروني يتنقل من مكان لآخر عبر شبكات الاتصال

وقد يستغل في رصد وتحليل المعلومات عن الجاني بل ويمكن من خلاله تسجيل تحركات الأفراد وسلوكياتهم فهو يجعل من عمليتي البحث والتحقيق القضائي يجدان غايتيهما بسهولة مقارنة مع الدليل التقليدي[1].

ثانيا: ضوابط الاعتماد على الدليل الإلكتروني في الجرائم المعلوماتية

مهما كان نوع الدليل الإلكتروني وحتى يُعتمد عليه كدليل إثبات يجب أن تتوفر فيه مجموعة من الشروط الجوهرية والمتمثلة في؛

1- ضابط المشروعية

يجب أن يكون الدليل الإلكتروني نابعا من إجراءات مشروعة أيا كان مصدرها سواء من قاضي الموضوع بصورة مباشرة أو غير مباشرة أو من قبل المتهم واعترافه واستجوابه أو من قبل الغير بعد القيام بالقبض عليه أو تفتيشه أو ممارسة أي عمل من أعمال الخبرة الفنية.

2- صدوره عن إرادة حرة

يجب أن يكون الحصول على الدليل الإلكتروني دون اعتداء على إرادة المتهم أو إرادة الغير بحيث تكون طريقة إخراجه خالية من أي عيب يشوب تلك الإرادة[2].

ثالثا: أنواع الأدلة الإلكترونية المعتمد عليها في الجرائم المعلوماتية

لازالت قضايا الجرائم المعلوماتية في تزايد مستر خصوصا هذه الأيام وهو ما يحتم معه معرفة كيفية إثباتها وذلك في سبيل الحصول على دليل إلكتروني يُستند إليه في المحاكم المختصة، وعلى الرغم من صعوبة الأمر إلاّ أنّ الشركات ومؤسسات الدولة ومختلف المرافق العامة يجب أن يضعوا في الحسبان

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت، ط الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011، ص232.

[2] هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحسوبة، د ط، دار النهضة العربية، القاهرة، مصر 2009، ص258.

إمكانية تواجدهم كطرف في الدعوى العمومية وهم ملزمون بتزويد المحكمة بدليل إلكتروني لدعم حججهم أمام قاضي الموضوع[1]، هذا الدليل الذي هو في الأصل معد ليكون وسيلة للإثبات أو معد لغير لذلك.

1- أدلة أعدت لتكون وسيلة إثبات

صور هذا النوع من الأدلة من خلال الآتي؛

أ- السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

ب- السجلات التي يحفظ جزء منها بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة و تتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

2- أدلة لم تعد لتكون وسيلة إثبات

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنّها أثر يتركه الجاني دون أن يكون راغبا في وجوده ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميته أيضاً بالآثار المعلوماتية الرقمية[2]، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

هذا ويعتبر النوع الثاني من الأدلة الرقمية هو الأكثر أهمية من النوع الأول لأنّه لم يُعد أصلاً ليكون أثرا لمن صدر عنه، فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجرائم المعلوماتية ومرتكبيها أمّا النوع الأول من الأدلة الرقمية يتميز بسهولة الحصول عليه ذلك أنّه أُعد أصلاً حتى يكون دليلا على

---

[1] أحمد محمد عبد الباقي، الرجع السابق، ص260.

[2] خالد عياد الحلبي، المرجع السابق، ص234.

الوقائع التي يتضمنها، في حين يكون الحصول علي النوع الثاني من الأدلة بإتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، ولأنّ النوع الأول قد أعد كوسيلة إثبات لبعض الوقائع فإنّه عادة ما يُعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه، على عكس النوع الثاني حيث لم يعد ليحفظ ما يجعله عرضة للفقدان[1] لأسباب بسيطة.

الفرع الثاني: حجية الدليل الإلكتروني في الجرائم المعلوماتية أمام قاضي الحكم

كأصل عام فإنّ جوهر العملية الإثباتية يكون من خلال تحويل الواقعة المتنازع عليها إلى أمر مقبول، أي تحويل حالة الشك في الواقعة التي يراد إثباتها إلى حالة التيقن بحدوثها وذلك من خلال الوصول إلى اقتناع القاضي بحقيقة ذلك عن طريق ما يقدم في الدعوى من وسائل قادرة على ذلك[2] هذا ونظرا للطبيعة الخاصة التي يتميز بها الدليل الإلكتروني فإنّها تجعل من مسألة إثبات الجرائم المعلوماتية بهذا النوع من الأدلة أمام قاضي الموضوع صعبا للغاية، وهنا تبرز الأهمية في أن يُترك للقاضي الحرية في تأسيس حكمه على أدلة أخرى يرتاح فيها ضميره وفقا لقناعته الشخصية[3].

وكأصل عام فإنّ سلطة القاضي الجزائي في تقدير الدليل لا يمكن التوسع في شأنها، كما أنّ هذه السلطة تمتد لتشمل الأدلة العلمية، فقاضي الموضوع وبالرغم من ثقافته القانونية لا يستطيع إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، فضلا عن ذلك فإنّ هذا الأخير يتمتع من حيث قوته الثبوتية بقيمة قد تصل إلى حد اليقين، من هنا لا يمكن القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها الدليل الإلكتروني المتاح، لكن هذا لا يناقض بأنّ يكون هذا الدليل الأخير

---

[1] فلاك مراد، آليات الحصول عمى الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية، مجلة الفكر القانوني والسياسي، العدد 5 كلية الحقوق والعلوم السياسية، جامعة الأغواط، الجزائر، جوان 2019، ص208.

[2] هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص257.

[3] محمد عبد الرحمان عنانزه، المرجع السابق، ص228.

موضع شك في سلامته من العبث من ناحية وصحة الإجراءات التي اتبعت من أجل الحصول عليه من ناحية أخرى[1].

أولا: حجية الدليل الإلكتروني في نظام الإثبات الجنائي الحر

يسود هذا النظام الجانب الأكبر من التشريعات الإجرائية المقارنة خاصة تشريعات معظم دول أوروبا الغربية والدول العربية، بحيث يرتكز هذا النظام على حرية القاضي الجنائي في تكوين اقتناعه الشخصي وعدم التقيد في اقتناعه بدليل معين إلاّ إذا نص القانون على غير ذلك بل ويستطيع تكوين اقتناعه من أي دليل من الأدلة التي تقدم إليه في الدعوى طالما كان هذا الاقتناع غير مجافي للمنطق أو مخل بالأصول المسلم بها في الاستدلال القضائي ومسببا، ومن بين التشريعات التي أقرت باتخاذها لهذا النظام كل من التشريعين الفرنسي[2] والتشريع المصري[3].

هذا التشريع الأخير الذي أقر ضمنا بحجية الدليل الإلكتروني إذا توافرت فيه الشروط العامة الواجب توافرها في الدليل الجنائي، أمّا التشريع الآخر الفرنسي الذي جعل من الأدلة الإلكترونية ومخرجات الحاسب الآلي مقبولة في الإثبات الجنائي من حيث المبدأ، بل وأكد وقضى بقبول التسجيلات الممغنطة أمام القضاء الجنائي الفرنسي على شرط الحصول عليه بطريقة مشروعة وعلى نحو نزيه وكذلك مناقشتها وجاهةً من قبل الخصوم[4].

ثانيا: حجية الدليل الإلكتروني في نظام الإثبات الجنائي المقيد

إنّ حجية الدليل الإلكتروني في ظل هذا النظام تعتمد على تحديد أدلة الإثبات من قبل المشرع وليس تقديرها من قبل القاضي الذي يلعب دورا سلبيا فيها، بحيث إذا لم تكن هذه الأدلة متواجدة فلا يستطيع القاضي الحكم بالإدانة بصرف النظر عن اقتناعه الشخصي حتى ولو كان يميل إلى إدانة

---

[1] خالد عياد الحلبي، المرجع السابق، ص247.

[2] قانون الإجراءات الجنائية الفرنسي.

[3] قانون الإجراءات الجنائية المصري.

[4] محمد كمال شاهين، المرجع السابق، ص380.

المتهم ومن أبرز الأنظمة المتبعة لهذا النظام التشريع البريطاني الذي يعتمد على مبدأ تعاضد الأدلة في إثبات الجريمة، وهو الأمر الذي يزيد من صعوبة إثبات الجرائم المعلوماتية، هذه الأخيرة التي تستوجب إدخال تعديلات تتلاءم والطبيعة الخاصة لها.

وهو ما جرى خاصة في ظل الطفرة التكنولوجية الهائلة الحاصلة في مجال المعلوماتية وشبكة الإنترنيت، فقد لوحظت بعض التغييرات على حدة هذا النظام بحيث صار يقبل بمبدأ حرية القاضي في تقدير الأدلة والذي تأخذ به جل التشريعات القانونية، يبقى فقط الاختلاف في صياغته القانونية فالأنظمة اللاتينية مثلا تسميه بمبدأ الاقتناع القضائي على عكس الأنظمة الأنجلوسكسونية التي تطلق عليه اسم الإدانة بدون أي شك معقول أو الإدانة الخالية من أي شك[1].

ثالثا: حجية الدليل الإلكتروني في نظام الإثبات الجنائي المختلط

يعتبر نظام الإثبات الجنائي المختلط نظاما توفيقيا يجمع بين النظامين نظام الإثبات المقيد ونظام الإثبات الحر، ويسود هذا النظام في العديد من التشريعات التي تأخذ بمجملها بمبادئ ونظام الإثبات الحر، وعلى سبيل الاستثناء وفي جرائم محددة تأخذ بنظام الإثبات المقيد، هذا وقد اعتبر البعض أن نظام الإثبات المختلط جاء نتيجة للتطور الذي وقع على مفهوم الإثبات الحر ونظرا لطبيعة بعض الاستثناءات التي وردت عليه[2]، وعليه فإنّ الدليل الإلكتروني الذي تثبت به الجرائم المعلوماتية يبقى الاعتداد به مرهونا أولا بمدى نص التشريع عليه من عدمه وثانيا مدى إلزامية هذا التشريع لقاضي الموضوع على الأخذ به.

هذا وبالرجوع إلى التشريع الجزائري يلاحظ تبنيه لنظام الإثبات الحر في مجال الإثبات الجنائي، لأنّه فتح باب الحرية في وجه تقديم الأدلة وتركها لمعيار القناعة الشخصية لقاضي الموضوع، وهو أمر

---

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، المرجع السابق، ص407.

[2] آمال عبد الرحمن يوسف حسن، الأدلة العلمية الحديثة ودورها في الإثبات الجنائي، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، الموسم الجامعي 2012/2011، ص21.

إيجابي من حيث أنّه يعزز من مبدأ إثبات قرنية البراءة ومجال ممارسة حقوق الدفاع الفردية، أمّا على الجانب الآخر السلبي فهذا الإطلاق بدون تحديد وتخصيص يعد قصورا تشريعا واضحا، ذلك أنّه لا وجود في هذا التشريع ما يدل على أنّ الدليل الإلكتروني هو دليل من نوع خاص شأنه شأن الجرائم المعلوماتية.

فغياب أدنى نص قانوني في هذا الشأن من نتائجه أن تثار إشكالات متعلقة بطبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنيات المعلوماتية دحض هذا الدليل وعدم الإعتداد به ولو كان حائزا على القوة الثبوتية وتتوفر فيه كافة شروط الصحة وكذلك العكس صحيح[1]، فيظل الدليل الإلكتروني عموما خاضعا لضوابط المشروعية والقانونية المحددة لقبول الأدلة، فيتم استخلاصه أو مراجعته بمعرفة مختص لديه معرفة تقنية خاصة (الخبير)، هذا مع مراعاة إمكانية العبث بهذا النوع من الأدلة كما في حالة اعتراض المراسلات والتقاط الصور وتسجيل الأصوات ومراعاة ضرورة الحقوق الثابتة التي يتمتع بها المتهم، فالأصل في الإثبات الجزائي قرينة البراءة[2].

الفرع الثالث: المشكلات المتعلقة بالدليل الإلكتروني في الجرائم المعلوماتية

كنا قد تطرقنا في فروع سابقة عن طبيعة الدليل الإلكتروني من حيث أنواعه وأشكاله، هذا الدليل بالرغم من أنّ قاضي الموضوع بإمكانه أن يتطرق إليه في أي فترة من فترات المحاكمة إلاّ أنّه قد تعترضه بعض العقبات والمشكلات المتعلقة بهذا النوع من الأدلة نفسه وحتى مشكلات متعلقة بإجراءات وطرق الحصول عليه وذلك ما سيتم شرحه وفق ما هو آت؛

أولا: المشكلات الموضوعية للدليل الإلكتروني

تتمثل مجمل هذه المشكلات الموضوعية في الدليل الإلكتروني نفسه، هذا الأخير الذي قد يُغيب أصلا في بعض الجرائم المعلوماتية عن مسرح الجريمة، كما قد يسهل إخفاؤه أو إعاقة الوصول إليه وحتى

---

[1] ربيعي حسين، المرجع السابق، ص278.

[2] طارق عفيفي صادق أحمد، المرجع السابق، ص288.

أنّه قد يصعب فهمه في حالة الوصول إليه من قبل المحققين، ولعل أغلب هذه المشاكل تبرز من خلال الاعتداء على الجوانب المعنوية المتعلقة بالمعالجة الآلية للمعطيات والتي يصعب معها إقامة والوصول إلى الدليل الإلكتروني، وذلك كله بسبب الطبيعة المعنوية المعقدة للمحل المعلوماتي الذي وقعت عليه هذه الجريمة المعلوماتية[1].

فضلا عن ذلك فإنّ هذا الدليل تعترضه عقبة أخرى تكمن في أنّ المجرمين المعلوماتيين يجتهدون في إخفاء هوياتهم وذلك للحيلولة دون تعقبهم وكشف أمرهم وحتى تظل أنشطتهم مجهولة وبمنأى عن علم السلطات المختصة بمكافحة الجرائم المعلوماتية[2]، لذلك ليس من الغريب أن يكون هناك غيابا تاما للدليل الإلكتروني في بعض الجرائم المعلوماتية كجرائم السرقة أو الاختلاس أو التزوير أو الإتلاف داخل منظومة معلوماتية، ذلك أنّ هذه الجرائم ترتكب بالاعتماد على موضوع العملية الإلكترونية المشفرة وذات بيانات الدخول السرية وكذا النبضات، الأمر الذي يصعب معها اقتفاء آثار مرئية حول هذه الاعتداءات[3].

هؤلاء المجرمين المحترفين والنوابغ في مجال المعلوماتية يسهل عليم إخفاء الدليل الإلكتروني لاعتداءاتهم المعلوماتية غير المشروعة، بل وقد تكون بعض اعتداءاتهم حكرا عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار، بل ومما يزيد من خطورة إخفاء الدليل الإلكتروني إمكانية وسهولة محوه أو تدميره في زمن قصير حتى لا يتم الكشف والوصول إلى جرائم هؤلاء المجرمين، والتي وإن كشفت فإنه يُستهدف بالمحو السريع عدم استطاعة سلطات التحقيق إقامة الدليل ضدهم.

---

[1] أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2018 ص144.

[2] طارق عفيفي صادق أحمد، المرجع السابق، ص279.

[3] أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، المرجع السابق، ص143.

بل إنّ هؤلاء المجرمين بإمكانهم فرض تدابير أمنية لمنع التفتيش المتوقع عمله ضدهم وذلك بطريق استخدام كلمات سر حول مواقعهم أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل إلكتروني يخلفه نشاطهم الإجرامي، هذا الدليل الذي يعد شكلا استثنائيا للأدلة المقدمة في الدعوى العمومية والذي يمكن طلبه بناء على طلب أحد الخصوم في الدعوى أو قاضي الموضوع، هذا الأخير يعتبر طلبه من المسائل الفنية التي لا يجوز للمحكمة أن تحل فيها محل الخبير، إلاّ أنّها غير ملزمة بندب خبير وحتى بناء على طلب الخصوم طالما أن الواقعة قد وضحت لها وكان بمقدورها الفصل فيها[1].

ثانيا: المشكلات الإجرائية التي تواجه الدليل الإلكتروني

لعلها مشكلات تتعلق بالدرجة الأولى في كيفية وطريقة الحصول على هذا النوع من الأدلة، وهذا واضح من خلال ارتفاع تكاليف الحصول على الدليل الإلكتروني، والتي في غالب الأحيان ومن أجل أن يتم التعامل مع هذا الدليل الفني لابد وأن يتم الاعتماد على الخبرة، هذه الأخيرة لها دور مهم وكبير خاصة مع نقص معرفة رجال القانون بالجوانب التقنية فيما يتعلق بالجرائم المعلوماتية، هذا النقص سيلقي بطبيعة الحال بآثاره على المحاكمة ذلك أنّ الكشف على هذه النوعية من الجرائم وكذا إثباتها تتطلب استراتيجيات ومهارات خاصة على رجال القانون اكتسابها[2].

فالواقع العلمي يشير إلى أنّ جرائم معلوماتية كثيرة ارتكبت على مرأى ومسمع من رجال الأمن بل وقد قام بعض هؤلاء الرجال بتقديم المساعدة لمرتكبي هذه الجرائم دون علم وقصد منهم، وحتى وإن كان هناك كوادر فنية مدربة من أجهزة القضاء في شأن ضبط هذا النوع من الجرائم، فإنّ هناك مشكل آخر وهو أنّ الدليل الإلكتروني بالرغم من مشقة الحصول عليه وكذا تسليما بالقواعد التقليدية في الإثبات فإنّه لا يتم الاعتماد عليه وحده كدليل إثبات ما لم تؤازره أدلة أخرى، وهو الأمر الذي أدى وسيؤدي حتما إلى إفلات العديد من الجناة المعلوماتيين من العقاب[3].

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، المرجع السابق، ص92.

[2] أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي دراسة مقارنة، المرجع السابق، ص149.

[3] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، المرجع السابق، ص94.

المطلب الثاني: استعانة قاضي الحكم بأدلة الإثبات الأخرى العادية

إنّ مجرد الحصول على الدليل الإلكتروني من قبل قاضي الموضوع لا يكفي لاعتماده وحده كدليل إدانة، ذلك أنّه ذو طبيعة فنية خاصة تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، كما أنّه يثور الشك في مصداقيته كدليل للإثبات الجزائي لأنّ نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة[1]، إذن لابد على قاضي الموضوع أن يحصل على مزيد من الأدلة يعزز بها إثباته ويحسن من خلالها إصدار حكمه.

