وزارة التعليم العالي والبحث العلمي

جامعة أحمد دراية أدرار

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة أحمد دراية.أدرار-الجزائر
Université Ahmed DRAIA. Adrar-Algérie

الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال

رسالة مقدمة لنيل شهادة الدكتوراه (LMD) في الحقوق.

تخصص: القانون الجنائي

إعداد الطالب:

التوجي محمد

إشراف الأستاذ الدكتور:

باخويا دريس

أعضاء لجنة المناقشة:

أ.د / المصري مبروك	أستاذ التعليم العالي	جامعة أدرار	رئيساً
أ.د / باخويا دريس	أستاذ التعليم العالي	جامعة أدرار	مشرفاً ومقرراً
د. كابوية رشيدة	أستاذة محاضرة "أ"	جامعة أدرار	مناقشاً
د.بن عومر محمد الصالح	أستاذ محاضر "أ"	جامعة أدرار	مناقشاً
د. مايو جيلالي	أستاذ محاضر "أ"	جامعة بشار	مناقشاً

الموسم الجامعي: 2019/2018

بسم الله الرحمن الرحيم

﴿ يَا أَيُّهَا الَّذِينَ آَمَنُوا إِذَا قِيلَ لَكُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا يَفْسَحِ اللَّهُ لَكُمْ وَإِذَا قِيلَ انْشُزُوا فَانْشُزُوا يَرْفَعِ اللَّهُ الَّذِينَ آَمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ ﴾

[المجادلة: الآية 11]

التكنولوجيا نجحت في تحديد موقعك على الأرض، تبقّى البحث عن تقنية تحدد فيها موقعك في الحياة.

جمال حسين علي

الإهـــــــداء

تضيق الكلمات وتقصر المعاني، فأنت الرقيقة والرفيقة وجنة الله على الأرض، إليك وحدك يهدى هذا العمل ... "أمي"

الطالب: التوجي محمد

شـــــــكر و عـــــرفـــان

من لا يشكر الناس لم يشكر الله، من هذا الباب أتقدم بأسمى عبارات الشكر والعرفان للبروفيسور **"باخويا دريس"** والذي كان خير عون وأوفى مرشد لإنجاز هذا العمل، والذي لم يبخل عليَّ بملاحظاته ونصائحه طيلة مدَّة انجاز هذا العمل، وفَّقَك الله لما يحب ويرضى.

والشكر موصول لكل من كان عوناً من قريب أو بعيد في انجاز هذا العمل خاصة الدكتور "شوقي نذير" و البروفيسور "منصوري المبروك" والزميل العزيز: "عثماني عبدالقادر" .

وإلى أعضاء لجنة المناقشة الكريمة لقبولهم مناقشة هذه الرسالة كل باسمه: أ. د/ المصري مبروك، د. كابوية رشيدة، د. بن عومر محمد الصالح، و د. ماينو جيلالي".

قائمـــة المختصرات:

ج.ر.ج.ج	الجريدة الرسمية للجمهورية الجزائرية
ج.ر.ج.م	الجريدة الرسمية للجمهورية المصرية
ق.ع.ج	قانون العقوبات الجزائري
ق.ع.ف	قانون العقوبات الفرنسي
ق.ع.م	قانون العقوبات المصري
ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري
ب.ط	بدون طبعة
ب.س.ط	بدون سنة طبعة
ب.ب.ن	دون بلد النشر
ط	الطبعة
ص	الصفحة
ج	الجزء
ع	العدد

مقدمـــــــــة

مقـــدمـــة

لطالما شكلت الجريمة ظاهرة اجتماعية منبوذة تقف ضد الأنظمة القانونية التي تسير النظام العام للدولة، والأعراف الخاصة بالمجتمع، فالجريمة سلوك يعكس خلل ما في شخصية المجرم الذي قد يكون مجرماً بالفطرة نظراً لتركيبته النفسية، أو حتى الجسمية على حد تعبير الكاتب الإيطالي "سيراز لومبروزو"[1]، بحيث تكون له نزعة إجرامية بالوراثة تدفعه لارتكاب جريمة ما، أو إيذاء غيره سعياً وراء التَّلذذ والبهجة، أو قد يكون مجرماً يهدف إلى الانتقام، ففي كثير من الجرائم يكون الدافع من ارتكاب الجريمة هو الانتقام وذلك بصورة فردية؛ كأن يقوم الجاني بالإعتداء على شخص معين له معه سابقة ما، أو عن طريق الانتقام من جميع المجتمع على أساس ظرف معين قد عاشه المجرم في طفولته، ولم يجد من يرشده أو يعينه عليه، مما يجعله أداة حادة تهدد كل فئات المجتمع.

ولا يمكن القول أن الجريمة وليدة عصر معين أو مجتمع محدد بعينه، فالجريمة ظاهرة وجدت على الأرض بوجود الإنسان، والذي لا شك فيه أن أول جريمة تم ارتكابها على سطح الأرض كانت هي الأخطر والأبشع من نوعها إلى وقتنا الحالي، كما لا توجد جريمة توازي في الخطورة الإجرامية جريمة القتل[2]، ولكن الشيء الذي يتغير من عصر إلى عصر هو الطريقة والأداة التي ترتكب بواسطتها الجريمة، والذي يظهر في العديد من الحالات عبقرية الإنسان ومقدرة العقل على أن يسبق الأنظمة العرفية أو القانونية في إيجاد آليات جديد متطورة وفعالة، تسهل ارتكاب الجريمة وتحد من تطبيق القانون، وهو بالفعل ما يحدث مع العديد من الجرائم التي يعجز القانون على المعاقبة عليها تطبيقاً لمبدأ الشرعية.

---

1 سيراز لومبروزو: طبيب إيطالي شهير وعالم في الجريمة ولد في سنة 1836، وتوفي سنة 1909، واضع أسس الحركة العلمية في مجال الدراسات الإجرامية، مؤسس المدرسة التكوينية والتي اهتمت بنظريات تفسير السلوك الإجرامي، وله نظريه شهيرة تعرف "بالرجل المجرم". **انـظر**: أحمد عبد اللاه المراغي، الظاهرة الإجرامية-دراسة تحليلية تأصيلية مقارنة لأسباب الجريمة-، ب. ط، مركز الدراسات العربية للنشر والتوزيع، مصر، 2018، ص 79.

2 تعتبر جريمة قتل قابيل لهابيل أو جريمة ارتكبت على سطح الأرض، ويعتبر القتل أخطر الجرائم إلى وقتنا الحالي، ولقد تطرق القرآن إلى هذه الجريمة في الآية من 27 إلى 31 من سورة المائدة، وذلك في قوله تعالى: ﴿وَاتْلُ عَلَيْهِمْ نَبَأَ ابْنَيْ آدَمَ بِالْحَقِّ إِذْ قَرَّبَا قُرْبَاناً فَتُقُبِّلَ مِن أَحَدِهِمَا وَلَمْ يُتَقَبَّلْ مِنَ الآخر قَالَ لأَقْتُلَنَّكَ قَالَ إِنَّمَا يَتَقَبَّلُ اللَّهُ مِنَ الْمُتَّقِينَ*لَئِن بَسَطتَ إِلَيَّ يَدَكَ لِتَقْتُلَنِي مَآ أَنَاْ بِبَاسِطٍ يَدِيَ إِلَيْكَ لأَقْتُلَكَ إِنِّي أَخَافُ اللَّهَ رَبَّ الْعَالَمِينَ*إِنِّي أُرِيدُ أَن تَبُوءَ بِإِثْمِي وَإِثْمِكَ فَتَكُونَ مِن أَصْحَابِ النَّارِ وَذَلِكَ جَزَآءُ الظَّالِمِينَ*فَطَوَّعَتْ لَهُ نَفْسُهُ قَتْلَ أَخِيهِ فَقَتَلَهُ فَأَصْبَحَ مِنَ الْخَاسِرِينَ*فَبَعَثَ اللَّهُ غُرَاباً يَبْحَثُ فِي الأرضِ لِيُرِيَهُ كَيْفَ يُوَارِي سَوْءة أَخِيهِ قَالَ يَا وَيْلَتَا أَعَجَزْتُ أَنْ أَكُونَ مِثْلَ هَذَا الْغُرَابِ فَأُوَارِيَ سَوْءة أَخي فَأَصْبَحَ مِنَ النَّادِمِينَ﴾.

وفي ظل التطورات التكنولوجية السريعة والإكتشافات العلمية المتلاحقة، سارع المجرمون إلى العمل على الاستفادة من هذه الأدوات بطريقة تكفل ارتكاب الجريمة بكل سهولة، ودون بذل أي مجهود عضلي، بما يضمن عدم اكتشفها أو الحصول على أدلة تدين فاعلها، ومن بين هاته الجرائم التي نتجت عن الثورة العلمية ما يعرف "بالجريمة الإلكترونية".

إن المتتبع لتطور ما يعرف بالجريمة الإلكترونية يتوقف عند ثلاثة مراحل هامة تحدد السياق التاريخي لظهور هذه الجريمة وتطورها، ويعود التأريخ للجريمة الإلكترونية من بداية ظهور الإنترنت إلى غاية السبعينات من القرن العشرين، حيث يمثل ظهور الإنترنت ساعتها ثورة في مجال تكنولوجيا المعلومات والاتصالات، واقتصرت الجريمة الإلكترونية المرتكبة وقتها على جرائم العبث بالبيانات المخزنة في الحاسوب وتدميرها سواء كانت تابعة لمؤسسات عامة أو خاصة، أما عن المرحلة الثانية فقد شهدت تنامي كبير للمعلوماتية، وظهور جرائم جديدة وخطيرة مثل اختراق الحواسيب، واختراع الفيروسات الإلكترونية التي تعمل على الاختراق والإتلاف والتدمير، فضلاً عن ظهور فئة إجرامية جديدة يطلق عليها تسمية "الهاكرز"[1].

المرحلة الثالثة تمتد من بداية التسعينات إلى وقتنا الحالي؛ وهي أكثر المراحل خطورة، فالجريمة الإلكترونية لم تعد مجرد صورة للاعتداء على نظام معلوماتي معين عن طريق استخدام الفيروسات أو غيرها من الوسائل الأخرى، إنما صارت لها أبعاد وأهداف خطيرة، فهي اليوم تعمل على إلحاق الضرر بكل الثوابت والمبادئ العامة للمجتمعات، فهي تساعد في نشر الإرهاب والمساعدة على التجنيد له، بالإضافة إلى العمل على توسيع أنشطة الجريمة المنظمة بمختلف صورها، إذ بالقدر الذي استطاعت به تكنولوجيا المعلومات والإنترنت أن تساعد في نشر التواصل والعولمة بين الناس، بقدر ما استطاعت أن تساعد في تفشي أخطر صور الإجرام بين المجتمعات، بعض النظر عن مستوى تطور هذه المجتمعات من عدمه.

1 ناجي ملاعب، الأمن السيبراني: تعريف الجرائم السيبرانية وتطورها، مقالة منشور على شبكة الإنترنت، متاح على الرابط: *http://www. sdarabia.com*، تاريخ الإطلاع: 02/ 2019/03 .

وجدير بالذكر أن من أبرز مظاهر الجريمة الإلكترونية في عصرنا الحالي؛ الجريمة الإلكترونية المرتكبة بواسطة الهاتف النقال، والتي لا تقل خطورة عن الجرائم المرتكبة بواسطة الحاسوب أو الإنترنت.

وانطلاقاً من هذه الخطورة، وإدراكاً من بعض التشريعات الغربية لها، عملت على وضع قوانين تحد من هذه الظاهرة؛ وذلك من خلال إضافة مواد عقابية تجرم هذا النوع من الجرائم على غرار كل من التشريع الفرنسي والإنجليزي والأمريكي، بينما في التشريعات العربية في غالبيتها لم تقم بتجريم توظيف الهاتف النقال في ارتكاب جريمة ما، مع وجود بعض الإستثناءات في ذلك؛ مثل المشرع الإماراتي والسعودي، بينما المشرع الجزائري لم يجرم النشاطات المرتكبة بواسطة الهاتف النقال إلا في جرائم محدد تمس الإساءة لشخص الرسول صلى الله عليه وسلم، أو المعلوم من الدين، أو الإساءة لشخص رئيس الجمهورية عن طريق استخدام الهاتف النقال.

وفي نفس السياق نجد بأن الجانب الإجرائي قد واكب هذا التطور من خلال العمل على الإستعانة بالهاتف النقال، أو غيره من الوسائط الإلكترونية الأخرى في الكشف عن الجرائم ومرتكبها، وهو ما يظهر في بعض نصوص قانون الإجراءات الجزائية الجزائري[1]، وما جاء به القانون رقم: 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[2]، والذي حدد فيه المشرع جميع الإجراءات التي يجب على سلطات التحري والتحقيق العمل بها، وهم بصدد التحقيق في جريمة ذات طابع إلكتروني، كما أن المشرع الجزائري بموجب هذا القانون عمل على تأسيس هيئة وطنية لمكافحة الجرائم ذات الطابع الإلكتروني.

وبناءً على ما ذكر؛ تظهر أهمية الدراسة من خلال عاملين أساسيين؛ الأول يتمثل في علاقة الهاتف النقال بالمجتمع حيث أصبح وسيلة التواصل الأولى في العالم، مع جهل غالبية الأفراد مخاطر

---

1 الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو 1966 المعدل والمتمم، المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 48، المؤرخة 9 يونيو 1966.

2 القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ: 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الأعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، المؤرخة 16 غشت 2009.

هاته الوسيلة، لذلك نحاول من خلال هذه الدراسة لفت نظر المجتمع إلى خطورة الهاتف النقال، بحيث يشكل تهديداً على الحياة الخاصة والاقتصادية للأفراد، مما يوجب التعامل معه بطريقة حذرة وعدم الإعتماد عليه بشكل مطلق في تخزين المعلومات السرية والهامة.

أما بالنسبة للعامل الثاني؛ فيتمثل في الفراغ التشريعي الذي يواجه الجرائم المرتكبة بواسطة الهاتف النقال في بعض الحالات، وخاصة الخطيرة منها، مما يوجب ضرورة تنبيه المشرع إلى خطورة هذه الوسيلة والأنشطة الإجرامية التي قد تنتج عنها، فضلاً عن العمل على دفع المشرع إلى استحداث قوانين خاصة بالجرائم المرتكبة بواسطة الهاتف النقال، والتي لا تتم متابعتها في معظم الأحيان، وفي حالة ما تمت متابعتها يتم تطبيق نصوص تقليدية لا تتلاءم والجريمة المرتكبة التي تأخذ الطابع الإلكتروني أكثر منه الطابع التقليدي.

ومن خلال ما سبق التطرق إليه، تطرح الدراسة الإشكالية التالية: إلى أي مدى استطاعت النصوص الجنائية التقليدية مكافحة الأنماط المستحدثة في عالم الجريمة، وخاصة تلك المرتكبة بواسطة الهاتف النقال ؟ وما مدى حاجة المجتمعات إلى نصوص جنائية معاصرة قادرة على مكافحة هذه الأنماط ؟

ويندرج تحت هذه الإشكالية التساؤلات الفرعية التالية:

- ما المقصود بجرائم الهاتف النقال، وما خصائصها التي تميزها عن باقي الأنماط الإجرامية الأخرى ؟
- فيما تتمثل صور الجرائم المرتكبة بواسطة الهاتف النقال ؟
- فيما تتمثل الإجراءات المتبعة الخاصة بالتحري والتحقيق عن الجرائم المرتكبة بواسطة الهاتف النقال ؟
- ما مدى حجية الدليل الإلكتروني في إثبات الجرائم المرتكبة بواسطة الهاتف النقال، مقارنة بحجية الأدلة التقليدية ؟

للإجابة عن هذه الإشكالية تمت الإستعانة بمجموعة من المناهج المتمثلة في: المنهج الوصفي؛ وذلك بالنظر إلى الطبيعة التقنية للموضوع، والتي تحتاج في الكثير من الأحيان الوقوف على وصف بعض الجرائم المرتكبة بواسطة الهاتف النقال، والطرق التي تتم بها هذه الجرائم؛ الأمر الذي يتطلب

الوصف الدقيق لمختلف الأجزاء والبرمجيات التي يتكون منها الهاتف النقال باعتباره الوسيلة الرئيسية لارتكاب هذا النوع من الجرائم. والمنهج التحليلي من خلال تحليل النصوص القانونية التي اعتمدنا عليها في دراستنا، والتي وجب تحليها لإظهار أوجه الصواب والقصور فيما اعتمده المشرع الجزائري من أحكام خاصة بالجرائم التي ترتكب بواسطة الهاتف النقال، فضلاً عن الآراء الفقهية التي تقتضي الضرورة في بعض الحالات تحليلها وعرض الرأي بشأنها؛ سواء من خلال الترجيح أو النقد. إضافة إلى المنهج المقارن الذي تمت الإستعانة به من أجل مقارنة الأحكام والإجراءات التي نص عليها المشرع الجزائري فيما يتعلق بالجرائم الإلكترونية، لا سيما المرتكبة منها بواسطة الهاتف النقال، ومقارنتها بما أورده التشريع المقارن في أحكامه، خاصة التشريعات ذات السبق في هذا المجال، وذلك قصد استنباط القصور لدى المشرع الجزائري وتقديم توصيات من شأنها تحسين المنظومة التشريعية الجزائرية المرتبطة بهذا النوع من الجرائم.

وعطفاً على ما سبق، تم تقسيم هذه الدراسة إلى فصل تمهيدي وبابين؛ خصص الفصل التمهيدي للأحكام العامة للجرائم المرتكبة بواسطة الهاتف النقال، وذلك من خلال دراسة المضامين المفاهيمية لتكنولوجيا الهاتف النقال في المبحث الأول، ثم للإطار المفاهيمي للجرائم المرتكبة بواسطة الهاتف النقال في المبحث الثاني.

أما بالنسبة للباب الأول؛ فقد خصص للحماية الموضوعية من الجرائم المرتكبة بواسطة الهاتف النقال، وذلك من خلال دراسة جرائم الأشخاص والأموال المرتكبة بواسطة الهاتف النقال في الفصل الأول، أما الثاني فقد خصص لدراسة جرائم الإختراق الإلكتروني بواسطة الهاتف النقال.

الباب الثاني من الدراسة تم التطرق فيه للحماية الإجرائية من الجرائم المرتكبة بواسطة الهاتف النقال، وذلك من خلال دراسة آليات البحث والتحري عن الجرائم المرتكبة بواسطة الهاتف النقال في الفصل الأول، وكذلك من خلال التعرض لأدلة الإثبات في الجرائم المرتكبة بواسطة الهاتف النقال في الفصل الثاني، وتفصيل ذلك على النحو التالي:

الفصل التمهيدي:
الأحكام العامة للجرائم المرتكبة بواسطة الهاتف النقال

الفصل التمهيدي:
الأحكام العامة للجرائم المرتكبة بواسطة الهاتف النقال

يشكل الهاتف إحدى أهم انجازات القرن الحادي والعشرون، حيث تم اختراعه على يد الأمريكي "الكسندر جراهام بل"، لتتوالى بعدها العديد من التحسينات على هذا المشروع على يد الكثير من الباحثين، ولعل من أهمهم الباحث "مارتن كوبر" الذي كان يشغل منصباً مهماً في شركة "موتورولا".

ولم يتوقف الهاتف في تطوره عند مرحلة معينة، بل واصل تطوره بتطور التقنيات المضافة إليه من حقبة زمنية إلى أخرى، بحيث شهدت تقنيات الهاتف تطورات في استخداماته وفي طرق استعماله من شخص لآخر، إلى أن أصبح يشكل علامة تجارية تمثل رأس مال كبير في الأسواق العالمية، وذلك من خلال عديد الشركات التي تتسابق في هذا المجال من أجل انجاز أهم العلامات والإصدارات، وقد صاحب هذا التطور عدة استخدامات غير مشروعة للهاتف النقال ظهرت في شكل جرائم مرتكبة بواسطته، فمنها ما هو ذو طبيعة تقليدية، ومنها ما يشكل جرائم إلكترونية حديثة، فكلما تطور الهاتف النقال وتقنياته، كلما زادت هذه الجرائم اتساعاً وخطورةً.

وعليه سنحاول من خلال هذا الفصل التمهيدي التطرق إلى المضامين المفاهيمية لتكنولوجيا الهاتف النقال (المبحث الأول)، ثم للإطار المفاهيمي للجرائم المرتكبة بواسطة الهاتف النقال (المبحث الثاني).

الـمبحث الأول:
الـمضامين الـمفاهيمية لتكنولوجـيا الهاتــف النقال

نتج عن تكنولوجيا المعلومات ما يعرف اليوم بالأمة الرقمية، التي تعتمد في تواصلها على الوسائط الإلكترونية غالباً، والتي من بينها الهاتف النقال الذي يعتبر أكثرها استعمالاً وشيوعاً بين الناس، ويعود ذلك إلى عدَة أسباب؛ من أهمها سهولة استخدامه، فهو في معظم الأحيان لا يتطلب معرفة فنية كبيرة، بالإضافة إلى خفة وزنه التي تتيح إمكانية التنقل به من مكان لآخر دون أن يسبب أي إزعاج.

لذلك ونظراً لأهميته في حياة الأفراد، نتطرق إلى مفهومه (المطلب الأول)، ثم تقنيات وشبكات الهاتف النقال (المطلب الثاني).

المطلب الأول: مفهوم الهاتف النقال.

إن الهاتف النقال كغيره من الأدوات التكنولوجية الأخرى لم يكن وليد الصدفة والعشوائية، إنما ظهر نتيجةً لجهود وأبحاث علمية مستمرة حاول من خلالها الباحثين كسر حاجز المكان والزمان، وهذا ما يجعلنا نبحث في نشأة الهاتف (الفرع الأول)، ثم نتطرق لتعريفه بعد ذلك (الفرع الثاني)، فمكونات الهاتف النقال (الفرع الثالث).

الفرع الأول: نشــأة الهاتــف.

يعود تاريخ اختراع الهاتف إلى العام 1860م حيث أجريت أول مكالمة هاتفية ناجحة، وكان ذلك على يد الألماني "فيليب رايز"، بينما يعتبر الأمريكي "الكسندر جراهام بل" أول من أنشأ نظام الهواتف، فضلاً عن تأسيسه أول شركة للتليفونات تحت مسمى: "شركة بل للتليفونات" في العام 1877م، وتم افتتاح أول مركز للهواتف عام 1978م في مدينة "نيوهافن" بولاية "كونيكتيكت" الأمريكية، وفي العام 1915 استطاع "بل" إجراء حديث هاتفي مع "توماس واتسون" بين نيويورك وسان فرنسيسكو[1].

---

1 الجمال سمير حامد عبد العزيز، المشكلات القانونية لاستخدام الهاتف النقال، مجلة الفكر القانوني والاقتصادي، المجلد 1، العدد 2، جامعة بنها، 2010، ص 209.

وشهد العام 1896م أول اختراع للاسلكي من طرف الإيطالي "ماركون"، وذلك من خلال نقل الصوت على مسافات بعيدة نسبياً دون الحاجة إلى أسلاك، وفي العام 1971م طرحت شركة "بل" أول نظام للهاتف النقال، وفي سنة 1991م بدأ استخدام النظام الرقمي للهواتف النقالة بالولايات المتحدة الأمريكية، وهو نفس العام الذي طبق فيه النظام الشامل الكوني لاتصالات الهاتف النقال في أوروبا، وهو النظام المستخدم في أغلب الدول العربية[1].

الفرع الثاني: تعريف الهاتف النقال.

من خلال هذا الفرع نتطرق إلى تحديد مصطلح الهاتف النقال من الناحية اللغوية والإصطلاحية:

أولاً– التعريف اللغوي:

كلمة هاتف مشتقة من الفعل هتَفَ، ويقال الهتف والهُتاف، وتأتي بمعنى الصوت الجافي العالي، وقيل الصوت العالي، وسمعت الصوت يهتف إذا كنت تسمع الصوت ولا تبصر أحد[2].

ثانياً– التعريف الإصطلاحي:

يعتبر تعريف الهاتف النقال من الناحية الإصطلاحية شديد التعقيد، ويرجع ذلك إلى الطبيعة التقنية للهاتف، ولذلك فإن معظم التعريفات الفقهية ما هي إلا وصف للحالة التقنية للهاتف النقال، فعُرِفَ على أنه: "الآلة التي تحول الصوت والإشارات الصحيحة الأخرى إلى الشكل الذي يمكن أن يرسل إلى المواقع البعيدة، حيث يستلمان ويعيدان الموجات إلى الإشارات الصحيحة"[3].

إن هذا التعريف يعتبر بأن الهاتف عبارة عن آلة تختص بتحويل الصوت وإشارات السماع أو الرؤية من بعيد، وذلك من خلال استلام وإعادة توجيه الموجات في إشارات صحيحة، ويؤخذ على هذا التعريف أنه جاء بسيط وركز على جانب الصوت أكثر من الجوانب الأخرى، مما يجعل هذا التعريف ينطبق على الهاتف السلكي دون الهاتف النقال ذو الميزات والخصائص المتطورة.

---

1 الجمال سمير حامد عبد العزيز، نفس المرجع، ص 10.

2 ابن منظور، لسان العرب، ج 15، ط. الثالثة، دار إحياء التراث، بيروت، ص 26.

3 قاسم حسن عبد القادر، مكافحة جرائم الهاتف النقال – دراسة تحليلية مقارنة– بحث مقدم إلى مجلس القضاء كجزء من متطلبات الترقية تم طبعه في 2012، متاح على الموقع: www.krjc.org، تاريخ الإطلاع 2018/05/05.

ويعرف الهاتف النقال أيضاً على أنه: "وسيلة اتصال لاسلكية تعمل من خلال شبكة من أبراج البث الموزعة لتغطية مساحات معينة، وتترابط فيما بينها بواسطة خطوط ثابتة وأقمار صناعية"[1].

هذا التعريف وبخلاف التعريف الأول، يشير إلى نوعية تكنولوجيا الهاتف النقال، والتي تدخل ضمن نظام الاتصالات اللاسلكية وهو ما يجعلها مختلفة عن الهاتف الثابت، فضلاً عن طريقة عمل الهاتف النقال الذي يعمل من خلال شبكة أبراج البث الموزعة لتغطية مساحات معينة، وهو ما يعرف "بشبكة التغطية".