الفرع الأول: استعانة قاضي الحكم بالاعتراف لإثبات الجريمة المعلوماتية

الإقرار حجة ثابتة بالكتاب وبالسنة وبالإجماع، يقول الله سبحانه وتعالى في كتابه الكريم: " وَإِذْ أَخَذَ ٱللَّهُ مِيثَٰقَ ٱلنَّبِيِّـۧنَ لَمَآ ءَاتَيْتُكُم مِّن كِتَٰبٍ وَحِكْمَةٍ ثُمَّ جَآءَكُمْ رَسُولٌ مُّصَدِّقٌ لِّمَا مَعَكُمْ لَتُؤْمِنُنَّ بِهِۦ وَلَتَنصُرُنَّهُۥۚ قَالَ ءَأَقْرَرْتُمْ وَأَخَذْتُمْ عَلَىٰ ذَٰلِكُمْ إِصْرِىۖ قَالُوٓاْ أَقْرَرْنَاۚ قَالَ فَٱشْهَدُواْ وَأَنَا۠ مَعَكُم مِّنَ ٱلشَّٰهِدِينَ "[2]، ومن السنة ما ثبت في الصحيحين أنّ النبي صل الله عليه وسلم قال:" أغد يا أنيس إلى امرأة هذا فإن اعترفت فارجمها"، فغدا عليها فاعترفت فأمر بها رسول الله صلى الله عليه وسلم فرجمت، وكما روي أنّه عليه أفضل الصلاة والسلام رجم ماعزا والغامدية نتيجة لإقرارهما[3].

هذا الاعتراف قد يكون صادرا أمام المحكمة التي تنظر في الجريمة المعلوماتية موضوع الدعوى العمومية بحيث يطلق عليه مصطلح الاعتراف القضائي، وقد يكون صادرا خارج القضاء أو أمامه لكن في غير إجراءات الدعوى التي رفعت إليها موضوع الجريمة المعلوماتية المعترف بها، ويطلق عليه مصطلح

---

[1] خالد حسن أحمد لطفي، آليات التحقيق في جرائم تقنية المعلومات، المرجع السابق، ص142.

[2] الآية 81 من سورة آل عمران.

[3] أبو داود، كتاب الحدود. باب رجم ماعز 4\573، 4419\ حديث متفق عليه، أخرجه البخاري مطولا ومختصرا، والترمذي تم استرجاعه في 2021/20/05 الساعة 15:00 من موقع www.islamspirit.com.

الاعتراف غير القضائي[1]، كالاعتراف الذي يصدر أمام ضباط الشرطة القضائية أو أمام جهة إدارية أو اعتراف مكتوب في محرر صادر من المتهم[2]، وكذا الاعتراف الصادر أمام محكمة مدنية فهو يعتبر اعتراف غير قضائي[3] في مواجهة القاضي الجزائي.

هذا الاعتراف القضائي الذي يكون معيبا إذا ما صدر تحت تأثير إكراه مادي أو إكراه معنوي كالتعذيب أو التهديد المباشر أو صدر تحت تأثير تدليس أو خداع، فالأصل أنّ أي قدر من الإكراه أو التدليس يكفي حتى يكون الاعتراف معيبا، على شرط أن تكون هناك علاقة سببية بين الإكراه أو التدليس وبين الاعتراف، ويُثبت بذلك بأنّ المتهم المعلوماتي ما كان ليعترف لولا حصول الإكراه أو الخداع، لذلك فإنّ قاضي الموضوع ملزم في حكمه بالقول بأنّ حصول الإكراه أو التدليس جاء كافيا بأن يكون الاعتراف معيبا[4] وكذا توافر علاقة سببية بينهما.

هذا وباستطاعة قاضي الموضوع أن يحتفظ بالاعتراف كأساس للإدانة كما يستطيع استبعاده ويصدر حكما ببراءة المتهم إذا ما تبين له أن هذا الاعتراف مشتبه فيه أو متناقض مع وسائل الإثبات الأخرى أو مشكوك في جديته، على عكس الإقرار المنصوص عليه في القانون المدني الجزائري[5] الذي قد يصرح به أمام القاضي المدني، هنا الإقرار حجة قاطعة على المقر[6]، ولا يحوز القاضي هنا أي سلطة

---

[1] تميم بن عبد الله بن سيف التميمي، المرجع السابق، ص164.

[2] عبد الحميد الشواربي، الإثبات الجنائي في ضوء القضاء والفقه. د ط، منشأة المعارف الإسكندرية، مصر،1996، ص71.

[3] محمد علي سكيكر، موسوعة الدفوع الجنائية، د ط، دار الجامعة الجديدة، مصر، 2011، ص33.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر القانوني، الإسكندرية، مصر، 2009 ص253.

[5] الأمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، يتضمن ق م الجزائري، ج ر رقم 78، المؤرخة في 30 سبتمبر 1975.

[6] تنص المادة 342 من ق م الجزائري، ج ر رقم 78، المؤرخة في 30 سبتمبر 1975 بأنّ:" الإقرار حجة قاطعة على المقر، ولا يتجزأ الإقرار على صاحبه إلاّ إذا قام على وقائع متعددة وكان وجود واقعة منها لا يستلزم حتما وجود الوقائع الأخرى".

تقديرية في حالة النطق بهذا الإقرار أمامه بل وأكثر من ذلك فإنّ الاعتراف المدني له قوة إثبات ضد كل وسائل الإثبات الأخرى[1].

إنّ الواقعة موضوع الاعتراف في الجرائم المعلوماتية تضل بحاجة لأدلة أو قرائن أو استدلالات حتى تضفي عليها القيمة القانونية، فالاعتراف بارتكاب جريمة معلوماتية عبر الوسائط الإلكترونية لا يتصور دون الحصول على دليل رقمي من الجهاز الذي ارتكبت بواسطته أو من ملقمات أجهزة الحاسوب الكبيرة لدى مزود خدمة الإنترنت، خاصة إذا كانت الجريمة قد ارتكبت عبر شبكة الإنترنت[2].

هذا ولا تختلف أحكام الاعتراف في الجرائم المعلوماتية عن تلك الأحكام العامة في الجرائم التقليدية الأخرى، فلا يكفي مجرد اعتراف المتهم بارتكابه أحد صور الجرائم المعلوماتية بل يجب على هذا الأخير أن يحدد ويبين لقاضي الموضوع الكيفية التي من خلالها اقتراف هذه الجريمة، كما يجب أن يتطابق هذا الاعتراف مع الأسلوب الحقيقي الذي تمت فيه الجريمة المعلوماتية، لأنّه إذا تبين أنّ المعترف لا يعرف أساسا أية تقنية عن استخدام الحاسب الآلي والولوج إلى الإنترنيت فلا يمكن الاستناد إل اعترافه وإدانته بهذا الجرم[3]، فالاكتفاء بالاعتراف النظري في ارتكاب الجرائم المعلوماتية أمر يرفضه المنطق السليم ما لم يُقترن بالاعتراف العملي الذي يؤكد صحة ما جاء به لسان المتهم المعلوماتي.

الفرع الثاني: استعانة قاضي الموضوع بالدليل الكتابي

لم يكتفي المشرع الجزائري بوصفه للكتابة التقليدية على أنّها مجموعة حروف وإنّما زاد عليها كل ما يؤدي إلى معنى متفق عليه بين الأطراف من أوصاف أو أرقام أو علامات أو رموز، بل وأضاف بأي وسيلة كانت ومهما كانت طريقة إرسالها، على شرط أن تكون الرموز والحروف والإشارات واضحة

---

[1] محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، د ط، ديوان المطبوعات الجزائرية، الجزائر 1999، ص473.

[2] محمد محمود عمري، الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد 12، العدد 2 الجمعية العلمية للبحوث والدراسات الاستراتيجية، كلية الحقوق، أكاديمية البورك للعلوم، الدنمارك،، 2016، ص313.

[3] محمد طارق عبد الرؤوف الخن، المرجع السابق، ص319.

لا لبس فيها وتؤدي إلى معنى واحد مشترك، أمّا إذا كانت تلك الرموز والحروف والإشارات مشفرة يصعب حلها مما يؤدي لعدم معرفة الموقع فإنّه ينجم عنه بالضرورة عدم صحة المخرج من الحاسب الآلي[1].

هذه المخرجات قد تكون ذات طبيعة ورقية مسجلة فيها المعلومات ولإخراجها يجب استخدام الطابعات على اختلاف أنواعها وخصائصها واستعمالاتها، وقد تكون ذات طبيعة إلكترونية والتي هي موجودة بكميات كبيرة من خلال العرض المرئي، خاصة في الوقت الحاضر الذي تزايدت فيه كميات المعلومات المنتجة على أوعية لا ورقية أو غير مطبوعة كالأشرطة والأقراص الممغنطة[2] أو الضوئية، هذه المعلومات يحصل المستخدم على مخرجاتها بمجرد إدخال بياناتها[3]، من هذا المنطلق تدخل المحررات الإلكترونية في صورة المعلومات والمعطيات التي تحتويها الأقراص الصلبة أو المرنة أو التي يتم كتابتها بواسطة الحاسب الآلي وإرسالها ونشرها على شبكة الإنترنيت في دائرة الكتابة المعتمدة عليها كدليل إثبات في الجرائم المعلوماتية.

هذا وتبقى مسألة قبولها كدليل إثبات صعبة من الناحية القانونية وهو ما أدى إلى بروز جهود ذات طابع دولي والتي تمخضت عنها مجموعة قوانين اليونسيترال النموذجية المتعلقة بمجالات شتى كالتجارة الإلكترونية والتوقيع الإلكتروني وغيرها، أين سعت غالبية الدول إلى مسايرة التطور والانتقال من مرحلة التعامل بالورق إلى التعامل بالشكل الإلكتروني فحاولت تهيئة بيئة قانونية ملائمة لقبول

---

[1] مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، د ط، دار الخلدونية، الجزائر العاصمة، الجزائر، 2018، ص242.

[2] Gaudrat , droit de la preuve et nouvelles technologies de l' information, françoise gallouédec, une société sans papier, nouvelles technologies de de l' information et droit de la preuve, France,, 1990, p172.

[3] مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الثاني، ط خامسة، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2013 ص460.

وسائل المعطيات الإلكترونية كأدلة إثبات[1] ومن بينهم المشرع الجزائري الذي نجد أنّه واكب هذه التشريعات المقارنة.

الفرع الثالث: استعانة قاضي الموضوع بالقرائن

القرينة هي: " استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات "[2]، وهي وسيلة يُلجأ إليها في حالات يصعب فيها على المشتكي إقامة الدليل على ما يدعيه، فيفترض ثبوت واقعة معينة بمجرد ثبوت واقعة أخرى، ويُعفى المشتكي من إقامة الدليل على الواقعة التي يدعيها ويكفي منه إثبات الظروف اللازمة لقيام القرينة، والقرائن نوعان قانونية وأخرى قضائية موضوعية، فالقانونية مستمدة من نص القانون وهي واردة على سبيل الحصر ولا يقاس عليها ولا حاجة لإثباتها، أما النوع الآخر والمتمثل في القرائن القضائية فيستخلصها القاضي من ظروف الدعوى[3].

هذا وتنقسم القرينة القانونية إلى قسمين قرينة قانونية قاطعة والتي لا يجوز للقاضي أو الأطراف التغاضي عنها ومن أمثلتها ما جاء في المادة 43 من الدستور[4] بنصها: " لا إدانة إلاّ بمقتضى قانون صادر قبل ارتكاب الفعل المجرم "، وقرينة قانونية بسيطة والتي أجاز المشرع للأطراف إثبات ما يخالفها كقرينة البراءة بنص المادة 41 من نفس الدستور: "كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته، في إطار محاكمة عادلة ".

أمّا القرينة القضائية[5]فهي قرينة بسيطة يجوز إثبات عكسها ولا حصر لها[6]، وأحد أهم صورها في الدعوى العمومية المتعلقة بالجرائم المعلوماتية هو الدليل الإلكتروني.

---

[1] مناصرة يوسف، المرجع السابق، ص275.

[2] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط ثانية، دار النهضة العربية، القاهرة، مصر 1988، ص487.

[3] محمد محمود عمري، المرجع السابق، ص318.

[4] التعديل الدستوري الجزائري 2020 ، المرسوم الرئاسي السابق رقم 20-442.

[5] يقول الدكتور عبد الرزاق أحمد السنهوري في كتابه الوسيط القانون المدني أن : " للقرينة القضائية عنصران : (1) واقعة ثابتة يختارها القاضي من بين وقائع الدعوى وتسمى هذه الواقعة بالدلائل أو الأمارات، و(2) عملية اتنباط يقوم بها القاضي ليصل من هذه الواقعة الثابتة إلى الواقعة المراد إثباتها " .

[6] نجيمي جمال، المرجع السابق، ص381.

هذا الأخير الذي يعود تقدير قيمته إلى قاضي الموضوع، فمثلا معرفة عنوان الإنترنيت الرقمي " IP address"، يشير فقط إلى الحاسب الآلي الذي ارتكبت بواسطته الجريمة المعلوماتية دون معرفة الفاعل بدقة، فمعرفة العنوان الرقمي هو قرينة قضائية على ارتكاب هذه الجريمة لكنّها لا تكفي لبناء منطق الإدانة القائم على اليقين والجزم ما لم تتوفر أدلة أخرى تؤكد ارتكاب مالك الحاسب الآلي لهذه الجريمة، فعلى قاضي الموضوع أن يواصل البحث عن أدلة معينة تفيد بارتكاب المجرم المعلوماتي لهذه الجريمة[1]، كإثباته مثلا بأنّ هذا المجرم يمتلك أسلوبا خاصا أضحى به معروفا بحيث لا ترتكب هذه النوعية من الجريمة المعلوماتية إلاّ من خلاله.

المطلب الثالث: إجراءات التحقيق التكميلية لقاضي الحكم في الجرائم المعلوماتية

بالتزامن مع ارتفاع حالات وقضايا الجرائم المعلوماتية أصبح من اللازم معرفة كيفية إثباتها في سبيل الحصول على دليل إلكتروني يمكن من الاستناد عليه[2] من طرف قاضي الموضوع في حكمه، هذا الأخير خول له القانون بعض السلطات والإجراءات التي يقوم من خلالها بمعرفة واستخراج هذا الدليل بل ومعرفة أدلة أخرى لم يتم التطرق إليها في مراحل الدعوى العمومية السابقة، هذه الإجراءات أعطاها المشرع الجزائري اسم التحقيق التكميلي الذي يقوم به قاضي الموضوع بناءا على حكم صادر عنه[3].

الفرع الأول: القيام باستجواب المتهم بالجريمة المعلوماتية

كنا قد تطرقنا في الفصل السابق من هذه الدراسة بشيء من التفصيل عن هذا الإجراء المهم والمتمثل في استجواب المتهم المعلوماتي، والذي في الحقيقة أنّه يشكل صعوبة لدى المحقق عندما يقوم باستجواب هذا المتهم ويحاول الحصول منه على اعتراف، وذلك عندما يقوم بمجابهته بالأدلة المختلفة القائمة ضده، فالاستجواب من خلال مرحلة التحقيق الابتدائي يكون بغرض جمع الأدلة، أمّا من

---

[1] محمد طارق عبد الرؤوف الخن، المرجع السابق، ص313.

[2] أحمد محمد عبد الباقي، المرجع السابق، ص260.

[3] المادة 356 من القانون رقم 01-08، المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001.

خلال مرحلة المحاكمة فتختلف التشريعات المقارنة في إجازته أصلا، فهناك من التشريعات المقارنة كالتشريع المصري لا تجيزه لقاضي الحكم إلاّ على شرط قبوله من قبل المتهم ومحاميه إن وجد[1].

على عكس التشريع الجزائري الذي منح لقاضي الموضوع إمكانية استجواب المتهم المعلوماتي وتلقي أقواله وذلك قبل البدء بسماع الشهود، وأجاز كذلك القيام بهذا الإجراء للنيابة العامة، بل وأجازه كذلك للمدعي المدني وللدفاع على شرط طلب ذلك من رئيس الجلسة[2]، هذا ويبقى نجاح هذا الاستجواب على عاتق المستجوب نفسه، هذا الأخير الذي عليه الاستعداد جيدا قبل القيام به وعند البدء في اتخاذ خطواته وعند إجرائه وذلك حتى يستطيع تحقيق الهدف والغرض من القيام به[3].

ففي العادة يطلق مجرمو المعلوماتية على أنفسهم اسم النخبة ذلك أنّهم الفئة الأكثر معرفة بأسرار المعلوماتية وعالم الحاسوب وشبكة الانترنت، على عكس رجال السلطة القضائية ورجال القضاء قليلي الخبرة والمعرفة بمجال النظم المعلوماتية، الأمر الذي أصبحت فيه مهام التحقيق في الجرائم المعلوماتية في بعض التشريعات المقارنة توكل لهيئات خاصة في هذا المجال بل وشركات خاصة في مجال المعلوماتية، ومن هذا المنطلق يرى بعض الفقهاء أنّه من الخطورة تخلي الأجهزة القضائية عن دورها في التحقيق[4] في مثل هذا النوع من القضايا لصالح تلك الهيئات والشركات الخاصة، لما فيه من ضياع لحقوق المجتمع وجعلها تحت رحمة هذه الهيئات الغير مكلفة بتحقيق العدالة والتي همها الوحيد تحقيق مكاسب مالية.

الفرع الثاني: القيام بسماع أقوال الشاهد على الجريمة المعلوماتية

تعتبر شهادة الشهود في الدعوى العمومية من الأساسيات التي تبنى عليها الدعوى خاصة في مرحلة المحاكمة والتي تنتهي إمّا بإدانة المتهم أو بالقضاء ببراءته، فسماع أقوال الشهود تبنى على إمكانية تقديم الشاهد لأدلة إثبات مفيدة في الدعوى تكشف بها الحقيقة، وهذه الأدلة التي يمكن تقديمها

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص241.

[2] المادة 224 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص245.

[4] ربيعي حسين، المرجع السابق، ص252.

لإثبات الجرائم المعلوماتية المرتكبة تتلخص أساسا في البحث عن دليل إلكتروني مقدم يثبت هذه الجريمة وارتكاب المتهم لها، هذا وتقوم المحكمة بالاستماع للشهادة وتسجيلها كما لها أن تأخذ منها ما تشاء أو تلتفت عنها إذا ما لم تقتنع بها[1].

هذا وتقضي القاعدة العامة حول شكل الشهادة بأن تكون شفوية واستثناء مكتوبة، هذه الشهادة التي قد تأتي بصفة مباشرة حول الجرائم المعلوماتية المرتكبة، خاصة في هذه المرحلة من الدعوى أين يدلي بها الشاهد أمام قاضي الموضوع بما شاهده من قيام المتهم المعلوماتي بأي ترتيبات برمجية أو باختراقات لأي ملفات إلكترونية أو بارتكاب أي صورة أخرى تتعلق بالجريمة المعلوماتية[2] وكذلك قد تأتي هذه الشهادة بطريقة غير مباشرة سماعية أي نقلا عن ما سمعه من الشاهد الذي رأى الجريمة المعلوماتية بعينه أو سمعها بأذنه، أو نقلا عن الشخص الذي سمع من الشاهد الأصلي.

وباعتبار أنّ المحاكمة هي المرحلة الفاصلة في الدعوى الجزائية، إذن على قاضي الموضوع إن هو أخذ بالدليل المقدم من الشاهد فيجب أن يوضح أسبابه والعلة من أخذه ومدى ارتباطه بالدعوى، بل ويقع على عاتقه تقدير الدليل الفني المقدم من قبل الخبير الشاهد، ولا يستلزم الأمر التطابق بين الدليل المقدم وشهادة الشهود بل يكفي أن تتحد الأسباب والمضمون الذي يفضي إليه[3]، هذا ويجوز لقاضي الحكم أن يطرح شهادة من لا يطمئن لشهادته من الشهود[4]، بل وعليه أن يذكر تعليل طرحه لهذه الشهادة من غير تحليل أو تفصيل لهذا التعليل[5].

هذا وتبقى من مميزات القضاء الجزائي الشفوية في الاستجواب والمناقشة والمرافعة فلا تدون أقوال الشهود يوم المحاكمة بل يسجل القاضي ما يراه مناسبا منها، حتى تصريحات الشهود في مرحلة

---

[1] ناير نبيل عمر، المرجع السابق، ص176.

[2] تميم بن عبد الله بن سيف التميمي، المرجع السابق، ص199.

[3] ناير نبيل عمر، المرجع السابق، ص179.

[4] المادة 237 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادة 379 من القانون رقم 82- 03 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 7، المؤرخة في 16 فيفري 1982.

التحقيقات الأولية أمام ضباط الشرطة القضائية والتي تدون فيها دون حلف اليمين فلا يعتد بها قاضي الموضوع إلاّ على سبيل الاستئناس، أمّا تصريحاتهم أمام قضاة التحقيق أو قضاة الحكم فتكون بعد حلف اليمين[1]، فيكون الاعتماد عليها بناء على أقوال الشهود الذين استمع إليهم وتمت مناقشتهم فيها بحضور جميع الأطراف.

ولقاضي الحكم الاختيار في أن يستند أو يستأنس بمحاضر الشهود المسموع إليهم من طرف قاضي التحقيق، وعادة ما يوجه رئيس الجلسة دعوة أخيرة لكل شاهد قبل إقفال باب المرافعة إذا كان يظن بأنّ فيه شهادة زور من قبل بعض الشهود ليقول الحق[2]، بحيث لكل شاهد الحق في التراجع عن الشهادات وأن يبدي بعض التغيرات أو الإضافات والتي يجب أن تدون من قبل كاتب الجلسة بكل حذر وانتباه[3].

الفرع الثالث: استعانة قاضي الحكم بالخبرة المعلوماتية

تعتبر الخبرة عامة والخبرة المعلوماتية خاصة ذات أهمية كبيرة في المسائل الجزائية، وهي شأنها شأن باقي أدلة الإثبات الأخرى من جانب خضوع حجيتها ومدى تأثير أعمال الخبرة فيها لتقدير قاضي الموضوع واقتناعه الذاتي على التوالي[4]، هذا وتعتبر المحكمة غير مقيدة أساسا بندب خبير إذا ما رأت من الأدلة المقدمة في الدعوى ما يكفي للفصل فيها دون ما حاجة لندبه، إلاّ في حالة طلبه من الدفاع خاصة إذا كان طلب ندب خبير لتحقيق دفاع جوهري يعتبر من الطلبات الهامة لتعلقه بتحقيق الدعوى

---

[1] براهيمي صالح، الإثبات بشهادة الشهود في القانون الجزائري، عمل مقدم لنيل شهادة الدكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر، 2012، ص195.

[2] المادة 237 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] براهيمي صالح، المرجع السابق، ص197.

[4] منير محمد الجنبهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط أولى، دار الفكر الجامعي، الإسكندرية، مصر 2018، ص101.

لإظهار وجه الحق فيها، هنا ويبقى على المحكمة إجابته فيها أو أن ترفضه بناء على أسباب مبررة وإلاّ كان الحكم معيبا نظرا لقصوره من الإيضاح الواجب[1].

أمّا فيما يخص الحقيقة العلمية التي جاءت بها الخبرة فلا يستطيع القاضي مناقشتها فهي من المسائل الفنية التي لا علاقة لها باختصاص قاضي الموضوع، وإلاّ لما كان يطلب في أحيان كثيرة أن تجرى خبرة فنية كحالة مناقشته لجريمة معلوماتية ما[2]، من خلال فحصه أولا لشرعية الأدلة وشروط قبولها في عملية الإثبات الجزائي مع إمكانية طرحه واستبعاده للعناصر التي تم جمعها بطريقة مخالفة للقانون لينتقل بعد ذلك إلى ممارسة سلطته التقديرية مع مراعاته لجملة من الضوابط الأساسية[3] من أهمها ضابط امتناع القاضي الجزائي عن القضاء بعلمه الشخصي[4]، ليدحض ما جاء به الخبير الفني وإنّما يتعين عليه إذا ما ساوره الشك فيما قرره هذا الخبير بأن يحاول استجلاء الأمر بالاستعانة بخبير آخر ما دام أن الجريمة المعلوماتية تعد من المسائل الفنية البحتة التي لا يصح للمحكمة أن تحل محل الخبير فيها.

هذا ويقر القانون لقاضي الموضوع في الدعوى العمومية بسلطة تقديرية واسعة في مجال تقدير رأي الخبير، بحيث له أن يأخذ به أو لا يأخذ به بحسب مدى اقتناعه بالأسباب التي بنا عليها أو الاعتراضات التي وجهت إليه، كما له أن يأخذ برأي خبير دون آخر أو بجزء من تقرير دون غيره أو بأن يفاضل بين تقارير الخبراء إذا ما تعددوا، فيأخذ بما يراه ويطرح ما عداه، بل ويستطيع أحيانا أن يأخذ بالتقرير ولو لم يكن يقينيا بني على الترجيح خاصة إذا ما كانت وقائع الدعوى بالنسبة له تؤدي إلى اقتناعه[5].

---

[1] محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات) د ط، المكتب الجامعي الحديث، الإسكندرية، مصر، 2018، ص256.

[2] فروحات سعيد، المرجع السابق، ص132.

[3] تتمثل هذه الضوابط في: ضابط ورود الأدلة بملف الدعوى المطروح أمام القاضي وضابط وجوبية مناقشة الدليل الوارد بملف الدعوى بالجلسة وضابط حياد القاضي الجزائي وضابط امتناع القاضي الجزائي عن القضاء بعلمه الشخصي.

[4] سدود مختار، ضوابط السلطة التقديرية للقاضي الجزائي الجزائري في تقدير الأدلة، مجلة قانون النقل والنشاطات المينائية، المجلد 5 العدد 1، جامعة محمد بن أحمد، وهران 2، الجزائر، 2018، ص63.

[5] محمود محمد محمود جابر، المرجع السابق، ص264.

وهذه السلطة التقديرية خاصة في مجال إثبات الجرائم المعلوماتية ليست على إطلاقها بحيث لا يمكن لقاضي الموضوع رفض رأي الخبير إلاّ لأسباب مبنية على حجج علمية صحيحة[1]، ولا يجب على هذا القاضي أن يتسلط أو يتحكم بها وفق هواه وإنّما عليه تحري مدى جدية التقارير ومقدار ما توحي به من ثقة ويتبع في ذلك أساليب الاستدلال المنطقية التي يقرها العلم ويجري بها العمل القضائي[2].

المبحث الثالث: المرحلة الثالثة من محاكمة المتهم بالجريمة المعلوماتية

يعتبر الجزء الثالث والأخير من جلسة محاكمة المتهم بالجريمة المعلوماتية ظرفا ووقتا حساسا جدا في الدعوى العمومية ككل، فخلالها يصدر قاضي الموضوع حكمه على هذا المتهم وذلك بعد تقديره لمختلف الأدلة المطروحة في الجلسة وبناء على اقتناعه الشخصي، وهذا الحكم إلاّ ويرتب آثارا معينة سواء أثناء وبعد إصداره، هذه الآثار تكفل القانون بترتيبها وتنظيمها ووضعها في قالبها وآجالها المحددة هذا وقبل التطرق لهذه الآثار من خلال المطالب الآتية أردنا أولا التطرق لأهم آلية دولية لها تأثيرها الخاص على حكم قاضي الموضوع، خاصة إذا ما كان المجرم المعلوماتي متواجدا خارج الدولة التي تتابع القضية، تتمثل هذه الآلية في المساعدة القضائية الدولية.

المطلب الأول: دور آلية المساعدة القضائية الدولية في الحكم على المتهم المعلوماتي

إنّ كشف الجرائم المعلوماتية غالبا ما يتجاوز الحدود أكثر من دولة، الأمر الذي يتطلب معه تحديث النصوص ووسائل الملاحقة والإثبات وتبادل المعلومات بين الدول وإمكانية اتخاذ إجراءات خارج حدود الدولة المعنية في شكل المساعدة القضائية، هذه الأخيرة تعتبر أحد أهم الآليات الدولية المساهمة في إثبات ومكافحة الجرائم المعلوماتية والتي تعبر عن تعاون وتضافر جهود أكثر من دولة مع بعضها البعض من أجل تضييق الخناق على المجرمين المعلوماتيين وكشف مخططاتهم الإجرامية.

---

[1] مناصرة يوسف، المرجع السابق، ص2018.

[2] محمود محمد محمود جابر، المرجع السابق، ص264.

هذه المساعدة تجلت بصورة عملية في القارة الأوروبية أوروبا خاصة من خلال إطلاق مشروع "iPROCEEDS-2" في ندوة عبر الانترنيت نظمها مجلس أوروبا، هذا المشروع الأخير المشترك بين الاتحاد الأوروبي ومجلس أوروبا الهادف لدعم صانعي السياسات والمسؤولين عن حماية الأطفال من جميع أشكال العنف بما في ذلك التسلط عبر الإنترنت، وكذلك دعم أخصائيون في حقوق الإنسان وسلطات العدالة الجنائية من قضاة ومدعون عامين ووكالات إنفاذ القانون والمنظمات غير الحكومية والباحثون وكذا الأوساط الأكاديمية المهتمة بالموضوع.

بحيث ركزت المناقشات على الجهود والإجراءات المتخذة من أجل مكافحة التسلط عبر الإنترنت وعلى توفير التوجيه لإنفاذ القانون والجهات الفاعلة الأخرى ذات الصلة لتحديد حالات التسلط عبر الإنترنت التي تتطلب مزيدًا من التحقيق، كما أدى النشاط إلى زيادة الوعي بتدابير الوقاية القائمة وتقديم المشورة بشأن اليقظة فيما يتعلق بالجوانب النفسية التي تشمل الضحية والمعتدي على حد سواء[1] لكن واضح بالرغم من الأهمية الكبيرة لهذه الآلية إلاّ أنّها تعتريها بعض العقبات جعلت من تفعيلها وتطبيقها على الصعيد الدولي العالمي أمرا يكاد ينعدم.

الفرع الأول: عقبات المساعدة القضائية الدولية أمام إثبات الجرائم المعلوماتية

تعتبر آلية المساعدة القضائية من بين الآليات التي يصعب وضع تعريف جامع لها وذلك لعدة أسباب منها اتساع النطاق والصور والأشكال التي يمكن أن يتخذها هذا التعاون ولعدم إمكانية حصرها في نطاق محدد وكذا ظهور الوسائل الجديدة والمتجددة التي تجعل من هذا التعاون ظاهرة متغيرة ومتطورة بشكل مستمر، ولارتباط التعاون الدولي بمفهومه الواسع ببعض المفاهيم الأخرى المشابهة مثل مفهوم العلاقات الدولية والنظام الدولي والأمن القومي[2].

[1] iPROCEEDS-2: Webinar cyberbullying: trends, prevention strategies and the role of law enforcement, sur web sit https://www.coe.int/fr/web/cybercrime, dat 22/03/2021.

[2] أشرف علي قوقزة، المرجع السابق، ص137.

ولعل أهم ما يعترض تطبيق هذه الآلية على أرض الواقع وجود عاملين أساسيين متمثلين في عامل تقييد سلطات الدولة بحدودها الإقليمية وما يترتب عليه من تقييد للقضاء بالمكان هذا من جهة أمّا العامل الآخر فيتمثل في عدم إمكانية تطبيق قانون العقوبات بدون قانون الإجراءات الجزائية، هذا الأخير الذي ينقل الأول من حالة السكون إلى حالة الحركة والتطبيق، إذن هما عاملين يتعارضان والطبيعة العالمية العابرة للحدود للجرائم المعلوماتية التي تقتضي في العديد منها القيام بأعمال إجرائية خارج حدود الدولة التي ارتكبت فيها الجريمة أو جزء منها على إقليمها[1].

فهناك العديد من الأمكنة والدول التي مستها الجرائم المعلوماتية بل وهي في تزايد مستمر، بسبب القدرة الهائلة والسريعة على الاتصال ونقل البيانات وتحويلها بين الحواسب الآلية من مسافات طويلة جدا، فمنها جاءت الخاصية المتحركة والسريعة التي تتمتع بها هذه النوعية من الجرائم، لذا كان من اللازم تحديد مكان وقوع هذه الأخيرة، بحيث يجب على أي نظام قضائي أن يتعامل معها إلاّ إذا كانت هذه الجريمة تتطلب تدخل دولتين أو أكثر فإنّ تصارع الأنظمة القضائية يكون أمرا واردا خاصة إن لم تكن هناك اتفاقيات أو قانون دولي تلتزم به الدول المعنية[2]، هذا وقد تم اقتراح واعتماد العديد من المبادرات لمكافحة الجرائم المعلوماتية إلاّ أنّها كانت ضمن نطاق ضيق وذات طابع واحد فقط.

فمثلا في الولايات المتحدة الأمريكية عام 2011 أصدر البنتاغون استراتيجية "Cyber 3.0"لتعزيز التدابير التقليدية لحماية الشبكة بحيث تم إنشاء العديد من الوكالات والإدارات من قبل الحكومة الأمريكية لإعلان الحرب على جرائم الإنترنت، ومثلها كندا والصين توجد لديهما سياسة وطنية لمكافحة الجرائم المعلوماتية، لكن الاعتماد بشكل أساسي على الطابع الوطني لهذه الدول يمثل عقبة رئيسية أمام إقامة معركة فعالة بحق ضد هذه الظاهرة[3]، ذلك أنّ العالم بحاجة إلى إجراءات مشتركة من

[1] محمد كمال شاهين، المرجع السابق، ص220.

[2] عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص355.

[3] Romain Boos, La référence précédente, p263.

جانب كل الدول لتكون قادرة على مكافحة الجانب العابر للحدود الخاص بالجرائم المعلوماتية، وهو أمر في غاية الصعوبة نظرا لتعدد الاختلافات في سياسات المكافحة.

وحتى وإن كان هناك اتفاقيات ما بين هذه الدول فيجب التعديل في الآلية التقليدية للتعاون الدولي من أجل إزالة عقبات تأخير تنفيذ إجراءات الإنابة القضائية وتحسين التعاون القضائي بينها مثلا من خلال الاتصال مباشرا بين سلطات التحقيق واعتماد البريد لنقل الإجراءات في دول مختلفة كما نصت على ذلك اتفاقية شنجن[1] عام 1990 فيا يخص الدول الأعضاء وكما جاء أيضا في إحدى توصيات المجلس الأوروبي واتفاقية بودابيست 2001 على التوالي فيما يخص اتخاذ الإجراءات المتعلقة بالمعلوماتية[2]وكذا مكافحة الجرائم المعلوماتية.

فطالما أن القوانين في التشريعات المقارنة العالمية ليست متقاربة من حيث المتابعة والجزاء، فسيظل هناك مجال لمجرمي الإنترنت للعمل تقريبًا دون عوائق معتقدين أن العقوبات المنخفضة تؤدي إلى مخاطر منخفضة وهي من بين العقبات العالية التي تجاوزها الاتحاد الأوروبي، فكل دولة فيه إلاّ وهي قادرة في الرد على الهجمات الإلكترونية في غضون ثماني (08) ساعات[3] من خلال طلبات المساعدة من الدول الأعضاء الأخرى.

وعليه فلابد من إبرام معاهدات واتفاقيات دولية وثنائية من شأنّها التصدي للجرائم المعلوماتية بفاعلية ولها أيضا صفة الإلزام بحيث تشكل رادعا قانونيا على المستوى الدولي، هذه الاتفاقيات والمعاهدات التي من شأنها أن تحقق الانسجام بين مختلف القوانين الجزائية الوطنية من خلال اعتماد قوانين نموذجية يتسع نطاقها ليشمل غالبية الجرائم المعلوماتية[4]، ومما لاشك فيه بالنسبة لطبيعة المخاطر

---

[1] اتفاقية شنغن هي معاهدة تاريخية متعددة الأطراف تسمح بحرية السفر والتنقل داخل وعبر الدول الأعضاء فيها. ترتب على هذه الاتفاقية ظهور منطقة شنغن والتي تشكّلت من 26 دولة أوروبية اتفقت على إلغاء الرقابة على الحدود الداخلية فيما بينها أمام المسافرين الذين يعبرون بين حدود تلك الدول التي تتشارك معًا في سياسة تأشيرات موحدة.

[2] فريد منعم جبور، المرجع السابق، ص220.

[3] Eddy Willems, The previous reference, P170.

[4] عادل مشموشي، المرجع السابق، ص588.

التي تنطوي عليها مثل هذه الجرائم أصبح من اللازم والضروري أكثر من أي وقت مضى اعتماد وتفعيل مبدأ عالمية النص الجزائي، ذلك أنّه يتيح ملاحقة هؤلاء المجرمين المعلوماتيين ومعاقبتهم في البلد الذي يلقى القبض عليهم فيه دون مراعاة لمكان ارتكاب الجريمة أو جنسية المجرم.

الفرع الثاني: تأثير المساعدة القضائية الدولية على حكم قاضي الموضوع

إن بعض الحالات تستدعي استخدام آليات تسليم المجرمين والمساعدة القضائية الدولية المتبادلة فضلا عن تقاسم أقل المعلومات الرسمية والمشتركة في التحقيقات، للوصول إلى الجناة عبر الحدود فبهذه الطريقة يمكن لتطبيق القانون أن يقترب أكثر نحو القدرة على مكافحة الجرائم المعلوماتية، فعلى الأقل لا تكون الحدود الإقليمية عقبة لا يمكن التغلب عليها، وحتى المحاكم تكون بذلك قادرة على تكييف وتطبيق القوانين التي تم تطويرها نسبيا في مكافحة الجرائم المعلوماتية[1]، هذه الأخيرة التي يعمل رجال إنفاذ القانون الحديث على مواجهتها.

فأحيانا ما تحتاج سلطة قضائية في دولة ما، مساعدة قضائية من دولة أخرى من أجل إثبات الجريمة المعلوماتية ذات الطبيعة المتعدية الحدود والتي ارتكبت إمّا على أحد رعاياها أو ارتكبت من طرف أحد رعاياها، هذه المساعدة قد تؤثر بشكل كبير على حكم قاضي الموضوع المحقق في هذه الجريمة المعلوماتية المرتكبة، حكمه هذا قد يستند على تبادل معلومات مهمة مع السلطة القضائية للدولة الأجنبية أو على حضور الشهود والخبراء من هذه الدولة الأخيرة.

أولا: استناد قاضي الموضوع على إجراء تبادل المعلومات

يقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها السلطة القضائية الأجنبية، هذه المعلومات قد تتعلق بالسوابق القضائية للجناة فتتعرف هذه السلطة القضائية بدقة على الجاني المحال

[1] Gregor Urbas, cybercrime jurisdiction and extradition : the extended reach of cross-border law enforcement, journal of internet law, volume 1 6, number 1, D L A piper, Londres, Royaume-Uni, july 2 0 1 2, p15.

إليها والتي من خلالها تساعد في تقرير الأحكام الخاصة بالعود من طرف قاضي الموضوع وكذا وقف تنفيذ العقوبة.