ويعرف الهاتف النقال كذلك على أنه: "أحد أشكال أدوات الإتصال، والذي يعتمد على الإتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة ضمن مساحات معينة، ومع تطور أجهزة الهاتف الخلوي أصبحت الأجهزة أكثر من مجرد وسيلة اتصال صوتي، بحيث أصبحت تستخدم كأجهزة كومبيوتر وتصفح الإنترنت، والأجهزة الجديدة يمكنها التصوير بنفس نقاء ووضوح الكاميرا الرقمية، وكذلك يمكن إرسال الرسائل القصيرة لأي مكان في العالم"[2].

إن استقراء هذا المفهوم يؤدي بنا إلى استخلاص النتائج التالية:

- الهاتف النقال هو أحد أشكال الاتصال.
- الهاتف النقال لا يمثل وسيلة اتصال صوتية فقط، وإنما يستخدم كجهاز كومبيوتر وأداة للاتصال بالإنترنت.
- إمكانية استخدام الجهاز النقال ككاميرا، وبنفس الامتيازات التي تتوفر عليها الكاميرا الرقمية.

ومن خلال ما سبق التطرق إليه من مفاهيم للهاتف النقال، يمكن القول بأنه: "آلة تكنولوجية حديثة يتم استخدمها في الإتصال اللاسلكي، تعمل عن طريق شبكة من أبراج البث موزعة لتغطية مساحات معينة عبر خطوط ثابتة وأقمار صناعية".

---

1 سائد سعيد محمد رضوان، اعتماد الشباب الفلسطيني على صحافة الهاتف المحمول كمصدر للأخبار وقت الأزمات- دراسة ميدانية- رسالة مقدمة استكمالاً للحصول على درجة الماجستير في الصحافة، كلية الآداب، الجامعة الإسلامية، غزة، الموسم الجامعي 2016-2017، ص 78.

2 طارق عفيفي صادق أحمد، الجرائم الإلكترونية (جرائم الهاتف المحمول)، ط. الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص 14.

الفرع الثالث: مكونات الهاتف النقال.

يتكون الهاتف النقال من تركيبة مادية، وأخرى غير مادية، وهذا ما سنتناوله من خلال هذا الفرع على النحو التالي:

أولاً– المكونات المادية للهاتف النقال:

تنقسم المكونات المادية للهاتف النقال إلى مكونات مادية خارجية، ومكونات مادية داخلية:

1– **المكونات المادية الخارجية:** تظهر المكونات المادية الخارجية في جميع الأدوات التي يمكن رؤيتها بالعين المجردة، كما ترتبط هذه الأدوات بنوعية الجهاز ومظهره الخارجي والجيل الذي ينتمي إليه[1]، ومن بين الأدوات الخارجية للهاتف الخلوي، وجه الجهاز الخارجي، ظهر الجهاز، السماعة، الشاشة، الشحن، اللوحة الداخلية، المايك، قاعدة كارت سيم (SIM).

2– **المكونات المادية الداخلية:** تتمثل المكونات المادية الداخلية لجهاز الهاتف النقال في جميع الأدوات التي يحتاجها الهاتف النقال من أجل التشغيل؛ وهي عبارة عن مجموعة مقاومات ومكثفات، حيث يتم توصيلها ببعضها البعض من خلال خيوط من النحاس، تتخلل البوردة (BOARD) في السبع طبقات، مكونة ما يعرف بدوائر النظام وهي دوائر أساسية، كدائرة الصوت ودائرة الذاكرة، وتختلف البوردة في الجهاز النقال باختلاف الجهاز، والجيل الذي ينتمي إليه، ومن بين المكونات الداخلية كذلك لوحة المفاتيح الداخلية، الشاشة، السماعة، الميكرفون، الجرس الهزاز، الكاميرا وغيرها من الأدوات الأخرى التي يحتاجها الهاتف النقال[2].

ثانياً– الأجزاء غير المادية للهاتف النقال:

تشكل الأجزاء غير المادية للهاتف النقال الكيان المنطقي الذي يشغَل الهاتف النقال، ولا يختلف عن نظيره في الحاسوب الآلي، بحيث قد يظهر في شكل أنظمة وُضِعَت خصيصًا لتشغيل الهاتف النقال، أو أنظمة قد تم تصميمها للجهاز الحاسوب، ولديها قابلية للتشغيل بواسطة الهواتف النقالة الذكية، وتعرف برامج تشغيل الهاتف النقال على أنها: "مجموعة من التعليمات التي يسمح

---

1 طارق عفيفي صادق أحمد، نفس المرجع، ص 16.

2 أحمد الجابري، دروس بعنوان شرح الهاتف المحمول خطوة بخطوة، موقع نجم الإبداع، الإمارات العربية المتحدة، متاح على موقع: *http:// ngmelabdaa.own0.com/t138-topic* تاريخ الإطلاع: 25-04-2018.

بمعاينتها على دعامة مقروءة من قبل الآلة لبيان أو أداء أو إنجاز وظيفة مهمة أو نتيجة معينة صادرة عن آلة قادرة على معالجة المعلومات"[1].

وتنقسم برامج التشغيل إلى نوعين، برامج أساسية يتم تصميمها خصيصًا لتشغيل الجهاز سواء كان هاتف نقال أو حاسب آلي، أما النوع الثاني فيظهر في شكل برامج تطبيقية تهدف إلى القيام بمهام محددة[2]، ومن أمثلة هذه التطبيقات فيسبوك والماسنجر والعديد من التطبيقات الأخرى.

وفضلًا عن البرامج، تكون المعلومات[3] أحد أهم المميزات الأساسية للهواتف الذكية، ويظهر ذلك في شكل وسيط أو أداة تغطي خدمة معينة، كرسائل البريد الإلكتروني أو البريد النصي التي قد ترد أو تبعث من الجهاز، كما قد تتوفر على ميزات أخرى كالصور الرقمية ومقاطع الفيديو المخزنة.

وتختلف أهمية المعلومات باختلاف استعمالها؛ فقد تتعلق بشخص المستخدم كأن تكون ذات صبغة تجارية، وقد تتعلق بوظيفته، كما قد تتضمن أسرار قد تشكل خطراً على أمن الدولة أو المصلحة العامة، فضلًا على إمكانية احتواءها على سر تجاري لشركة معينة، مما يشكل تهديدًا لمصالحها الإبتكاريَة والاقتصادية[4].

المطلب الثانـــي: تقنيات وشبكات الهاتف النقال.

يتميز الهاتف النقال بالعديد من الميزات والخصائص التكنولوجية والتقنية، والتي عرفت تطورات عديدة تنوعت بتنوع أجيال الهاتف النقال فضلاً عن طرازه ونوعيته، ومن الميزات الأخرى التي تتحكم كذلك في الهاتف النقال هو نوع الشبكات التي تعمل على تفعيل خدمة الاتصال في الهاتف النقال، والتي عرفت تطوراً كبيراً من الجيل صفر إلى الجيل الخامس، والذي يشكل طفرة في مجال الاتصالات

---

1 سعيدي سليمة، وحجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، ط. الأولى، دار الكفر الجامعي، الإسكندرية، 2017، ص 83.

2 هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، ب. ط، دار النهضة العربية، القاهرة 2011، ص 90.

3 تعرف المعلوماتية بأنها: "مجموعة المعلومات التي يمكن تخزينها وتوليدها ونقلها بوسائل تقنية المعلومات بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز الإشارات وغيرها". **انـظر**: عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، ب. ط، دار النهضة العربية، القاهرة، 2013، ص 29.

4 طارق عفيفي صادق أحمد، المرجع السابق، ص 18.

في وقتنا الحالي، وبناءً عليه قسمنا هذا المطلب إلى فرعين، يتم التطرق من خلالها إلى تقنيات الهاتف النقال (الفرع الأول)، ثم شبكات الهاتف النقال (الفرع الثاني).

الفرع الأول: تقــنيات الهاتف النقال.

تعتبر الميزات التي يوفرها الهاتف النقال من بين أهم العوامل التي ساعدت على انتشاره بين الناس، وتفاوتت هذه التقنيات بتفاوت القدرات التنافسية بين الشركات المنتجة للهاتف النقال، لذلك نحاول من خلال هذا الفرع استعراض بعض أهم الميزات التي يتميز بها الهاتف النقال.

1- الكاميرا الرقمية:

تعتبر هذه التقنية من بين أهم الميزات التي تتوفر عليها الهواتف النقالة الحديثة، بحيث تشتغل هذه التقنية عن طريق استخدام أداة الشحنات المترابطة (Charge-Coupled Device) CCD، والتي يتم من خلالها التقاط صور وتخزينها في شكل بيانات رقمية، بدلاً من تخزينها على هيئة فيلم، كما يمكن من خلال هذه الميزة إنزال مخرجاتها وتحميلها على جهاز الحاسوب الآلي من أجل وضع اللمسات النهائية أو تخزينها، كما تتوفر على خاصية توزيعها بسهولة في هيئة ملفات حاسوبية[1].

2- خدمة الــواب "wap" برتوكول التطبيقات اللاسلكية[2]:

هو عبارة عن خدمة تتيح إمكانية الولوج للشبكة العالمية عن طريق الهاتف النقال، وتعتمد تقنية الواب على مجموعة من المواصفات الفنية تدعى برتوكول الواب "application wap wireless protocol"، وقد ساعدت هذه التقنية على انتشار الإنترنت بطريقة غير عادية بين الناس[3].

---

1 عادل عزام سقف الحيط، جرائم الذم والقدح والتحفيز المرتكبة عبر الوسائط الإلكترونية "شبكة الإنترنت وشبكة الهواتف النقال"، دراسة قانونية مقارنة، ط. الأولى ، دار الثقافة، الأردن، 2011، ص 422، **مشار إليه عند:** محمود محمد محمود جابر، الجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، ط. الأولى، المكتب الجامعي الحديث، الإسكندرية، 2017، ص 27-28.

2 يختلف **(wap)** عن **(wab)** في كون الأولى تسمح بالولوج إلى الشبكة العالمية للإنترنت عن طريق الهاتف الخلوي، بينما الثانية تتيح فرصة الولوج للإنترنت عن طريق جهاز الحاسب الآلي، وتم تصميم هذه التقنيات عن طريق استخدام لغة خاصة تسمى لغة تحديد النصوص المرتبطة HTML. **للمزيد من المعلومات انظر:** على جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة-دراسة مقارنة-، ط. الأولى، منشورات زين الحقوقية، بيروت، 2013، ص 369.

3 أسد الدين التميمي، مصطلحات الإنترنت والحاسوب: أول معجم شامل بكل مصطلحات الإنترنت متداولة وفي العالم وتعريفاتها، ط. الأولى، دار أسامة للنشر والتوزيع، عمان، الأردن، 2009، ص 111.

3- تقنية "wi fi":

اختصار لكلمة "Wireless Fidelity" والتي يقصد بها الدقة في إرسال واستقبال الموجات للاسلكية، وهو عبارة عن تقنية يتم استخدامها بواسطة جهاز الكمبيوتر المحمول والهاتف النقال من أجل الولوج للإنترنت[1].

4- خدمة الرسائل النصية القصيرة "SMS":

تتيح هذه الخاصية خدمة إرسال أي رسالة نصية وذلك في شكل أحرف وأرقام ورموز، بحيث تتضمن هذه الرسائل 160 حرفًا في الحالة العادية، وتتوقف هذه الخدمة تلقائياً في حالة ما زاد عدد الأحرف، ولكن هذا لا يلغي إمكانية إرسال رسالة بخروف أكثر من خلال استخدام تقنية الرسائل المتعددة، ومما يجب الإشارة إليه أن أول رسالة تم بعثها عبر الهاتف النقال كانت في المملكة المتحدة سنة 1992[2].

5- تقنية البلوتوث "Bluetooth":

هي عبارة عن تكنولوجيا لاسلكية حديثة ذات مواصفات عالمية تقوم بالربط بين كافة الأجهزة المحمولة مع بعضها البعض، سواءٌ كانت هاتف نقال وهاتف نقال آخر، أو جهاز حاسب آلي وهاتف نقال، وتمُكّنُ هاته التقنية من تبادل المعلومات من غير أسلاك أو كوابل أو تدخل من المستخدم[3].

6- تقنية الواي ماكس:

"WiMax" تعتبر اختصار لعبارة تقنية الموجة الواسعة اللاسلكية (Worldwide Interoperability for Microwave Acces)، ويشكل الواي ماكس أحد التقنيات الحديثة التي تستعمل كأداة للاتصال اللاسلكي عريضة المجال، وتتميز بالسرعة العالية التي تصل إلى Mbps "07" ويعتبر الواي ماكس "WiMax" امتداد لتكنولوجيا الواي فاي "Wifi"من ناحية تطور الخدمات اللاسلكية ذات الحيز الواسع، وتهدف هذه الخدمة إلى التوسع في مناطق جديدة ومسافات أطول، فضلاً عن الحد من تكلفة الوصول للمناطق البعيدة[4].

---

1 محمد عبد الله العوَا، جرائم الأموال عبر الإنترنت، ط. الأولى، دار الفتح للطباعة والنشر، الإسكندرية، 2013، ص 23.

2 جميل إطيمزي، أنظمة وأدوات التعليم الإلكتروني، ب. ط، دار فليس فليسونغ، الولايات المتحدة، 2010، ص 166.

3 خالد أقيس، استراتيجيات وطرق التدريس العامة والإلكترونية، ب. ط، المنهال، بدون بلد النشر، ص 165- 166؛ **وانظر**:

4 محمود محمد محمود جابر، المرجع السابق، ص 29.

الفرع الثاني: شبكات الهاتف النقال.

مرت شبكة الهاتف النقال بعدَة تطورات منذ ظهور الهواتف النقالة حتى وقتنا الحالي، حيث عرفت ما يسمي بشبكة الجيل صفر، والذي يمثل تكنولوجيا الهواتف المحمولة السابقة على الهواتف النقالة في سبعينيات القرن العشرين، وكانت تُستعمل معظم هذه الهواتف في المركبات والسيارات، حيث كان يعمل هذا الجيل عن طريق استخدام موجات الراديو، ومن أهم سلبيات هذا الجيل أنه محدود الموجات مما ترتب عنه عدم نقاء الصوت، فضلاً عن ضعف وفقدان الإشارة، كما عرف هذا الجيل بجيل التردد الواحد، بحيث يفقد صاحب هذا الهاتف الإتصال في حال أي حركة خارج نطاق هذا التردد[1].

وبعد الجيل الصفر ظهر جيل آخر، أُطلق عليه الجيل الأول أو ما يعرف بالنظام التناظري؛ حيث كان أول ظهور لهذا الجيل في فترة الثمانينات من القرن الماضي[2]، وعُرفت بأنظمة الهواتف الجوالة المتطورة، وحصلت على الاعتماد من مؤسسة الإتصالات الدولية fcc، وتقوم فكرة عمل هذا الجيل على استخدام ما يعرف بحوالات AMPS والتي تتسع لحد من الترددات يتراوح ما بين 824 ميجاهيرتز و894 ميجاهيرتز، وتعتبر الولايات المتحدة الأمريكية من أوائل الدول التي سعت لاستعمال هذا النظام من شبكات الهاتف النقال[3].

وقد ظهر بعد هذا الجيل ما يعرف بالجيل الثاني الذي شكل ثورة في مجال الإتصال عن طريق العديد من الميزات التي يتوفر عليها، حيث كان يعمل عن طريق تحويل الإشارات اللاسلكية لشبكاته إلى رقمية، ما أضفى عليه نوع من الجودة، وكان هذا الجيل يعمل عن طريق العديد من التقنيات والتي عرفت بـ: (TDMA)، وكذلك ما يعرف بنظام الجي اس أم (GSM) وغيرها من التقنيات الأخرى، وشهد أول ظهور للجيل الأول في أوربا في العام 1991م، وذلك كأداة تعمل على نقل الصوت دون نقل البيانات، ومن بين المشاكل التي اعترضت هذا الجيل ما يعرف بمشكلة توافق المقاييس، والذي

---

1 Mohammed Meraj, Sumit Kumar, *Evolution of Mobile Wireless Technology from 0G to 5G*, International Journal of computer Science and Technologies, Vol 6 (3) 2015, p 2546.

2 محمد أديب عنيمي، مستقبل الحاسبات، ط. الأولى، المكتبة الأكاديمية، مصر، 2001، ص 78.

3 وسام كامل ياسين العقاد، مدى إمكانية استخدام تطبيقات الهاتف النقال في تطوير العمل (دراسة حالة عيادات وكالة الغوث في قطاع غزة)، رسالة مقدمة للحصول على درجة الماجستير في تخصص إدارة الأعمال، كلية التجارة، الجامعة الإسلامية، غزة، الموسم الجامعي 2013-2014، ص 30 .

كان نتيجة لتباين ترددات كل شركة، بحيث كان التردد يتناسب مع الإمكانات المادية لكل شركة وهو ما حال دون تطور هذا الجيل[1].

تلى هذا الجيل ما يعرف بالجيل الثالث؛ والذي عمل على تطوير ميزات الجيل الثاني من خلال العديد من التحسينات التي حاول الإتحاد العالمي للاتصالات أن يضيفها ضمن ما يعرف بمشروع (IMT2000) حيث يمثل الرقم 2000 النطاق الذي جرى التوافق عليه لتغطية هذا النظام، ونظرًا للتكاليف الباهظة التي تطلبها توفير هذا النوع من الشبكات كان هناك تباين في المعايير المعتمدة في العمل بهذه الشبكات، مما انعكس على نوع المعايير المعتمدة، وآلياً الإنتقال من الجيل الثاني للجيل الثالث، فضلاً عن إسناد عمليات وضع مواصفات الفنية إلى جهتين هما: الهيئة التشاركية لتطوير الجيل الثالث للاتصالات، والهيئة التشاركية الثانية لتطوير الجيل الثالث للاتصالات[2].

وبعد النجاح الكبير الذي حققه الجيل الثالث، ظهر ما يعرف بالجيل الرابع لشبكات الهاتف النقال، والتي استندت على ما يعرف بنظام (OFDM) والذي يعمل من خلال استخدام حوامل ترددية متجاورة وعديدة لنقل الإشارة الراديوية مع العمل على توفير تحسينات أخرى تمكن من تبادل المعطيات على نطاق ترددي يصل إلى 20MHZ ويعرف الجيل الرابع بالاسم التقني التالي (Lon Term Evolution)؛ والذي يعبر عن التطور المستمر لنظم الإتصالات والذي لا يعرف حدود[3].

المطلب الثالث: أضرار الهاتف النقال.

بالرغم من الميزات الإيجابية التي استطاع الهاتف النقال أن يوفرها للإنسان، إلا أن استعماله قد رافقه وجود العديد من الأضرار على عدَّة أصعدة مختلفة –صحية، بيئية، أمنية، وعلمية– لذلك سنحاول من خلال هذا المطلب التطرق إلى بعض هذه الأضرار، والتي من ضمنها الأضرار الكهرومغناطيسية (الفرع الأول)، الأضرار الأمنية (الفرع الثاني)، الأضرار العلمية (الفرع الثالث)، ثم الأضرار البيئية (الفرع الرابع).

---

1 رائد عبدالله الشيخ، تطور شبكات الاتصال عبر الأجيال، مجلة الرياض، العدد: 15220، منشورة بتاريخ 14 فبراير 2010، متاح على الرابط: *http://www.alriyadh.com* ، تاريخ الإطلاع: 2018/05/19.

2 هشام محمد شريف عروبكي، نظم الاتصالات الخلوية، ط. الأولى، دار الكتاب العالمية، بيروت، ب. س. ط، ص 22-23.

3 هشام محمد شريف عروبكي، نفس المرجع، ص 24.

الفرع الأول: الأضرار الكهرومغناطيسية.

تعتبر الأضرار الكهرومغناطيسية من بين أكثر الأضرار التي صاحبت استعمال الهاتف النقال، والتي تنجم عن محطات وأبراج البث أو عن الهاتف النقال نفسه، ولهذه الأضرار عدة انعكاسات على صحة الإنسان، أو على الهاتف نفسه، وهذا ما سنوضحه من خلال ما يأتي:

أولاً– أضرار أبراج البث على صحة الإنسان:

إن عمليات توزيع محطات وأبراج شبكات الهاتف بشكل عشوائي على أسطح المباني، وذلك من أجل تغطية دائرة نصف قطرها بضع كيلومترات، جعلها تثير العديد من التساؤلات بخصوص أضرارها على الإنسان، وما يمكن أن تشكله من خطر على صحته، وهو ما أدى إلى تباين كبير على مستوى الدراسات في هذا المجال، خاصة وأن الكثيرين يرون[1] وجود أضرار تنبعث من الموجات التي تصدرها هذه المحطات والأبراج، التي قد تنعكس على صحة الإنسان عن طريق العديد من الأمراض الخطيرة التي قد تنجم عنها مثل مرض سرطان العين، وذلك في حال عدم مراعاة المسئولون عليها قواعد السلامة التي يجب الإحتياط لها عند وضع مثل هذه الأبراج، بحيث يجب أن تكون بعيدة بقدر كافٍ عن المدارس والمستشفيات[2].

وبالرغم من عدم ووجود أخبار مؤكدة عن خطورة أبراج شبكات الهاتف النقال، إلا أننا نجد دولة مثل ألمانيا وضعت قانوناً ينظم قياس تأثير أبراج الهواتف النقالة على الإنسان، ويلزم هذا القانون شركات الهواتف النقال في حالة إنشاء أي برج جديد تقديم معلومات تقنية دقيقة ودراستها، ووضع

---

1 في تقرير صادر على منظمة الصحة العالمية جاء فيه ما يلى: "ومع ازدياد عدد محطات الهواتف الخلوية وكذلك عدد الشبكات اللاسلكية المحلية، يزداد أيضاً تعرض السكان للإشعاع الكهرومغناطيسي المنبعث من هذه المحطات. وتشير الدراسات الحالية إلى أن تعرّض السكان للمجالات الكهرومغناطيسية من هوائيات محطات الهواتف الخلوية يتراوح ما بين 0.002 % إلى 2 % من مستويات حدود التعرض المسموح بها دولياً، ويعتمد ذلك على عوامل مختلفة مثل بعد الشخص عن هوائي المحطة وكذلك على طبيعة البيئة المحيطة. ومستوى التعرض هذا أقل أو يعادل التعرض لمستويات موجات التردد اللاسلكي المنبعثة من هوائيات البث الإذاعي أو التلفزيوني. وهناك تخوف من العواقب الصحية المحتملة من التعرض لمجالات التردد اللاسلكي الناجم عن استخدام هذه التقنيات". **انظر في ذلك:** مركز وسائل الإعلام، المجالات الكهرومغناطيسية والصحة العامة، منظمة الصحة العالمية، على الرابط: https://www.who.int ، تاريخ الإطلاع: 2019/03/20.

2 صالح أحمد محمد أللهيبي، علاقة السببية في المسؤولية المدنية عن أضرار الهاتف النقال – دراسة تحليلية–، مجلة الفكر القانوني والاقتصادي، المجلد 1، العدد 2، جامعة بنها، 2010، ص 328.

مواصفات فنية تتعلق بهده الأبراج من حيث: موجاتها، وإحداثيات تشغيلها، وأماكن إنشائها، مع إنشاء هيئة متخصصة في إصدار التراخيص الخاصة في إنشاء هذا النوع من التراخيص[1].

ثانياً– الأضرار الكهرومغناطيسية الناتجة عن استعمال الهاتف النقال على صحة الإنسان:

هناك العديد من الأضرار الناتجة عن استخدام الهاتف النقال نذكر منها:

- إحداث مشاكل للرأس، والتي تتمثل بالشعور المستمر بالصداع وعدم التركيز[2].
- الإضرار بصحة القلب والأوعية الدموية، حيث أن الإشعاعات المنبعثة من الهاتف تؤثر على كرات الدم الحمراء الحاملة للهيموجلوبين، وبالتالي تزيد من خطر الإصابة بأمراض القلب[3].
- التسبب بحدوث اضطرابات بالجهاز العصبي لجسم الإنسان؛ حيث تؤثر الموجات الكهرومغناطيسية على بعض التفاعلات التي تدور في الخلايا الحية[4].
- التسبب في تلف وقصور الحاجز الدموي للمخ الذي يمثل الحاجز الذي يقي من الجراثيم والسموم والأدوية الضارة من أن تصل للمخ أو تأثر عليه[5].
- الإضرار بالأذن، حيث أن الموجات الكهرومغناطيسية المنبعثة من الهاتف تؤثر على الأذن بشكل كبير مما قد يؤدي للإصابة بأورام العصب السمعي[6].
- يؤثر على الخصوبة: ففي دراسة للمؤسسة الطبية البريطانية رأت إمكانية تشكيل الأشعة المنبعثة من الهاتف النقال خطراً على الحيوانات المنوية لدى الرجال، وذلك من خلال الربط بين نقص الحيوانات المنوية واستخدام الهاتف النقال، وإن كانت الدراسة لم تجزم بما يقطع اليقين على اعتبار

---

1 الجمال سمير حامد عبد العزيز، المرجع السابق، ص 234.

2 علي عدنان الفيل، شرح التلوث البيئي في قوانين حماية البيئة العربية، ط. الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2013، ص 97.

3 ناسي ياسين، أضرار الهاتف المحمول على صحة الإنسان، على الرابط: *http://mawdoo3.com*، تاريخ الاطلاع 2018/03/30 .

4 صالح أحمد محمد أللهيبي، المرجع السابق، ص 227.

5 عمر علي عذاب، تأثير الهاتف النقال على صحة الإنسان، مداخلة تم إلقائها في المؤتمر الوطني للتحديات البيئية: الواقع والطموح، المعهد التقني في كلارا، العراق، 2018، ص 6.

6 عمر علي عذاب، نفس المرجع، ص 8.

أشعة الهاتف النقال هي السبب الوحيد أو الأساسي؛ خصوصاً وأن الدراسة أجريت على رجال يعانون من مشكل الإنجاب وعلى عينات مختلفة من الهواتف النقالة[1].

الفرع الثاني: أضرار الهاتف النقال الأمنية.

نتج عن استعمال الهاتف النقال العديد من الأضرار الأمنية، والتي يمكن إجمالها في:

أولاً– استخدام هواتف غير مطابقة للمواصفات الفنية والتقنية:

يشكل هذا النوع من الهواتف تهديد مباشر للأمن القومي للدول، وذلك من خلال استخدام هواتف رديئة الصنع غير مطابقة للمعايير المعمول بها دولياً، فالغالب يؤدي استخدامها إلى الإضرار بشبكة الهاتف النقال فضلًا عن توفرها على نفس الأرقام المتسلسلة المتشابهة في الغالب تكون تقليد لأرقام تسلسلية لهواتف عالمية، وهذا في الغالب يحد من تتبع حركة هذا النوع من الهواتف[2].

ثانياً– استخدام الهاتف النقال في إزعاج السلطات:

هناك الكثير من الأشخاص الذين يستخدمون الهاتف النقال بشكل لا يليق بما صنع له، ومن هذه المظاهر الإبلاغ عن أخطار وحوادث وهمية، وذلك بهدف إبعاد السلطات عن موقع معين، وقد يتمادى البعض إلى درجة التبليغ عن ووجود قنبلة في أماكن عامة، مما قد يثير الرعب في نفوس العامة، أو حتى يترتب عنه أضرار مادية[3].

ثالثاً– استخدام الهواتف النقالة في التنصت:

إن التطور الكبير في تقنيات الهاتف النقال نتج عنه سهولة الاختراق والتنصت على الأشخاص عن طريق عملية التسجيل، أو حتى التقاط الأصوات، أو غيرها من العمليات الأخرى التي قد يستخدم فيها الهاتف النقال[4].

---

1 أحمد تامر، الهواتف الذكية هل تؤثر على خصوبة الرجال؟، موقع صحتك، على الربط: *https://www.sehatok.com*، تاريخ الإطلاع: 2019/03/22.

2 الجمال سمير حامد عبد العزيز، المرجع السابق، ص 230.

3 الجمال سمير حامد عبد العزيز، نفس المرجع، ص 231.

4 عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجي الاتصالات الحديثة، ط. الأولى، منشأة المعارف، الإسكندرية، 2009، ص 661.

الفرع الثالث: الأضرار العلمية.

إن استخدام الهاتف النقال في الغش في الإمتحانات من الظواهر الغريبة والمستهجنة التي رافقت تطور الهواتف النقالة من خلال استغلاله في عمليات الغش في الامتحانات وخاصة النهائية منها، ويظهر ذلك من خلال تصوير الأسئلة بواسطة الهاتف النقال ونشرها عن طريق مواقع التواصل الاجتماعي من خلال استخدام بيانات الهاتف النقال، وهناك العديد من أمثلة ذلك في هذا الصدد منها، ما حدث في امتحان البكالوريا لسنة 2015 في الجزائر، وما صاحبه من استخدام التلاميذ للهاتف النقال المزود بشبكات الجيل الثالث، والذي وفر وقتها سرعة فائقة في الولوج إلى مواقع الإنترنت وبالتالي تسهيل عملية الغش[1].

الفرع الرابع: الأضرار البيئية.

يشكل الهاتف النقال إحدى أخطر النفايات في حال عدم استعماله، وتثير إشكالية التخلص منه صعوبة كبيرة نظراً للمواد المصنوع منها، وهذا ما يجعل الدول الأجنبية تتخلص من هذا النفايات إما عن طريق ردم النفايات في دول العالم الثالث مقابل مبالغ مالية، أو تقديم مساعدات، أو عن طريق التجارة الدولية للمنتجات الإلكترونية المستعملة[2].

1 حليمي غانية، تدابير لقمع ظاهرة الغش في الجزائر: فهل نجحت، شبكة زدني للتعليم، الجزائر، متاح على الرابط: *http://zedni.com*، تاريخ الإطلاع: 2019/03/22.

2 الجمال سمير حامد عبد العزيز، المرجع السابق، ص ص 232- 245.

المبحث الثاني:
مفهوم الجريمة المرتكبة بواسطة الهاتف النقال.

شكل الهاتف النقال حدثًا كبيرًا في عالم التكنولوجيا والاتصال بالرغم من أن هذه الوسيلة الحديثة نتج عنها عدة أضرار مَسَّت بالإنسان، ومن بين هاته الأضرار الجرائم التي باتت ترتكب عن طريق هذه الوسيلة، وهي ما يعرف بجرائم الهاتف النقال، بحيث تتراوح خطورة هذه الجريمة باختلاف مرتكب هذه الجريمة والجهة المستهدفة، ولذلك يتم التطرق من خلال هذا المبحث إلى مفهوم هذه الجريمة وتبيان خصائصها (المطلب الأول)، ثم التطرق إلى طبيعتها القانونية (المطلب الثاني).

المطلب الأول: مفهوم جرائم الهاتف النقال وخصائصها.

يشكل الوقوف على المفاهيم المتعلقة بالجريمة أياً كان نوعها، مفتاح أساسي في فهم هذه الجريمة، وخاصة جرائم الهاتف النقال التي أصبحت ظاهرة تفرض نفسها بشكل كبير في المجال القانوني أو في أروقة المحاكم، لذلك نستعرض من خلال هذا المطلب تعريف جرائم الهاتف النقال انطلاقًا من الوسيلة التي ترتكب بها (الفرع الأول)، ثم التطرق إلى خصائص جرائم الهاتف النقال (الفرع الثاني).

الفرع الأول: تعريف جرائـــم الهاتف النقال.

تعرف الجريمة بصفة عامة على أنها: "سلوك (فعل أو امتناع) غير مشروع أخل بمصلحة أساسية صادرة عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً[1]"، ويعرفها آخر[2] على أنها :" كل فعل يتنافى مع القيم السائدة في المجتمع، والذي يتبع إتيانه ردود فعل من السلطة المختصة لحماية القيم عن طريق رسائل القصر والإرغام التي توقع على مرتكبي تلك الأفعال".

ورغم التباين بين المفهومين السابقين، إلاَ أنهما يتفقان على أن الجريمة فعل منافٍ للقانون والقيم السائدة في المجتمع، يطبق على مرتكبه عقوبة من قبل السلطات المختصة وفقاً لإجراءات وشروط معينة من أجل حماية النظام والقيم.

---

1 أحمد إبراهيم الزعارير، مدخل إلى علم الجريمة، ط. الأولى، دار البيروني للنشر والتوزيع، عمان، 2015، ص 28.

2 أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، ط. الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2014، ص 42.

أما بخصوص جرائم الهاتف النقال فتعرف على أنها: "كل فعل ينشأ عن استخدام غير مشروع للتقنية الاتصالية أو المعلوماتية للهاتف المحمول بهدف الاعتداء على مصلحة الغير"[1].

والملاحظ على هذا التعريف أنه جاء مختصراً وغير دقيق، حيث وصف جرائم الهاتف النقال بالاستخدام غير المشروع للوسائل الإتصالية أو المعلوماتية عامةً، كذلك نص على أن تكون المصلحة المهددة هي مصلحة الغير لا مصلحة متعلقة بالجاني في حد ذاته.

من جانب آخر، تُعرف جرائم الهاتف النقال أيضاً بأنها: "السلوك الإجرامي الذي ينسب إلى أحد الجناة نتيجة ارتكابه أحد الأفعال غير المشروعة عبر الفضاء الإلكتروني بالاستعانة بإحدى الخدمات المعلوماتية المضافة لجهاز الهاتف المحمول، أو إمكانيات الإتصال المتاحة له – سواء إمكانية الإتصال بشبكة الانترنت أو بشبكة اتصال الهاتف – ويترتب عليه إلحاق الأذى بشخص طبيعي أو معنوي في ماله أو جسده أو اعتباره"[2].

وما يؤخذ على هذا التعريف أنه جاء بصيغة موسعة نسبياً، مركزاً على اعتبار الجريمة المرتكبة بواسطة الهاتف النقال جريمة متعلقة بالفضاء الإلكتروني عن طريق استخدام وسائل المعلوماتية المتعلقة بالهاتف، وذلك من خلال إمكانيات الإتصال المتاحة في الهاتف النقال، كما أشار التعريف إلى الأشخاص التي يلحقها الضرر من هذا النوع من الجرائم، وهما الشخص الطبيعي والمعنوي على حدٍ سواء، بالإضافة إلى نوع الضرر الذي ينتج عن هذا النوع من الأفعال، بحيث قد يكون الضرر مادي (مالي، أو جسدي) أو معنوي كتشويه سمعة شخص ما.

الفرع الثاني: خصائص الجرائم المرتكبة عــبر الهاتف النقال.

تتميز الجريمة المرتكبة بواسطة النقال بعدة خصائص، بالرغم من أن هذه الخصائص لا تختلف كثيراً عن خصائص الجريمة الإلكترونية، ويرجع هذا الأمر إلى أن كلا الجريمتين تتم في الفضاء الإلكتروني وبوسائل إلكترونية، ويمكن حصر هذه الخصائص فيما يلــي:

1 محمود عمر محمود، المسؤولية الجنائية الناتجة عن جرائم المحمول (دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية)، رسالة مقدمة لنيل درجة الدكتوراه، جامعة عين شمس، الموسم الجامعي 2011، ص 13.

2 طارق عفيفي صادق أحمد، المرجع السابق 2015، ص 33.

1- جرائم تـــتميز بقلة العنف فـــي تنفيذها:

بحيث لا يتطلب هذا النوع من الجرائم استخدام القوة والعنف كما هو عليه الحال في الإجرام التقليدي، وإنما يتطلب نوع من الذكاء والحيلة في القيام بالجريمة[1]، ومثال ذلك ما يتم من خلال جريمة الإتجار بالبشر، ففكرة تجنيد ضحايا الجريمة يتم اليوم عن طريق الوسائط الإلكترونية بطرق احتيالية، وإما عن طريق عروض عمل زائفة في مواقع إلكترونية مشبوهة، أو عن طريق مواقع الزواج المنتشرة عبر مواقع التواصل الاجتماعي[2].

2- صعوبة اكتشاف الجريـــمة:

يعتبر هذا النوع من الجرائم من الأفعال الإجرامية صعبة الإثبات، وذلك بالنظر إلى سهولة تدمير الأدلة من طرف الجاني بسرعة فائقة، فضلاً عن عملية ارتكاب الجريمة والتي غالباً ما تتم من خلال الربط بين عدة وسائل تكنولوجية؛ كأن يتم التحكم في الجهاز الآلي عن طريق الهاتف المحمول الذكي، بالإضافة للأسباب السابقة قد تنعدم الخبرة الفنية والعلمية لدى السلطات المناط بها مهمة التحقيق والبحث عن هذا النوع من الجرائم، ناهيك عن إحجام المجني عليه عن التبليغ عن هذا النوع من الجرائم، وذلك كأن يكون المجني عليه مؤسسة مالية، أو شركة، أو مشروعاً صناعياً ضخماً، فمن باب عدم خسارة سمعتها لدى زبائنها تلجأ هذه المؤسسات إلى ترضية زبائنها، وتحجم عن التبليغ[3].

3- سرعة التطور فـــي ارتكاب الجريمة:

يمتاز هذا النوع من الجرائم بالتطور السريع في أدوات ارتكابها، بحيث كلما توصلت التكنولوجيا إلى أداة أو وسيلة حديثة إلا واستعملها الجناة في ارتكاب جرائمهم الخطيرة إذا لم يكن اختراع هذه الأدوات من هذه المجموعات الإجرامية في حد ذاتها، كما أن مرتكبي هذه الجرائم يستفيدون من هذه الوسائل عن طريق تبادل الخبرات الإجرامية[4].

---

1 محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، ط. الثانية، دار النهضة العربية، مصر، 2009، ص 39.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 197.

3 محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط. الأولى، دار الثقافة للنشر والتوزيع ، الأردن، 2004، ص 165-166.

4 محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، ب. ط، أكاديمية الشرطة، مصر، 2016، ص17.

4- تمتع مرتكبي هذه الجرائم بالخبرة والذكاء فـي وسائل الاتصال والمعلوماتية:

يتطلب هذا النوع من الجرائم أن يتمتع أصحابها بقدرة فائقة من الذكاء والخبرة الفنية في وسائل الاتصال والمعلوماتية[1]، وهذا ما يجعل مجموعات الإجرام المنظم تستعين وتضم هذا النوع من الفئات إلى كيانها، من أجل استغلال ذكاءهم وخبراتهم الفنية في القيام بأعمالهم الإجرامية.

5- إخـفاء الجريمة:

بالنظر لطبيعة الوسائل التي ترتكب بها هذه الجرائم فهي تتسم بالخفاء، حيث أن المجني عليه لا يلحظ ارتكاب هذه الجريمة رغم اتصاله بالشبكة أو استخدامه للوسيلة المحترفة إلا بعد مدة زمنية من وقوع الجريمة، وفي بعض الأحيان لا يكتشف حتى وقوعها، ويعود سبب هذه الخاصية نظراً للخبرة الفنية والمعرفة الكاملة بهذه الوسائل لدى الجاني[2].

6- جرائـم سهلة الارتكاب:

يطلق على الجرائم التي ترتكب بالوسائل التقنية الجرائم الناعمة أو جرائم ذوي الياقات البيضاء، وذلك باعتبار أن هذا النوع من الجرائم لا يتطلب الجهد العضلي ولا حتى أي سلوك مادي، بحيث أنه يكفي أن تتوفر لدى الجاني وسائل التقنية اللازمة للفعل، وينتج عن هذه السلوكيات إغراء المجرمين للقيام بهذا الفعل، وذلك بالنظر لسهولة القيام بالجريمة بالإضافة إلى المنفعة والمكسب المادي والمعنوي الكبير الذي ينتج عن هذه الجريمة[3].

7- جريـمة عابـرة للـدول:

بالنظر إلى طبيعة المجتمع الرقمي الذي جعل من الكرة الأرضية قرية صغيرة يخترق فيها الزمان والمكان دون أن تخضع لحرس الحدود، حيث تتيح وسائل الإتصال الحديثة لمستخدميها التنقل المعنوي بين كافة القارات والدول بدون أدنى صعوبات أو عوائق، ونتج عن هذه الخاصية العديد من الإشكالات، لعل أبرزها الدولة صاحبة الإختصاص القضائي في الجريمة بالإضافة إلى كافة الإجراءات الأخرى للمتابعة القضائية [4].

---

1 محمد إبراهيم سعد النادي، جرائم الإنترنت بين الشريعة الإسلامية والقوانين الوضعية-دراسة مقارنة-، ط. الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2017، ص 29.

2 أحمد محمد عبد الرؤوف المنيفي، السرقة الإلكترونية وحكمها في الإسلام، واد أي كتب، لندن، 2018، ص 41- 42.

3 أسامة أحمد المناعسة، وجلال محمد الزعبي، المرجع السابق، ص 97.

4 على جعفر، المرجع السابق، ص 98.

المطلب الثانـي: طبيعة جرائم الهاتف النقال.

شكل الهاتف النقال وسيلة تكنولوجية حديثة كان الغاية منها كسر حاجز العزلة بين البشر، إلا أن الإستعمال الخاطئ لهذه الوسيلة نتج عنه استعانة أصحاب النوازع الإجرامية به في ارتكاب عديد الجرائم، الأمر الذي يدفع إلى البحث عن الطبيعة القانونية للجريمة المرتكبة بواسطة الهاتف النقال، والتي قد تظهر في شكل جرائم أشخاص (الفرع الأول)، أو جرائم أموال (الفرع الثاني) أو جرائم ماسة بأمن الدولة والآداب العامة (الفرع الثالث).

الفرع الأول: جرائم الهاتف النقال جرائم أشخاص.

سهل الهاتف النقال ارتكاب العديد من الجرائم التي تصنف على أنها جرائم أشخاص، ولعل من أبرز هذه الجرائم، جريمة السب والقذف، وجرائم الإيذاء المُبهج، وجرائم الإعتداء على الخصوصية، وهذه الجرائم بطبيعتها يمكن ارتكابها بعدة طرق؛ فالهاتف النقال ساهم في انتشارها بشكل أوسع، والملاحظ أن بعض التشريعات مثل التشريع الجزائري بموجب القانون رقم 06-23 في المادتين 296 و297، وقانون العقوبات المصري رقم 58 لسنة 1938 المعدل والمتمم في المادة 311 وما يليها، حافظا على نفس السياسة الجنائية فيما يخص هذه الجرائم، حيث يتحتم على هذه التشريعات مواكبة هذا التطور بنصوص تشير صراحة إلى ارتكاب هذه الجرائم بواسطة التقنيات الحديثة.

الفرع الثاني: جرائم الهاتف النقال جرائم أموال.

تعتبر جرائم الأموال من بين أكثر الجرائم التي تقع بواسطة الهاتف النقال، كما هو الحال في جرائم السرقة والنصب وغسيل الأموال، أو عن طريق الإعتداء على الهاتف في حد ذاته، وهو ما يظهر في العديد من الصور الإجرامية الأخرى كالإتلاف والسرقة، وتأخذ جرائم الأموال المرتكبة بواسطة الهاتف النقال عدة أبعاد خطيرة؛ أبرزها الإضرار بالإقتصاد الوطني، والأمن المالي، خاصة إذا تعلق الأمر بالتجارة الإلكترونية أو غيرها من المعاملات التي يمكن القيام بها بواسطة الهاتف النقال[1].

الفرع الثالث: جرائم الهاتف النقال الماسة بأمن الدولة والآداب العامة.

تعتبر الجرائم الماسة بأمن الدولة من أكثر الجرائم التي يتم ارتكابها بواسطة الهاتف النقال خاصة الأجهزة المتطورة منها، حيث شهد العالم العديد من عمليات التجسس والإختراق التي يتم

---

1 محمود محمد محمود جابر، المرجع السابق، ص 41.

ارتكابها بواسطة أجهزة الهاتف النقال، فضلاً عن جرائم الإرهاب والاتصال بالعدو، وإثارة الفتن والتحريض عليها، والجرائم الماسة بالوحدة الوطنية، وتهديد السلامة العامة، كما أن هناك العديد من الجرائم التي تكيف على أنها جرائم مخلة بالآداب العامة التي يمكن ارتكابها بواسطة الهاتف النقال، من بين هذه الجرائم جريمة التحرش وجرائم الترويج للدعارة، وجرائم استغلال الأطفال في أنشطة جنسية غير مشروعة[1].

وعليه من خلال ما تم التطرق له في هذا الفصل، والذي حاولنا من خلاله عرض أهم التطورات التي وصل إليها الهاتف النقال، وبيان أهم الأضرار التي نتجت عن ذلك، منها الأضرار الماسة بصحة الإنسان وهي الأخطر على الإطلاق، وذلك عن طريق الموجات الكهرومغناطيسية التي تصدر عن أبراج ومحطات الهاتف النقال، أو حتى عن طريق الهاتف النقال في حد ذاته، ومن الأضرار الأخرى كذلك التي تطرقت إليها الدراسة بنحو من التفصيل؛ الأضرار الأمنية، والتي لا تقل خطورة عن سابقتها من حيث مسها بسمعة وأمن البلاد من عدَة جوانب حساسة، بالإضافة إلى الأضرار البيئية والتي يمكن أن تنجم عنها العديد من النتائج غير المحمودة العواقب.

وفضلاً عما سبق، تم التطرق كذلك إلى الجريمة المرتكبة بواسطة الهاتف النقال من خلال بيان مفهوم هذا النوع من الجرائم، وأهم الخصائص التي تتميز بها عن غيرها من الجرائم الأخرى، بالرغم من أنها لا تختلف كثيراً عن غيرها من الجرائم الإلكترونية. من جانب آخر، تم التطرق إلى طبيعة الجرائم المرتكبة بواسطة الهاتف النقال، والتي تنوعت بين جرائم الأشخاص، وجرائم الأموال، والجرائم الماسة بأمن الدولة والآداب العامة.

1 محمود محمد محمود جابر، نفس المرجع، ص 42.

الباب الأول:
الحماية الموضوعية من الجرائم المرتكبة بواسطة الهاتف النقال

الباب الأول:

الحماية الموضوعية من الجرائم المرتكبة بواسطة الهاتف النقال.

إن الأهمية الكبيرة للهاتف النقال في الحياة اليومية جعلته وسيلة التواصل الأولى في العالم، إذ يكاد لا يوجد إنسان لا يملك هاتف نقال في وقتنا المعاصر، حيث نتج عن هذه الوفرة أن الهاتف النقال أصبح جزءً لا يتجزأ من نمط حياتنا اليومية، نشارك به كل الأعمال والأحداث، وخاصة بعد ربطه بشبكة التجوال عبر الإنترنت، وعكس هذا التطور جوانب سلبية عديدة؛ منها ما كان له علاقة بالأشخاص فتمثل في صورة اعتداء على الأشخاص، وظهرت بذلك جرائم مستحدثة أخذ الهاتف حيزاً كبيراً من المشاركة في ارتكابها، وأخرى تقليدية لكنها تطورت بتطور هذه الآليات وزادت خطورتها بمساعدة هذه الأدوات، وهو نفس الشيء الذي ينطبق على جرائم الأموال التي حاول مرتكبيها الإستعانة بهذه الوسائل في ارتكاب جرائم تتفاوت في الخطورة والجسامة بين جرائم بسيطة، وأخرى منظمة.

وعَكس هذا التطور مدى هشاشة الأنظمة الحماية الإلكترونية للتكنولوجيا الحديثة، بحيث باتت جرائم المعلوماتية والقرصنة من بين أهم الجرائم الخطيرة التي تعرف تزايداً وحداثة في أدواتها يوم بعد آخر، ذلك أن الهاتف النقال عن طريق ما يوفره من تقنيات حديثة أصبح يشكل خطراً على الأشخاص نتيجة المساس بالآخرين وبحياتهم الشخصية من خلال الاعتداءات الكثيرة التي قد لا يسع الضحية في بعض الحالات حيالها إلا السكوت، إما لعدم معرفته بتجريم الفعل، أو لعدم معرفته بوقوع الفعل باعتبار أن هذا الفعل من الأفعال التي يتطلب مهارة فنية في الكشف عنها.

وبناءً على ما ذُكر أعلاه، سنتطرق في هذا الباب إلى الحماية الموضوعية من الجرائم المرتكبة بواسطة الهاتف النقال من خلال دراسة بعض أهم الجرائم التي تطرق إليها المشرع الجزائري أو غيره من التشريعات الأخرى بنوع من التحليل، لذلك قسمنا هذا الباب إلى فصلين؛ تمت فيهما دراسة الجرائم الماسة بالأشخاص والأموال، ودور الهاتف النقال في ارتكاب هذه الجرائم (الفصل الأول)، ثم التطرق إلى جرائم الإختراق الإلكتروني بواسطة الهاتف النقال (الفصل الثاني).

الفـصل الأول:

جرائــم الهاتف النقال الـماسة بالأشــخاص والأمــوال.

لقد نتج عن استخدام الهاتف النقال بطريقة غير مشروعة العديد من الظواهر اللاأخلاقية والتي حاولت المساس بالأشخاص في أعراضهم وحرياتهم الشخصية وأموالهم، فلم يتوقف الأمر عند حادثة واحدة أو اثنتان، وإنما تفاقم بشكل كبير لينتشر بسرعة فائقة، خاصة بين الشباب والمراهقين، بحيث تبدأ هذه الظواهر بشكل عادي تهدف من خلاله هذه الفئة من الشباب والمراهقين إلى تحقيق المتعة والتسلية، متناسين خرق قواعد الخصوصية وحرية الآخر، وفي بعض الأحيان يذهب الأمر إلى أبعد من ذلك، خاصة ما إذا كان الضحية في حالة خطر حيث يكتفي البعض بالتصوير والنشر.

ولقد تنوعت الجرائم المرتكبة ضد الأشخاص والأموال بواسطة الهاتف النقال في الخطورة والجسامة، بحيث تعتبر جرائم الأشخاص المرتكبة بواسطة الهاتف النقال أقل جسامة وضرر من جرائم الأموال، ذلك أن معظم جرائم الأشخاص المرتكبة ضد الأفراد ما هي إلا جرائم تقليدية استعان أصحابها في تنفيذها بوسائل التقنية الحديثة، ومن أمثلة هذه الجرائم السب والقذف والاعتداء على الخصوصية، أما فيما يخص جرائم الإيذاء المُبهج فهي جرائم يمكن تكييفها على أنها جرائم تقنية حديثة باعتبار أن الفعل لا يمكن تصوره إلا من خلال اعتماد الجاني على واسطة تكنولوجية يمكنها التقاط الصور وتسجيل الفيديوهات.

أما بالنسبة لجرائم الأموال فهي لا تختلف عن جرائم الأشخاص من حيث طابعها؛ فهي في الأساس جرائم تقليدية يمكن ارتكابها بدون الوسائل الإلكترونية، إلا أن استعانتها بهذه الأدوات زاد من الأضرار التي يمكن أن تنتج عنها، فضلاً عن اتساع نطاق هذه الجريمة، فقد تأخذ بعد عالمي أكثر منه وطني، ومن صور هذه الجرائم، جريمة السرقة والنصب وجرائم غسيل الأموال المرتكبة بواسطة الهاتف النقال.

ومن خلال ما سبق سنتناول في هذا الفصل جرائم الأشخاص المرتكبة بواسطة الهاتف النقال (المبحث الأول)، وجرائم الأموال المرتكبة بواسطة الهاتف النقال (المبحث الثاني).

المبحث الأول:

جرائـــم الأشخاص المرتكبـة بواسطـــة الهاتـف النـقال.

إن الإستغلال السلبي لتكنولوجيا الاتصالات الحديثة أثر على العديد من الأنماط المتعلقة بحياة الأشخاص، فالإنسان اليوم بالرغم من استفادته من هذا التطور إلا أنه قد يدفع ثمن ذلك من خصوصيته أو حياته الشخصية، حيث أصبح الهاتف النقال وسيلة اتصال تتيح للقراصنة التعدي على أعراض الناس وعلى حياتهم الشخصية دون إلقاء بالٍ للنتائج التي قد تنجم عن هذا النوع من الأفعال، ونظراً لهذه الخطورة تم تقسيم هذا المبحث إلى جرائم الإيذاء المبهج (المطلب الأول)، ثم جرائم الإعتداء على الخصوصية باستخدام الهاتف النقال (المطلب الثاني).

المطلب الأول: جرائـــم الإيـذاء المُبهِج.