ثانيا: استناد قاضي الموضوع على حضور ومساعدة الشهود والخبراء

إن حضور الشهود والخبراء من دولة إلى أخرى تعتبر صورة هامة أخرى من صور المساعدة القضائية الدولية في المجال الجزائي[1]، والتي يمكن لقاضي الموضوع أن يستند إليها قبل إصدار حكمه حول الجريمة المعلوماتية المرتكبة، هذا الحضور يكون وفق شروط معينة، كما يجب أن يتمتع هؤلاء الشهود أو الخبراء بحصانة ضد اتخاذ أي إجراءات جزائية ضدهم بسبب أفعالهم السابقة.

فهذه المساعدة القضائية الدولية غايتها تسهيل مهمة المحاكمة الجزائية من خلال ما تطرقنا إليه سابقا من تبادل للمعلومات والوثائق بين الدول وعن طريق نقل الإجراءات والتحقيق من دولة لصالح دولة أخرى بناء على اتفاقية وضمن شروط معينة في شكل إجراء إنابة قضائية دولية والذي ترفعه الدولة الطالبة إلى الدولة المطلوبة إليها تمهيدا للفصل بمسألة معروضة أمام القضاء الجزائي في الدولة الطالبة هذا الإجراء ونظرا للطبيعة الخاصة للجرائم المعلوماتية المتميزة بالسرعة في تبادل معلوماتها على شبكة الإنترنيت تقتضي ردودا سريعة خشية التلاعب بالبيانات وإخفاء الأدلة.

المطلب الثاني: الحكم الفاصل في الدعوى العمومية المتعلقة بالجريمة المعلوماتية

يعتبر صدور الحكم هو النتيجة التي ستؤول إليها التحقيقات في مراحل سير الدعوى العمومية وكذا مصير المتهم بالجريمة المعلوماتية إمّا بالبراءة أو الإدانة، لذلك لابد لقاضي الموضوع قبل إصداره لحكمه في الدعوى العمومية المتعلقة بالجرائم المعلوماتية أن يعمل أولا على تقدير أدلة الإثبات التي أتيحت له أثناء جلسة المحاكمة وأن يزنها جيدا وأن يستخلص منها قدر المستطاع قصد المتهم؛ وذلك

[1] عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص34.

حتى يكون حكمه صادرا وفق قناعة قوية لا يهزها الشك وحتى يستطيع إحاطة هذا الحكم بتسبيب مناسب لا يخرج عن نطاق العلم والمنطق القانونين.

الفرع الأول: أثر تقدير قاضي الموضوع لأدلة الإثبات على حكمه في الدعوى

تسود لدى التشريعات الجزائية قاعدة في الإثبات مفادها أنّ المحكمة تحكم في الدعوى بناء على اقتناعها الذي تكون لديها من الأدلة المقدمة في أي دور من أدوار التحقيق أو المحاكمة، كما أنّ هذه الأدلة التي تستسقي منها المحاكم قناعتها ليست محددة حصرا، وهذه الأدلة ذكرها القانون في الغالب الشائع والمتمثلة في الاعتراف وشهادة الشهود ومحاضر التحقيق والمحاضر وكذا المحاضر الرسمية الأخرى وتقارير الخبراء والفنيين، إضافة للقرائن والأدلة الأخرى المقررة قانونا، كل هذه الأدلة يكون لقاضي الموضوع فيها كامل الحرية في تقديرها إذا ما طرحت عليه في الدعوى الجزائية[1].

أمّا بالنسبة لإثبات القصد الجزائي في الجرائم المعلوماتية فهو في غاية الصعوبة والتعقيد كونه أمر يبطنه الجاني ومتعلق بإرادته ونفسيته فهو غير محسوس وغير مرئي، هذا وبالرغم من الطبيعة الخاصة للجرائم المعلوماتية إلاّ أنّ قاضي الموضوع ومن خلال سلطته التقديرية يستطيع أن يستدل على عدم مشروعية ما قام به المجرم المعلوماتي من أفعال في بيئة الأنظمة المعلوماتية والشبكة المعلوماتية[2]، وذلك من خلال الملابسات المحيطة بالجريمة ومن خلال قرائن الدعوى وظروفها ومعطيات الجريمة والأدلة وكذا القرائن الخارجة المحيطة بها، فعلى قاضي الموضوع أن يستخلص نية الجاني وغايته من أي دليل بعينه ما دام هذا الدليل مشروعا.

هذا وتجدر الإشارة أيضًا إلى أنّ تثبيت برنامج السلامة قد يكون قرينة لمعرفة بعض الأشخاص أنّه ليس لديهم الحق في الدخول أو البقاء في النظام، لذلك عندما يدخل هؤلاء لنظام محمي يمكن إثبات نيتهم، ذلك أنّ العناصر المكونة للجرائم المعلوماتية يتم إنشاؤها عندما يصل شخص ما أو يحتفظ

---

[1] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، المرجع السابق، ص365.

[2] محمد عبد الرحمان عنانزه، المرجع السابق، ص239.

بنفسه في جزء من النظام بدون ترخيص مع إدراك المخالفة من فعله هذا[1]، وعلاوة على ذلك يمكن للمتهم التهرب من المسؤولية الجزائية عن طريق إظهار حالته العقلية البريئة أين يمكنه إثبات حسن نيته أو خطأه أو وقوع حادث.

فقاضي الموضوع صاحب الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات وتمحيصها بما له من سلطات باعتباره صاحب القرار النهائي بالفصل في الدعاوى المرفوعة أمامه كما له السلطة في أن يفاضل بينها ليأخذ بما يطمئن إليه منها ويعرض عما لا يطمئن إليه من أدلة أخرى؛ لهذا فقد أقر المشرع الجزائري للدليل الرقمي ذات الحجية المقررة للأدلة التقليدية الأخرى، ويبقى للقاضي الجزائي الحرية في تقدير جميع الأدلة المطروحة في الدعوى العمومية بغض النظر عن مصدرها الذي استمدت منه طالما كان ذلك المصدر مشروعا[2]، هذا ولا يمكن بأي حال من الأحوال التذرع بدافع الجريمة لمحاولة الهروب من المسؤولية الجزائية[3].

الفرع الثاني: وجوب صدور حكم قاضي الموضوع عن قناعة شخصية

القناعة لغة بمعنى الرضا والقانع بمعنى الراضي وهو من الأضداد وسمِّيت قناعةً لأنّه يقبل على الشيء الذي له راضيًا[4]، أمّا اصطلاحا فيرى بعض الفقه أنّها اتجاه نفسي يرمي التوصل إلى إيجاد حدث معين والمتمثل في تطبيق القانون، هذا ويرى اتجاه آخر أنها ضمير القاضي ووجدانه كما عرفوا الضمير بأنّه : " ضوء داخلي ينعكس على كل وقائع الحياة فهو قاضي أعلى يقيم كل الأفعال لكي يوافق

---

[1] Ibtissem Maalaoui, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, Mémoire vue de l'obtention du grade de Maîtrise en droit (L.L.M.) option droit des affaires, Faculté des études supérieures, Université de Montréal, Canada, 2011, p34.

[2] لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية ومقارنة، مجلة الميزان للدراسات الإسلامية والقانونية المجلد الرابع، العدد 01، جامعة العلوم الإسلامية العالمية، عمان، الأردن، 2017، ص209.

[3] Ibtissem Maalaoui, La référence précédente, P34.

[4] عن موقع https://www.dorar.net/akhlaq/1201/، بتاريخ 2021/02/03، الساعة 09:48.

عليها أو يهجرها أو يدينها وهو مستودع القانون وللقواعد الأخلاقية التي بمقتضاها تتم التفرقة بين العدل والظلم والحق والزيف والصدق والكذب".

هذا ويمتلك قاضي الموضوع سلطة تقديرية واسعة في تمحيص الأدلة المعروضة عليه في الدعوى ووزنها من حيث قيمتها القانونية في الإثبات وله أن يتقيد بالأخذ بهذا الدليل دون ذلك، وله أن يطرح الدليل الذي لا يولد له القناعة الكافية وأن ينبذه، فله مثلا أن يهدر الشهادة ويأخذ بالقرينة أو يهدر اعتراف المتهم إذا كان هناك ما يكذبه ويدحضه، على أن يكون كل ذلك مؤسسا على أسباب قانونية مقبولة والتي يجب أن تدرج في صلب الحكم أو القرار الذي تصدره المحكمة أو الغرفة الجزائية المختصة[1].

بل ويستطيع الاعتماد في حكمه أو قراراه على محاضر ضباط الشرطة القضائية فقط إذا ما كانت حسب اعتقاده ترقى إلى مستوى الدليل طالما كانت تحقق اطمئنانه وقناعته الشخصية، ولا يجوز له أنّ يبني اقتناعه على معلومات شخصية كان قد حصل عليها من خارج نطاق الدعوى المطروحة أمامه والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها، ذلك أنّها من جهة لم تكن موضع مناقشة شفاهة بحضور أطراف الدعوى[2] فتكون بذلك مفاجئة لهم وتمس بعدم احترام حقوق الدفاع ومن جهة ثانية يظهر القاضي فيها وهو يحمل في شخصه صفتين متناقضتين صفة الشاهد وصفة القاضي وهو ما لا يجيزه القانون مما يترتب عليه بطلان الحكم.

وبالرغم من أنّ قاضي الموضوع ملزم بفحص الدليل الإلكتروني أو الدليل الجزائي كقاعدة عامة من أجل أن يتوصل إلى تشكيل قناعته انطلاقا من عرض هذا الدليل على مناقشة الأطراف كما هو منصوص عليه ضمن المادتين 212 و234 من ق إ ج، إلاّ أنّ الفراغ يبقى قائما حول إمكانية ضبط

---

[1] ضياء عبد الله الجابر الأسدي، القناعة القضائية في الإثبات الجنائي، مقال ضمن كتاب أبحاث في القانون العام، المرجع السابق ص267.

[2] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2015 ص239.

الأدلة ومشروعيتها خاصة في حالة ارتباط النهاية الطرفية للنظام المعلوماتي بجهاز ألي آخر تواجد خارج مكان ارتكاب المتهم للجريمة المعلوماتية والذي قد يكون خارج الوطن[1].

بل ويجب أن تكون عقيدة قاضي الموضوع واقتناعه الشخصي بالأدلة الإلكترونية قد استمدت من مخرجات إلكترونية وطرحت بالجلسة، فحكمه يجب أن يكون بناء على التحقيقات التي تحصل بالطرق والشروط القانونية وليس بناء على معلوماته الشخصية أو على ما قد يكون رآه بنفسه في غير مجلس القضاء، هذا ولا ينبغي كذلك أن يؤسس حكمه بناء على دليل ناتج من الحاسب الآلي لحقه سبب يبطله ويعدم أثره[2]، وذلك كله تحقيقا لليقينية والشفوية وكذا المشروعية التي يجب أن يتمتع بها الدليل الإلكتروني في سبيل إثبات الجريمة المعلوماتية المرتكبة.

فالجهد الاستنباطي الذي يبذله قاضي الموضوع من خلال نشاطه العقلي في سبيل تكوين اقتناعه الشخصي يستند على ثلاثة طرق هي:

- يقبل جميع الأدلة المطروحة أمامه في الجلسة ولا يُحظر على القاضي أو يُفرض عليه دليل معين فلا يتقيد إلاّ بقيد مشروعية الدليل والذي تم طرحه للمناقشة بالجلسة.

- يقوم بوزن كل دليل على حدا عن باقي الأدلة المطروحة أمامه بحيث يستطيع إهدار أي دليل مهما كانت قيمته طالما لم يطمئن إليه.

- التنسيق بين الأدلة المطروحة أمامه ويبين تساند هذه الأدلة فيما بينها[3].

الفرع الثالث: تسبيب حكم القاضي الصادر بحق المتهم بالجريمة المعلوماتية

إنّ العدالة الإلهية عدالة مطلقة وذلك لأنها تتطابق مع الحقيقة الواقعية المطلقة وتنفذ إلى الباطن فلا ريب أنّها من صنع الله الحكم العدل، العليم ببواطن وظواهر الأمور على عكس العدالة البشرية التي تعد عدالة نسبية فهي من صنع بشر معرضين في أحكامهم للصواب والخطأ كل بحسب قدرته المحدودة

[1] زيبحة زيدان، المرجع لسابق، ص173.

[2] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، ص366.

[3] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص215.

التي تقوم على الظاهر وتعجز عن الوصول إلى الباطن الذي يترك علمه لله وحده لا شريك له؛ فقد روت أم سلمه عن النبي – صلى الله عليه وسلم - أنّه قال: "إنّما أنا بشر ، وإنّكم تختصمون إلي ، ولعل بعضكم أن يكون ألحن بحجته من بعض فأقضي بنحو ما أسمع، فمن قضيت له من حق أخيه شيئا فلا يأخذه فإنّما أقطع له قطعة من النار فليأخذها أو ليتركها"[1].

هذا ويأخذ الإسلام بمبدأ تقييد سلطة القاضي في الحدود وإعطائه سلطة التقدير في الأدلة إلاّ أنّه في باب التعزير أخذ بمبدأ حرية القاضي نظرا لكثرة هذه النوعية من الجرائم ونظرا لتقاربها وكذا اختلافها من مجتمع لآخر وحسب ظروف كل جريمة، لهذا ترك الإسلام للقاضي حرية إثبات التعازير بكافة وسائل الإثبات والتي من خلالها يستطيع بناء قناعته خلافا لجرائم الحدود[2]، كما أنّ النفس البشرية حباها الله بحاسة العدالة فلا تطمئن ولا تقتنع إلاّ بما هو عادل، مع هذا فإنّ القاضي وإن حاول أن يكون عادلا إلّا أنّه لا يستطيع الوصول إلى العدل المثالي المطلق بمعنى الإنصاف، فقضاؤه لابد وأن يكون معرضا للخطأ سواء أكان هو نفسه مصدر هذا الخطأ أم أنّ الخطأ يكمن في الأدلة التي استمد منها اقتناعه الشخصي[3].

لكن هذا لا يمنعه من أن يجتهد وأن يقترب في عدله قدر الإمكان من الإنصاف وذلك حتى يبرأ ذمته أمام خالقه ويكون بذلك من السابقين إلى ظله يوم القيامة، فالأحكام التي هي من صنع البشر أيّا كان نوعها أو موضوعها سواء كانت منازعة مدنية أو جزائية حتى تكون صحيحة وقريبة من العدل لابد على القاضي أن يبين الأسباب الكافية والسائغة التي تبرر صدور حكمه في الواقع والقانون على النحو الذي صدر منه وإلاّ كان الحكم معيبا ومعرضا للطعن والبطلان؛ لذلك فإنّ الالتزام بالتسبيب

---

[1] صحيح البخاري لأبي عبد الله محمد ابن إسماعيل البخاري، ط أولى، دار ابن كثير، بيروت، لبنان، 2002، حديث رقم 7185 ص 1776.

[2] خالد حسن أحمد لطفي، آليات التحقيق في جرائم تقنية المعلومات، المرجع السابق، ص148.

[3] بندر بن منصور السعدون، ضمانات المتهم في مرحلة المحاكمة أمام ديوان المحاكمات العسكرية السعودي، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2012، ص50.

يعد أحد الركائز الأساسية التي تحكم العملية القضائية التي تأخذ بها كافة الأنظمة القانونية المتقدمة وكل هذا في سبيل الوصول إلى العدل والإنصاف.

وبالرغم من ذلك يبقى تقييد القاضي الجزائي عند تقديره للأدلة الإلكترونية منها والبسيطة بمختلف الضوابط سواء المتعلقة بالدليل نفسه أو المتعلقة بالاقتناع من خلال إجراء التسبيب هي عملية غير كافية لمنع استبداد وتسلط بعض القضاة عند إصدارهم للحكم في الدعوى المتعلقة بإحدى الجرائم المعلوماتية مثلا؛ لهذا لابد من وجود ضمانة أخرى تكون أقوى من سابقيها تجعل من السلطة التقديرية لقاضي الموضوع تدور في مجال معتدل يهدف للوصول إلى الحقيقة الواقعية[1]، هذه الضمانة في التشريع الجزائري تتمثل في رقابة المحكمة العليا على هذه السلطة التقديرية الممنوحة قانونا لهذا القاضي الأخير.

المطلب الثالث: آثار إصدار الحكم على المتهم المعلوماتي في التشريع الجزائري

يعتبر الحكم القضائي تعبيرا عن الشكل العام للعمل القضائي ذلك أنّه يجب أن يصدر هذا الأخير في شكل الحكم ما لم ينصص القانون على خلاف هذا، ويعد الحكم القضائي وسيلة من الوسائل التي اعتمدها المشرع لأجل تحقيق وظيفة القضاء من خلال حماية القانون وكذا الحقوق والمراكز القانونية للأفراد، بل ويمحص كل ما قدم إليه ويطبق القواعد القانونية على الموضوع المطروح عليه[2] ليصل إلى إصدار حكم يزيل به العوارض التي واجهت الحقوق والمراكز القانونية للأفراد ويشبع بموجبه مصالحهم ويؤدي به واجبه.

إذن هذا الحكم هو خاتمة المطاف في الخصومة ونقطة النهاية في سباق ترافع فيه أطراف الدعوى بأساليب وأدوات وحجج قانونية، فهو يعتبر تتويجا لجهود كبيرة وجبارة وإجراءات طويلة يقوم بها أطراف الدعوى العمومية في الجرائم عامة وبعض الجرائم الخاصة والمعقدة كالتي في شكل موضوع الدعوى والدراسة الحالية ألا وهي الجرائم المعلوماتية، هذا الحكم إلاّ ويرتب آثار أولها من حيث تعرضه لموضوع

---

[1] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، المرجع السابق، ص244.

[2] محمد سعيد عبد الرحمان، المرجع السابق، ص14.

الدعوى فقد يأتي فاصلا فيها كما قد يأتي عكس ذلك، وثانيها من حيث قابليته للطعن فقد يأتي حكما ابتدائيا أو حكما نهائيا، وثالثها من حيت غياب وحضور المتهم في الجلسة.

الفرع الأول: آثار الحكم على المتهم المعلوماتي من حيث تعرضه لموضوع الدعوى

كأصل عام تأتي الأحكام في أغلبها فاصلة في موضوع الدعوى إذا ما كانت تبت سواء في ببراءة المتهم أو في بإدانته على أن يتم ذلك بطبيعة الحال بعد الفصل في الطلبات والدفوع المقدمة من طرف النيابة العامة من جهة ودفاع المتهم والطرف المدني إن وجد من جهة ثانية وذلك بعد المناقشات والمرافعات التي دارت بجلسة المحاكمة؛ أمّا الاستثناء فقد تأتي هذه الأحكام قبل الفصل في موضوع الدعوى[1] والتي تكون أحكاما جزئية لا تصل إلى حد الحسم في براءة المتهم أو إدانته.