يُعتبرُ مصطلح جرائم الإيذاء المبهج مصطلح جديد نسبياً، وقد ارتبط بما يعرف بالجرائم ذات الطابع الرقمي التي تعتمد على آلة رقمية أو إلكترونية في ارتكابه، ولعل من بين أكثر هذه الوسائل استخداماً في ارتكاب هذه الجريمة الكاميرا الرقمية، غير أنه بالنظر إلى التطور الهائل الذي وصل له الهاتف النقال من خلال توفره على عديد الخصائص التي سبق الإشارة إليها في الفصل التمهيدي، أضحى بمثابة الوسيلة الأولى لارتكاب هذه الجريمة، لذلك سنحاول من خلال هذا المطلب التطرق إلى مفهوم جرائم الإيذاء المبهج (الفرع الأول)، ثم السلوك الإجرامي للجريمة (الفرع الثاني)، والعقوبة المقررة لها (الفرع الثالث)، ثم تقييم المسلك الفرنسي (الفرع الرابع)، وموقف المشرع الجزائري (الفرع الخامس).

الفرع الأول: مفهوم جرائـــم الإيـذاء المبهج.

بالنظر إلى حداثة هذا الموضوع من حيث الطرح تحاول الدراسة من خلال هذا الفرع الوقوف على بعض النقاط المهمة التي تساعد على فهم الفلسفة العامة التي تقوم عليها هذه الجريمة، من خلال تقديم لمحة تاريخية عنها، ثم تعريفها فضلاً عن التطرق إلى طبيعتها القانونية.

أولاً– لـمحة تاريـخيـة عن الإيـذاء المبهج:

تقوم فلسفة الإيذاء المبهج على القيام بإيذاء شخص معين من خلال الإعتداء عليه جسدياً أو جنسياً، ثم القيام بتصوير فيديو لهذا الاعتداء على أساس نوع من الترفيه أو المرح، وأول ظهور لهذه

الظاهرة كان في بريطانيا، حيث ظهر في سنة 2004 شريط باسم "SLAP TV" يحتوي هذا الشريط على مشاهد اعتداء تم تسجيلها، وحظي هذا الشريط على نسب مشاهدة عالية باعتباره برنامج تليفزيوني، بعدها بمدَة أشارت جريدة "Times" البريطانية من خلال تقرير تم نشره عن وجود ظاهرة إجرامية مستحدثة في ملحقها التربوي بتاريخ 2005/01/21، وذلك من أجل إتاحة الفرصة للمعلمين والتربويين للإطلاع عليه[1].

وفي الوقت الذي شغلت فيه هذه الظاهرة المجتمع في بريطانيا تعددت أسباب تفسيرها، بين من يرجعها إلى عدم وجود سبب أو دافع حقيقي لوجود هذه الظاهرة سوى الضحك والمرح، أو أن الملل هو الذي يدفع إلى القيام بمثل هذا السلوك، أو إلى محاولة الربط بينها وبين عدد من البرامج التي كانت تذاع وقتها مثل برنامج "Jackkas" و"Bumfights" و"Dirtysanche" والتي استلهم منها المشاهدون ظاهرة العنف والاعتداء، أو تفسيرها على أنها جرائم مستحدثة يسعى أصحابها من خلالها إلى التقاط فيديوهات تحتوي على الكثير من العنف والعدوانية[2].

ولم تتوقف هذه الظاهرة في الحدود البريطانية فقط، وإنما امتدت لتشمل دول أخرى مثل فرنسا وشمال أمريكا، ومن أبرز القضايا ما حدث في إحدى المدارس الفرنسية في سنة 2005، حيث قام أحد الجناة باغتصاب ضحيته، ثم لجأ إلى نشر الفيديو داخل المدرسة من أجل إيذاء ضحيته[3]، وفي واقعة مغايرة سنة 2006 قام أحد التلاميذ بالاعتداء على معلمته، فيما قام زميله الآخر بتصوير الواقعة[4].

---

1 فتيحة محمد قوراري، أحكام جرائم الإيذاء المبهج – دراسة تحليلية مقارنة لجرائم مستحدثة تتعلق بالهواتف النقالة–، مداخلة مقدمة لمؤتمر الجوانب القانونية والإقتصادية للهاتف المحمول، المنعقد بتاريخ 27-2010/04/28، في كلية الحقوق، جامعة بنها، القاهرة، ص 9.

2 محمود محمد محمود جابر، المرجع السابق، ص 382-383.

3 طارق عفيفي صادق أحمد، المرجع السابق، ص 173.

4 محمود محمد محمود جابر، نفس المرجع، ص383، ومن القضايا الشهيرة كذلك في هذا الصدد ما يعرف بقضية فتاة الباندا، والتي وقعت في دولة السعودية في عام 2004، حيث تتلخص وقائعها في أن شاب سعودي برفقة شاب من أفريقيا، حيث قام هذا الأخير بالإعتداء على شابة سعودية في الثامنة عشر من العمر، بينما قام الشاب السعودي بتصوير هذا الفيديو بجهاز نوكيا الذي كان يعرف وقتها بـ: (الباندا 6600) ثم عمل على نشر الفيديو من خلال هاتفه النقال عبر التقنيات الإرسال والنشر التي يحتوي عليها هذا الجهاز، ولعل هذه القصة من بين أهم الدوافع التي جعلت الدول الخليجية تقوم بوضع قانون خاص

وبعد تفشي هذه الظاهرة على نطاق واسع في فرنسا، كان المشرع الفرنسي السبّاق في سن تشريع يهدف إلى تجريم هذه الأفعال اللاأخلاقية، والتي باتت تهدد الإستقرار في المجتمع الفرنسي، وذلك من خلال القانون رقم: 297-2007 المؤرخ 5 مارس 2007، والذي يهدف للوقاية من الإجرام، حيث أجازه المجلس الدستوري الفرنسي بتاريخ: 03 مارس 2007، ومن خلال هذا القانون أصبح المشرع الفرنسي يعاقب على هذه الجرائم بنصوص خاصة، ويرجع الفضل في تشريع هذا القانون إلى وزير الداخلية الفرنسي آنذاك "NICOLAS SARKOZY"، والذي طالب بالبحث عن آليات ردعية جديدة تكون على قدر جسامة هذا الفعل[1].

ثانياً– تعريف جرائم الإيذاء المبهج:

يعرف البعض[2] جرائم الإيذاء المبهج على أنها: "تلك الممارسة المتمثلة في تصوير أو تسجيل مقاطع فيديو يُوثقُ الإعتداء على شخص يستوي أن يكون جسدياً أو جنسياً أياً كانت جسامته، وبأي وسيلة كانت، وعلى أي دعامة كانت، ثم نشر هذه الصور أو مقاطع الفيديو على الوسائط الإلكترونية".

ومن خلال تحليل التعريف السابق، نلاحظ أنه قدَّم تعريف شامل لجرائم الإيذاء المبهج من خلال ذِكر مفصل للصور التي يمكن حدوثها في حال تمت هذه الجريمة، وذلك في حال ما إذا قام الجاني "بتصوير أو تسجيل مقطع".

ويعرفه البعض الآخر[3] على أنه: "تصوير فعل الإعتداء الجسدي أو الجنسي على المجني عليه بغرض نشره والاستمتاع برؤيته".

وعليه يشير هذا التعريف إلى النشاط الإجرامي الناتج عن التصوير، مما قد يجعل السلوك الإجرامي للإيذاء المبهج محصوراً في فعل التقاط الصور دون تسجيل مقطع فيديو.

بالجرائم المعلوماتية والإتصال. **انـــظر**: علي عبد الله، "برجس": المقطع الذي أطلق أول شرارة لــ: "فضائح البلوتوث" في السعودية، جدة، متاح على الرابط:*archive. Aawsat.com*، تاريخ الإطلاع: 2018/06/30.

1 فتيحة محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج –دراسة تحليلية مقارنة لجرائم مستحدثة تتعلق بالهواتف النقالة–، مجلة الشريعة والقانون، المجلد 24، العدد 42، 2010، جامعة الشارقة، ص 237.

2 فؤاد بن الصغير، بحث بعنوان أركان جريمة الإيذاء المبهج في حالة اغتصاب فتاة حافلة البيضاء، متاح على الرابط: *http://m.hespress.com*، تاريخ الإطلاع: 2018/07/01 .

3 طارق أحمد صادق عفيفي، المرجع السابق، ص 171.

كما أشار كلا التعريفين إلى نقطة جوهرية؛ وهي أن الإيذاء المبهج ناتج عن جريمة أصلية تقليدية، وذلك من خلال إشارة كلا التعريفين إلى عملية "توثيق الاعتداء"، وهو ما جاء في التعريف الأول، بينما أشار التعريف الثاني إلى تصوير فعل الاعتداء الجسدي أو الجنسي، ويختلف التعريف الأول عن الثاني في ذكر الغاية من الفعل الإجرامي حيث نص التعريف الثاني على ذلك بقوله: "بغرض نشره والاستمتاع برؤيته"، بينما غاب عن التعريف الأول ذكر الهدف أو الغاية من هذه الجريمة.

ومن خلال ما سبق يمكن تعريف جريمة الإيذاء المبهج بأنها: سلوك غير قانوني يقوم به الجاني من خلال تصوير أو تسجيل مقاطع بنفسه أو بمساعدة غيره في حال اعتداءه جسديًا أو جنسيًا على الضحية، وفي الغالب يكون عن طريق استعمال الهاتف النقال.

ومن المرجح أن الوسيلة الأكثر استعمالاً في هذه الجريمة هي الهاتف النقال، وذلك لعدَة اعتبارات أهمها:

- الهاتف النقال مزود بتقنيات ووسائل حديثة كالكاميرا الرقمية.
- احتواء الهاتف النقال على خدمة الإنترنت، مما يسهل إمكانية نشر الفيديو بسرعة وانتشاره بين الناس.
- القدرة على وضع بث مباشر لوقائع الاعتداء، وذلك من خلال استخدام بيانات الهاتف وخدمة البث المباشر التي تحتوي عليها بعض التطبيقات في الهاتف النقال.
- سهولة التنقل بالهاتف النقال، مما جعله يحل مكان العديد من الأجهزة الرقمية الأخرى.

ثالثاً– الطبيعة القانونية لجريمة الإيذاء المبهج:

تثور العديد من الخلافات فيما يخص الطبيعة القانونية لجرائم الإيذاء المبهج، وهو ما سنحاول التطرق إليه على النحو الآتي:

1. **الرأي الأول:**

يرى أنصار هذا الرأي ضرورة إخضاع جرائم الإيذاء المبهج لجرائم المساهمة التبعية[1]، ويسند أصحاب هذا الاتجاه إلى عدة حجج منها[1]:

---

1 من بين الذين أسسوا لهذا الرأي " أعضاء الجمعية الوطنية الفرنسية" وذلك في إطار مناقشتهم للقانون الذي قضي بتجريم ظاهرة تصوير وقائع الاعتداء ونشرها، انظر: طارق عفيفي صادق أحمد، المرجع السابق، ص 174.

- اعتبار هذا النشاط أو السلوك الإجرامي من قبيل الأعمال التبعية التي تأتي على هامش السلوك الإجرامي الأصلي، ومنه فهذه الجرائم هي عبارة عن نشاطات تبعية.
- تطابق مقومات هذا النشاط مع الشروط التي يتطلبها الإشتراك في الجريمة، من حيث ضرورة تعدد الجناة (اثنان أو أكثر)، فضلاً عن وحدة الجريمة والهدف الإجرامي.
- كما يرى أصحاب هذا الإتجاه أن الإشتراك القائم في هذه الصورة، يعد اشتراك بالمساعدة باعتبار أن النشاط الذي قام به نشاط سلبي وليس إيجابي، وهذا يتعارض مع ما هو معمول به في النصوص التقليدية للإشتراك وفقاً لقانون العقوبات[2].

وحتى نكون أمام حالة الإشتراك وفقاً لهذا الرأي، يجب أن تتوافر الشروط الآتية[3]:

- عدم وجود تحريض أو صفة المحرض لدى القائم بفعل التصوير والنشر، بمعنى أن يقوم بالفعل دون أن يدفعه أحدهم إلى القيام بهذا الفعل.
- أن يكون هذا الإلتقاط أو التصوير استغلال لموقف عرضي؛ حيث أن المجرم شاهد الفعل الأصلي بمحض الصدفة فقام باستغلال تواجده في مسرح الجريمة فسجل وقائعها.
- أن يشكل فعل الجاني دعماً معنوياً للجُناة في حال ارتكابهم لجريمتهم، وهذا ما عملت به محكمة النقض الفرنسية في أحد أحكامها الصادر بتاريخ 20 يناير 1992، حيث تتلخص وقائع هذه القضية في أن المتهمة تنتمي إلى مجموعة إجرامية، وأنها وقت ارتكاب شركاؤها لجريمتهم اكتفت بمشاهد السلوك الإجرامي للجريمة والمتمثل في وقائع العنف المرتكبة، مما أثبت قصدها الجنائي وانضمامها كلياً للقصد الجنائي للمجموعة الإجرامية، بحيث رأت المحكمة أنها دعمت الجناة معنوياً في ارتكابهم لجريمتهم[4].

---

1 فتيحة محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج، المرجع السابق، ص 241.

2 تنص المادة 42 من قانون العقوبات الجزائري على: "يعتبر شريكاً من يشترك اشتراكاً مباشراً، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة له مع علمه بذلك".

3 معاذ سليمان راشد محمد الملا، المسؤولية الجنائية عن إساءة استعمال الهاتف المحمول (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، جامعة عين شمس، القاهرة، الموسم الجامعي: 2013/2012، ص 275-276.

4 Cass. Crim 20 Janvier 1992, ***N*** 90-86. 604: Juris Date no 1992.

وقد يثار التَّساؤل حول نوع اشتراك الجنائي في حال ما إذا كان من ضمن المجموعة التي قامت بالفعل، حيث يتوفر لديه نفس القصد الجنائي الذي يتوفر لدى أفراد المجموعة، ففي هذه الحالة يعتبر مساهم تبعي إيجابي، وذلك تأسيساً على دوره في الجريمة المتمثل في التصوير والتسجيل، ومن بين الحالات التي تم عرضها على القضاء الفرنسي في هذا الصدد قضية علم أحد التلاميذ مسبقاً بنية أحد زملاءه بضرب زميل لهم، حيث قام بتصوير واقعة الضرب بهاتفه المحمول وقام بنشر هذا المحتوى، مما جعل محكمة فرساي تكيف هذا الفعل على أنه جريمة اشتراك في أعمال العنف العمدية المرتكبة أثناء دخول وخروج التلاميذ من مؤسسة تعليمية[1].

ولقد تعرض هذا الرأي إلى العديد من الإنتقادات، ولعل من أبرز هذه الانتقادات:

- توفر نية التصوير تؤدي حتماً إلى توفر القصد الجنائي للفاعل، مما يؤكد إصرار الفاعل على القيام بهذا الفعل[2]، وهذا ما يجعلنا نفترض أو نجزم أن صفة القائم بالتصوير أو النشر قد تتعدى صفة الشريك إلى صفة الفاعل الأصلي في الجريمة التبعية (التقاط الصور ونشرها).
- عدم قابلية نظرية الشريك بالتبعية للتطبيق على أفعال الإيذاء المبهج باعتبار أن السلوك الإجرامي لجرائم الإيذاء المبهج يتكون من فعلين معاصران لبعضها البعض، الفعل الأول يتمثل في الاعتداء الجسدي أو البدني، والفعل الثاني يتمثل في التقاط الصور ونشرها، وهذا بطبيعة الحال يتنافى مع أحكام الإشتراك التي تقتضي وحدة الفعل، والتي تمثل شرطاً أساسياً حتى نكون أمام ما يعرف بالاشتراك وفقاً لأحكام قانون العقوبات[3].
- لا توجد مصلحة من الفصل بين فعل الإعتداء وفعل التصوير والنشر، إلا إذا كانت هناك مصلحة أقوى بين الفاعل في فعل الإعتداء والفاعل في فعل التصوير والنشر، بحيث أن النتيجة النهائية للفعل هي نشر الصور أو المقاطع المسجلة، حيث أن كلا الفعلين مكملاً للآخر، فضلاً عن وجود مصلحة تربط مرتكب كلا الفعلين ببعضهما البعض، وهذا ما نكيفه بوحدة صفة الفاعل الأصلي لمرتكب كلا الفعلين[4].

---

1 فتحية محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج ، المرجع السابق، ص 247.

2 معاذ سليمان راشد محمد الملا، المرجع السابق، ص 289.

3 معاذ سليمان راشد محمد الملا، نفس المرجع، ص 289 .

4 معاذ سليمان راشد محمد الملا، نفس المرجع، ص 289.

2. **الـرأي الـثانـي:**

يصرح هذا الرأي بإمكانية إخضاع النشاط الإجرامي المرتكب من خلال التصوير والنشر إلى قواعد قانون العقوبات، وذلك من خلال إدراج هذا الفعل ضمن الأنشطة الإجرامية الآتية:

أ. إخضاع جرائم الإيذاء المبهج للنصوص المتعلقة بالإعتداء على حرمة الحياة الخاصة[1]:

يذهب أصحاب هذا الإتجاه إلى فكرة تجريم الإيذاء المبهج ضمن هذا السلوك باعتبار التوافق أو الترابط الموجود بين فعل الإيذاء المبهج، والإعتداء المتعلق بحرمة الحياة الخاصة، ذلك أن الإعتداء على الحياة الخاصة يتعلق في بعض صوره بالتقاط صور أو تسجيل مقطع فيديو، مثال ذلك ما نصت عليه المادة 303 مكرر من ق. ع. ج بقولها: "... التقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه"[2].

وما يمكن استنتاجه من خلال نص هذه المادة أن هذا الفعل ينطبق على ما يعرف بالإيذاء المبهج، وقد تم تكريس هذا الرأي قضائياً في فرنسا من خلال الحكم الصادر عن محكمة فرساي، في قضية تتلخص وقائعها "في أن أحد التلاميذ وعن طريق استعمال الهاتف المحمول قام بتصوير واقعة اعتداء بدني قام بها أحد زملاءه ضد معلمتهم، ثم قام بنشر الفيديو بين زملاءه الآخرين، ما أدى إلى انتشار الفيديو على نطاق واسع، وحتى أن الفيديو تم إعادة نشره في وسائل إعلام سمعية وبصرية، وهذا ما أدى بالمحكمة إلى أن تدين التلميذ على واقعة عدم تقديم المساعدة لشخص في حالة خطر كما هو منصوص عليه في المادة 223-6 من ق.ع.ف، فضلاً عن إدانته على واقعة الإعتداء على الحياة الخاصة وفقاً للمادة 226-1 من ق.ع.ف، حيث قضت المحكمة بالحبس لمدة سنة، مع الحكم

---

1 يعرف البعض الحياة الخاصة على أنها: "إن الوضعيات والأنشطة التي من خلالها يكون للشخص الحق في أن يترك في هدوء تعد جزء من ميدان الحياة الخاصة" **انظر في ذلك:** نويري عبد العزيز، الحماية الجزائية للحياة الخاصة في القانون الجزائري والفرنسي – دراسة مقارنة- ، ط. الثانية، دار هومة، الجزائر، 2016، ص 65.

2 القانون رقم 06-23 المؤرخ في 04 ذي الحجة 1427 الموافق 20 ديسمبر 2006، المعدل والمتم للأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر.ج.ج، المؤرخة في: 2006/12/24، ع 84، ص 23.

بوقف التنفيذ الجزئي بمقدار ستة أشهر من العقوبة المحكوم بها، وذلك عملاً بانتفاء السوابق الإجرامية للمحكوم عليه[1].

وعليه إن فلسفة الإعتداء على الحياة الخاصة تختلف وفلسفة الإيذاء المبهج، حيث أن الأولى تشترط مكان معين حتى يتحقق فعل الاعتداء على الحياة الخاصة، بينما جرائم الإيذاء المبهج لا تتطلب ذلك، حيث قد يحدث التصوير والنشر في أماكن عامة، مما قد يؤدي إلى إخراج جرائم كثيرة من هذا النوع من نطاق التجريم باعتبار أنها لا تمثل مساس بالحياة الخاصة[2].

ب. إخـــضاع جرائم الإيذاء الـمبهج للنصوص المتعلقة بعدم تقديـــم المساعدة لشخص فـــي حالة خطر:

يذهب هذا الإتجاه إلى ضرورة إسناد جرائم الإيذاء المبهج إلى جرائم الإمتناع عن تقديم المساعدة للغير في خالة خطر، وذلك وفقاً لما تنص عليه المادة 223-6 من ق.ع.ف، كما تنص نفس المادة في فقرتها الثانية على أن: "يعاقب بالحبس مدة خمس سنوات وغرامة قدرها 7500 يورو كل شخص يمتنع إرادياً عن تقديم المساعدة لشخص في حالة خطر والذي كان بمقدوره تقديمها شخصياً أو بطلب النجدة، دون تعريض نفسه أو غيره للخطر"[3]، ومن الأحكام التي أخذت نفس الإتجاه ما ذهبت إليه محكمة فرساي في أحد أحكامها، والذي تضمن: "ويبدو أن المتهم لم يقدم أدنى بادرة أو محاولة لإنقاذ الضحية ووثق الاعتداء عليها، في الوقت الذي كان بإمكانه إتيان ذلك، طالما أنه بادر بالإمساك بهاتفه، وقام بتشغيله للتصوير، مع الاقتراب من مشهد العنف، وبالتالي تتم إدانة المتهم بجريمة عدم تقديم المساعدة لشخص في حالة خطر"[4].

وعليه إن التسليم بضم جرائم الإيذاء المبهج لجرائم عدم تقديم مساعدة للشخص في حالة خطر لا يقوم على اعتبارات وأسس قوية، حيث يمكن دفع ذلك بأن الخطر الحقيقي الذي قد يهدد الغير أو حتى المصور لا يوجد أو غير متوقع مثل ما تم ذكره سابقاً في قضية (فتاة الباندا)، أو أنه في حال

---

1 T.G.I de Versailles, 8eme,27 juin 2007. Voir : http://legalis.net/spip.php? Pagejurisprudence-decision&id-article 2021.

2 فتحية محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج، المرجع السابق، ص 254.

3 محمود محمد محمود جابر، المرجع السابق، ص 387.

4 T.G.I de Versailles, 8 eme ,27 juin 2007. *http://legalis.net/spip.php*? Pagejurisprudence-decision&id-article 2021.

تدخل المتصور على أساس دفع الخطر عن الغير، قد يخشى من استفزازه لمرتكبي الاعتداء، مما قد يدفعهم بالرد عليه بقوة.

ج. إخضاع جرائم الإيذاء المبهج للنصوص المتعلقة بالنشر:

يذهب هذا الإتجاه إلى إمكانية تطبيق النصوص المتعلقة بالنشر على مثل هذه الجرائم، وذلك على اعتبار أن المشرع الفرنسي عاقب على مثل هذا السلوك ضمن المادة 24/227 من ق.ع.ف، والتي تعاقب بالحبس لمدة ثلاث سنوات وغرامة قدرها 7500 يورو على واقعة نشر رسالة تتضمن عنفاً[1].

وبناءً على ما سبق، تعرض هذا الرأي للعديد من الإنتقادات التي نتطرق للبعض منها على النحو الآتـــــي:

- أن تكييف جرائم الإيذاء المبهج كونها وقائع نشر مخالف للصواب، بحيث أن فعل الإيذاء المبهج يتكون من فعلين التصور والنشر، ولو سلمنا بتكييفها ضمن جرائم النشر نكون قد صرفنا النظر عن الواقعة الأصلية وهي التصوير، وهذا ما لا يمكن الأخذ به[2].
- اختلاف القصد الجنائي: بحيث لا يمكن الأخذ بعموم القصد الجنائي، فقد يتصور وجود قصد جنائي في فعل التصوير، ولكن الغالب على جرائم النشر الناتج عن الإيذاء المبهج يكون قصد الفاعل منها التسلية والمرح فقط[3].

ومن خلال ما سبق، نستنتج أن القضاء الفرنسي كان له السبق في العمل على تجريم مثل هذه السلوكيات الخطيرة الماسة بأمن وسلامة المجتمع، وأن هذه الجريمة استغرقت كثيراً من الأحكام التي تفاوتت وقائعها في الخطورة بين قضية وأخرى، كما ويلاحظ أن معظم مرتكبي هذه الجريمة هم من طائفة الشباب والمراهقين، ويرجع ذلك إلى الهدف من ارتكاب هذه الجريمة، والذي في الغالب يتمثل في المرح والتسلية.

---

1 Art227-24: "le fait soit… de diffuser par quelque moyen que ce soit et quelle qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humain, …est puni de trois ans d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur. " Loi n° 2011-267 du 14 mars 2011-art.5

2 محمود محمد محمود جابر، المرجع السابق، ص 389.

3 فتحية محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج " صفعة سعيدة"، المرجع السابق، ص 254.

الفرع الثانـــي: مكافحة جريمة الإيـذاء المبهج في التشريع الفرنسي.

نتطرق من خلال هذا الفرع إلى الأفعال التي تشكل السلوك الإجرامي للفعل المكون لجريمة الإيذاء المبهج، كما نتطرق إلى الصور التي تشكل الإعتداءات السابقة للفعل الإجرامي.

أولاً– مـحل جريـمة الإيذاء المبهج:

يعتبر محل الجريمة من بين أهم الشروط الضرورية حتى يتصور وقوع الجريمة، وهو ما نص عليه المشرع الفرنسي بموجب القانون رقم: 297-2007 المؤرخ في 5 مارس 2007[1]، ويمكن حصر هذه الأفعال في الصور الآتيـــة:

1– المجموعة الأولـى:

تنحصر هذه الطائفة في مجموعة الأعمال التي تشكل اعتداء على سلامة الشخص وتندرج ضمن هذه المجموعة أفعال التعذيب بمختلف أشكاله، بالإضافة إلى جميع جرائم الإيذاء البدني العمدية، وذلك باستثناء الأعمال التي تتحقق أو تنتج عن طريق إعطاء مواد ضارة، كما يُستثنى من ذلك مخالفات الإيذاء البدني العمدية البسيطة.

والملاحظ على هذه الطائفة أنها لا تتحقق إلا من خلال أعمال العنف البدنية التي تظهر في شكل ضرب، صفع، والدفع، وهذا بالضرورة يتلاءم مع طبيعة هذا النوع من الجرائم[2].