أولا: الأحكام الفاصلة في موضوع الجرائم المعلوماتية في التشريع الجزائري

بعد التحقيق في القضية المتعلقة بالجريمة المعلوماتية على مستوى جهة الحكم المختصة، قد تقضي المحكمة إمّا بإدانة المتهم أو تبرئته أو إعفائه من المسؤولية أو إعفائه من العقاب وبحكمها هذا تنتهي الدعوى العمومية وتخرج من يدها، فيجب إخلاء سبيل المتهم المحبوس مؤقتا الذي تم تبرئته حالا ما لم يكن محبوس لسبب آخر[2] ولا يجوز متابعته مرة ثانية على نفس الوقائع حتى ولو كيفت تكيفا آخر[3] أمّا إذا ما ثبتت التهمة في حق من حركت الدعوى العمومية ضده هنا تقضي المحكمة المختصة بالعقوبة

---

[1] علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الثاني التحقيق والمحاكمة، ط ثالثة، دار هومة، الجزائر، 2017 ص203.

[2] الفقرة 1 من المادة 365 من الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41 ، المؤرخة في 29 يوليو 2015: " يخلى سبيل المتهم المحبوس مؤقتا فور صدور الحكم ببراءته أو بإعفائه من العقوبة أو الحكم عليه بعقوبة العمل للنفع العام أو بالحبس مع إيقاف التنفيذ أو بالغرامة، وذلك رغم الاستئناف ما لم يكن محبوسا لسبب آخر ".

[3] تنص الفقرة 2 من المادة 311 من القانون رقم 17-07، المعدل والمتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري جر رقم 20، المؤرخة في 29 مارس 2017بأنّه: " ولا يجوز أن تعاد متابعة شخص قد برئ قانونا أو اتهامه بسبب الوقائع نفسها حتى ولو صيغت بتكييف مختلف ".

المقررة قانونا[1] للجريمة المعلوماتية موضوع الدعوى العمومية ككل، بل ويتحمل المصاريف القضائية[2] التي على عاتق المدعي المدني إن وجد.

أمّا في حالة ما ثبت لدى المتهم بالجريمة المعلوماتية ظرفا شخصيا كحالة الجنون أو الإكراه وحالة الضرورة وصغر السن هنا يتم إعفاؤه من المسؤولية الجزائية، هذا الإعفاء تخف حدته بحسب ظرف المعفى، فمثلا لا يعفي القاصر الذي لم يكمل 13 سنة من المسؤولية المدنية بل ويجوز اتخاذ تدبير من تدابير الأمن والحماية والتهذيب[3]، أمّا عن إعفاء[4] المدان بالجريمة المعلوماتية من العقاب عند صفح الضحية ، فالملاحظ أن هذا الإجراء مس فقط الطفل[5] الذي لم يكمل 10 سنوات وكذلك مرتكب جريمة المساس بحرمة الحياة الخاصة بأية تقنية[6]، هذا وكان بإمكان المشرع أن يعمم هذا الإجراء على الكثير من الجرائم المعلوماتية كالاحتيال أو السرقة أو النصب المعلوماتي الذي قد يقع ما بين الأصول والفروع.

هذا ولما كانت الجرائم المعلوماتية في التشريع الجزائري داخلة تحت وصف الجنحة، فقاضي الحكم إذا رأى بأنّ الواقعة محل التحقيق النهائي تمثل جريمة من الجرائم المعلوماتية عليه أن يقضي بالعقوبة المقررة

---

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، المرجع السابق، ص256.

[2] تنص الفقرة 3 من المادة 367 من القانون رقم 78-01، المؤرخ في 28 يناير 1978، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 6، المؤرخة في 07 فبراير 1978، بأنّه: " ولا يلزم المدعي المدني الذي قبل ادعاؤه مصروفات ما دام الشخص المدعى ضده قد اعتبر مدانا في جريمة ".

[3] الفقرة 1 من المادة 49 من الأمر رقم 66-156، المتضمن ق ع الجزائري، ج ر رقم 49 المؤرخة في 11 يونيو 1966: " لا توقع على القاصر الذي لم يكمل الثالثة عشرة إلاّ تدابير الحماية أو التربية".

[4] الإعفاء من العقاب يكون بالرغم من قيام الجريمة بكامل عناصرها، وذلك بسبب أن المشرع ولاعتبارات خاصة تمس طبيعة المجتمع يرى أنّه لا جدوى من توقيع العقاب.

[5] تنص الفقرة 1 من المادة 56 من القانون رقم 15-12، المتعلق بح ط، ج ر رقم 39 المؤرخة في 19 يوليو 2015: " لا يكون محلا للمتابعة الجزائية الطفل الذي لم يكمل العشر (10) سنوات ".

[6] تنص المادة 303 مكرر من القانون رقم 06-23، المعدل والمتمم للأمر66-156 المتضمن ق ع الجزائري، ج ر رقم 84 المؤرخة في 24 ديسمبر 2006: " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000دج، آل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت.....

..... ويضع صفح الضحية حدا للمتابعة الجزائية ".

لها، وأن يحكم عند الاقتضاء في الدعوى المدنية وله كامل السلطة في أن تُدفع مؤقتا كل أو جزء من التعويضات المدنية المقدرة، بل وله أن يقرر للمدعي المدني مبلغا احتياطيا قابل للتنفيذ به رغم المعارضة أو الاستئناف في حالة ما إن لم يكن ممكنا إصدار حكم في طلب التعويض المدني بحالته[1]، هذا وفي حالة ما ارتبطت الجنحة المعلوماتية بمخالفة فعليه أن يقضي فيهما بحكم واحد قابل للاستئناف[2].

وإذا تبين من المرافعات بأن الواقعة لا تمثل جريمة معلوماتية وإنّما عبارة عن مخالفة فقط فعلى قاضي الحكم أن يقضي في هذه المخالفة[3] بعقوبة، ويفصل كذلك عند الاقتضاء في الدعوى المدنية، أمّا إذا كانت واقعة الجنحة المعلوماتية من الطبيعة التي تستحق توقيع عقوبة جنائية فإنّ قاضي الحكم في هذه الحالة يقضي بعدم اختصاصه فيها ويحيلها للنيابة العامة للتصرف فيها حسبما يراه، ويصدر في القرار نفسه أمرا بإيداع المتهم بالجريمة المعلوماتية في مؤسسة إعادة التربية أو أمرا بالقبض عليه وهذا بعد سماع أقوال النيابة العامة[4]، هذه الأخيرة التي تحيل القضية وموضوع الدعوى إلى غرفة الاتهام[5].

هذه الأخيرة من خلال تحقيقها في واقعة الجريمة المعلوماتية إذا رأت بأنّها تكون جنحة فإنّها تقضي بإحالة القضية إلى المحكمة المختصة[6] بنظرها[7]، أمّا إذا رأت بأنّ الوقائع المنسوبة للمتهم بالجريمة المعلوماتية لها وصف الجناية فإنّها تقضي إمّا بإحالة المتهم إلى محكمة الجنايات الابتدائية[8]أو إلى القطب الجزائي

---

[1] المادة 357 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] المادة 360 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[3] المادة 359 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[4] المادة 362 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] المادة 363 من القانون رقم 82-03، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 7، المؤرخة في 16 فيفري 1982.

[6] المحكمة المختصة قد تكون محكمة عادية أو القطب الجزائي الوطني المتخصص بالجرائم الاقتصادية والمالية الأكثر تعقيدا.

[7] المادة 196 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[8] المادة 196 من القانون رقم 17-07 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20، المؤرخة في 29 مارس 2017.

الاقتصادي والمالي[1] إذا ما كانت تظم منظمات إجرامية وطنية ودولية، ذلك أنّ الجرائم المعلوماتية أصبحت أكثر نموا على الصعيدين الوطني والدولي وأكثر احترافًا من خلال إنشاء شبكات منظمة بشكل متزايد ومتخصصة في الاتجار بالمخدرات أو الدعارة أو غسيل الأموال أو التجسس الصناعي[2].

ثانيا: الأحكام غير الفاصلة في موضوع الجرائم المعلوماتية

هي أحكام جزئية لا تصل إلى حد الحسم في براءة المتهم أو إدانته لكنها تتعلق بالدعوى رغم أنّها لم تفصل في موضوعها، فتكون إمّا أحكاما تحضيرية أو تمهيدية وإمّا أحكاما وقتية أو قطعية[3].

1- الحكم التحضيري والحكم التمهيدي

الأول التحضيري تصدره المحكمة تحضيرا للدعوى دون أن تفصح فيه عن الاتجاه الذي ستسلكه في دعوى الجريمة المعلوماتية وذلك من أجل ثبوت التهمة أو نفيها كالحكم بإجراء تحقيق تكميلي[4] أمّا الثاني التمهيدي فمن خلاله تفصح المحكمة عن الاتجاه الذي ستسلكه في دعوى الجريمة المعلوماتية بعد أن أصبح لديها قناعة بثبوت التهمة في حق المتهم المعلوماتي، فتلجأ المحكمة إلى الخبرة مثلا لتقدير نسبة الضرر ذلك أن مقدار التعويض الذي ستحكم به المحكمة لصالح الضحية يتوقف على تقرير هذه الخبرة التي أمرت بها.

---

[1] المادة 211 مكرر3 من قانون رقم 20-04 المعدل والمتمم للأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51 المؤرخة في 31 غشت 2020.

[2] Comment s'irganiser contre la cybercriminalité Lettre d'information : bon a savoir (N°32), cellule de traitement du renseignement financier, ministére des finances, algerie, vu sur sit internet https://fr.scribd.com/document/407011952/Bulletin-32-Cyber, date 03/06/2020.

[3] علي شملال، المرجع السابق، ص203.

[4] تنص الفقرة 1 من المادة 356 من القانون رقم 01-08 المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001 بأنّه: " إذا تبين من اللازم إجراء تحقيق تكميلي يجب أن يكون ذلك بحكم ويقوم بهذا الإجراء القاضي نفسه ".

2- الحكم الوقتي أو الحكم القطعي

الأول ينصب على إجراء معين تصدره المحكمة قبل الفصل في دعوى الجريمة المعلوماتية كالحكم بالإفراج المؤقت عن المتهم[1] إلى حين الفصل في الجريمة المعلوماتية متى كان حبس هذا الأخير مؤقتا غير ضروري ومهم، أمّا الثاني القطعي فهو الذي يحسم في مسألة فرعية ويكسب حجية اتجاه المحكمة التي أصدرته بحيث لا يجوز لها الرجوع عنه كالحكم بعدم اختصاص المحكمة[2] بنظر الجريمة المعلوماتية لعدم اختصاصها نوعيا أو إقليميا فيها.

الفرع الثاني: آثار الحكم على المتهم المعلوماتي من حيث قابليته للطعن

تنقسم الأحكام كأصل عام من حيث قابليتها للطعن إلى أحكام ابتدائية وأخرى نهائية، فالأحكام الابتدائية تقبل الطعن سواء بالمعارضة أو الاستئناف ما لم ينقضي ميعاد الطعن فيها، أمّا الأحكام النهائية فيرى جانب من الفقه[3] بأنّها لا تقبل الطعن أصلا سواء بطرق الطعن العادية أو غير العادية ويصبح فيها الحكم حائزا قوة الشيء المقضي فيها، أما الجانب الآخر[4] فيرى بأنّها تقبل الطعن فقط بطريق النقض واعتبر أن الأحكام الباتة هي التي لا تقبل الطعن سواء بطرق الطعن العادية أو غير العادية ويصبح فيها الحكم حائزا قوة الشيء المقضي فيها.

---

[1] تنص الفقرة 1 من المادة 128 من القانون رقم 01-08 المعدل والمتمم للأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001 بأنّه: " إذا رفعت الدعوى إلى جهة قضائية للفصل فيها أصبح لهذه الجهة حق الفصل في الإفراج ".

[2] تنص الفقرة 1 من المادة 362 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966 بأنّه: " إذا كانت الواقعة المطروحة على المحكمة تحت وصف جنحة من طبيعة تستأهل توقيع عقوبة جنائية، قضت المحكمة بعدم اختصاصها وإحالتها للنيابة العامة للتصرف فيها بحسب ما تراه ".

[3] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، المرجع السابق، ص275.

[4] عبد الرحمان خلفي، المرجع السابق، ص382.

أولا: الحكم الابتدائي في الجرائم المعلوماتية

يصدر هذا الحكم كأصل عام من جميع الجهات القضائية الجزائية محاكم الجنح والمخالفات والغرف الجزائية بالمجالس القضائية ومحكمة الجنايات الابتدائية[1]، ولما كان موضوع الدعوى العمومية هو الجرائم المعلوماتية فإنها تأخذ وصف الجنحة، فالحكم الذي يصدر حولها في الأول يكون ابتدائيا يقبل الطعن بالمعارضة والاستئناف بحسب ما إذا كان غيابيا أو حضوريا، وكقاعدة عامة يعتبر حكما ابتدائي متى كان يجوز استئنافه كأحكام البراءة أو كالأحكام التالية؛

1- الأحكام الصادرة في مواد الجنح إذا قضت على الأشخاص الطبيعية بعقوبة الحبس أو الغرامة التي تتجاوز 20000 دج أو قضت بأكثر من 100000 دج بالنسبة للأشخاص المعنوية[2]، والجريمة المعلوماتية كجنحة تدخل في هذه الطائفة.

2- الأحكام الصادرة في شؤون الأحداث[3]، خاصة وأنّه في حالات ما يكون فيها المجرم المعلوماتي طفلا.

3- قرارات محكمة الجنايات الابتدائية[4]، تدخل فيها الجريمة المعلوماتية في حالة تغير وصفها وتكييفها بأن أصبحت جناية أخرى كجريمة التخابر المتطرق إليها في الفصل السابق[5].

ثانيا: الحكم النهائي في الجرائم المعلوماتية

كنا قد أشرنا من خلال هذا الفرع للاختلاف القائم بين من يعتبر ومن لا يعتبر الحكم النهائي حكما حائزا قوة الشيء المقضي فيه، وطالما أننا تطرقنا في هذه الدراسة بما جاء به التشريع الجزائري

---

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، المرجع السابق، ص269.

[2] المادة 416 من القانون رقم 17-07، المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20، المؤرخة في 29 مارس 2017.

[3] تنص الفقرة 1 من المادة 90 من القانون رقم 15-12 المتعلق ق ح ط الجزائري، ج ر رقم 39 المؤرخة في 19 يوليو 2015 بأنّه: " يجوز الطعن في الحكم الصادر في الجنح والجنايات المرتكبة من قبل الطفل بالمعارضة والاستئناف ".

[4] الفقرة 3 من المادة 248 من القانون رقم 17-07 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[5] الفرع الرابع من المطلب الأول من المبحث الأول من الفصل الأول من الباب الثاني من هذا البحث والدراسة، ص12.

فإننا نميل لجانب الفقه الذي يرى أنّه لا وجود للحكم البات، وأنّ الحكم الجزائي الحائز قوة الشيء المقضي فيه هو حكم نهائي[1]فلا يجوز الطعن فيه بأي طريق من طرق الطعن ولا يجوز مع وجوده العودة لنفس الموضوع والوقائع ونفس الأشخاص[2]، وبالتالي لا يجوز قانونا مؤاخذة المتهم عن الجريمة المعلوماتية مرتين.

كما لا يعاد متابعة هذا المتهم المعلوماتي إن هو بُرئ قانونا أو اتهامه بالوقائع نفسها حتى ولو صيغت بتكييف آخر[3]، بل ولا يجوز متابعة أي أجنبي اقترف جريمة معلوماتية في الجزائر وأثبت بأنّه حوكم نهائيا من أجلها في الخارج وأنّه عُوقب عليها أو تقادمت أو صُدر عفوٌ عنها[4]، فالحكم النهائي بهذا المفهوم تنقضي به الدعوى العمومية[5] بالنسبة للمتهم بالجريمة المعلوماتية، فيكون حكما صادرا من الجهة القضائية المختصة وقابلا للطعن فيه إلاّ أن صاحب الحق لا يستعمل طعنه بتفويت الآجال القانونية المحددة له أو باستعمال طعنه وصدور حكم فيه، فيكتسب هذا الحكم قوة الشيء المقضي فيه ولا يجوز الطعن فيه بعد ذلك بأي طريق من طرق الطعن في الأحكام المقررة قانونا.

الفرع الثالث: آثار الحكم من حيث تواجد المتهم المعلوماتي بالجلسة

تنقسم الأحكام من حيث تواجد المتهم بالجريمة المعلوماتية في جلسة المحاكمة إلى ثلاثة أقسام حكم حضوري وحكم غيابي وآخر حضوري اعتباري وهي بالتفصيل من خلال الآتي؛

---

[1] المادة 95 من قانون رقم 15-12 المتعلق ق ح ط الجزائري، ج ر رقم 39 المؤرخة في 19 يوليو 2015، تستعمل مصطلح " الحكم النهائي " ويقابله في اللغة الفرنسية " jugements et arréts définitifs" وهو حكم يقبل الطعن بالنقض أمام المحكمة العليا، هذا ويرى الأستاذ عبد الله أوهايبية بأنّه مصطلح في غير محله في النسختين من ق ح ط باللغتين العربية والفرنسية.

[2] الفقرة 3 من المادة 1 من القانون رقم 17-07 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[3] الفقرة 2 من المادة 311 من القانون رقم 17-07 المعدل والمتمم للأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20 المؤرخة في 29 مارس 2017.

[4] المادة 589 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[5] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، المرجع السابق، ص274.

أولا: الحكم الحضوري في الجرائم المعلوماتية

يحضر فيه المتهم بالجريمة المعلوماتية جميع جلسات المرافعة بحيث يُجرى فيها عدة إجراءات للتحقيق في هذه الجريمة مع هذا المتهم، تطرقنا لها بالذكر سابقا كسماع الشهود مثلا أو الخبرة، وهذا الحكم لا يقبل الطعن بالمعارضة، وغالبا ما يحرص المشرع عليه حتى يتمكن قاضي الموضوع من تقدير العقوبة الملائمة لشخصية المتهم، كما أنّ هذا الأخير يبدي دفاعه حتى تكتشف الحقيقة[1].

ثانيا: الحكم الحضوري الاعتباري في الجرائم المعلوماتية

وهو حكم يصدر على علم من المتهم بالجريمة المعلوماتية لكن هذا الأخير لا يكون متواجدا بالجلسة أثناء النطق بالحكم، وقد أراد المشرع من خلال اعتبار هذا الحكم حضوريا التقليل من عيوب الحكم الغيابي الذي يفتح باب الطعن بالمعارضة وإطالة الإجراءات، ويكون ذلك في حالة ما؛

1- إذا كان التكليف بالحضور قد سلم شخصيا إلى المتهم المعلوماتي ولم يحضر أو لم يقدم للمحكمة عذرا مقبولا[2].

2- إذا غادر المتهم المعلوماتي باختياره قاعة الجلسة بالرغم من إجابته قبلا النداء باسمه.

3- إذا قرر المتهم المعلوماتي التخلف عن الحضور أو رفض الإجابة رغم حضوره الجلسة.

4- إذا حضر المتهم المعلوماتي إحدى الجلسات و امتنع عن الحضور للجلسات المؤجلة أو جلسة الحكم[3].

---

[1] أحمد شوقي الشلقاني، المرجع السابق، ص461.

[2] المادة 345 من الأمر رقم 69- 73، المؤرخ في 16 سبتمبر 1969 يعدل ويتمم الأمر رقم 66 – 155، يتضمن ق إ ج الجزائري، ج ر رقم 80، المؤرخة في 19 سبتمبر 1969.

[3] المادة 347 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

ثالثا: الحكم الغيابي في الجرائم المعلوماتية

لا يحضر فيه المتهم بالجريمة المعلوماتية جميع جلسات المرافعة في الدعوى الصادرة فيها ذلك أنّه لم يبلغ شخصيا بالتكليف للحضور[1]أو أنّ هذا المتهم قد قدم عذرا قبلته المحكمة ومع ذلك حكمت في الدعوى[2].

[1] المادة 346 من الأمر رقم 66-155، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

[2] أحمد شوقي الشلقاني، المرجع السابق، ص462.

الخاتمة

أخيرا وبعد دراستنا لمختلف الجوانب الإجرائية من خلال سير مراحل الدعوى العمومية التي ستطبق على الجرائم المعلوماتية في حالة ثبوت ارتكابها، وباعتمادنا كذلك على خطة ومناهج بحث تتناسب والطبيعة الدراسية لموضوع هذه الأطروحة والتي جاءت بعنوان " إجراءات سير الدعوى العمومية في الجرائم المعلوماتية " نقول وعلى الرغم من تبني المشرع الجزائري لإجراءات جديدة مستحدثة على الصعيدين المحلي والدولي تُكافح بها مختلف الجرائم المعلوماتية فإنّ المشوار لا يزال طويلا للقول بإمكانية القضاء أو على الأقل التخفيف من حدتها نظرا لطبيعتها الفنية المعقدة وشساعة فضائها الغير متحكم فيه من جهة والتأخر وعدم التحكم الواضحين في مجال الصناعة المتعلقة بتكنولوجيا المعلومات والاتصالات من جهة أخرى.

هذا وقد خلصنا من خلال هذا الموضوع ومحل هذه الدراسة إلى مجموعة من النتائج الآتية؛

- تبقى الجرائم المعلوماتية تلقي بتهديداتها نحو المستقبل ذات أنّها مرتبطة بالتطور التكنولوجي السريع لمختلف التقنيات، هذه التكنولوجيا الحديثة لا تبرز إلاّ ومعها مجموعة من الجرائم المعلوماتية الجديدة الأخرى لم تكن معروفة من قبل.
- الطبيعة الفنية للجرائم المعلوماتية كانت ولازالت تحمل في طياتها العديد من التهديدات الخطيرة على سلامة وأمن الأشخاص بصفة عامة.
- الطبيعة الفنية التي يتمتع به النظام المعلوماتي هي السبب الرئيسي وراء العديد من الجرائم المعلوماتية التي لم تكتشف بعد والتي اكتشفت إلا بعد فوات الأوان والتي لم يكتشف مرتكبوها بعد.
- تحديات جبارة وعقبات كبيرة تواجه المجتمع الدولي ككل من جراء ظهور أنواع جديدة من الجرائم المعلوماتية وزيادة عددها يوما بعد يوم.

- إنّ القول بإمكانية القضاء بصفة كلية على الجرائم المعلوماتية في الوقت الحالي يعتبر ضربا من الخيال العلمي، ربما يمكن القول بذلك مستقبلا.
- المبادئ الكلاسيكية في تطبيق النص الجزائي غير كافية في حالات كثيرة لمحاسبة المجرمين المعلوماتيين.
- لم يصل المشرع الجزائري بعد إلى إيجاد تعريف دقيق وشامل للجرائم المعلوماتية ويتجلى ذلك من خلال النصوص القانونية المتعلقة بهذه الجريمة أين أبقى على وصف الجنحة عليها وأعطى وصفا بل وتكييفا آخر لجرائم خطيرة ترتكب بوسائل إلكترونية كجريمة التخابر.
- إنّ تعريف المشرع الجزائري للجرائم المعلوماتية غير الدقيق هذا يجعل من إمكانية تحويل كل الجرائم المنصوص عليها في قانون العقوبات وفي القوانين الخاصة إلى جرائم معلوماتية إذا ما ارتكبت بوسيلة إلكترونية.
- السلطات الأمنية والقضائية المختصة في هذا النوع من الإجرام ما زالوا يفتقرون للمهارة والاحترافية الضروريتين في مجال كشف وإحباط مخططات واعتداءات المجرمين المعلوماتيين.
- عدم التبليغ وعدم تقديم الشكوى عن الجرائم المعلوماتية يبقيان من بين الأسباب الرئيسية في عدم كشف العديد منها.
- حالات التلبس تكاد تكون منعدمة في الجرائم المعلوماتية.
- إجراءات المعاينة والتفتيش والضبط في الجرائم المعلوماتية في غالبها تكون ذات طبيعة فنية خالصة سواء في مرحلة التحقيقات الأولية أو مرحلة التحقيق الابتدائي.
- الكثير من الجرائم المعلوماتية كشفت من خلال اعتماد أساليب التحريات الخاصة من اعتراض للمراسلات والتقاط للصور وتسجيل للأصوات ومراقبة للاتصالات الإلكترونية.
- غالبا يكون التصرف في نتائج التحقيقات الأولية حول الجرائم المعلوماتية بتحريك الدعوى العمومية من طرف النيابة العامة.

- التحقيق الابتدائي أهم مرحلة من مراحل الدعوى العمومية في الجرائم المعلوماتية، ذلك أنّ قاضي التحقيق يستعمل إجراءات وسلطات متنوعة وعديدة مقارنة بالمراحل الأخرى من الدعوى.
- يمتد في الجرائم المعلوماتية الاختصاص المحلي لقاضي التحقيق ووكيل الجمهورية لدى المحكمة ذات الاختصاص الموسع إلى دائرة اختصاص المحاكم الأخرى المحددة في التنظيم.
- يستطيع قاضي التحقيق من خلال التحقيق حول الجرائم المعلوماتية تطبيق الإجراءات التقليدية المطبقة على الجرائم العادية من استجواب وسماع ومواجهة وكذا تطبيق مختلف سلطاته بأوامر القبض والإيداع والرقابة القضائية بل وحتى الاستعانة بآلية تسليم المجرمين ذات الطابع الدولي.
- تصرف قاضي التحقيق في نتائج تحقيقاته حول الجرائم المعلوماتية غالبا يكون من خلال الأمر بالإحالة سواء إلى المحكمة المختصة أو إلى غرفة الاتهام، وذلك شكا منه في براءة المتهم على عكس قاضي الموضوع.
- تعتبر مرحلة المحاكمة في الجرائم المعلوماتية المرحلة النهائية من الدعوى العمومية والتي من خلالها يقوم قاضي الموضوع بتمحيص مختلف الأدلة التي أمامه خاصة الأدلة ذات الطبيعة الإلكترونية وذلك حتى يصل لحكم مبني على اليقين ومسببا تسبيبا شافيا.
- يستطيع قاضي الموضوع أن يقوم بتحقيق تكميلي حول الجرائم المعلوماتية موضوع الدعوى بناء على حكم يصدره، ويكون ذلك من خلال استجواب المتهم بالجريمة المعلوماتية وكذا سماع ومواجهة الأشخاص الداخلين في إطار الدعوى العمومية.
- لما كانت الجرائم المعلوماتية ذات طبيعة فنية في أغلبها فإنّ قاضي الموضوع وحتى قضاة التحقيق وضباط الشرطة القضائية يجدون أنفسهم مجبرين على اتباع إجراءات الخبرة ويكون قاضي الموضوع حكمه مبنيا عليها في أغلب القضايا.

- يجب أن يصدر حكم قاضي الموضوع حول الجرائم المعلوماتية عن قناعة شخصية لا يهزها الشك، لذلك عليه أن يبين الأسباب الكافية والسائغة التي تبرر صدور حكمه في الواقع والقانون على النحو الذي صدر منه وإلاّ كان الحكم معيبا ومعرضا للطعن والبطلان.
- إذا كانت واقعة الجنحة المعلوماتية من الطبيعة التي تستحق توقيع عقوبة جنائية فإنّ قاضي الحكم في هذه الحالة يقضي بعدم اختصاصه فيها ويحيلها للنيابة العامة للتصرف فيها حسبما تراه مناسبا، هذه الأخيرة التي تحيل القضية وموضوع الدعوى إلى غرفة الاتهام.
- إذا رأت غرفة الاتهام من خلال تحقيقها في واقعة الجريمة المعلوماتية بأنّها تكون جنحة فإنّها تقضي بإحالة القضية إلى المحكمة المختصة بنظرها، أمّا إذا رأت بأنّ الوقائع المنسوبة للمتهم لها وصف الجناية فإنّها تقضي بإحالة المتهم إلى محكمة الجنايات الابتدائية.
- أحسن المشرع الجزائري من خلال إصداره لنصوص إجرائية تنظم مسألتي التحقيق والمحاكمة بطريق المحادثة المرئية عن بعد، ذلك أنّها تفيد في احترام الآجال وفي ضبط الأدلة قبل اندثارها خاصة تلك المتعلقة بموضوع الدراسة والدعوى العمومية المتمثل في الجرائم المعلوماتية.
- لازال مبدأ سيادة الدول على مجال إقليمها يشكل عائقا كبيرا في مواجهة الجرائم المعلوماتية ذات الطبيعة المتعدية للحدود الإقليمية.

من خلال النتائج المتوصل إليها من هذه الدراسة الشاملة لمراحل الدعوى العمومية في موضوع الجرائم المعلوماتية نقترح بعضا من الاقتراحات والحلول الإجرائية لهذه الظاهرة ذات الطبيعة المعلوماتية الواقعة في غالبيتها ضمن العالم الافتراضي، والتي مازالت لم تكشف عن كل أسرارها وجرائمها وتهديداتها المستقبلية بعد، هذه الاقتراحات وبعض الحلول تتمثل في الآتي؛

- نقترح على المشرع الجزائري أن يجد أولا معيارا مناسبا يفرق به بين الجرائم المعلوماتية بحيث يبين الجرائم التي ترتكب بوسيلة إلكترونية والتي لا تدخل في إطار الجرائم المعلوماتية كجريمة

التخابر والجرائم التي ترتكب بوسيلة إلكترونية والتي تدخل في إطار الجرائم المعلوماتية كجرائم الغش المعلوماتي.

- النشر الإعلامي لثقافة الوعي بمخاطر الجرائم المعلوماتية وثقافة استعمال الوسائل التقنية وكذا ثقافة التبليغ عن هذه الجرائم في حينها بل وحتى نشر الأحكام الجزائية الصادرة في حق المجرمين المعلوماتيين لتحقيق نوع من الردع العام.
- يجب على الدولة الإسراع في عملية إنهاء المشاريع المتعلقة بتوطين المعلومات داخل الوطن كإجراء وقائي من مختلف الاعتداءات المعلوماتية من جهة والاستثمار بها مع دول أجنبية من جهة أخرى.
- يجب على الدول العربية والدول الإفريقية العمل معا على التصدي للجرائم المعلوماتية من خلال أولا تغيير سياستها القديمة إلى سياسة حديثة تواكب التحديات والتطلعات المستقبلية التي تلقيها تكنولوجيا المعلومات والاتصالات، وثانيا من خلال جلب الاستثمارات القوية والناجحة في مجال الوقاية من الجرائم المعلوماتية وكذا الكشف عنها وإحباط تهديداتها.
- على عاتق التشريعات العربية والتشريعات الإفريقية الوصول لسياسة تشريعية إجرائية جديدة تواكب طرق وعمليات ارتكاب هذه النوعية من الجرائم وفي نفس الوقت تحبط الاعتداءات المعلوماتية وتكشف مخططات وتهديدات المجرمين المعلوماتيين.
- على عاتق التشريعات العربية والتشريعات الإفريقية إبرام معاهدات التي من شأنها أن تحقق الانسجام بين مختلف القوانين الجزائية الوطنية وذلك من خلال اعتماد قوانين نموذجية يتسع نطاقها ليشمل غالبية الجرائم المعلوماتية.
- نقترح على المشرع الجزائري وعلى مختلف التشريعات العربية والإفريقية تبني سياسة استقطاب واستغلال الطاقات والأدمغة البشرية المحترفة في مجال المعلوماتية من خلال توفير مختلف الإمكانيات والتسهيلات المادية والمعنوية لهذه الطاقات.

- نقترح على المشرع الجزائري إعادة النظر في نص المادة 65 مكرر11 الخاصة بإجراء التسرب بأن يجعله يشمل جميع الاعتداءات المعلوماتية التي ترتكب على أو بواسطة منظومة معلوماتية.
- على المشرع الجزائري أن يرفع من عقوبات بعض الجرائم المعلوماتية الخطيرة ذلك أنّ العقوبات المنخفضة تؤدي إلى شعور المجرمين المعلوماتيين بمخاطر منخفضة.
- محاولة الدولة إبرام معاهدات واتفاقيات دولية وثنائية من شأنّها التصدي للجرائم المعلوماتية بفاعلية ولها أيضا صفة الإلزام بحيث تشكل رادعا قانونيا قويا على المستوى الدولي والإقليمي.
- نقترح على المشرع الجزائري أن يوسع من نطاق الاختصاص سواء نوعيا أو مكانيا للمحاكم الناظرة في الجرائم المعلوماتية المرتكبة خارج الإقليم الوطني الجزائري، مسايرا بذلك التشريعات المقارنة كالقانون الأمريكي والقانون الإنجليزي والقانون الفرنسي.
- نقترح على المشرع الجزائري أن يعمم إجراء الإعفاء من العقاب على الكثير من الجرائم المعلوماتية كالاحتيال أو السرقة أو النصب المعلوماتي الذي قد يقع ما بين الأصول والفروع.
- نظرا للمخاطر التي تثيرها الآن الجرائم المعلوماتية أصبح من اللازم والضروري أكثر من أي وقت مضى اعتماد وتفعيل مبدأ عالمية النص الجزائي، ذلك أنّه يتيح ملاحقة هؤلاء المجرمين المعلوماتيين ومعاقبتهم في البلد الذي يلقى القبض عليهم فيه دون مراعاة لمكان ارتكاب نوع الجريمة المعلوماتية أو جنسية المجرم المعلوماتي.

قائمة المصادر والمراجع

أولا– قائمة المصادر

1– القرآن الكريم

2– صحيح البخاري لأبي عبد الله محمد ابن إسماعيل البخاري، ط أولى، دار ابن كثير بيروت، لبنان، 2002.

3– النصوص القانونية والتنظيمية

أ– التشريع الأساسي

– قانون رقم16-01، المؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري الجزائري ج ر رقم 14 المؤرخة في 7 مارس 2016 .

– التعديل الدستوري ل 2020، الصادر وفق مرسوم رئاسي رقم 20-442، الصادر بتاريخ 30 ديسمبر 2020، ج ر رقم 82، المؤرخة في 30 ديسمبر 2020.

ب– المعاهدات والاتفاقيات الدولية

– الإعلان العالمي لحقوق الإنسان الصادر عام 1948.

– الاتفاقية الأوروبية لحماية حقوق الإنسان الأساسية الصادر عام 1950.

– الاتفاقية الدولية للحقوق المدنية والسياسية لعام 1966.

– اتفاقية شنجن عام 1990.

– اتفاقية بودابيست المتعلقة بالجرائم المعلوماتية 2001.

ت– النصوص ذات الطابع التشريعي

– أمر رقم 66-155، المؤرخ في 8 يونيو 1966، المتضمن ق إ ج الجزائري، ج ر رقم 48 المؤرخة في 10 يونيو 1966.

– أمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 49 المؤرخة في 11 يونيو 1966.

- أمر رقم 69– 76 المؤرخ في 16 سبتمبر 1969 يعدل ويتمم الأمر رقم 66 – 155 يتضمن ق إ ج الجزائري، ج ر رقم 60، المؤرخة في 19 سبتمبر1969.

- أمر رقم 69- 73، المؤرخ في 16 سبتمبر 1969 يعدل ويتمم الأمر رقم 66 – 155 يتضمن ق إ ج الجزائري، ج ر رقم 80، المؤرخة في 19 سبتمبر 1969.

- أمر رقم 75-58، المؤرخ في 26 سبتمبر 1975، يتضمن ق م الجزائري، ج ر رقم 78 المؤرخة في 30 سبتمبر 1975.

- القانون رقم 78-01، المؤرخ في 28 يناير 1978، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 6، المؤرخة في 07 فبراير 1978.

- القانون 82-03 المؤرخ في 13 فيفري 1982 يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 7، المؤرخة في 16 فيفري 1982.

- القانون رقم 86- 05 المؤرخ في 04 مارس 1986 يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 10 المؤرخة في 05 مارس 1986.

- قانون 90-24، المؤرخ في 18 أوت 1990، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 36، المؤرخة في 22 أوت 1990.

- قانون رقم 2000 – 03 المؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية ج ر رقم 48، المؤرخة في 6 غشت 2000.

- قانون رقم 01- 08 المؤرخ في 26 يونيو 2001 يعدل ويتمم الأمر 66- 155 والمتضمن ق إ ج الجزائري، ج ر رقم 34 المؤرخة في 27 يونيو 2001.

- قانون 01 – 09، المؤرخ في 26 يونيو 2001، يعدل ويتمم الأمر 66 – 156 المؤرخ في 8 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 34، المؤرخة في 26 يونيو 2001.

- قانون رقم 03 – 05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة ج ر رقم 44، المؤرخة في 23 يوليو 2003.

- قانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71، المؤرخة في 10 نوفمبر 2004.

- قانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-156 المتضمن ق ع الجزائري، ج ر رقم 71، المؤرخة في 10 نوفمبر 2004.

- قانون رقم 06– 01، المؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته ج ر رقم 14، المؤرخة في 8 مارس 2006.

- قانون رقم 06-22، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

- قانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر 66-156 المتضمن ق ع الجزائري، ج ر رقم 84، المؤرخة في 24 ديسمبر 2006.

- قانون رقم 08– 01 المؤرخ في 23 يناير 2008 يتمم ويعدل القانون 83 – 11 المؤرخ في 2 يوليو 1983 والمتعلق بالتأمينات الاجتماعية، ج ر رقم 4، المؤرخة في 27 يناير 2008.

- قانون رقم 08-09، المؤرخ في 25 فيفري 2008، المتضمن قانون الإجراءات المدنية والإدارية، ج ر رقم 21، المؤرخة في 23 أبريل2008.

- قانون رقم 09-04، المؤرخ في 5 أوت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر رقم 47، المؤرخة في 16 أوت 2009.

- قانون رقم 11– 14، المؤرخ في 2 غشت 2011، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 44، المؤرخة في 10 غشت 2011.

- قانون عضوي رقم 12– 05 المؤرخ في 12 يناير 2012، يتعلق بالإعلام، ج ر رقم 2 المؤرخة في 15 يناير 2012.

- قانون رقم 14– 01، المؤرخ في 4 فبراير 2014، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966، المتضمن ق ع الجزائري، ج ر رقم 7، المؤرخة في 16 فبراير 2014.

- أمر رقم 15-02، المؤرخ في 23 يوليو 2015، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 41 ، المؤرخة في 29 يوليو 2015.

- قانون رقم 15 – 04 المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر رقم 6، المؤرخة في 10 فبراير 2015.

- قانون رقم 15-12 مؤرخ في 15 يوليو 2015، يتعلق بح ط، ج ر رقم 39 المؤرخة في 19 يوليو 2015.

- قانون رقم 17-07، المؤرخ في 27 مارس 2017، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 20، المؤرخة في 29 مارس 2017.