2– المجموعـــة الثانيـــة:

تندرج ضمن هذه الطائفة جميع الأفعال التي تشكل اعتداءً جنسياً على الأشخاص مثل الاغتصاب، واستثنى المشرع من هذه الأفعال العرض الجنسي، وكذلك ما يعرف بالحث على الممارسات الجنسية[3].

ولقد تعرض المسلك الفرنسي في تصنيف جرائم الإيذاء المبهج للعديد من الانتقادات، ويرجع سبب ذلك إلى استبعاد المشرع الفرنسي للكثير من الأنماط التي تشكل بطبيعتها جرائم إيذاء مبهج،

---

1 Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, JORF n°0056 du 7 mars 2007 page 4297.

2 فتحية محمد قوراري، نفس المرجع، ص 275.

3 محمود محمد محمود جابر، المرجع السابق، ص 391.

والتي تعد في معظمها أقل خطورة وجسامة من الأفعال السابقة الذكر، كما ويعاب على المشرع الفرنسي أنه بالرغم من أخذه بالجسامة كمعيار لتحديد محل جرائم الإيذاء المبهج، إلا أنه لم يأخذ بهذا المعيار على إطلاقه، حيث استثنى جرائم أكثر خطورة من الجرائم السابقة الذكر، كجرائم القتل[1].

ثانياً– أركان جريـمة الإيذاء المبهج:

تتمثل أركان جريمة الإيذاء المبهج في المظاهر الآتيــة:

1– الركـــن الـمادي:

يتألف الركن المادي لجريمة الإيذاء المبهج من فعلين متتابعين، يتمثل الفعل الأول في تسجيل الإعتداء، فيما يتمثل الفعل الثاني في نشر مقاطع الاعتداء.

أ– تسجـــيل الإعتـــداء:

يمثل تسجيل الإعتداء الفعل الأول الذي يقوم به الجاني، حيث جرم المشرع الفرنسي بمقتضى قانون العقوبات[2] هذا السلوك أو الفعل ضمن أحكام المادة 3/33/222 والتي تنص على أن: "يعد اشتراكاً في الإعتداءات العمدية على سلامة الشخص المنصوص عليها في المواد 1/222 إلى 1/14/222، 23/222 إلى 31/222، ويعاقب بذات العقوبات المنصوص عليها في تلك المواد، القيام عمداً بالتسجيل بأي وسيلة كانت، وعلى أي وسيط أياً كان نوعه، صور تتعلق بارتكاب هذه الجرائم"[3].

ويتضح من خلال نص المادة السابقة أن المشرع الفرنسي أخذ بنفس العقوبات الأصلية للفعل الأصلي، وهذا تطبيقًا لما يعرف بمبدأ استعارة الإجرام، والمنصوص عليه وفقاً للمادة 6/121 من قانون

---

1 طارق عفيفي صادق أحمد، المرجع السابق، ص175، **انظر كذلك**: محمود محمد محمود جابر، المرجع السابق ص 391.

2 Le code pénal français est modifié et complete.

3 Art 222-33-3: " Est constitutif d'un acte de complicité des atteintes volontaires à l'intégrité de la personne prévues par les articles 222-1 à 222-14-1 et 222-23 à 222-31 et est puni des peines prévues par articles de la fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission de ces infractions.
Le fait de diffuser l'enregistrement de telles images est puni de cinq ans d'emprisonnement et de 75000 Euros d'amende.
Le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer la public ou est réalisé afin servir de preuve en justice."

العقوبات الفرنسي، حيث اعتبر المشرع الفرنسي القائم بفعل التصوير شريكاً في الجريمة، وذلك على الرغم من انتفاء العلاقة بينه وبين مرتكب الفعل في بعض الحالات[1].

ولعل هذا ما جعل الفقه الفرنسي ينتقد المشرع الفرنسي في أخذه بهذا المسلك، حيث خرج عن القواعد العامة للمسؤولية الجنائية، كما أن المشرع الفرنسي كان جليًا به أن يُجرِّم هذا الفعل كفعل مستقل على الجريمة الأصلية.

وما يمكن كذلك استنتاجه من النص أن المشرع الفرنسي لم يشر إلى وسيلة التصوير؛ حيث اكتفى بالقول: "بأي وسيلة كانت"، وهذا ما يجعل من النص يتلاءم مع جميع التطورات الحاصلة في المجال الرقمي، وخاصة الهاتف المحمول الذي بات يشكل أكثر الوسائل استخداماً من حيث التقنيات التي يوفرها[2].

ب- نشر صور أو مقاطع الإعتـــداء:

ويعني إطلاع الغير على صور أو مقاطع الإعتداء بصرف النظر عن عدد الأشخاص الذين اطلعوا على هذا المقطع، وفي الغالب ما يكون نشر هذه المقاطع عن طريق البلوتوث أو الإنترنت، أو غيرها من الوسائط الإلكترونية، وهو ما يعرف بالنشر الإلكتروني[3].

ولقد سلك المشرع الفرنسي نفس فلسفة التجريم التي انتهجها مع جريمة التصوير، حيث جعل من جريمة النشر جريمة مستقلة عن الجرائم الأخرى، وتقوم هذه الرؤية في التجريم لدى المشرع الفرنسي على اعتبار أن الأشخاص الذين ينشرون الصور في الغالب ما يكونون مستقلين عن أولئك الذين قاموا بالتسجيل[4].

---

1 فتحية محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج، المرجع السابق، ص 270.

2 محمود محمد محمود جابر، المرجع السابق ص 175.

3 يعرف النشر الإلكتروني على أنه: "استخدام وسائل التقنية الحديثة في بث، أو إرسال، أو استقبال، أو نقل المعلومات المكتوبة، والمرئية، والمسموعة، سواء كانت نصوصاً، أو مشاهد أو أصوت، أو صوراً ثابتة أو متحركة، لغرض التداول". **انظر**: أحمد عبد الفتاح، جرائم النشر الإلكتروني، مركز الدراسات القضائية التخصصي، السعودية، متاح على الرابط: *www.cojss.com/vb/showthead.php?16746* تم الاطلاع عليها بتاريخ: 2018/07/03.

4 فؤاد بن الصغير، أركان جريمة الإيذاء المبهج في حالة اغتصاب فتاة حافلة البيضاء، متاح على الرابط: *http://m.hespress.com* تاريخ الإطلاع: 2018/07/03 .

2- الركـــن الـمعنوي:

تعتبر جريمة الإيذاء المبهج من الجرائم العمدية، وذلك بحسب ما نصت عليه المادة 3/33/222 من قانون العقوبات الفرنسي، والتي وردت فيها عبارة: "واقعة التسجيل العمدية"، بحيث يتطلب الركن المعنوي توفر القصد الجنائي العام بعنصريه العلم والإرادة، بحيث يكون الجاني على علم تام بالفعل الذي يقوم به بأنه منافٍ للقانون، وفي حالة انتفى العلم ينتفي القصد الجنائي، ومن أمثلة ذلك أن يجذب أحدهم تجمع جمهور ما حول واقعة ما، فيقوم بتصوير الواقعة عن طريق الهاتف النقال دون أن يبين فعل الإعتداء البدني أو الجنسي إلا بعد التصوير، ففي هذه الحالة ينتفي العمد، أما الإرادة وهي العنصر الثاني فتعني اتجاه إرادة الجاني إلى القيام بهذا الفعل، وعدم اقتران الإرادة بالفعل لا ينفي ووجود القصد الجنائي، ومما تجب الإشارة إليه كذلك أن جريمة الإيذاء المبهج تعتبر من الجرائم التي لا تتطلب قصد جنائي خاص، وإنما يكفي توفر القصد الجنائي العام[1].

الفرع الثالث: العقوبـــة المقررة لجريمـــة الإيـــذاء المبهـــج.

سنعالج من خلال هذا الفرع العقوبات المقررة لجريمة الإيذاء المبهج، ثم ظروف الإباحة، على النحو التالـــي:

أولًا: العقوبـــة:

تأكيدًا لما ذُكر سابقاً، فصل المشرع الفرنسي بين جريمة التسجيل وجريمة النشر، حيث جرم المشرع جريمة التصوير طبقاً للمادة 3/33/222 واعتبر الفعل في جميع الحالات التي يرتكب فيها جناية، وفصل في ذلك على النحو الآتـــي[2]:

1- جرائم التعذيب والجرائم الوحشيـــة:

جرمها بمقتضى المواد من 1/222[3] إلى 1/6/222[1]، حيث يعاقب على هذا الفعل بـ: خمسة عشر (15) سنة، وتكون العقوبة السجن المؤبد في حال ما إذا كانت الجريمة مترافقة أو تالية لجناية أخرى غير القتل والاغتصاب.

1طارق صادق عفيفي، المرجع السابق، ص 395.

2 فتحية محمد قوراري، المرجع السابق، ص 270.

[3]Article 222-1¨ Le fait de soumettre une personne à des tortures ou à des actes des barbarie est puni de quinze ans de réclusion criminelle¨.

2- جرائم العـــنف:

جرمها بمقتضى المواد 7/222 إلى 2/16/222، ويعاقب على هذا الفعل بالسجن لمدة خمسة عشر (15) سنة .

3- جريـمة الاغتصاب:

جرمها بمقتضى المواد 23/222 إلى 26/222، بحيث يعاقب على هذا الفعل بالسجن لمدة خمسة عشر (15) سنة، وقد تصل إلى عشرين (20) سنة في حال اقترانها بظرف من ظروف التشديد.

4- الاعتداءات الجنســية الأخرى:

بمقتضى المواد من 27/222 إلى 32/222، يعاقب المشرع الفرنسي على جرائم الإعتداءات الجنسية الأخرى بالسجن خمس (5) سنوات، وغرامة مالية قدرها 7500 يورو، وفي حال توفر أحد ظروف التشديد تمتد العقوبة إلى سبع (7) سنوات سجن وغرامة قدرها 1000 يورو.

وأما عن جريمة النشر فقد اعتبرها المشرع الفرنسي جنحة وعاقب عليها طبقاً للمادة 3/33/222، حيث قرر لها عقوبة تقدر بخمس (05) سنوات وغرامة مالية قدرها 75000 يورو[2].

والملاحظ في تفرقة المشرع الفرنسي في العقوبة بين التسجيل والنشر، في كون الجريمة الأولى أخطر من الجريمة الثانية، وذلك باعتبار أن الجريمة الثانية لا تتحقق إلا إذا تمت الجريمة الأولى، فضلاً عن أن الجريمة الأولى تظهر خطورة الجاني الذي خلى من المشاعر الإنسانية، حيث يرتكب أمامه فعل أقل ما يقال عنه شديد الوحشية كالاغتصاب بالرغم من كل هذا لا تتحرك إنسانيته لنجدة الضحية، فهو بذلك لا يختلف عن الجناة الأصليين إن لم يكن أخطر منهم.

ثانياً: أســباب الإباحــة:

بالرجوع للمادة 3/33/222 من قانون العقوبات الفرنسي بين المشرع الفرنسي الحالات التي لا تطبق عليها العقوبة المقررة لجرائم الإيذاء المبهج، والتي تتمثل في الحالات التالية:

1- الإباحــة لغرض الإعلام:

---

[1]Article 222-6-1:¨ Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent paragraphe encourent , outre l'amende suivant les modalités prévues par l'article 131-38 les peines prévues par l'rticle 131-39¨.

2 محمود محمد محمود جابر، المرجع السابق ص 396.

في هذه الحالة أباح المشرع الفرنسي فعل الإيذاء المبهج، إلا أنه قيد ذلك بشروط وجب توافرها في الشخص القائم بالعمل الصحفي في حال إعداد مثل هذه التقارير، وتتمثل هذه الشروط في:

- أن يكون القائم بالتسجيل أو النشر صحفي أو إعلامي، وذلك بغض النظر عن الوسيلة الإعلامية التي ينشط فيها (تليفزيون، إنترنت، أو صحافة مكتوبة).
- أن يكون الهدف من الفعل إعلام الجمهور بالواقعة، وأن يتقيد الصحفي بأحكام قانون حرية الصحافة[1].

2- إباحـــة الفعل لغرض الإثـــبات:

كما أقر المشرع الفرنسي فعل الإيذاء المبهج في حال ما إذا كان الغرض منه إثبات الواقعة الأصلية، وما يجب الإشارة إليه أن الإباحة تقتصر على التسجيل دون النشر، بحيث لو قام الجاني بنشر التسجيل ينتفي سبب الإباحة[2].

الفرع الرابع: تقـييم المشرع الفرنسي في تجريـم جرائم الإيـذاء المبهج.

بالرغم من الدور الإيجابي الذي قام به المشرع الفرنسي؛ حيث كان السباق في تجريم هذا الفعل، إلا أنه تعرض لعدَة انتقادات من طرف الفقه الفرنسي، لذلك يتم التطرق لبعض أهم الإنتقادات التي تعرض إليها المشرع الفرنسي، وذلك على النحو الآتـــي:

أولاً: من بين أهم الانتقادات التي وجهت للمشرع الفرنسي إدراجه لجرائم الإيذاء المبهج ضمن الجرائم المتعلقة بالاعتداء على السلامة الجسدية، وهو أمر ينافي الصواب حتى وإن كانت الأفعال الأصلية للجريمة تمس بالسلامة الجسدية والجنسية للأشخاص، حيث وجب على المشرع الفرنسي إدراج جرائم الإيذاء المبهج ضمن الجرائم المتعلقة بكرامة الشخص[3].

ثانياً: من بين الانتقادات التي وجهت للمشرع الفرنسي كذلك اتهامه بتقيد حرية الإعلام والحريات، حيث منع الهواة من المواطنين العاديين من تسجيل مثل هذه الاعتداءات، وذلك حتى يتحقق لدى هذه الفئة نفس الحق عند الصحفي أو الإعلامي، ففي معظم الأحيان التقارير التي تعدها

---

1 فتحية محمد قوراري، المرجع السابق، ص 298.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 177.

3 فتحية محمد قوراري، المرجع السابق، ص 300.

هذه الفئة تكون غنية بالمعلومات، ويستدل البعض على ذلك في أعمال الشغب التي ضربت الضواحي الفرنسية، حيث استمدت الدلائل من أشرطة الهواة التي كانت الشاهد الوحيد على هذه الأعمال التخريبية[1].

ثالثاً: ومن بين أهم الانتقادات التي تعرض لها المشرع الفرنسي كذلك، هو أنه حصر الجرائم السابقة للإيذاء المبهج بجرائم محدودة تتراوح بين الجرائم البسيطة والجرائم الخطيرة دون أن يتطرق لأي من هذه الجرائم، إلا أن المصلحة كانت تقتضي أن يشمل التجريم كافة الأفعال بعض النظر عن تكييفها ويراعى في ذلك العقوبة المقررة لكل فعل[2].

رابعاً: غاب على المشرع الفرنسي تطبيقه لأحكام الاشتراك على جرائم الإيذاء المبهج، والتي يرى البعض[3] أنه نتج عنها عدة سلبيات، لعل من بين أبرزها اختلاف العقوبة المقررة لكل من الفعلين حيث جرم فعل التسجيل على أساس أنه جناية، بينما جرم فعل النشر على أنه جنحة مع أن كلا الفعلين مكملين لبعضهم البعض، مما يستوجب وجود عقوبة موحدة لنفس الفعل.

وعليه بالرغم من الانتقادات التي وجهت للمشرع الفرنسي، إلا أننا نؤيد وجهة نظره فيما ذهب إليه في تجريم هذا الفعل، وذلك من أجل المحافظة على كرامة الإنسان من استغلاله من بعض الأشخاص الذين أخذهم شغف التكنولوجيا أو الشهرة إلى استغلال حالات الخطر والوضع غير الإنساني الذي يتعرض له البعض الآخر.

الفرع الـخامس: موقف المشرع الجـزائـري من جرائم الإيـــذاء المبهج.

المشرع الجزائري كغيره من التشريعات العربية لم يتطرق إلى تجريم الإيذاء المبهج وفق نصوص خاصة كما هو معمول به في التشريع الفرنسي، واكتفى ببعض النصوص المتفرقة والتي منها على سبيل المثال المادة 303 مكرر من قانون العقوبات، والتي تحمي الحياة الخاصة.

---

1 كما اعتبر البعض أن تجريم الإيذاء المبهج يخالف ما ذهبت إليه المحكمة الأوروبية لحقوق الإنسان في هذه المادة ، حيث أن المادة 10 تكفل حرية التعبير لأي شخص، دون التمييز تبعاً لطبيعة الهدف أو الأشخاص، سواء كانوا طبيعيين أم اعتباريين، وممارسة هذه الحرية لا تتعلق فقط بمحتوى المعلومات، بل أيضاً بوسائل النشر مع فرض قيود في الحصول على المعلومات أو نقلها. **انظر في ذلك:** محمود محمد محمود جابر، المرجع السابق ص 397.

2 فتيحة محمد قوراري، المرجع السابق، ص 301.

3 فتيحة محمد قوراري، نفس المرجع، ص 301.

وتأسيساً على ما سبق، نرى أن النص الذي يحمي الحياة الخاصة لا يتسع لأن يشمل جرائم الإيذاء المبهج، وذلك للاعتبارات الآتيـــة:

- أن جريمة الإيذاء المبهج لا تستهدف مكان معين فهي ترتكب في أماكن عامة أو خاصة على حدٍ سواء، وهذا بخلاف الإعتداء على الحياة الخاصة والذي يتطلب أن ترتكب في مكان خاص فقط[1]، كما أن جريمة الإيذاء المبهج لا تستهدف شخصيات بعينها كما في جرائم الاعتداء الحياة الخاصة التي في الغالب تستهدف المشاهير أو أصحاب النفوذ والمسؤولية.
- جرائم الإيذاء المبهج هي جرائم تبعية، بحيث يستلزم وقوعها وجود جريمة سابقة لها، على عكس جرائم الاعتداء على حرمة الحياة الخاصة التي تعتبر جريمة أصلية[2].
- جرائم الإيذاء المبهج تتراوح عقوبتها بين الجناية والجنحة، بينما جرائم الاعتداء على الحياة الخاصة تعتبر جنحة فقط.

المطلب الثانـــي: جرائم الاعتداء على الخصوصية باستخدام الهاتف النقال.

تعتبر جرائم الاعتداء على الخصوصية من بين أكثر الجرائم التي يتم ارتكابها بواسطة الهاتف النقال، وذلك بالنظر لسهولة ارتكابها، فضلاً عن إحجام معظم ممن يكونون ضحايا لهذا النوع من الجرائم عن الإبلاغ عنها، وتتنوع هذه الجرائم بين التقاط الصور والتنصت على مكالمات (الفرع الأول)، بالإضافة إلى القذف (الفرع الثاني)، والسب (الفرع الثالث)، والتشهير (الفرع الرابع).

الـفرع الأول: جرائـم التقاط الصورة الخاصـة وتسجيل المكالمات.

تندرج هذه الجريمة ضمن ما يعرف بالإعتداء على حرمة الحياة الخاصة، والتي تعرف بأنها: "الحق في أن يكون الفرد حراً وأن يعيش كما يريد دون أدنى حق للتدخل الخارجي"[3]. ولقد جرم المشرع الجزائري هذه الجريمة بموجب المادة 303 مكرر من قانون العقوبات، والتي نصت على أن :"يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50000 دج إلى 300000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص أو بأي تقنية كانت وذلك:

---

1 بهاء المري، جرائم المحمول والإنترنت، ب. ط، منشأة المعارف، الإسكندرية، 2017، ص 338.

2 انظر المادة 303 من ق.ع.ج.

3 أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص 241.

1- بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير أذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة، ويضع صفح الضحية حد للمتابعة الجزائية".

من خلال هذا النص يتضح أن المشرع الجزائري لم يشترط وسيلة معينة لارتكاب الجريمة، حيث نص على: "... بأي تقنية كانت"، مما يعني أن المشرع جعل النص يقبل كل التأويلات بحيث كلما استجدت تقنية قد تساعد على الإعتداء على خصوصية الإنسان، فهي بذلك تدخل ضمن مقتضيات هذا النص، ولذلك يعتبر الهاتف من بين هذه الوسائل إن لم يكن أهمها في وقتنا الراهن[1].

وسنحاول من خلال هذا الفرع التفصيل في هذه الجريمة على النحو الآتي:

أولاً– الإعتـــداء على الصورة:

تعرف الصورة بأنها: "الاعتداء الضوئي على جسم الإنسان، فهي تشير إلى خصوصية صاحبها"[2]، كما تعرف في علم البصريات بأنها: "تشابه أو تطابق للجسم الناجم عن انعكاس

---

1 بالرغم من قابلية النص للتطبيق على جرائم الاعتداء الماسة بحرمة الحياة الخاص، إلا أنه كان حلي بالمشرع نهج المسلك الذي قام به المشرع السعودي الذي جرم الفعل مباشرة، حيث نص في المادة 3 من نظام مكافحة الجريمة المعلوماتية على أن: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الآتية:

- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي دون مسوغ نظام صحيح أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص، أو ابتزازه لحمله على القيام، أو الامتناع عنه لو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.
- التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة". **انـــظر**: هيئة الاتصالات وتقنية المعلومات، نظام مكافحة الجرائم المعلوماتية، السعودية، متاح على الرابط: *www.citc.gov.sa*، تاريخ الاطلاع: 2018/07/20.

2 محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، ب. ط، دار النهضة، مصر 2005، ص 217.

الأشعة الضوئية المنبعثة منه على عدسة أو مرآة"[1]، فالصورة بذلك تشكل تجسيد للإنسان في موقف معين، ولذلك حمى المشرع الصورة بتجريم الاعتداء عليها وفقاً لنص المادة 303 مكرر من ق.ع.ج.

1- السلوك الإجرامي لـجريمة الإعتـــداء على الصورة:

تضمنت المادة 303 مكرر في فقرتها الثانية السلوك الإجرامي لجريمة الإعتداء على الصورة، والتي تظهر في أحد الأشكال التالية :

- **التقاط الصـــورة:** ويقصد به تثبيت الصورة على مادة حساسة أو خاصة يمكن من خلالها الإطلاع على الصورة.
- **التسجيل:** ويتمثل في تصوير مقطع فيديو للضحية وهو في مكان خاص.
- **النقل:** ويقصد به نقل الصورة من واسطة إلكترونية إلى أخرى، أو تداولها عن طريق تقنيات البلوتوث أو الإنترنت أو غيرها من مواقع التواصل الاجتماعي.

ولكي يتحقق السلوك الإجرامي كاملاً لا بد أن تكون الصورة الملتقطة صورة إنسان، وهذا ما نصت عليه المادة 303 مكرر صراحة بقولها: "...صورة لشخص..."، بحيث يخرج من نطاق التجريم كل صورة ليست للإنسان مهما بلغت أهميتها، وفضلاً عن كون الصورة صورة إنسان لابد أن تكون صورة تم التقاطها في مكان خاص[2]، بحيث لا تتحقق الجريمة إذا التقطت في مكان عام[3].

والجدير بالذكر أن المشرع المصري سلك نفس مسلك المشرع الجزائري في التجريم، وذلك ما نصت عليه المادة 309 مكرر1 من قانون العقوبات المصري بحيث تضمنت: "...التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص"[4]، وهذا مغاير لما ذهبت له بعض التشريعات العربية التي نذكر منها على سبيل المثال؛ التشريع الكويتي والذي يجرم على الفعل حتى ولو

---

1 **نقلاً عـــن:** محمد الشهاوي، نفس المرجع، ص 217.

2 هناك اختلاف بين الفقهاء الفرنسيون في تحديد طبيعة المكان الخاص، حيث تبنى البعض منهم معياراً موضوعياً لتحديد هذا المفهوم، فذهب إلى تعريف هذا المكان بتعداد صور المكان العام، وما دون ذلك يدخل في إطار المكان الخاص كالمسكن، بينما البعض الآخر تبنى معياراً شخصياً، فعرف المكان الخاص بأنه مكان مغلق يتعذر بلوغه بنظرات من الخارج، ويمكن دخوله بناءً على إذن مالكه أو مستغله أو المنتفع فيه. **انظر فـــي ذلك:** معاذ سليمان راشد محمد الملا، المرجع السابق، ص 187.

3 عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، الطبعة الأولى، بهجات للطباعة، مصر، 2009، ص 152.

4 القانون 95 الصادر بتاريخ 1969/06/30 المتعلق بقانون العقوبات المعدل والمتمم، ج.ر.ج.م ، ع 25.

تم في أماكن عامة[1]، وبالإضافة إلى الشروط السابقة اشترط المشرع كذلك أن يكون الفعل بدون إذن المجني عليه أو رضاه، وفي حال إذا لم تتوافر هذه الشروط تكون الجريمة كأن لم تكن.

2- الركـــن المعنـــوي لجريمة الإعتـــداء على الصـــورة:

تعتبر جريمة الإعتداء على الصورة من الجرائم العمدية، وذلك طبقاً لما جاء في المادة 303 مكرر من قانون العقوبات الجزائري، والتي جاء فيها:"...كل من تعمد المساس..."، لذلك وجب توافر القصد الجنائي بعنصرية العلم بمكونات الجريمة، فضلاً عن إرادة ارتكابها، ففي حال انتفى أحد العناصر ينتفي قيام الجريمة[2].

3- العقوبة المقررة لجريمة الاعتـــداء على الصورة:

اعتبر المشرع جريمة الإعتداء على الصورة من قبيل جرائم الجنح، فعاقب عليها بالحبس مدة تتراوح ما بين ستة (6) أشهر إلى ثلاث (3) سنوات، وغرامة مالية تتراوح ما بين 50000 دج إلى 300000 دج، كما تتم مصادرة الأجهزة التي ارتكبت بها الجريمة، بالإضافة إلى الحرمان من الحقوق المنصوص عليها في المادة 9 من ق.ع.ج[3].

ثانياً- جرائـــم الاعتـــداء على المراسلات والمحادثـــات (المكالمات):

نصت على جريمة الاعتـــداء على المراسلات والمحادثـــات[4] المادة 303 مكرر من ق.ع.ج في فقرتها الثانية، وفيما يلي نتطرق للأركان العامة والعقوبة الخاصة بهذه الجريمة:

---

1 معاذ سليمان راشد محمد الملا، المرجع السابق، ص 310.

2 شنة زواوي، الحماية الجنائية لحق الشخص على صورته، مجلة دفاتر السياسة والقانون، العدد الثالث عشر، جوان 2015، جامعة ورقلة، ص 364.

3 انظر المادة 303 مكرر من قانون العقوبات الجزائري .

4 تعرف المراسلات على أنها: "النبأ الذي يهم صاحبه كتمانه"، بينما يعرف الحق في سرية المراسلات على أنه: "الحرص على سرية المراسلات البريدية والبرقية والاتصالات الهاتفية للأفراد، وعدم إطلاع أي شخص، أو أي جهة عليها إلا على النحو المبين في القانون"، **انظر في ذلك:** رزان محمد ياسر العلبي، صفاء أوتاني، حق الإنسان في سرية مراسلاته البريدية واتصالاته السلكية واللاسلكية، مجلة جامعة البعث، المجلد 38، العدد 7، العراق، 2016، ص 87. هذا وتعرف المحادثات على أنها: "الأقوال والأصوات الصادرة عن الأشخاص بشكل مباشر أو غير مباشر، والتي جرت في مكان خاص أو عبر الهاتف، وقد تكون هذه المحادثات مباشرة كتلك التي تدور بين الأفراد وجها لوجه، أو تلك المحادثات غير مباشرة، وهي تلك التي يتم تبادلها بين الأفراد عبر وسائل الاتصال الحديثة السلكية وللاسلكية، كالهاتف وشبكة الانترنت، ويرى بعض الفقه أن الحديث الذي يتم بين الأفراد من خلال الهاتف هو حديث خاصاً، **انـظر:** حسني محمود نجيب، شرح قانون العقوبات القسم الخاص، ط. الثانية، دار

1- السلوك الإجرامي لجريمة الإعتداء على المراسلات والمحادثات:

يظهر السلوك الإجرامي لهذه الجريمة من خلال إتيان أحد الأفعال الآتية:

- **الالتقاط:** ويقصد به التقاط الأصوات بواسطة تقنية من التقنيات، سواءٌ بطريقة مباشرة أو طريقة غير مباشرة.
- **التسجيل:** ويتمثل في حفظ المراسلات أو المحادثات على مادة معدة لذلك من أجل الاستماع إليها، أو إعادة مشاهدتها لاحقاً، ويتم التسجيل بالتقاط مضمون المراسلات أو المحادثات عن الوسائل المعدة لذلك[1].
- **النقل:** ويقصد به نقل المرسلات والأحاديث وتداولها عبر الوسائط الالكترونية، وغيرها من الوسائط.

والملاحظ من نص المادة أن المشرع لم يقيد الاعتداء على المراسلات والأحاديث بأماكن معينة أو خاصة كما فعل مع جريمة الاعتداء على الصورة، إذ تقوم الجريمة حتى ولو وقعت في أماكن عامة، كما اشترط كذلك أن يتم الفعل بدون إذن أو رضى المجني عليه، وأضاف المشرع الفرنسي على ذلك أن تكون الأحاديث ذات طابع خاص وسري، وذلك وفقاً للمادة 266-2 من ق.ع.ف.[2]

2- الركن المعنوي لجريمة الإعتداء على المراسلات والمحادثات:

النهضة العربية، القاهرة، 1992، ص 789. **مشار إليه لدى:** رزان محمد ياسر العلبي، وصفاء أوتاني، المرجع السابق، ص 87-89. بينما تعرف المكالمات الهاتفية على أنها: "كل المحادثات الشخصية التي يتحدث بها شخص إلى غيره سواءٌ كانت هذه المكالمات سلكية أو لا سلكية أو عن طريق الموبايل، الأقمار الصناعية أو غيرها من تقنيات الإتصالات الحديثة". **انظر في ذلك:** عبدالفتاح بيومي حجازي، المرجع السابق، ص 440.

1 طلعت الشهاوي، المسؤولية الجنائية عن جرائم الاتصالات –دراسة مقارنة–، ط. الأولى، دار النهضة العربية، القاهرة،2017، ص 503.

2 Article 226-1 modifie par ordonnance n°2000-916 du 19 septembre2000-art.3 (v) JORF 22 septembre2000 en vigueur le l[er] janvier 2002 " Est puni d'un an d'emprisonnement et de 45000 euros d'amende le fait, au moyen d' un procédé quelconque, volontairement de porter atteinte à l' intimité de la vie privée d' autrui: 1° En captant, enregistrant ou transmettant, Sant le consentement de leur auteur, des paroles prononcées è titre privé ou confidentiel"

ينطبق على الركن المعنوي لجريمة الإعتداء على المراسلات والمحادثات نفس الأحكام المطبقة على جريمة الإعتداء على الصورة، حيث تتطلب قصد جنائي عام بعنصريه علم الجاني بأفعال الجريـمة، وأن

تتجه إرادته إلى القيام بالفعل، وفي حالة عدم توفر أحد العناصر تنتفي الجريمة[1].

3- العقوبة المقررة للجريمة لجريمة الإعتداء على المراسلات والمحادثات:

رتب المشرع الجزائري على هذا الفعل المكيف على أنه جنحة عقوبة تتراوح ما بين ستة (6) أشهر إلى ثلاث (3) سنوات وغرامة مالية ما بين 50000 دج إلى 300000 دج، كما تصادر الأجهزة التي ارتكب بها الفعل، مع الحرمان من الحقوق المنصوص عليها طبقا للمادة 9 من ق.ع.ج.[2]

الفرع الثانـــي: جريـــمة القذف بواسطة الـــهاتف النقال.

---

1 نصت محكمة النقض المصرية في قرارها رقم: 14348 لعام 2007 على أنه: "من المقرر أن القصد الجنائي الذي يتطلبه الشارع في جريمة استراق السمع المنسوبة إلى المطعون ضده والمعاقب عليها بنص المادة 309 مكرر من قانون العقوبات هو القصد العام الذي يتحقق بمجرد ارتكاب الفعل المادي، تستوي البواعث التي دفعت المتهم إلى فعله، وأن مجرد الاعتداء على حرمة الحياة الخاصة باستراق السمع ويفترض فيه القصد إذا ما توافر عنصراه العلم والإرادة". **انـــــظر**: نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المرسلات عبر البريد الإلكتروني، رسالة مقدمة لنيل درجة الماجستير في الحقوق، جامعة القاهرة، ص 104-105.

2 يتضمن نص المادة 9 العقوبات التكميلية المتمثلة فـــي:

- الحجز القانوني،
- الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية،
- تحديد الإقامة،
- المنع من الإقامة،
- المصادرة الجزئية للأموال،
- المنع المؤقت من ممارسة مهنة أو نشاط،
- إغلاق المؤسسة،
- الإقصاء من الصفقات العمومية،
- الحظر من إصدار الشيكات و/أو بطاقات الدفع،
- تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة،
- نشر أو تعليق قرار الإدانة.

يتم التطرق في هذا الفرع إلى جريمة القذف بواسطة الهاتف النقال، لكن قبل التطرق إلى طبيعة جريمة القذف عبر الهاتف النقال، لا بد من تعريف جريمة القذف (أولاً)، ثم بيان أحكامها في النصوص التقليدية (ثانياً)، وصولاً إلى العقوبة المقررة لها (ثالثاً).

أولًا– تعريـــف القذف:

هو "إسناد فعل أو أمر محدد إلى شخص أو أشخاص لو صح هذا الفعل لكون جريمة يسأل عنها من أسندت إليه، أو توجب احتقاره عند أهل وطنه"[1]. ويعرف كذلك على أنه: "إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسناداً علنياً عمدياً"[2].

ومن خلال هذين المفهومين نستنتج أن القذف عبارة عن ادعاء كاذب يقصد من خلاله المدعي إسناد واقعة غير حقيقية لشخص آخر (طبيعي/أو معنوي)، كما قد يكون القصد منه التحقير أو انتقاص من قيمة المقصود بالقذف في مجتمعه أو بيئته التي ينشط فيها، وفي الغالب تكون دوافع القذف دوافع شخصية، سواءٌ في مجال السياسة أو الاقتصاد، أو في المجال الاجتماعي.

ثانياً– أركان جريـمة القـذف:

جاء في نص المادة 296 من ق.ع.ج: "يعد قذفاً كل ادعاء بواقعة من شأنها المساس بشرف أو اعتبار الأشخاص أو الهيئة المدعى عليها به، أو إسنادها إليهم أو إلى تلك الهيئة، ويعاقب على نشر هذا الإدعاء أو ذلك بإسناد مباشرة أو بطريق إعادة النشر، حتى ولو تم ذلك على وجه التشكيك، أو إذا قصد به شخص أو هيئة دون ذكر الاسم، ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة".

وفقاً للنص السابق، وحتى تقوم جريمة القذف لا بد من توفر العناصر الآتيـــة:

1– السلوك الإجرامي للقذف:

يتكون السلوك الإجرامي لجريمة القذف من الأفعال الآتية:

– **الإسناد:** يتمثل الإسناد في نسبة أمر أو واقعة ما، لشخص معين وذلك عن طريق استعمال أي وسيلة من وسائل التعبير والتي تؤدي الغرض، حيث قد يكون عن طريق القول أو عن طريق

---

1 انسام سمير طاهر الحجامي، جريمتي القذف والسب عبر الإنترنت، مجلة رسالة الحقوق، العدد الثاني، جامعة كربلاء، العراق، 2015، ص 339.

2 علي جعفر المرجع السابق، ص 321-322.

الكتابة أو الإشارة، على سبيل الجزم أو الشك، وذلك ما عبر عنه المشرع بلفظ "ادعاء"؛ حيث قد يكون ما قيل في هذه الحالة يقبل التصديق أو الكذب، أو بلفظ إسناد والذي في الغالب يأتي على سبيل الجزم والتأكيد[1].

- **العلانية**[2]: تعتبر العلانية من بين الأفعال التي يجب توفرها في جريمة القذف، بحيث قد تكون العلانية في شكل يمكّن العامة من الاطلاع على ما تم نسبته للشخص المقذوف، ولا يعتد بالوسيلة التي تم بها الإعلان، بحيث يمكن أن يكون عن طريق مواقع إلكترونية أو عن طريق الحاسوب أو غيرها من طرق الإعلان الأخرى، ويستوي في ذلك أن يكون الذم والقدح قي شكل عبارات أو رسوم أو صور مركبة[3].

ونتساءل في هذه الحالة عن صلاحية الهاتف النقال في أن يكون وسيلة إعلانية يعتد بها في ارتكاب جريمة القذف ؟

إن التقنيات التي يتيحها الهاتف النقال جعلت من اليسير استعماله في أعراض قذف الغير أو الإساءة إليهم، حيث يستطيع الجاني بث كل ما يشكل قدح في الغير من خلال إرسال رسائل متعددة الوسائط، وعن طريق استعمال تقنية البلوتوث في نشر ما يريد من صور أو تسجيلات أو

---

1 مريوان سليمان، القذف في نطاق النقد الصحفي، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2014، ص 184.

2 حدد المشرع الفرنسي طرق العلانية فيما يخص جريمة القذف بنص المادة 23 من قانون الإعلام المؤرخ في 1881/07/29 وقد قسمها المشرع إلى ثلاث (03) طرق تتمثل في:

أولاً: وسيلة القول أو الصياح أو التهديد: ويشترط المشرع في هذا الحال أن يكون القول صادر عن حنجرة إنسان؛ أي أن يكون صوت الضحية ذاته، أو عبر جهاز صوتي ومنه يعتد بأي صوت آخر غير صوت الشخص الذي صدر منه القول، كما يجب أن يكون الصوت من القوة التي تسمع الغير أو من جانبه، أو اشترط فضلاً عن ذلك التهديد أيضاً.

ثانياً: وسيلة الكتابة أو وسائل التمثيل الأخرى: تتحقق العلانية في هذه الحالة عن طريق التعبير للجمهور بالكتابة أو البيع أو التوزيع أو غيرها من الطرق الأخرى التي تفي بهذا الغرض.

ثالثاً: الوسائل الإلكترونية: كما بينت المادة 29 من قانون الاعلام أن إمكانية العلانية قد تحقق من خلال القول أو الكتابة عن طريق استخدام الوسائط الإلكترونية سواء كانت حواسيب أو أجهزة الهواتف، أو غيرها من الوسائط الأخرى.

انظر في ذلك: أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص ج 1، ط. العشرون، دار هومه، الجزائر، 2018، ص 203-206.

3 أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص 333.

غيرها من الأغراض الأخرى[1]، كما تعتبر التطبيقات الحديثة المدرجة في الهاتف النقال من بين أكثر الوسائل التي ساعدت على تفشي جريمة القذف بواسطة الهاتف النقال.

تجدر الإشارة أن المشرع الجزائري لم يُحِط الهاتف النقال أو غيره من الوسائط الإلكترونية الأخرى بنصوص خاصة، كما لم يلجأ حتى إلى وضعها ضمن ظرف مشدد للوسائل المرتكب بواسطتها هذه الجريمة، وذلك من أجل ردع من يقوم بهذه السلوكيات عبر الهاتف النقال، باستثناء ما جاء في نص المادة 144 من ق.ع.ج والتي نصت على أن: "يعاقب بغرامة من 100000 دج إلى 500000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن سباً أو قذفاً سواءٌ كان ذلك عن طريق الكتابة أو الرسم أو التصريح بأي آلية لبث الصوت أو الصورة، أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى. وتباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيًا. وفي حالة العود تضاعف الغرامة"[2].

وعليه في النص السابق كان المشرع يعاقب على هذه الجريمة بالحبس أو الغرامة أو هما معاً، إلا أن المشرع وفقاً للتعديل الجديد حصر العقوبة المطبقة على هذه الجريمة في الغرامة فقط مع مضاعفة قيمتها، كما أن الملاحظ من هذا النص أنه متعلق برئيس الجمهورية فقط دون غيره، وإن كانت الدراسة ترى أنه كان على المشرع العمل بهذا المبدأ في جميع الجرائم الأخرى، كما يجب أن يشمل بالتعديل حتى تلك الجرائم التي تركب ضد الأفراد العاديين. كما أشارت المادة إلى كيفية المتابعة والتي تحرك تلقائياً من طرف النيابة العامة، وهو ما قد يطرح عدة أسئلة عن طريق المتابعة في حال ارتكاب الجريمة بواسطة الوسائل الإلكترونية عن وسائل الإثبات المعتمدة في ذلك، فضلاً عن قواعد الاختصاص المطبقة على الجريمة[3].

---

1 طارق عفيفي صادق أحمد، المرجع السابق، ص 56.

2 أضيفت هذه المادة بموجب القانون رقم 01-09، وجاء بالصيغة التالية: "يعاقب بالحبس من ثلاثة أشهر إلى اثني عشر شهر وبغرامة من 50000 دج إلى 250000 دج أو بإحدى هاتين فقط. كل من أساء إلى رئيس الجمهورية بعبارات تتضمن قذفا إهانة أو سباً أو قذفاً سواءٌ كان ذلك عن طريق الكتابة أو الرسم أو التصريح، أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى. تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائياً. وفي حالة العود، تضاعف عقوبات الحبس والغرامة المنصوص عليها في هذه المادة". عدلت هذه المادة بموجب القانون رقم 11-14 المؤرخ في 2 أوت 2011 المعدل والمتمم للقانون 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر.ج.ج، ع 44، المؤرخة 10 عشت 2011، ص 4.

3 زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائر وفي التشريع الدولي، ب. ط، دار الهدى، الجزائر، 2011، ص 84.

وخلافاً للمشرع الجزائري، ذهب المشرع الإماراتي إلى تجريم القذف المرتكب بواسطة الهاتف النقال من خلال نص خاص، بموجب المادة 347 من قانون العقوبات الاتحادي والتي جاء فيها: "يعاقب بالحبس مدة لا تزيد على ستة (06) أشهر أو بالغرامة التي لا تتجاوز خمسة آلاف (5000) درهم إذا وقع القذف أو السب بطريق الهاتف، أو في مواجهة الجاني وبحضور غيره"[1]. وكذلك المشرع المصري سار على نفس نهج المشرع الإماراتي، حيث جاء في المادة 308 مكرر من ق.ع.م أن: "كل من قذف غيره بطريق التليفون يعاقب بالعقوبة المنصوص عليها في المادة 303".

2- الركن المعنوي لـــجريمة القذف بواسطة الهاتف النقال:

تعتبر جريمة القذف من الجرائم العمدية التي تتطلب قصد جنائي عام بعنصريه العلم والإرادة، حيث يكون الجاني على علم بأركان جريمة القذف ونتيجتها الإجرامية، فضلاً عن ذلك يجب أن تتجه إرادة الجاني إلى القيام بهذا الفعل، ولا تتطلب جريمة القذف قصد جنائي خاص[2]، إذ يكفي أن يأتي الجاني بأحد الأفعال الذكورة في المادة 296 من ق.ع.ج.

ثالثاً- العقوبة المقررة لجريـــمة القذف بواسطة الهاتــف النقال:

كما هو مبين في الدراسة سابقاً، لم يتعرض المشرع الجزائري كنظيره الإماراتي إلى استحداث نص خاص بالقذف عن طريق الهاتف النقال، مما يعني أنها تندرج ضمن الأحكام العامة للعقوبة المنصوص عليها فيما يخص جريمة القذف الواردة في المادة 296 من ق.ع.ج، والتي تنص على أن: "يعاقب على القذف الموجه إلى الأفراد بالحبس من شهرين (2) إلى ستة (6) أشهر وبغرامة من 25000 دج إلى 50000 دج أو بإحدى هاتين العقوبتين. ويضع صفح الضحية حداً للمتابعة الجزائية. ويعاقب على القذف الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من شهر (1) إلى سنة وبغرامة من 10000 دج إلى 100000 دج أو بإحدى هاتين العقوبتين فقط إذا كان الغرض هو التحريض على الكراهية بين المواطنين أو السكان"[3].

---

1 قانون العقوبات الاتحادي الاماراتي رقم 2005/34 المعدل والمتمم للقانون 1987/03، متاح على الرابط: *http://sai.gov.ae*، تاريخ الإطلاع: 2019/03/23.

2 محمود محمد محمود جابر، المرجع السابق، ص 63.

3 القانون رقم 06-23 المورخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر.ج.ج، ع 84، المؤرخة 24 ديسمبر 2006، ص 22.

ومنه يتبين من خلال النص السابق أن المشرع الجزائري كيَّف القذف على أنه جنحة رتب عليها جزاء مادي ومالي أو كليهما، وهذا على عكس ما ذهب إليه المشرع المصري في نص المادة 303 من ق.ع.م، والذي عاقب على الفعل في الحالات العادية بعقوبة مالية فقط: "يعاقب على القذف بغرامة لا تقل عن خمسة آلاف (5000) جنيه ولا تزيد على خمسة عشر ألف (15000) جنيه"[1]. كما أن المشرع الجزائري عمد إلى تشديد العقوبة على القذف، وذلك في الحالات المنصوص عليها في الفقرة الثانية من المادة 298 من ق.ع.ج. وذلك في حال ما كانت الجريمة تحض على التحريض والكراهية.

ومن خلال ما سبق ذكره ندعوا المشرع الجزائري إما إلى تجريم القذف بواسطة الهاتف النقال بنصوص خاصة، أو أن يقوم بإدراج نص ضمن نفس المادة يتضمن ارتكاب الجريمة بواسطة الهاتف النقال.

الفرع الثالث: جريمة الســـب بواسطة الــهاتف النقال.

يعرف السب على أنه: "خدش شرف شخص واعتباره عمداً دون أن يتضمن ذلك إسناد واقعة معينة إليه"[2]. كما عرِّف على أنه: "نشاط من شأنه أن ينال من شرف وكرامة شخص معين ويحط من قدره بأي لفظ ازدراء أو سباب"[3]، ويعرفه آخرون على أنه: "خدش شرف شخص أو اعتباره، بإلصاق صفة أم عيب مشين إليه"[4].

أما بالنسبة لجريمة السب المرتكبة بواسطة الهاتف النقال فتعرف بأنها: "إلصاق صفة مشينة أو نسبة فعل فاضح إلى شخص من خلال استخدام تقنيات الهاتف المحمول، سواءٌ بإرسال رسالة نصية إلى هاتف الضحية أو الغير أو بث (نشر) عبارات السب عبر مواقع التواصل الاجتماعي أو غرف الشات الخاصة بها أو عبر صفحات الويب العادية"[5].

---

1 القانون رقم 93 المؤرخ 1995/05/28 المتعلق بقانون العقوبات، ج.ر.ج.م، ع 21 مكرر.

2 انسام سمير طاهر الحجامي، المرجع السابق، ص 344.

3 علي جعفر، المرجع السابق، ص 350.

4 محمد بن عبد العزيز بن صالح المحمود، المسؤولية الجنائية عن إساءة استخدام مواقع التواصل الاجتماعي الحديثة (دارسة تأصيلية تطبيقية)، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الدكتوراه، جامعة نايف العربة للعلوم الأمنية، الرياض، 2014، ص 143.

5 طارق عفيفي صادق أحمد، المرجع السابق، ص 162.

وعليه من خلال التعريفات السابقة نستنتج أن السب عبارة عن واقعة تتضمن إيذاء الغير عن طريق قدحه أو الانتقاص من شأنه دون أن يستند الجاني إلى واقعة معينة، وإن كان هذا ما يميز جريمة السب عن جريمة القذف، كما بَين التعريف الأخير كيف تتم جريمة السب بواسطة الهاتف النقال سواءٌ عن طريق استخدام الرسائل النصية أو بث عبارة السباب عبر مواقع التواصل الاجتماعي أو غيرها من الوسائل المرفقة بالهاتف النقال.

أما بالنسبة للمشرع الجزائري فقد جرم السب وفقًا للمادة 297 من ق.ع.ج والتي تضمنت الآتـــي: "يعد سبًا كل تعبير مشين أو عبارة تتضمن تحقيراً أو قدحاً لا ينطوي على إسناد أي واقعة". وعليه من خلال هذه المادة يظهر أن المشرع الجزائري لم يُضَمِّن المادة الطرق التي يمكن أن يتم من خلالها السب، حيث ترك السلطة التقديرية للقاضي، باستثناء ما ورد في المادة 144 مكرر المذكورة آنفاً، وهذا عكس ما ذهب إليه المشرع المصري الذي ضمن التليفون كوسيلة يمكن أن يرتكب من خلالها جريمة السب، وذلك ما تضمنته المادة 308 مكرر في فقرتها الثانية[1].

أولاً– الركن المادي في جريـمة السب عــبر الهاتف النقال:

يتمثل الركن المادي لجريمة السب بصفة عامة في إتيان الجاني خدش أو انتقاص من المجني عليه، وذلك بوصفة أو نعته بسلوك غير لائق، أو من خلال التلفظ بأقوال يستهجنها العرف ويعدها المجتمع سباً[2]، والسب قد يقع بأي طريقة من الطرق سواءٌ عن طريق استخدام الجاني الكتابة أو الفعل أو القول، كما قد يكون بطريقة ضمنية أو بالتعبير الصريح بشرط أن تتوفر فيه العلانية[3]، ويرى البعض[4] أنه لا يشترط في العلانية أن تكون حقيقية بحيث تتصل الواقعة المسندة إلى الجمهور بل قد تكون العلانية مفترضة، ومثاله كأن يتم السب عن طريق رسالة نصية إلى الضحية فقد تقتصر العلانية على

---

1 تنص المادة 308 مكرر في فقرتها الثانية على أن: "... وكل من وجه إلى غيره بالطريق المشار إليه بالفقرة السابقة سباً لا يشمل على إسناد واقعة معينة، بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار، يعاقب عليه بالعقوبة المنصوص عليها في المادة 308".

2 محمد عبيد الكعبي، المرجع السابق، ص 132.

3 شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت–دراسة مقارنة– ب. ط، دار النهضة العربية، القاهرة، 2009، ص 154.

4 مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، بدون طبعة، دار النهضة العربية، القاهرة، 2000، ص 89.

الضحية في هذه الحالة دون غيره[1]. ولا يخرج السلوك المادي لجريمة السب بواسطة الهاتف النقال عن أحد الطرق المذكرة سابقاً، حيث لا تتغير إلا الوسيلة التي استخدمها الجاني في الجريمة، وإن كان ارتكاب الجريمة عبر الهاتف النقال قد يتطلب بعض الأعمال التحضيرية وقد يظهر ذلك في كتابة الرسالة، أو تسجيل الرسالة سواءٌ عن طريق تقنية التسجيل الصوتية أو عن طريق تسجيل الفيديو[2].

ثانياً– الركن المعنوي في جريـمة السب عـبر الهاتف النقال:

يعتبر السب من قبيل الجرائم العمدية التي لا تتطلب إلا توفر قصد جنائي عام، وذلك من خلال علم الجاني بأن ما يأتيه من أفعال يشكل جريمة سب في حق الضحية، كما يجب أن تتجه إرادة الجاني إلى القيام بهذا الفعل[3].

ثالثاً– العقوبة المقررة لجريمة السب عبر الهاتف النقال:

لم يقرر المشرع الجزائري عقوبة خاصة بجريمة السب المرتكبة بواسطة الهاتف النقال، مما يعني تطبيق النص الخاص بجريمة السب العادية، والتي يعاقب عليها المشرع الجزائري بـ: "يعاقب على السب الموجه إلى فرد أو عدة أفراد بالحبس من شهر (1) إلى ثلاثة (3) أشهر وبغرامة من 10000دج إلى 25000 دج"[4].

ومن خلال نص هذه المادة السابقة يتضح أن جريمة السب تُكيف على أنها مخالفة، كما أن المشرع الجزائري عاقب عليها بعقوبة سالبة للحرية وعقوبة مالية أو إحدى تلك العقوبات، بينما نجد المشرع المصري قد عاقب على جريمة السب المرتكبة بواسطة التليفون وفقاً للمادة 306 من ق.ع.م والتي تنص على أن: "كل سب لا يشمل إسناد واقعة معينة بل يتضمن وجه من الوجوه خدشاً

---

1 وأمثلة ذلك الحكم الذي صدر عن محكمة مصرية، رقم 68 لسنة 2013، والذي تتلخص وقائعه في أن رجل تم الاعتداء عليه من قبل زوجته السابقة من خلال إرسالها لرسائل نصية متضمنة عبارات السب والقذف في حقه، مما تسبب في إزعاج مستمر له وذلك على الهاتف الخاص، وتضمنت هذه الرسائل عبارات غير لائقة، **انظر في ذلك:** حسن إبراهيم خليل، تطبيقات قضائية على جريمة الإزعاج المعتمد عن طريق وسائل الاتصالات الحديثة، ط. الأولى، دار الفكر والقانون للنشر والتوزيع، مصر، 2015، ص 23.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 164.