- قانون رقم 18– 05 المؤرخ في 10 مايو 2018 يتعلق بالتجارة الإلكترونية، ج ر رقم 28 المؤرخة في 16 مايو 2018.

- قانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر رقم 34، المؤرخة في في 10 يونيو 2018.

- قانون رقم 19-10، المؤرخ في 11 ديسمبر 2019، يعدل ويتمم الأمر رقم 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 71، المؤرخة في 18 ديسمبر 2019.

- أمر رقم 20-03، المؤرخ في 30 غشت 2020، يتعلق بالوقاية من عصابات الأحياء ومكافحتها، ج ر رقم 51، المؤرخة في 31 غشت 2020.

- أمر رقم 20-04 المؤرخ في 30 غشت 2020، يعدل ويتمم الأمر 66-155 المتضمن ق إ ج الجزائري، ج ر رقم 51، المؤرخة في 31 غشت 2020.

- أمر رقم 21-01، المؤرخ في 10 مارس 2021، المتضمن القانون العضوي المتعلق بنظام الانتخابات، ج ر رقم 17، المؤرخة في 10 مارس 2021.

ث: التنظيمات

- المرسوم الرئاسي رقم 04- 183 المؤرخ في 26 جوان 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر رقم 41 المؤرخة في 27 جوان 2004.

- المرسوم الرئاسي رقم 04- 432 المؤرخ في 29 ديسمبر 2004 المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي ج ر رقم 36، المؤرخة في 29 ديسمبر 2004.

- مرسوم تنفيذي رقم 06– 348 المؤرخ في 5 أكتوبر 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر رقم 63، المؤرخة في 8 أكتوبر 2006.

- القرار الوزاري المشترك المؤرخ في 14 أفريل 2007 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج ر رقم 36 المؤرخة في 3 يونيو 2007.

- مرسوم رئاسي 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 رقم 53 المؤرخة في 8 أكتوبر 2015.

ثانيا– قائمة المراجع

1– قائمة المراجع باللغة العربية

أ– الكتب

- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص(الجرائم ضد الأشخاص، الجرائم ضد الأموال، بعض الجرائم الخاصة)، ط سابعة عشر، دار هومة للطباعة والنشر والتوزيع، الجزائر 2014.

- أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزئري، الجزء الثاني، د ط ديوان المطبوعات الجامعية، الجزائر العاصمة، الجزائر، 1999.

– أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الكتاب الأول، ط عاشرة، دار النهضة العربية، القاهرة، مصر، 2016.

– أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، د ط، دار النهضة العربية، القاهرة، مصر 2015.

– أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، ط ثانية، دار الثقافة للنشر والتوزيع، ، عمان ، الأردن، 2014.

– أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي دراسة مقارنة، د ط دار الجامعة الجديدة، الإسكندرية، مصر، 2018.

– أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2015.

– أشرف علي قوقزة، الوسائل الإلكترونية لارتكاب جرائم الذم والقدح والتحقير في التشريع الأردني والاتفاقيات الدولية دراسة تحليلية مقارنة، د ط، دار المناهج للنشر والتوزيع، عمان، الأردن 2017.

– أشرف محمد إسماعيل، أثر المراقبة الإلكترونية على حق العامل في الخصوصية دراسة مقارنة ط أولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2017.

– أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، ط أولى مكتبة الوفاء القانونية، الإسكندرية مصر، 2016.

– أمل لطفي حسن جاب الله، نطاق السلطة التقديرية للإدارة في مجال تسليم المجرمين دراسة مقارنة. ط أولى، دار الفكر الجامعي، الإسكندرية، مصر، 2013.

– أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنيت، د ط، دار المطبوعات الجامعية الإسكندرية، مصر، 2008.

– أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، ط أولى مكتبة الوفاء القانونية، الإسكندرية، مصر، 2016.

– أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، ط أولى مكتبة القانون الاقتصادي، الرياض، السعودية، 2015.

– بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط أولى منشورات الحبلى الحقوقية بيروت، لبنان، 2009.

– بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، د ط، دار الخلدونية، الجزائر القبة القديمة الجزائر، 2017.

– تميم بن عبد الله بن سيف التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص (قذف . سب . تشهير) وفقا للشريعة الإسلامية والنظام السعودي والقانون القطري، ط أولى، مكتبة القانون والاقتصاد، الرياض، السعودية، 2016.

– جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، ط أولى دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

– جهاد رضا الحباشنة، الحماية الجزائية لبطاقات الوفاء، ط أولى، دار الثقافة للنشر والتوزيع عمان، الأردن، 2008.

– حسني عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الانترنيت (دراسة مقارنة بين الشريعة والقانون) د ط، دار النهضة العربية، القاهرة، مصر، 2011.

– خالد داودي، الجريمة المعلوماتية، ط أولى، دار الإعصار العلمي للنشر والتوزيع، عمان الأردن 2018.

– خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، د ط، دار الفكر الجامعي، الإسكندرية، مصر، 2020.

– خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، ط أولى، دار الفكر الجامعي، الإسكندرية، مصر، 2019.

– خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، د ط، الدار الجامعية، الإسكندرية، مصر 2008.

– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط أولى، دار الفكر القانوني الإسكندرية، مصر، 2009.

– خلفي عبد الرحمان، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط ثالثة منقحة ومعدلة دار بلقيس للنشر والتوزيع، الجزائر، 2017.

– خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

– رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة ط أولى، المكتب الجامعي الحديث، الإسكندرية، مصر، 2018.

– زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011.

– سامى علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنيت، د ط، دار الفكر الجامعي الإسكندرية، مصر، 2007.

– ستان ديفيس، بناء الاقتصاد المبني على المعرفة، مؤلف جماعي بعنوان تنمية الموارد البشرية في اقتصاد مبني على المعرفة، ط أولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي الإمارات العربية المتحدة 2004.

– سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، ط ثانية المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، 1999.

– سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين دراسة مقارنة، د ط دار الجامعة الجديدة الإسكندرية، مصر، 2007.

– صابر غلاب، أصول الإثبات والمحاكمات الجنائية، د ط، دار الفكر والقانون للنشر والتوزيع المنصورة، مصر، 2017.

– ضياء عبد الله الجابر الأسدي وآخرون، أبحاث في القانون العام، د ط، منشورات زين الحقوقية بيروت، لبنان، 2013.

– ضياء مصطفى عثمان، السرقة الإلكترونية دراسة فقهية، ط أولى، دار النفائس للنشر والتوزيع، عمان، الأردن، 2011.

– طارق إبراهيم الدسوقى عطيه، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.

– طارق إبراهيم الدسوقى عطيه، الموسوعة الأمنية الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

– طارق عفيفي صادق أحمد، الجرائم الإلكترونية جرائم الهاتف المحمول، ط أولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2015.

– طاهر محمود أبو القاسم، الجرائم المعلوماتية صعوبات التحقيق فيها وكيفية مواجهتها، د ط المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2019.

– عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

– عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية في مكافحة جرائم بطاقات الائتمان الإلكترونية والتعاون الأمني الدولي حيالها، د ط، دار الجامعة لجديدة، الإسكندرية مصر 2015.

– عادل مشموشي، جرائم المعلوماتية وتحديات مسارحها الافتراضية أدواتها الإلكترونية أساليبها التقنية مقتضياتها التشريعية، ط أولى، المؤسسة الحديثة للكتاب، بيروت، لبنان 2019.

– عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، ط أولى، دار المستقبل للنشر والتوزيع عمان الأردن، 2009.

– عبد الحميد الشواربي، الإثبات الجنائي في ضوء القضاء والفقه. د ط، منشأة المعارف الإسكندرية، مصر،1996.

– عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط ثانية منقحة ومعدلة دار بلقيس للنشر، الدار البيضاء، الجزائر، 2016.

– عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الثاني، د ط، دار إحياء التراث العربي، بيروت، لبنان، 1952.

– عبد الصبور عبد القوى علي مصري، الجريمة الإلكترونية، ط أولى، دار العلوم للنشر والتوزيع القاهرة، مصر، 2008.

– عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية، ط أولى، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012.

– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، د ط دار الكتب القانونية، القاهرة، مصر، 2006.

– عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنيت في التشريعات العربية، ط أولى، دار الكتب القانونية، القاهرة، مصر 2009.

– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، ط أولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

– عبد الكريم خالد الردايدة، الظواهر الإجرامية المستحدثة وسبل مواجهتها، ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2010.

– عبد الله أوهايبية، محاضرات في قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، د ط دار هومة، الجزائر،2011.

– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، ط سادسة دار هومة، 2006.

– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، ط مزيدة ومنقحة دار هومة للطباعة والنشر والتوزيع، الجزائر العاصمة، الجزائر، 2018.

– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الثاني، ط مزيدة ومنقحة، دار هومة للطباعة والنشر والتوزيع، الجزائر العاصمة، الجزائر، 2018.

– عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام)، د ط، المؤسسة الوطنية للفنون المطبعية، الرغاية الجزائر، 2015.

– عبد الله عبد العزيز اليوسف، التقنية والجرائم المستحدثة، مؤلف جماعي بعنوان الظواهر الإجرامية المستحدثة وسبل مواجهتها، ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2014.

– عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت (الجرائم الالكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنيت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط أولى، منشورات الحبلى الحقوقية، بيروت، لبنان، 2007.

– علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، ط أولى، المؤسسة الحديثة للكتاب طرابلس لبنان، 2006.

– علي جابر الحسيناوي، جرائم الحاسوب والانترنيت، د ط، دار اليازوري للنشر والتوزيع عمان، الأردن 2009.

– علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الثاني التحقيق والمحاكمة، ط ثالثة، دار هومة، الجزائر، 2017.

– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، د ط، الدار الجامعية للطباعة والنشر بيروت، لبنان 1999.

– عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنيت، دار المطبوعات الجامعية الإسكندرية مصر 2011.

– عمرو عيسى الفقى، الجرائم المعلوماتية جرائم الحاسب الآلي في مصر والدول العربية، د ط المكتب الجامعي الحديث، الإسكندرية، مصر، 2006.

– عواطف عبد الرحمان، الإعلام والعولمة البديلة، ط أولى، العربي للنشر والتوزيع، القاهرة، مصر 2006.

– غانم مرضي الشمري، الجرائم المعلوماتية (ماهيتها، خصائصها، كيفية التصدي لها قانونيا)، ط أولى، الدار العلمية الدولية للنشر والتوزيع، عمان، الأردن، 2016.

– غسان رباح، الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، ط أولى، منشورات الحبلى الحقوقية، بيروت، لبنان، 2008.

– فريد منعم جبور، حماية المستهلك عبر الإنترنيت، ومكافحة الجرائم المعلوماتية دراسة مقارنة ط ثانية، منشورات الحبلى الحقوقية، بيروت، لبنان، 2012.

– فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، مصر 1999.

– لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي وعوامل حجية الصورة والصوت في الإثبات الجنائي، ط أولى، مركز الدراسات العربية، الجيزة، مصر، 2018.

– محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، ط أولى، الأكاديميون للنشر والتوزيع عمان، الأردن، 2014.

– محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، د ط، دار المطبوعات الجامعية الإسكندرية مصر 2003.

– محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، د ط، دار المطبوعات الجامعية الإسكندرية مصر 2004.

– محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، د ط، دار هومة للطباعة الجزائر 2008.

– محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط ثانية، دار الثقافة للنشر والتوزيع عمان الأردن.

– محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د ط دار الجامعة الحديثة، الإسكندرية، مصر، 2007.

– محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط أولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007.

– محمد سعيد عبد الرحمان، الحكم القضائي أركانه وقواعد إصداره، ط أولى، دار الفكر الجامعي الإسكندرية، مصر، 2008.

– محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنيت، ط أولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011.

– محمد عبد الرحمان عنانزه، القصد الجرمي في الجرائم الإلكترونية، ط أولى، دار الأيام للنشر والتوزيع، عمان، الأردن، 2017.

– محمد عبد الله أبو بكر، جرائم الكمبيوتر والإنترنيت (موسوعة جرائم المعلوماتية)، د ط المكتب العربي الحديث، الإسكندرية، مصر، 2007.

– محمد علي سكيكر، موسوعة الدفوع الجنائية، د ط، دار الجامعة الجديدة، مصر 2011.

– محمد حسن قاسم، مراحل التفاوض في عقد الميكنة المعلوماتية، ط ثانية، دار الجامعة الجديدة الإسكندرية، مصر، 2016.

– محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2018.

– محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، د ط، دار الجامعة الجديدة للنشر الإسكندرية، مصر،2001.

– محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، د ط ديوان المطبوعات الجزائرية، الجزائر، 1999.

– محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنيت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنيت، مرمز للدراسات العربية للنشر والتوزيع، الجيزة، مصر، 2017.

– محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط أولى، دار الثقافة للنشر والتوزيع عمان الأردن، 2009.

– محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، د ط، المكتب الجامعي الحديث، الإسكندرية، مصر 2018.

– محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط ثانية، دار النهضة العربية، القاهرة مصر، 1988.

– مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الأول، د ط، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2013.

– مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الثاني، ط خامسة، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2013.

– مزهر جعفر عبيد، شرح قانون الإجراءات الجزائية العماني، الجزء الأول، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

– مصطفى محمد موسى، التحقيق الجنائي في الجرائم المعلوماتية، ط أولى، دار الكتب القانونية مصر 2009.

– مصطفى يوسف كافي، جرائم الفساد – غسيل الأموال – السياحة – الإرهاب الإلكتروني – المعلوماتية مكتبة المجتمع العربي للنشر والتوزيع، الأردن، 2014.

– ممدوح محمد الجنبهي، منير محمد الجنبهي، أمن المعلومات الإلكترونية، د ط، دار الفكر الجامعي الإسكندرية، مصر، 2005.

– مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، د ط، دار الخلدونية، الجزائر العاصمة الجزائر، 2018.

– منير محمد الجنبهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط أولى، دار الفكر الجامعي، الإسكندرية، مصر 2018.

– منير محمد الجنبهي، ممدوح محمد الجنبهي، جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها د ط، دار الفكر الجامعي، الإسكندرية، مصر، 2004.

– مولاي ملياني بغدادي، الإجراءات الجزائية في التشريع الجزائري، د ط، المؤسسة الوطنية للكتاب، الجزائر 1992.

– نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، ط أولى منشورات الحبلى الحقوقية، بيروت، لبنان، 2005.

– ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، د ط، النشر الجامعي الحديث، تلمسان، الجزائر، 2018.

– ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2012.

– نبيلة إسماعيل رسلان، التأمين في مجال المعلوماتية والشبكات، د ط، دار الجامعة الجديدة إسكندرية، مصر، 2007.

– نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، ط ثانية، دار هومه، الجزئر، 2016.

– نظير فرج مينا، الموجز في الإجراءات الجزائية، ط ثانية، ديوان المطبوعات الجامعية، الجزائر 1992.

نظير فرج مينا، الموجز في الإجراءات الجزائية، ط ثانية، ديوان المطبوعات الجامعية، الجزائر، 1992.

– نعيم مغبغب، مخاطر المعلوماتية والانترنيت (المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن)، ط ثانية، منشورات الحبلى الحقوقية، بيروت، لبنان، 2008.

– نهلا عبد القادر المومنى، الجرائم المعلوماتية، ط أولى، دار الثقافة للنشر والتوزيع، عمان، الأردن 2008.

– هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، د ط، دار النهضة العربية مصر 1992.

– هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحسوبة د ط، دار النهضة العربية، القاهرة، مصر، 2009.

- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات – قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة، د ط دار الجامعة الجديدة الإسكندرية، مصر، 2019.

ب- الأطروحات و الرسائل

- **الأطروحات**

- براهيمي صالح، الإثبات بشهادة الشهود في القانون الجزائري، عمل مقدم لنيل شهادة الدكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر 2012.
- بلولهي مراد، بدائل إجراءات الدعوى العمومية، عمل مقدم لنيل شهادة الدكتوراه في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر 2019.
- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، عمل مقدم من أجل متطلبات نيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد تلمسان، الجزائر 2018.
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، عمل مقدم لنيل شهادة الدكتوراه في الحقوق كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر 2016.
- شرف الدين وردة، الإثبات الجنائي بالأدلة الإلكترونية دراسة مقارنة، عمل مقدم لنيل شهادة الدكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر 2017.
- عبد القادر قائد سعيد المجيدي، شكوى المجني عليه كقيد من قيود تحريك الدعوى الجزائية في القانون اليمني والقانون الجزائري، عمل مقدم لنيل شهادة الدكتوراه في القانون العام كلية الحقوق جامعة الجزائر 1، الجزائر الموسم الجامعي 2014/2013.
- عمارة فوزي، قاضي التحقيق، عمل مقدم لنيل شهادة الدكتوراه علوم، كلية الحقوق جامعة الإخوة منتوري قسنطينة، الجزائر، الموسم الجامعي 2010/2009.

- كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي عمل مقدم لنيل شهادة الدكتوراه في الحقوق كلية الحقوق، جامعة عين شمس القاهرة، مصر 2016.
- محمد علي أحمد الكواري، مسرح الجريمة ودوره في كشف غموض الجريمة، أطروحة تخرج من كلية علوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2007.

- **الرسائل**

- آمال عبد الرحمن يوسف حسن، الأدلة العلمية الحديثة ودورها في الإثبات الجنائي عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط عمان، الأردن الموسم الجامعي 2012/2011.
- أيمن عبد العال، الجرائم الإلكترونية في التشريع الفلسطيني، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية غزة، فلسطين 2013.
- بلحو نسيم، سلطة النيابة العامة في حفظ أوراق الدعوى الجزائية (دراسة مقارنة)، عمل مقدم لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر 2007.
- بلولهي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، عمل مقدم لنيل شهادة الماجستير في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر 2011.
- بندر بن منصور السعدون، ضمانات المتهم في مرحلة المحاكمة أمام ديوان المحاكمات العسكرية السعودي، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2012.

- بن لاغة عقيلة، حجية أدلة الإثبات الجنائية الحديثة، عمل مقدم لنيل شهادة الماجستير تخصص قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر1، الجزائر 2012.
- حسين العلمي، دور الاستثمار في تكنولوجيا المعلومات والاتصالات في تحقيق التنمية المستدامة دراسة مقارنة بين ماليزيا وتونس والجزائر، عمل مقدم لنيل شهادة الماجستير كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة فرحات عباس سطيف 1، الجزائر2013.
- سعيد بن عبد الله بن بدوي الكناني الزهراني، الاستجواب والمواجهة في نظام الإجراءات الجزائية السعودي، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2008.
- خالد بن محمد المهوس، الاستجواب الجنائي وتطبيقاته في النظام الإجرائي السعودي عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2003.
- زايد بن عبد الرحمن الطويان، الأمر بحفظ الدعوى بعد التحقيق والقرار بأن لا وجه للسير فيها (دراسة مقارنة)، عمل مقدم لنيل شهادة الماجستير في العدالة الجنائية تخصص التشريع الجنائي الإسلامي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية الرياض، السعودية 2004.
- سعيد ظافر ناجي القحطاني، الضوابط المهارية في محاضر جمع الاستدلالات وآثارها في توجيه مسار التحقيق (دراسة تطبيقية على قضايا متنوعة بمدينة الرياض)، عمل مقدم لنيل شهادة الماجستير في العلوم الشرطية التحقيق والبحث الجنائي، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2004.
- عبد الرزاق مقران، ضمانات المشتبه فيه أثناء حالة التلبس، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة قسنطينة 1، الجزائر 2014.