3 أحس بوسقيعة، المرجع السابق، ص 222.

4 القانون رقم: 06/23 المؤرخ 20 ديسمبر 2006، المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، ج.ر.ج.ج، ع 84، المؤرخة 24 ديسمبر 2006، ص 22.

للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بغرامة لا تقل عن ألفي (2000) جنيه ولا تزيد على عشرة آلاف (10000) جنيه"[1]. حيث ذهب المشرع المصري في مسلك مغاير لما ذهب إليه المشرع الجزائري وذلك بأن عاقب على الفعل بالغرامة فقط دون عقوبة الحبس، وهو نفس ما قام به فيما يخص جريمة القذف.

من جانب آخر، نجد أن المشرع الجزائري عاقب على السب الذي قد يستهدف مجموعة بسبب انتماءهم العرقي والمذهبي أو الديني، وهو ما نصت عليه المادة 298 مكرر من ق.ع.ج[2].

وشدد المشرع المصري العقوبة على جريمة السب المرتكبة بواسطة الهاتف النقال وفقاً للمادة 308 من ق.ع.م والتي جاءت على الشكل الآتي: "إذا تضمن العيب أو الإهانة أو القذف أو السب الذي ارتكب بإحدى الطرق المبينة في المادة 171 طعناً في عرض الأفراد أو خدشاً لسمعة العائلات تكون العقوبة الحبس والغرامة معاً في الحدود المبينة في المواد 179، و181، 182، و303، 306، 308 على ألا تقل الغرامة في حالة النشر في إحدى الجرائد أو المطبوعات عن نصف الحد الأقصى، وألا يقل الحبس عن ستة (06) شهور"[3].

الفرع الرابـع: جريـمة التشهير عبر الهاتــف النقال.

يعرف التشهير على أنه: "الاعتداء على سمعة أحد بذكره سواء لدى عدة أشخاص، أو في الصحف أو غيرها من طرق العلانية"[4].

وعليه نستنتج من هذا المفهوم أن جريمة التشهير هو سلوك يأتيه الجاني من أجل المساس بمقام أو مكانة إنسان من خلال التلفيق عليه أو ذكره بأمر يفترض فيه الستر، وذلك من خلال نشره بين عدة أشخاص، أو عن طريق وسائل الإعلام، أو غيرها من الطرق الأخرى التي تؤدي إلى إعلام الآخرين به.

---

1 القانون رقم 148 المؤرخ في 2006/07/15، المتعلق بقانون العقوبات، ج.ر.ج.م، ع 28 مكرر.

2 تنص المادة 298 على أن: "يعاقب على السب الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من خمسة أيام (5) أيام إلى ستة (6) أشهر وبغرامة من 5000 إلى 50000 دج أو بإحدى هاتين العقوبتين فقط".

3 القانون رقم 95 المؤرخ في 1996/06/30 المتعلق بقانون العقوبات، ج.ر.ج.م ، ع رقم 25 مكرر.

4 أشرف السعيد أحمد، القرصنة الإلكترونية، ب. ط، مطابع الشرطة، مصر، 2013، ص 74.

أولاً– الركن المادي لجريـمة التشهير عبر الهاتـف النقال:

يتكون الركن المادي لجريمة التشهير من فعل التشهير، وعلانية التشهير.

1– فـــعل التشهير:

يتمثل فعل التشهير في ذلك التعبير عن فكرة ما أو معنى، بقصد ذكر الغير بما يؤدي إلى إلحاق الأذى به، سواء عن طريق التشهير به لدى عدَّة أشخاص، أو عن طريق أحدى وسائل الإعلام، أو بواسطة وسائل الإتصال الحديثة، كما يتم ذلك عن استخدام وثيقة عمومية بعض النظر عن نوع هذه الوثيقة إذا كانت وثيقة صحيحة أم لا[1].

ومن أمثلة التشهير نشر صور فاضحة للمجني عليها بحيث يكون الهدف منها الحط من مكانتها واعتبارها، بغض النظر عن صحة هذه الصورة، وهو ما تساعد عليه الهواتف النقالة عن طريق التطبيقات والتقنيات التي تتيح فرصة للجاني تركيب الصورة كيفما يشاء[2].

2– علانـــية التـــشهير:

تتمثل العلانية في تبليغ أو نشر الصور أو المستندات التي يحوز عليها الجاني حتى يطلع عليها الجمهور، وذلك بغض النظر عن وسيلة النشر والتبليغ[3]، وإن كنا نرى أن الهاتف النقال من أخطر الوسائل التي يمكن أن تُستعمل لارتكاب هذه الجريمة عبر وسائل الاتصال الحديثة، وذلك من خلال سرعة هذه الوسائل في نشر ما يسعى الجاني إلى نشره، فضلاً عن انتشار هذه الوسائل بشكل كبير بين الناس.

ثانياً– الركن المعنوي لجريمة التشهير بواسطة الهاتف النقال:

تعتبر هذه الجريمة من الجرائم العمدية التي تتطلب توفر قصد جنائي عام، وذلك من خلال علم الجاني بعناصر الجريمة التي يقوم بها، سواء من خلال فبركته لصور الضحية، أو حيازته مستندات أو وثائق، بغض النظر عن صحتها تقلل من شأن المجني عليه، حيث يقوم الجاني بنشرها أو الإعلان عنها، كما يجب أن تتجه إرادة الجاني إلى القيام بهذا الفعل من أجل الإضرار بالضحية[4].

---

1 أشرف السعيد أحمد، نفس المرجع، ص 75.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 169.

3 أشرف السعيد أحمد، المرجع السابق، ص 77.

4 أيمن بن ناصر بن حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الإجتماعي –دراسة مقارنة–، ط. الأولى، مكتبة القانون والإقتصاد، الرياض، 2015، ص 107.

ثالثاً– موقف المشرع الجزائري من جريمة التشهير عبر الهاتف النقال:

لا يوجد نص صريح يـجرم هذا النوع من الأفعال فـي القانون الجزائري، وإن كانت هناك بعض النصوص العامة مثل المادة 371 من ق.ع.ج والتي جاء فيها: "كل من تحصل بطريقة التهديد كتابة أو شفاهة، أو بإفشاء أو نسبة أمور شائنة على أموال أو أوراق مالية أو على توقيع أو على أحد المحررات المبينة في المادة 370، أو شرع في ذلك، يكون قد ارتكب جريمة التهديد بالتشهير"[1]، وعليه من خلال نص هذه المادة يتضح أن المشرع الجزائري قصد ولو بطريقة غير مباشرة حماية شرف واعتبار الأشخاص، بالرغم من أن هذه المادة تهدف إلى أبعد من ذلك، حيث أن هذه الجريمة المسماة بجنحة التهديد بالتشهير صنفها المشرع الجزائري ضمن جرائم الفصل الثالث المعنون بالجنايات والجنح ضد الأموال، كما يتضح أن الهدف منها هو الحصول على مال من الضحية أكثر منه استغلال الضحية عن طريق ابتزازه بأسرار، أو أمور شائنة تهدد وظيفته، أو سمعته، أو حياته الخاصة ولو بطرق ثانوية، وإن كنا نرى إمكانية أن يُستغل الهاتف النقال في هذه الجريمة، سواءٌ في المرحلة التحضيرية للجريمة كأن يقوم الجاني بتصوير الضحية في فيديو مشين، أو يلتقط له صور أو يسجل له، فضلاً عن إمكانية القيام بذلك من خلال نشر ما تم التحصل عليه عن طريق استخدام الهاتف النقال.

وتعاقب المادة 371 من ق.ع.ج على هذا الفعل بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 2000 دج إلى 30000 دج، كما قد يحكم على الجاني بالحرمان من كافة الحقوق المنصوص عليها في المادة 14 من ق.ع.ج والتي نصت على: "يجوز للمحكمة عند قضائها في جنحة، وفي الحالات التي يحددها القانون، أن تحظر على المحكوم عليه ممارسة حق أو أكثر من الحقوق الوطنية المذكورة في المادة 9 مكرر 1، وذلك لمدة لا تزيد عن خمس (5) سنوات. وتسري هذه العقوبة من يوم انقضاء العقوبة السالبة للحرية أو الإفراج عن المحكوم عليه."

1 القانون رقم 82-04 المؤرخ في 13 فيفري 1982، المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتمم، ج.ر.ج.ج، ع 7، المؤرخة 16 فبراير 1982، ص327.

المبحث الثاني:
جرائم الأموال المرتكبة بواسطة الهاتف النقال.

تعتبر جرائم الأموال من بين أهم الجرائم التي استفادت من التطور التكنولوجي، ويرجع ذلك إلى عدة عوامل؛ أهمها تغير مفهوم النقود والتعاملات المالية، حيث أصبحت تأخذ الطابع الإلكتروني في جميع المجالات، خاصة في الدول المتطورة التي تعرف ما يسمي بالنقود الإلكترونية، والبنوك الإلكترونية، ولذلك يتم التطرق من خلال هذا المبحث إلى بعض أهم جرائم الأموال التي ترتكب عبر الهاتف النقال وبيان أحكامها؛ وذلك من خلال التطرق لجريمة السرقة والنصب بواسطة الهاتف النقال (المطلب الأول)، ثم جريمة غسيل الأموال بواسطة الهاتف النقال (المطلب الثاني).

المطلب الأول: جرائم السرقة والنـصب بواسطة الهاتـف النقال.

تعتبر جرائم السرقة والنصب من أقدم جرائم الأموال التي عرفها الإنسان، بالرغم من أن هذه الجرائم تتطور بتقدم العصور والأدوات، فكلما زاد تقدم المجتمع إلا وحاول المجرمين الاستفادة من هذا التقدم في ارتكاب جرائمهم، ونتيجة لهذا التغير، قسمنا هذا المطلب إلى فرعين، يتم من خلالهما دراسة جريمة السرقة بواسطة الهاتف النقال (الفرع الأول)، ثم جريمة النصب بواسطة الهاتف النقال (الفرع الثاني).

الفرع الأول: جريمة السرقة بـواسطة الـهاتف النقال.

نبين من خلال هذا الفرع الأحكام العامة للسرقة، ثم طرق ارتكابها بواسطة الهاتف النقال.

أولاً– مفهوم جريمة السرقة[1]:

هناك العديد من المفاهيم الفقهية للسرقة من بينها تعريف السرقة على أنها: "اختلاس مال منقول مملوك للغير بنية تملكه"[1].

---

1 تعرف السرقة في اللغة بأنها: "أخذ المال خفية، فالسين والراء والقاف أصل يدل على أخذ الشيء في خفاء وستر، ويقال استرق السمع، أي استمع مستخفياً، ويقال هو يسارق النظر إليه، إذا اهتبل غفلته لينظر إليه، والسارق جاء مستتراً إلى حرز فأخذ منه ما ليس له فإن أخذ من ظاهر فهو مختلس ومنتهب فإن منع مما في ده فهو عاصب". **انـــظر:** مجمع اللغة العربية، المعجم الوسيط، ط. الرابعة، مكتبة الشروق الدولية، مصر، 2004، ص 428.

تشريعياً عرفها المشرع الجزائري في المادة 354 من قانون العقوبات على أنها: "كل من اختلس شيئاً غير مملوك له يعد سارقًا ويعاقب بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من 100.000 دج إلى 500.000 دج"[2].

وعليه من خلال ما سبق، يتضح أن جريمة السرقة تتطلب لقيامها توفر الشروط الآتية:

- أن يكون موضوع السرقة مالاً.
- أن يكون منقولاً.
- أن يكون مملوك للغير.
- أن يكون في حيازة الغير غير المتهم.

ثانياً– صور جريمة السرقة المرتكبة بواسطـــة الهاتـف النقال:

تتحقق جريمة السرقة بواسطة الهاتف النقال من خلال قيام الجاني بأحد الأفعال الآتية:

1- سرقة الهاتف النقال (الجهاز):

تتحقق هذه الصورة في حال ما إذا ارتُكبت الجريمة ضد الآلة التي تستقبل الكلام وترسله، وذلك بغض النظر عن نوعية هذا الهاتف وجودته، وإن كان يستدل على الهاتف محل السرقة من خلال رقم "الشاسيه" أو "البورد"، إما بالإطلاع عليه داخل الجهاز، أو بإظهاره على شاشة عرض الجهاز بضغط عدد معين من الأرقام[3]، ولا اختلاف في هذه الحالة على اعتبار الهاتف النقال منقولاً، حيث تنطبق عليه جميع أحكام المنقول الواردة بموجب القانون المدني.

2- سرقـــة رصـــيد الهاتف النقال:

يعرف رصيد الهاتف النقال على أنه: "قيمة الخدمات الإتصالية والمعلوماتية التي تقدمها شركة الهاتف المحمول للحامل الشرعي للهاتف عندما تكون مدفوعة مقدماً، ويحصل العميل على هذا

---

1 أحمد حمد الله أحمد، جريمة السرقة المرتكبة بواسطة الهاتف النقال، مجلة كلية الحقوق، المجلد 16، العدد1، جامعة النهرين، العراق، 2014، ص 209.

2 القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للقانون 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات ج.ر.ج.ج، ع 84، ص 24.

3 زين العابدين عواد كاظم، جريمة سرقة الهاتف في القانون العراقي والمقارن، مجلة الكوفة للعلوم القانونية والسياسية، جامعة الكوفة، العدد 6، 2010، ص 183.

الرصيد بطرق عدة، منها شراء كارت الشحن أو الشحن الإلكتروني أو تحويل الرصيد"[1]. ويتم سرقة الرصيد عن طريق الإستيلاء على كارت الشحن، أو سرقة أرقام السرية للكارت دون الاستيلاء على الدعامة، أو عن طريق فك شفرة الكارت[2]، وتتحقق هذه الجريمة من خلال قيام الجاني بالولوج إلى النظام الخاص بشبكة الجهاز النقال، ثم يستولي على أرصدة خاصة ببعض المشتركين وتحويلها إلى ملكيته، مما يؤدي إلى إنقاص رصيد المجني عليه أو الاستيلاء عليه كله[3].

3- الشريـحة الإلكترونـــية:

وهي عبارة عن نوع من الرقائق المعدنية يُثبت عليها دوائر كهربائية ومغناطيسية متناهية الدقة، وتلعب الشريحة دور الوسيط بين شركة الاتصالات والعميل، بحيث ينحصر دورها في إعداد الهاتف المحمول لتلقي وإرسال الموجات المترددة[4].

4- سرقـــة الخـــط الـــهاتفي:[5]

يتمثل الخط الهاتفي في ذبذبات وموجات تتدفق عبر أسلاك تحتوي على رسائل صوتية أو مكتوبة أو مرئية، ومما يجب الإشارة إليه أن محكمة النقض المصرية استقرت في أحكامها على اعتبار سرقة الموجات والذبذبات جريمة سرقة شأنها شأن الجرائم الأخرى التي ينطبق عليها مفهوم السرقة، كما أنه وفقاً للقانون المدني المصري تعتبر الموجات والذبذبات منقولاً تنطبق عليه الأحكام العامة للمنقول[6].

5- ســـرقة الـــمعلومات:

---

1 طارق عفيفي صادق أحمد، المرجع السابق، ص 100.

2 طارق صادق عفيفي، نفس المرجع، ص 100.

3 محمود محمد محمود جابر، المرجع السابق، ص 174.

4 زين العابدين عواد كاظم، المرجع السابق ، ص 184.

5 من بين الاستخدامات الأخرى لخطوط التليفون أن تستعمل في نقل الأصوات والإشارات التليفزيونية والصور والبيانات الرقمية الصادرة عن أجهزة الكمبيوتر، المعلومات المقروءة آلياً بواسطة جهاز الكمبيوتر، ومن الوسائل الأخرى كذلك المرتبطة بخطوط التليفون، ما يعرف الفاكسميل، التليتايب، والوصول المباشر، واللمس النغمي التليفوني، الكابلات وغيرها، **انظر في ذلك:** محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية – دراسة مقارنة- ط. الأولى، دار الفكر والقانون، المنصورة، مصر، 2017، ص 88-89.

6 قرار محكمة النقض المصرية رقم 69/1155 ق، الجلسة 2000/01/02، غير منشور.

تعرف المعلومات (المعلوماتية) على أنها: "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال، أو للتفسير والتأويل (Interpretation)، أو للمعالجة (Processing)، سواءٌ بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة"[1].

وتعتبر سرقة المعلومات من المواضيع التي أثارت جدلًا واسعاً؛ وذلك بالنظر إلى طبيعة المعلومات وإمكانية تعرضها للسرقة، مما جعل الفقه ينقسم إلى اتجاهين وهما كالآتي:

أ- الاتـــجاه الأول:

يميل هذا الاتجاه إلى فكرة عدم إمكانية تطبيق أحكام السرقة التقليدية على سرقة المعلومات، ويرون بعدم تكييفها بالسرقة، ويبررون ذلك بعديد من الأسباب لعل من أهمها[2]:

- أن الأمر يتعلق بالمعلومات سواء تعلقت بالحاسب الآلي أو الهاتف النقال، فهي عبارة خدمات وليست أموال، حيث أن مجرد بث هذه المعلومات من طرف صاحبها على أي شبكة من الشبكات، واعتراض الآخرين لها لا يتعلق بالسرقة، كون هذه المعلومات لا تتوفر فيها صفة المنقول.
- عدم قابليتها للتملك، كما يرون بأن أي توسيع في النصوص الجنائية يمثل خرقاً لمبدأ الشرعية، حيث أن المشرع لم يدرج سرقة المعلومات في النص المتعلق بالسرقة، مما يعني أن النص لا ينطبق عليها، ومن الأمثلة التي يستند عليها أصحاب هذا الاتجاه أن محكمة استئناف باريس رفضت تطبيق نصوص السرقة على قيام عاملة بالتصوير الضوئي لمستندات كانت تعمل بها، حيث قامت بذلك ليتوفر لديها دليل لإثبات حقوقها قِبل الشركة، وهو نفس الشيء الذي أيدته محكمة باريس حيث رأت "أن الإختلاس يفترض خروج الشيء من حيازة صاحبه الأصلي"[3].

ب- الاتـــجاه الثانـــي:

---

1 محمد عبد الله العوّا، المرجع السابق، ص 67.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 107.

3 الحكم رقم 020274، صادر عن محكمة باريس، بتاريخ 12 فيفري 1996. **نقلاً عـن:** نائلة عادل محمد فريد قورة، المرجع السابق، ص 134.

بعكس الرأي الأول يميل هذا الاتجاه إلى تأييد فكرة تطبيق السرقة على المعلومات، ويستندون في ذلك إلــى:

- إمكانية ترجمة المعلومات إلى أفكار، فضلاً عن نسخها على شريط أو قرص ممغنط، ثم معرفة ما فيها والاستحواذ عليه.
- كما أن الجاني يهدف من خلال استحواذه على هذه المعلومات الانتفاع منها، من خلال ما تحققه من أرباح مالية كانت ستعود على صاحبها الأصلي.
- كما يرى البعض[1] أن فعل الاختلاس إنما يتحقق بحسب صفة الشيء المختلس، فالإختلاس قد يتحقق بمجرد الإطلاع أو السماع، وإن كان في هذه الحال لا تتم المعاقبة عليه.

ويشير أصحاب هذا الاتجاه[2] في الغالب إلى القياس على حكم الكهرباء، حيث تعتبر مال غير ملموس إلا أنه تنطبق عليها أحكام السرقة، كما أن القضاء الفرنسي قد أدان سرقة المعلومات فيما يعرف بقضية Logabax الذي كان يعمل موظفاً في شركة تقوم بتصوير مستندات سرية ضد رغبة صاحبها، حيث أن المحكمة لم تشترط في قضية الحال تحقق الاختلاس كما في السرقة العادية، حيث ترى مقدرة تحققه على أساس اليد العارضة، فضلاً على اعتبار الجاني قد استولى على المستندين التابعين للشركة المذكورة بدون علم ورضاء رب العمل[3].

ونحن بدورنا نؤيد الاتجاه الثاني فيما ذهب إليه، ويرجع ذلك إلى إمكانية اعتبار المعلومات قابلة للسرقة، ذلك أن سرقة المعلومات أخطر وأشد من سرقة المال المادي، ما قد ينتج عن المال المعنوي المتمثل في المعلومات من نتائج، سواء تمثل في ناتج مادي؛ خاصة إذا كانت هذه الأفكار أو

---

1 نائله عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية –دراسة نظرية وتطبيقية، ط. الأولى، منشورات الحلبي، بيروت، 2005، ص 152.

2 هنا من يرى أنه لا يجب الخلط بين الطاقة الكهربائية والمعلومات من حيث القياس، حيث يعتبر الطاقة الكهربائية قابلة للقياس والتحديد، بينما المعلومة لا تقبل ذلك، كما لا يجوز الخلط بين المعلومة ومالها من قيمة، ويضيف صاحب الرأي أن هناك اختلاف من حيث الطبيعة بين الطاقة الكهربائية التي تعتبر مال مادي حتى ولو كانت غير ملموسة، وبين المعلومات التي يجري البحث عن محتواها الفكري، **انـــظر**: جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، ط. الثانية، دار النهضة الحديثة، القاهرة، 2012، ص 69-70.

3 Cass. Crim, 29 avril 1986, J.C.P, 1987, ll, 20788 .N° 5.

المعلومات قيَمة وقابلة للتطبيق على أرض الواقع، أو ناتج معنوي قد يظهر في صورة تشهير بالآخرين أو ابتزازهم من أجل الحصول على أموال أو أي منفعة أخرى.

جدير بالذكر أن هناك ثلاثة طرق يتم من خلالها سرقة المعلومات من الهاتف النقال، تتمثل في:

1) الإلتـقاط الذهــني للمعلومات:

ويعرف على أنه: "الالتقاط البصري أو الاستحواذ البصري على البيانات؛ بمعنى حيازتها والتقاطها ذهنياً وبصرياً من الشاشة، وقد يأتي الجاني هذا السلوك في عدَة طرق، منها الالتقاط البصري، كأن يشاهد ما على شاشة الهاتف النقال دون علم صاحبه، خاصة ما إذا كان معلومات مهمة، وتشترط توفر نوع من السرية بالنسبة لأصحابها، أو أن يقوم الجاني بالتنصت على رسائل صوتية تخص الضحية عن طريق الهاتف النقال، كما هو عليه الحال في استخدامنا لتطبيقات التسجيل الصوتي مثل تطبيقي "واتساب، وماسنجر"، ويذهب البعض[1] إلى تأييد هذه الفكرة؛ حيث يرون أن القيام بمثل هذا السلوك يستوجب عقاب صاحبه، حيث أنه لا فرق بين كون الجاني قد حفظ الملف على مستند أو حفظه في ذاكرته، ففي كل الحالات يكون قد تحصل على المعلومات.

ونحن بدورنا نرى بأن هذا الرأي غير موفق بحيث يفتح الباب للولوج إلى نوايا الأشخاص، بحيث إذا لم تتحقق نتائج معينة تشير إلى إطلاع هذا الشخص على هذه المعلومات، فلا يمكن معاقبته على فعل يُعتبر مجرد فكرة لم يجسدها قول أو عمل.

2) النسخ غير الـمشروع للمعلومات الـمخزنة فـي نظام الهاتف النقال:

يتصور ارتكاب الجاني لهذه الجريمة من خلال النسخ؛ كأن يقوم بنسخ المعلومات الموجودة في هاتف الضحية على هاتفه، وذلك عن طريق تقنيات الإرسال المتوفرة على الهاتف كتقنية البلوتوث، أو تقنية شريط (SHAREIT)، أوعن طريق وصل الهاتف بكابل مع هاتف آخر أو جهاز حاسوب، أو باستعمال تقنية الواي فاي، أو الرسائل المفخخة بفيروسات والتي تقوم بنسخ المعلومات تلقائيًا[2].

3) الالتقاط الـهوائي لـموجات الهاتــف النقال:

---

1 محمود محمد محمود جابر، المرجع السابق، ص 176.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 107.

يعتبر الهاتف النقال من قبيل التكنولوجيات التي تعتمد أسلوب استقبال الرسائل الصوتية والنصية والصور، وذلك من خلال ما يعرف بموجات كهرومغناطيسية، وقد يتساءل البعض عن صلاحية هذه الموجات في أن تكون عرضة للسرقة، وهناك من يرى بعدم وقوع السرقة على مثل هذه الموجات الصادرة من الأجهزة المعلوماتية، أو حتى البيانات الإلكترونية أثناء تناقلها، وإن تجسدت هذه الموجات والأشعة في شكل صورة كهرومغناطيسية، ويرجع ذلك إلى عدم تحقق انتزاع أو سلب حيازتها[1].

ثالثاً– الركن الـمعنوي لـجريمة السرقة بواسطة الهاتـف النقال:

تعتبر جريمة السرقة من الجرائم التي تتطلب قصد جنائي عام وقصد جنائي خاص، يتمثل القصد الجنائي العام في علم الجاني بالسلوك الذي يقوم به، وأنه مجرم سواءٌ من خلال الاعتداء على الهاتف النقال في حد ذاته أو في الاعتداء على معطيات الهاتف النقال، وفضلاً على عنصر العلم يجب أن تتجه إرادة الجاني إلى القيام بهذا الفعل بحيث تكون حرة وغير مكرهة، أما القصد الجنائي الخاص فيتمثل في نية تملك شيء موضوع الاختلاس من خلال حرمان المالك منه والحلول مكانه[2].

الفرع الثاني: جريـــمة النصب بواسطة الـهاتف النقال.

تعتبر جريمة النصب من بين أكثر الجرائم المنتشرة عبر وسائل التقنية الحديثة، ويرجع ذلك لسهولة القيام بها، فضلاً عن سهولة استدراج الضحايا، لذلك سنتناول من خلال هذا الفرع أحكام جريمة النصب وصور ارتكابها بواسطة الهاتف النقال، على النحو التالـــي:

أولاً– مفهوم جريـــمة النصب:

يعرف النصب بأنه: "الاستيلاء على منقول مملوك للغير بخداع المجني عليه وحمله على تسليمه"[3]. وتعرف جريمة النصب المرتكبة بواسطة الهاتف النقال بأنها: "استغلال الجناة لتقنية الهاتف المحمول لخداع أحد الأفراد للاستيلاء على مال منقول مملوك له أو الحصول على امتياز مالي آخر"[4].