- محمد الأخضر مالكي، حقوق المجني عليه في الدعوى العمومية، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الإخوة منتوري قسنطينة الجزائر، الموسم الجامعي 2009/2008.

ت- المقالات

- إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون، العدد الثلاثون، الجزء الثاني جامعة الأزهر بطنطا، مصر، 2015.

- أحمد غراب، ضرورة التمييز بين مصطلحي الاختصاص والصلاحية في المجال القانوني، مجلة العلوم الاجتماعية والإنسانية، المجلد 18، العدد 37، جامعة باتنة 1 الحاج لخضر، الجزائر ديسمبر 2017.

- أسامة العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، مجلة الحقوق، العدد 4، كلية الشريعة والدراسات الإسلامية، جامعة الكويت، الكويت، 2015.

- الفحلة مديحة، حقوق المتهم أثناء الاستجواب في الشريعة الإسلامية والقانون الجزائري، مجلة لبدر، المجلد 8، العدد 2، جامعة بشار، الجزائر، فبراير 2016.

- أسامة العبيدي، الجهود الدولية في مكافحة الجرائم المعلوماتية، مجلة الحقوق، العدد 4، كلية الشريعة والدراسات الإسلامية، جامعة الكويت، الكويت، 2015.

- أشرف محمد عبد القادر سمحان، كفاية المظاهر الخارجية للتلبس للنهوض بدلائل الاتهام والآثار التي يرتبها القانون على توافرها، مجلة دراسات علوم الشريعة والقانون، المجلد 46، العدد 3 كلية الشريعة والقانون، جامعة الجوف، السعودية، 2019.

- بدر الدين شبل، الاختصاص الجنائي العالمي ودوره في تفعيل العدالة الدولية الجنائية، مجلة العلوم القانونية والسياسية، المجلد1، العدد 1، جامعة الوادي، الجزائر، جوان 2010.

– بحرية أسيا، دراسة تحليلية للحبس المؤقت في ظل الأمر 15-02 المعدل لقانون الإجراءات الجزائية، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 3، العدد 2، معهد العلوم القانونية والإدارية المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت، الجزائر، ديسمبر 2018.

– بوشليق كمال، أوامر قاضي التحقيق المقيدة للحرية، مجلة الدراسات القانونية والسياسية المجلد 06، العدد 02، جامعة عمار ثليجي الأغواط، الجزائر، جوان 2020.

– جميلة محلق، اعتراض المراسلات، تسجيل الأصوات، والتقاط الصور في قانون الإجراءات الجزائية الجزائري مجلة التواصل في الاقتصادة والإدارة والقانون، العدد 42، جامعة باجي مختار عنابة الجزائر، جوان 2015.

– حاليمية سفيان، بوالقمح يوسف، حصانة الدفاع في املواد الجزائية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 10، كلية الحقوق والعلوم السياسية، جامة محمد بوضياف المسيلة، الجزائر، جوان 2018.

– دايخ سامية، ضمانات المتهم أثناء الاستجواب أمام قاضي التحقيق في ظل قانون الإجراءات الجزائية الجزائري، مجلة العلوم الإنسانية، المجلد 6، العدد 1، كلية العلوم الإنسانية والعلوم الإسلامية جامعة وهران 1، الجزائر، جوان 2016.

– رابح وهيبة، التسرب في التشريع الإجرائي الجزائري، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، مجلد 1، العدد 36، جامعة القدس المفتوحة، فلسطين، حزيران 2015.

– رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية المجلد 3 العدد 2، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، جوان 2012.

– رمضاني ابتسام، تافرونت عبد الكريم، تطبيق نظام المراقبة الإلكترونية في التشريع الجزائي الجزائري، مجلة الباحث للدراسات الأكاديمية، المجلد 07، العدد 02، كلية الحقوق والعلوم السياسية جامعة باتنة الحاج لخضر، الجزائر، 2020.

– زروقي عاسية، الخبرة الجزائية ومدى سلطة القاضي الجزائي في تقديرها، مجلة معالم للدراسات القانونية والسياسية، المجلد 3، العدد 1، المركز الجامعي بتندوف، الجزائر، جوان 2019.

– زروقي عاسية، سلطة القاضي في تقدير القيمة الإثباتية لإجراءات الاستجواب، مجلة الحقوق والحريات، العدد 5، جامعة محمد خيضر بسكرة، الجزائر، 2018.

– زيكو مصطفى، عوامل السلوك الإجرامي، مجلة الحوار الثقافي، المجلد 2، العدد 1، جامعة عبد الحميد ابن باديس مستغانم، الجزائر، فبراير 2013.

– زينب بوسعيد، علانية المحاكمة الجزائية بين القاعدة والإستثناء، مجلة الحقيقة، المجلد 14 العدد 3، جامعة أحمد دراية – أدرار، الجزائر، سبتمبر 2015.

– سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية، مجلة الباحث للدراسات الأكادمية، العدد (9)، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، جوان 2016.

– سامية نوري، محمد الأمين نوري، نظام الإحالة على محكمة التنازع في التشريع الجزائري مجلة طبنة للدراسات العلمية الأكادمية، المجلد 3، العدد 1، المركز الجامعي سي الحواس بريكة، باتنة الجزائر جوان 2020.

– سدود مختار، ضوابط السلطة التقديرية للقاضي الجزائي الجزائري في تقدير الأدلة، مجلة قانون النقل والنشاطات المينائية، ، المجلد 5، العدد 1، جامعة محمد بن أحمد، وهران 2، الجزائر 2018.

– صالح جابر، خصخصة الدعوى العمومية في الفقه الإسلامي والتشريع الجزائي الجزائري المجلة الدولية للبحوث القانونية والسياسية، المجلد 04، العدد 03، جامعة الوادي، الجزائر، ديسمبر 2020.

– عبد العالي حاحة، آمال يعيش تمام، الترصد الإلكتروني كآلية للتحري عن جرائم الفساد بين متطلبات حماية الحقوق والحريات وضرورات الكشف عن الجريمة، مجلة كلية القانون الكويتية العالمية أبحاث المؤتمر السنوي الدولي الخامس، ملحق خاص، العدد 3، الجزء الثاني، أكتوبر 2018.

– عبد المجيد زعلالي، الإنابات القضائية لقاضي التحقيق، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 35، العدد 4، كلية الحقوق، جامعة الجزائر، ديسمبر 1998.

– عمر خوري، سلطات الشرطة القضائية في مواجهة الجريمة المتلبس بها، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 51، العدد 3، كلية الحقوق، جامعة الجزائر، سبتمبر 2014.

– فروحات سعيد، السلطة التقديرية للقاضي الجنائي في التعامل مع الخبرة الجنائية، مجلة الواحات للبحوث والدراسات، المجلد 9، العدد 2، جامعة غرداية، الجزائر، ديسمبر 2016.

– فلاك مراد، آليات الحصول عمى الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية، مجلة الفكر القانوني والسياسي، العدد 5، كلية الحقوق والعلوم السياسية، جامعة الأغواط، الجزائر جوان 2019.

– فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، عدد 33، جامعة الإخوة منتوري قسنطينة الجزائر جوان 2010.

– فوزي عمارة، غرفة الاتهام بين الاتهام والتحقيق، مجلة العلوم الإنسانية، المجلد 19، العدد 2 جامعة الإخوة منتوري قسنطينة، الجزائر، ديسمبر 2008.

– قحموص نوال، قواعد الاختصاص القضائي بجرائم الفساد، مجلة دراسات في الوظيفة العامة المجلد 2، العدد 1، المركز الجامعي بالبيض، الجزائر، جوان 2015.

– قتال جمال، عقابوي سلمى، بدائل العقوبة السالبة للحرية – السوار الإلكتروني، مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 02، كلية الحقوق والعلوم السياسية، جامعة المسيلة الجزائر جانفي 2020.

– قودة حنان، التصدي في مرحلتي التحقيق والمحاكمة، مجلة الباحث للدراسات الأكاديمية المجلد 6، العدد 1، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة 1، الجزائر، 2019.

34– كعوان أحمد، مبدأ الفصل بين سلطتي الاتهام والتحقيق في قانون الإجراءات الجزائية الجزائري، مجلة صوت القانون، المجلد 5، العدد 1، جامعة الجيلالي بونعامة بخميس مليانة، الجزائر 2018.

35– لخذاري عبد الحق، حقوق المتهم أثناء مرحلتي التحقيق والمحاكمة في الفقه الإسلامي والقانون الجنائي الجزائري، مجلة الحقيقة، المجلد 12، العدد 26، جامعة أدرار، الجزائر، ديسمبر 2013.

– لخضر رابحي، عبد الحليم بوقرين، الإجراءات المستحدثة لمواجهة الجريمة في التشريع الجزائري مجلة دراسات وأبحاث، مجلد 1، عدد 2، جامعة زيان عاشور بالجلفة، الجزائر، جوان 2019.

– لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية ومقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد الرابع، العدد 01، جامعة العلوم الإسلامية العالمية عمان الأردن، 2017.

– لويزة نجار، نظام المثول الفوري بديل للمحاكمة بإجراءات الجنح المتلبس بها، مجلة حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، المجلد 12، العدد 26، جامعة 08 ماي 1945 قالمة الجزائر، فيفري 2019.

– ليندة شرابشة، السياسة الدولية الإقليمية في مجال مكافحة الجريمة الالكترونية الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، المجلد 1، العدد 1، جامعة زيان عاشور الجلفة الجزائر، سبتمبر 2009.

– محمد محمود عمري، الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، المجلد 12، العدد 2، الجمعية العلمية للبحوث والدراسات الاستراتيجية، كلية الحقوق أكاديمية البورك للعلوم، الدنمارك، 2016.

– مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي نشرة القضاة، العدد 66، مديرية الدراسات القانونية والوثائق، المديرية العامة للشؤون القضائية والقانونية وزارة العدل، الجزائر، الديوان الوطني للأشغال التربوية، 2011.

– مسعودان فتيحة، الدور الإيجابي للقاضي في الخبرة القضائية، مجلة الدراسات القانونية، المجلد 3 العدد 2 جامعة يحي فارس بالمدية، الجزائر، جوان 2017.

– معمري كمال، الأمر بألا وجه للمتابعة، مجلة البحوث والدراسات القانونية والسياسية، المجلد 3، العدد 2، كلية الحقوق والعلوم السياسية، جامعة البليدة 2، العفرون، البليدة، الجزائر، جوان 2013.

– مهديد هجيرة، حق المتهم في الإحاطة بالتهمة في قانون الإجراءات الجزائية الجزائري، مجلة الدراسات القانونية، المجلد 3، العدد 2، جامعة يحي فارس بالمدية، الجزائر، جوان 2017.

– مولاي عبد المالك، فنينخ عبد القادر، الدفع بعدم الاختصاص الإقليمي أمام القاضي العقاري مجلة القانون العقاري والبيئة، المجلد 7، العدد 1، جامعة بن باديس بمستغانم، الجزائر، جوان 2019.

– نبيلة أحمد بومعزة، الحماية الجزائية للشاهد في القانون الجزائري، مجلة العلوم القانونية والسياسية المجلد 10، العدد 2، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، سبتمبر2019.

– نزار العنبكي، نحو قانون جنائي دولي لجرائم المعلوماتية والانترنيت ذات الصفة الدولية، مجلة العلوم القانونية والسياسية، المجلد 5، العدد 01، الجمعية العلمية للبحوث والدراسات الاستراتيجية كلية الحقوق، أكاديمية البورك للعلوم، الدنمارك، 2013.

– يامة إبراهيم، أساليب التحري الخاصة بالجريمة المنظمة في القانونين الجزائري والفرنسي، مجلة دفاتر السياسة والقانون، المجلد 11، العدد 2، جامعة قاصدي مرباح ورقلة، الجزائر، جوان 2019.

– يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 22، العدد 2، جامعة باجي مختار عنابة، الجزائر ديسمبر.2016

2– References in foreign language

A– Books

- Aamo Iorliam, Fundamental Computing Forensics for Africam : A Case Study of the Science in Nigeria, Springer International Publishing, AG Switzerland, 2018.

- Babak Akhgar, Saskia Bayerl, Fraser Sampson, Open Source Intelligence Investigation-From Strategy to Implementation, Springer International Publishing, AG Switzerland, 2016.

- Balsing Rajput, cyber Economic Crime in India : An Integrated Model for Prevention and Investigation, Springer Nature Switzerland AG, 2020.

- Bokhari, Namrata Agrawal, Dharmendra Saini, Cyber Security Proceedings of CSI 2015, Springer Nature Singapore Pte Ltd, 2018.

- Easttom Chuck, Taylor Jeff, Computer Crime Investigation and the Law, eBook Academic, Collection Trial Boston, US, 2011.

- Eddy Willems, cyberdanger, undestanding and guarding against cybercrime, company Springer Nature Switzerland AG 2013.

- Joakim Kävrestad, Fundamentals of Digital Forensics (theory, methods, and real –life applications), second edition Springer Nature Switzerland AG 2018, 2020.

- Karen Lumsden-Emily Harmer, Online Othering Exploring Digital Violence and Discrimination on the Web This Palgrave Macmillan Springer Nature Switzerland AG 2019.

- Michael cross, scene of the cybercrime, second edition syngress publishing INC,2008.

- Robert moore, Search and Seizure of Digital Evidence LFB Scholarly Publishing, New York United States of America, 2005.

- Shipley todd, bowker art, investigating internet crimes : in introduction to solving crimes in cyberspace, Waltham, MA Syngress, 2014.

-Tim owen-jessica marshall, rethinking cybercrime critical debates, Palgrave macmillan, Cham, Switzerland AG, 2021.

13- Qianyun Wang, A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe, erasmus university rotterdam, 2016.

C- Thèses

- Ibtissem Maalaoui, Les infractions portant atteinte à la sécurité du système informatique d'une entreprise, Mémoire vue de l'obtention du grade de Maîtrise en droit (L.L.M.) option droit des affaires, Faculté des études supérieures Université de Montréal, Canada, 2011.

- Romain Boos, La lutte contre la cybercriminalité au regard de l'action des États, Doctorat de droit privé et sciences criminelles, faculté de droit sciences économique gestion Université de Lorraine, Nancy, France, 2017.

B- Articles

-Anil Kumar - Jaini Shah, The Threat of Advancing Cyber Crimes in Organizations: Awareness and Preventions International Journal of Advanced Research in Computer Science, Volume 5, numero 8, Udaipur , India, Nov-Dec 2014.

-Chuck Easttom and Jeff Taylor, Computer crime investigation, and the law, revue routledge taylor& francis group volume 13, numero 6, Royaume-Uni December 2012.

- Eoghan casey, digital evidence and forensic science computer and the internet, computer crime, 1st ed Academic press, USA, UK, 2000.

-Florence de Villenfagne, Séverine Dusollier, La Belgique sort enfin ses armes contre la cybercriminalité :A propos de la loi du 28 novembre 2000 sur la criminalité informatique Contribution à un journal/une revue, Faculte de droit, Centre de recherche information, droit et societe, Belgique, 2002 .

- Franck Guarnieri et Éric Przyswa, Cybercriminalité et expertise: enjeux et défis, revues Sécurité et stratégie, Club des Directeurs de Sécurité des Entreprises Paris, France, 2012.

- Gaudrat , droit de la preuve et nouvelles technologies de l' information, françoise gallouédec, une société sans papier nouvelles technologies de de l' information et droit de la preuve France, 1990.

-Greg Gogolin and James Jones, Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business revue Information Security Journal: A Global Perspective Copyright Taylor & Francis Group, LLC Royaume-Uni 2010.

- Gregor Urbas, cybercrime jurisdiction and extradition : the extended reach of cross-border law enforcement, journal of internet law, volume 1 6, number 1, D L A piper, Londres Royaume-Uni, july 2 0 1 2.

- Hui kai lung . Kim seung hyun . Wang Qiu hong Cyber crime deterrence and international legislation evidence from

distributed denial of service attacks, Revues MIS Quarterly, Vol. 41, Issue 2, MIS Research Center, USA Jun2017 .

- I-WAYS, Cybercrime Laws Prevention and Enforcement Capacity Builds, Digest of Electronic Commerce Policy and Regulation, IOS Press, 2003.

- MIke Nellis and Dominik Lehner, scope and definitions electronic monitoring, Council for Penological Cooperation european committee on crime problems, council of europe Strasbourg, France, October 2012.

- Milos Deset, European Standards and actual issues of the tapping in slovak criminal procedure law, Revues International Multidisciplinary Scientific Conference on Social Sciences & Arts SGEM, Vol 6, Sofia, Bulgaria, 2019.

- Tamas Gaidosch, la filiere bien structuree de la cybercriminalite revue finance &developement Washington USA, juin 2018.

- Welch Thomas, Computer crime investigation and computer forensics, Information Systems Security, Vol 6 Edition 2, Summer97 Texte intégral HTML.

-Xingan Li, Crucial Elements in Law Enforcement against Cybercrime, international journal of information security science, volume *7, Numero3,* international institute for innovation society, helsinki, finland, septembre 2018.

D– Raports

- Daue Dominique, la criminalité informatique : l'informatique, ses risques et ses dangers, Atelier des fucam à Mons, expose upch, les professions comptables face au droit penal financier, Mons, Belgique, 2010.

- Ebauche de Office des nation unies contre la drogue et le crime Vienne, Étude détaillée sur la Cybercriminalité, United nations, New York, usa, 2013.

- Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face rapport Délivré par Office des Nations unies contre les drogues et le crime, Vienne, Autriche 25-28 février 2013.

- Liang Jiansheng, Criminalite informatique, Rapport de stag Travail soumis pour l'obtention d'un Diplome Professionnel superieur en Sciences de l' information et des Bibliotheques Ecole Nationale Superieure des Sciences de 1'information et des Bibliotheques, lion, France, 1999.

- Marine valzer, La cybercriminilaté et les infractions liées à l'utilisation frauduleuse d'internet élements de mesure et d'analyse pour l'année 2014, rapport annuel de l'observatoire national de la délinquance en cas réponses pénales, France 2015.

- Mohamed CHAWKI, Essai sur la notion de cybercriminalité, IEHEI, document provient du site iehei.org Université Lyon III ,France , juillet 2006.

E- sites Internet

- https://www.asjp.cerist.dz
- https://www.alukah.net
- https://www.almaany.com
- https://www.coe.int
- https://www.droit-finances.commentcamarche.com
- https://www.dorar.net
- echhands.wordpress.com
- https://futureuae.com
- https://www.fr.scribd.com
- http://www.ijarcs.info/index.php/Ijarcs/index
- https://www.ingentaconnect.com
- https://www.interpol.int
- https://www.islamspirit.com
- https://www.google.com
- https://www.sndl.cerist.dz
- https://www.undocs.org
- https://www.vie-publique.fr

الفهرس