---

1 محمود محمد محمود جابر، المرجع نفسه، ص 178.

2 أحسن بوسقيعة، المرجع السابق، ص 276.

3 محمد إبراهيم سعد النادي، المرجع السابق، ص 81؛ **انظر كذلك:** محمد عبيد لكعيبي، المرجع السابق، ص 220.

4 طارق عفيفي صادق، المرجع السابق، ص 109.

ومن المفاهيم الواردة أعلاه يتضح بأن النصب يقوم على أساليب الاحتيال والخداع التي يأتيها الجاني من أجل إيهام الضحية بربح مالي أو مادي، أو الحصول على شيء ذو قيمة لدى الضحية، وفي المقابل يقوم الجاني بالاستيلاء على منقول مملوك للغير أو الحصول على أي امتياز آخر، بحيث تقوم الضحية بتسليمه له بكامل إرادتها الشخصية، أما استعمالات الهاتف النقال في جريمة النصب فهي متعددة سيتم التطرق لها عند دراسة صور استخدام الهاتف النقال في جريمة النصب.

وبناءً على ما ذكر من مفاهيم نرى بأن جريمة النصب بواسطة الهاتف النقال هي: كل فعل يقوم به الجاني من أجل الاستيلاء على أموال منقولة مملوك للغير يستخدم فيها تقنية الهاتف النقال بحيث يحدث في نفس الضحية وهم بالربح أو الحصول على امتياز ما.

ثانياً– الركن الـــمادي لجريمة النصب بواسطة الهاتف النقال:

جرم المشرع الجزائري جريمة النصب بنص المادة 372 من ق.ع.ج، التي اشترط من خلالها المشرع الجزائري من أجل قيام هذه الجريمة أن يأتي الجاني إحدى الطرق الإحتيالية التاليـــة[1]:

- استعمال أسماء أو صفات كاذبة أو سلطة خيالية.
- اعتماد مال خيالي.
- إحداث أمل بالفوز بأي شيء.
- وقوع حادث أو أية واقعة وهمية.

فضلاً عن إتيان الجاني أحد الأفعال الاحتيالية السابقة، وجب عليه أن يستولي على ما لدى الضحية من أموال أو منقولات أو سندات أو غيرها من المصالح الواردة بنص المادة 372 من

1 جاء نص المادة 372 على الشكل التالي: "كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو بإحداث الأمل بالفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها، يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20000 دينار..."

ق.ع.ج، كما أن مجرد الكذب لا يكفي لقيام الجريمة، وهو ما استقر عليه الفقه وذلك مهما كان الجاني بارعاً، وكل ما يقول يدعو إلى تصديقه[1].

أما عن طرق النصب بواسطة الهاتف النقال فهي كثيرة ومتعددة وتظهر في أشكال مختلفة منها:

1- تنظيم المسابقات الوهمية والدعوى لها عن طريق الهاتف النقال:

من أجل التأثير على البعض حتى يتم استدراجهم والاستيلاء على ما يملكون من أموال، وحتى يكون الاحتيال أكثر مصداقية غالباً ما يضع أصحاب هذه المسابقات شروط صارمة وذلك من خلال الالتزام بإدخال البيانات، فضلاً عن اشتراط وضع رقم الهاتف والعنوان[2].

2- الاستيلاء على رصيد الهاتف النقال:

وذلك باستخدام طرق احتيالية عديدة من بينها استخدام الرسائل النصية من خلال بعث رسالة مصطنعة من خلال الجاني على أساس أنها تحتوي على رصيد، ويقوم بإنهاء هذه الرسالة بأرقام مختصرة في العادة تكون مشابهة لأرقام الشركة، ليتصل الجاني بعدها بالمجني عليه وإقناعه بكل براعة عن طرق التمثيل والكذب من أجل إعادة إرسال الرصيد مرة ثانية.

3- استعمال الهاتف في الدعايات الكاذبة:

خاصة ما تعلق منها بأسواق الأسهم والسندات، حيث يتم وهم الضحية بسعر وهمي للسندات، مما يضطره لبيعها بمبلغ زهيد خوفاً من الخسارة[3].

ومن طرق الاحتيالية الأخرى، أن يتم التواصل مع الضحية بعد الحصول على رقم هاتفه بطريقة ما من قبل الجاني وإبلاغه أن أحد أقربائه في منطقة ما قد وقع له حادث، وأنهم من أجل إسعافه يحتاجون مبلغ مالي من النقود[4].

---

1 وهو نفس ما ذهبت إليه محكمة النقض المصرية بأن جريمة النصب لا تتحقق بمجرد الأقوال والادعاءات الكاذبة ولو كان قائلها قد بالغ في توكيد صحتها حتى تأثر بها المجني عليه، بل يجب أن يكون قد اصطحب بأعمال مادية ومظاهر خارجية تحمل المجني عليه من الاعتقاد بصحته". **انـــظر**: محمد عبيد، المرجع السابق، ص 224.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 110.

3 طارق عفيفي صادق أحمد، نفس المرجع، ص 110-111.

4 ومن أمثلة هذه الحالات ما حدث لمواطن سوداني يدعى خالد، حيث هَاتفه أحد الأشخاص وقال له بأن والده تعرض لحادث بمنطقة تدعى "سوبا"، وحتى يتم إسعافه عليك إرسال مبلغ مائة وخمسون جنيها على هذا الرقم، وقال له بأنه وجد رقم هاتفه

ثالثاً– الركن المعنوي لجريمة النصب بواسطة الهاتف النقال:

تعتبر جريمة النصب من الجرائم العمدية التي تتطلب قصد جنائي عام، يتمثل في علم الجاني بالسلوك الإجرامي الذي يقوم به، من خلال إتباعه طريقة احتيالية ما، بالإضافة إلى توجه إرادة الجاني الحرة إلى القيام بهذا الفعل، فضلاً عن القصد الجنائي العام تحتاج جريمة النصب إلى قصد جنائي خاص، وهو نية الجاني على الاستيلاء على أموال الضحية، ونقلها من ملكية الضحية إلى ملكية الجاني الخاصة[1].

المطلب الثاني: جريمة غسيل الأموال المرتكبـة بواسطة الهاتف النقال.

تعتبر جريمة غسيل الأموال من الجرائم المعاصرة التي تندرج ضمن ما يعرف بالجريمة المنظمة والتي تعد أخطر أنواع الإجرام؛ لما لها من بعد عالمي وتأثير على اقتصاديات الدول، وفي الغالب ما تمارس هذه الجرائم على مستوى عالي من الإحترافية والدقة، لذلك سنعالج من خلال هذا المطلب، مفهوم جريمة غسيل الأموال (الفرع الأول)، ثم التطرق لغسيل الأموال بواسطة الهاتف النقال (الفرع الثاني)، فموقف التشريعات من غسيل الأموال بواسطة الهاتف النقال (الفرع الثالث).

الفرع الأول: مفهوم جريـــمة غسيل الأمـــوال.

سنتطرق من خلال هذا الفرع إلى تعريف جريمة الأموال، وطرق غسيل الأموال، وذلك على النحو الآتـــــي:

أولاً– تعريف جريمـــة غسيل الأموال[2]:

مسجل بابني العزيز على هاتف والده، وأسرع بتحويل المبلغ وبعدها تحرك مباشرة لمنزل أسرته الكبيرة، حتى يخبر والدته من أجل ألا تفزع وهي المصابة بالسكري، ليصل بعدها للمنزل ليتفاجأ بوالده يفتح عنه الباب، ليعرف بعدها أنه نصب عليه. **انـــظر في ذلك:** دعاء محمد محمود، مسلسل النصب والاحتيال عبر رسائل الهاتف الجوال مازال مستمراً، موقع سودارس، السودان، متاح على الرابط الإلكتروني التالي: *https://www.sudaress.com/alkharlahza/121*، تاريخ الإطلاع: 2018/08/15.

1 محمود محمد محمود جابر، المرجع السابق، ص 210-211.

2 يعتبر لفظ **"غسيل أموال"** من الألفاظ التي ظهرت في الولايات المتحدة وذلك خلال فترة العشرينات من القرن الماضي التي شهدت ما يعرف بعصابات الشوارع، والتي كانت تبحث عن غطاء شرعي لأموالها الناتجة عن أعمال إجرامية، وذلك من أجل إخفاء مصدرها الإجرامي عن الشرطة، فاتجه أفراد هذه العصابات إلى القيام بأعمال مثل الخدمات ذلك لسهولتها، ولأنها كانت تقوم على النقد، ومن بين أكثر هذه الخدمات اختياراً كان غسيل الملابس، وغسيل السيارات، ومن هنا شق لفظ "غسيل الأموال" وذاع صيته وانتشر استعماله. **انـــظر:** محمد عبد الله الغوا، المرجع السابق، ص 446.

هناك العديد من المفاهيم لجريمة غسيل الأموال، والتي تنوعت بين التعريف القانوني والتعريف الفقهي، وبين من يضيق في التعريف، ومن يوسع فيه بحسب الجرائم التي تترتب عنها جريمة غسيل الأموال.

يعرف البعض[1] جريمة غسيل الأموال بـأنها: "مجموعة من العمليات المالية المتداخلة لإخفاء المصدر غير المشروع للأموال، وإظهارها في صورة أموال متحصلة من مصدر مشروع، أو المساهمة في توظيف أو إخفاء أو تحويل العائد المباشر أو غير المباشر لجريمة هي جناية أو جنحة". ويعرفها آخر[2] بأنها: "توظيف الأموال داخل الدولة أو خارجها في أعمال مشروعة لطمس الأصل غير المشروع لهذه الأموال من خلال تسلل هذه الأموال إلى المشروعات الاقتصادية والتأثير فيها، وبذلك تمر الأموال المتحصل عليها من جرائم من خلال قنوات استثمار شرعية، ويعاد استغلالها بعد ذلك على أنها مصدر ربح مشروع".

نستنتج من خلال التعريفات السابقة أن جريمة غسيل الأموال هي من الجرائم التبعية التي تهدف إلى إخفاء المصدر غير المشروع للأموال المتحصلة بطرق غير مشروعة، وذلك من خلال استثمارها أو توظيفها في أعمال مشروعة، تتيح لأصحابها إعادة استغلالها فيما بعد على أنها أموال مشروعة.

وفي الغالب ما ترتبط جريمة غسيل الأموال بالمخدرات، وإن كانت هذه رؤية الإتجاه الذي ضيَق من مصادر هذه الجريمة، بينما يرى الإتجاه الموسع أنها كل الأموال الناتجة عن أية جناية أو جنحة[3].

ثانياً– خصائص جريـــمة غسيل الأموال:

هناك العديد من الخصائص التي تمتاز بها جريمة غسيل الأموال ومن بين هذه الخصائص:

1- غسيل الأموال جريـــمة عالمية:

تعتبر جريمة غسيل الأموال من قبيل الجرائم المنظمة العابرة للحدود وساعد على ذلك ثورة الاتصالات والمعلومات، فضلاً عن هشاشة الأنظمة الرقابية لبعض البلدان، وغياب التشريعات والقوانين الرادعة[4].

---

1 عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، ب. ط، ب.د.ن، مصر، 2010، ص 32.

2 محمد عبدالله الغوا، المرجع السابق، ص 443.

3 شلبي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، ب. ط، دار هومة، الجزائر، 2013، ص 125.

4 باسل عبدالله الضمَّور، غسيل الأموال في المصارف–دراسة مقارنة–، ط. الأولى، مكتبة القانون والاقتصاد، الرياض، ص 25.

2- غسيل الأموال جريمة منظمة:

تعتبر جريمة غسيل الأموال إحدى الصور التي تضمنتها الإتفاقية الدولية الخاصة بالجريمة المنظمة، والتي ترتكب من قبل عصابات ومجرمين خطرين على مستوى عالي من التنظيم والاحترافية[1].

3- غسيل الأموال جريمة اقتصادية:

تعتبر جريمة غسيل الأموال من بين الجرائم الاقتصادية، وذلك يعود لعدة أسباب منها مساهمة هذا النوع بطريقة مباشرة في اقتصاد الدول خاصة الدول الهشة كما أن لهذه الأموال القدرة على التهديد بانهيار اقتصاديات بعض الدول بحيث تصبح الأموال المشروعة لا فائدة منها ولا تؤدي أي دور أو دعم للاقتصاد[2].

4- غسيل الأموال جريـــمة تابعــة:

تعتبر جريمة غسيل الأموال من الجرائم التي تتطلب قيام جريمة قبلها فلا يتخيل قيامها بشكل منفرد، فلابد أن يأتي الجاني بفعل أصلي كأن تكون جريمة اتجار بالمخدرات، ثم يحاول إضفاء الشرعية على هذه الأموال، وهذا ما يسمى بغسيل أموال[3].

5- استعمال وسائل التقنية الحديثة في تنفيذ جريمة غسيل الأموال:

تعتبر جريمة غسيل من بين أكثر الجرائم المنظمة التي تعتمد على وسائل التقنية الحديثة في ارتكابها، كما أن هذه الوسائل التكنولوجية ساهمت في انتشار وتفشي هذه الجريمة على الصعيد العالمي، بحيث أصبحت عمليات غسيل الأموال تتم عن طريق الهاتف النقال والإنترنت وغيرها من الوسائط الأخرى[4].

ثالثاً- أسباب انتشار جرائـــم غسيل الأموال:

1هيثم عبد الرحمن البقلي، غسيل الأموال –كإحدى صور الجريمة المنظمة بين الشريعة والقانون المقارن–، ب.ط، دار العلوم، مصر، 2010، ص 24.

2 شلبي مختار، نفس المرجع ص 126.

3 عبد الله الزمامي، غسيل الأموال في المملكة العربية السعودية، ب.ط، مكتبة القانون والاقتصاد، الرياض، 2010، ص 28.

4 طارق كاظم عجيل، جريمة غسيل الأموال (دراسة في ماهيتها والعقوبة المقررة لها)، مجلة النزاهة والشفافية للبحوث والدراسات، العدد 1، كلية القانون، جامعة ذي قار، 2009، ص 41.

هناك العديد من الأسباب التي أدت إلى تفشي وانتشار جريمة غسيل الأموال، ومن بين هذه الأسباب الآتية:

1- الفساد الإداري:

يعتبر الفساد الإداري من بين أهم الأسباب التي أدت إلى تفشي ظاهرة غسيل الأموال، حيث يظهر هذا الفساد في العديد من السلوكيات اللاأخلاقية التي يقوم بها بعض الموظفين، مثل الرشوة والمحاباة وغيرها من المظاهر الأخرى للفساد الإداري، كما قد يظهر الفساد في تمكين المسؤولين بعضهم البعض، أو الأشخاص ذوي صلة بهم من قروض بمبالغ كبيرة من دون تقديم أي ضمانات على هذه القروض، ثم يتم تهريبها للخارج بعدما تم غسلها داخلياً[1].

2- سيطرة النظام الرأسمالي على الفكر الإنساني:

إن من أهم أسباب تفشي جريمة غسيل الأموال هو النظام الرأسمالي الذي يسيطر على أغلب الأنظمة الاقتصادية والسياسية، والذي يعتمد على سياسة المصلحة والمادة، مما انعكس على أخلاق الكثيرين فلم يعد يميزون بين ما هو ممنوع وما هو مباح، حيث أصبح كسب المال وجني الثروات أهم هدف يسعى إليه الأفراد والمنظمات بغض النظر عن أي شيء آخر[2].

3- مبدأ سرية الحسابات في البنوك:

إن اعتماد البنوك سياسة غض الطرف عن الأموال التي تُضح فيها بشكل كبير دون السؤال عن مصدرها أو طبيعة عمل أصحابها من أكثر العوامل التي زادت في انتشار هذه الجريمة[3].

رابعاً- مراحل ارتكاب جريمة غسيل الأموال:

يمر ارتكاب جريمة غسيل الأموال بعدة مراحل متتالية، كل مرحلة تتسم بالصعوبة أكثر من سابقتها، لذلك يحاول المجرمون دائماً التطوير من أدواتهم وأساليبهم حتى لا ينكشف أمرهم، وتتمثل هذه المراحل فـــــي:

1- مرحلـــــة الإحلال:

---

1 علاء عبد المحسن جبر السيلاوي، الجريمة المنظمة وأثرها في انتشار الفساد الإداري، مجلة الكوفة، العدد الثاني، ص 223.

2 محمد فوزي صالح، الجريمة المنظمة وأثرها على حقوق الإنسان، مذكرة مقدمة لنيل شهادة الماجستير في القانون الدولي الإنسان، جامعة يحي فارس المدية، الموسم الجامعي، 2008-2009، ص 136.

3 محمد فوزي صالح، نفس المرجع السابق، ص 138.

تتمثل هذه المرحلة في إدخال الأموال أو توظيفها في مشاريع معينة، وتعتبر هذه المرحلة من بين أخطر المراحل وأشدها على الجناة، وذلك لما يمكن أن تثيره هذه الأموال من شك في حال ما كانت ضخمة مما يسهل اكتشاف أمرها[1].

2- مرحلة التمويه والإخـــفاء:

من خلال هذه المرحلة يتم استعمال الأموال المحللة بعدَّة طرق بحيث توظف في شراء عقارات بسعر كبير يتجاوز سعرها الحقيقي بأضعاف مضاعفة، أو من خلال إيداعات مصرفية، أو شراء مجوهرات ولوحات فنية غالية، وبعد عمليات الشراء يتم الفصل بين العائدات والأموال غير المشروع في محاولة لتمويه السلطات المختصة في الدول، وفي الغالب ما تتم هذه المرحلة في دول ذات نظام مالي متساهل، وفي نفس الوقت تعتمد قواعد السرية في نظام الإيداعات، وفي هذا الصدد هناك دول خاصة يتم اللجوء إليها من أجل هذه العمليات مثل جزر البهاما والكايمان، باكستان، وبنما وهذه الدول يطلق عليها الملاذات الآمنة أو الدول جناة الضريبة[2].

3- مرحلـــة الدمج:

تمثل هذه المرحلة آخر مراحل عمليات غسيل الأموال، ويطلق عليها البعض بمرحلة التعميم، حيث يقوم الجاني ببعض المعاملات المالية ذات الشكل المعقد، وذلك من خلال استعمال عدة وسائل وتقنيات متطورة، كأن يلجأ الجناة إلى التحويل الإلكتروني للنقود وذلك لسرعة هذا النوع من التحويلات ثم يعمل الجناة بعدها على القيام بتحويلات أخرى مختلفة في دول مختلفة[3].

خامساً- أساليب غسيل الأموال:

يتم غسيل الأموال عن طريق أحد الأساليب الآتيـــة:

1- غسيل الأموال عن طريق الـــمجال الـــمصرفـــي:

---

1 زياد عبد الكريم رشيد، عبد القادر عبد الوهاب عبد القادر، دراسة تحليلية لظاهرة غسيل الأموال "مع الإشارة للعراق"، وزارة المالية، العراق، متاح على الرابط: *http://www.mof.gov.iq* ، تاريخ الاطلاع: 2019/03/23.

2 أدية محمد صالح، الجريمة المنظمة دراسة قانونية مقارنة، ب. ط، منشورات كردستان للدراسات الإستراتيجية، السليمانية، العراق، 2009، ص 136.

3 باخويا دريس، جريمة تبييض الأموال (المكافحة والعوائق) ، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد الأول، المركز الجامعي تمنراست، يناير 2012، ص 163.

من خلال العنوان يتضح أن دور البنك في هذه الحالة أساسي وضروري، ويتم ذلك من خلال التحويلات المالية التي تجري من خلال البنوك والتي من أمثلتها[1]:

- الإيداع والتحويل عن طريق البنك.
- إعادة الاقتراض.
- بطاقة الائتمان.
- البطاقات الذكية.

2- أساليب غسيل الأموال فـــي المجال غير المصرفي:

تعتبر من أكثر الأساليب استخداماً؛ وذلك بالنظر لما تعتمد عليه من بساطة وتواري عن الرقابة المالية للدولة، وتظهر في العديد من الطرق منها:

- الفواتير المزورة أو الصفقات الوهمية.
- استخدام شركات الواجهة أو ما يعرف بشركات الوهمية.
- تهريب العملة.
- المكاسب الوهمية عن طريق ألعاب القمار.
- غسيل الأموال باستخدام شبكة الإنترنت[2].
- القيام بالأعمال الخيرية مثل الهبات، من أجل تحسين صورتها
- العمل على المساهمة في الأنشطة الرياضية، وذلك بهدف كسب رضاء الشعوب والسلطة، فضلاً عن الاستفادة من عمليات الإشهار من وراء هذه الأندية أو تلك البطولات، بالإضافة إلى الأموال التي سوف يذرها هذا النوع من الأنشطة، حيث أصبحت الرياضة تحتل مكان مرموقة وتدر أرباحاً كبيرة[3].

---

1 فريدة علواش، جريمة غسيل الأموال (المرحل والأساليب)، مجلة العلوم الإنسانية، العدد الثاني عشر، جامعة بسكرة، نوفمبر 2007، ص 256-257.

2 فريدة علواش، نفس المرجع، ص 261.

3 كعرار سفيان، الجريمة المنظمة عبر الوطنية وأثرها على الأمن الإنساني، مذكرة مقدمة لاستكمال متطلبات الماجستير، جامعة سطيف، الموسم الجامعي 2014/2013، ص 97.

الفرع الثانـــي: طرق غسيل الأموال بواسطة الـهاتف النقال.

تتطرق الدراسة من خلال هذا الفرع إلى الطرق التي يستعملها المجرمون من خلال الهاتف النقال من أجل القيام بجرائم غسيل الأموال، وهي عبارة عن مجموعة طرق يمكن حصرها في الآتـي:

أولاً– البنـــك الـــخلوي:

يعمل البنك الخلوي على فكرة تزويد تقديم الخدمات المصرفية للزبائن في أي وقت وفي أي مكان، وتشمل هذه الخدمة العديد من المزايا منها الاستعلام عن الرصيد، فضلاً على الإطلاع على العروض التي تقدمها المصارف لعملائها، كما تتيح لهم فرصة الإطلاع على أسعار العمولات والفوائد ومعدلاتها، بالإضافة إلى تقديم النصائح والاستشارات فيما يخص القروض، وغيرها من الخدمات الأخرى التي يمكن للزبون أن يستفيد منها[1].

ويعمل البنك الخلوي على فكرة تزويد العميل بالخدمات خلال 24 ساعة وعلى مدار الأسبوع، ويعمل هذا النوع من البنوك على إقامة قناة اتصال مباشرة بين كل من العميل والبنك؛ وذلك عن طريق تقنية "WAP"[2] وهي اختصار لكلمة WIRELESS APPLICATION PROTOCOL، وهو النظام الذي يتيح إمكانية الولوج للإنترنت من خلال الهاتف النقال وذلك من خلال استخدام الكارت الذكية "SIM"[3].

ونظراً للمزايا التي يقدمها البنك الخلوي للزبائن، تلقى رواجاً واسعاً، واستطاع أن يحقق أرباح خيالية بالنظر للتعاملات التي تقوم بها البنوك التقليدية، وذلك يرجع إلى أسلوب المعاملة، فضلاً عن

---

1 يونس عزب، بحث بعنوان البنوك الخلوية –التجارة الخلوية– المعطيات الخلوية، عصر جديد يتنبأ بانطلاق عصر ما بعد المعلومات، مكتبة توت شامي، متاح على الرابط: *http://www.tootshamy.com* ، تاريخ الاطلاع: 2018/07/15.

2 تتمثل خدمة "wap" في حزمة من المقاييس تتضمن بروتوكولات نقل المعلومات ولغة الترميز اللاسلكية والتي يعبر عنها ب (wireless markup language) وهي لغة برمجيات مشابهة لـ: (HTM L) ولكنها مخصصة للأجهزة اللاسكية، أو تعزيز المعلومات إلى الهواتف الذكية عبر بوابة WAP1، وحتى تؤمن البنوك هذه العمليات تصدر ما يعرف بالـ: (USSD) وهو اختصار لكلمة (Unstructured Supplemmentery Servvice Data) بحيث يعمل هذا البرنامج على تأمين الاتصال بين مزود الخدمة والهاتف الخلوي، وذلك من خلال الوصول إلى تطبيق محدد لتحقيق عمليات الاستعلام وتبادل في اتجاهين أو للاختيار من قائمة محددة لتنفيذ خدمات ما أو الدفع الإلكتروني، وتمثل البنوك الخلوية أداة جديد لتوظيف البطاقات الذكية، إذ تعد الواسطة الرئيسية لتحزين تطبيقات الخلوية بأنواعها، **انـظر في ذلك:** شادية أحمد، الصرافة الخلوية تتيح لك أن تحمل البنك في جيبك، مجلة آفاق المستقبل، ع 24، مركز الإمارات للدراسات والبحوث الإستراتيجية، ديسمبر 2014، ص 96.

3 محمود محمد محمود جابر، المرجع السابق، ص 223.

السرعة في تقديم الخدمة، كما أن خدمات البنك الخلوي تعتمد على استغلال بيانات الزبون والاستفادة منها فيما قد يحتاج من خدمات، وعرضها عليه في شكل نصيحة تقدم للعميل، ومن أمثلة ذلك؛ أن يعرض على العميل شراء سيارة لابنه، واستكمال دراسته في الخارج من أجل الحصول على دراسات عليا، أو الحصول على وثيقة تأمين[1].

وبالرغم من المخاطر التي قد تصاحب هذا النوع من العمليات المصرفية، إلا أنها تلقى رواجاً كبيراً منذ العمل بها سنة 1998 بدولة التشيك، ليطبق بعدها العمل بهذا النوع من العمليات البنكية في كل من السويد سنة 1999، ثم استراليا التي شهدت أول تعاون بين بنك الكومنولث وشبكة فودافون العالمية، بينما تم فتح أول بنك في الولايات المتحدة الأمريكية تحت مسمى "بنك أوف أمريكا" والذي وفر خدامات الاتصال بالبنك عن طريق الهاتف المحمول للزبائن[2].

إن الهاتف النقال من خلال خدمة البنك التي يوفرها فتح المجال للمجرمين من أجل الاستفادة من هذه التقنيات، حيث خولت هذه التقنية فرصة نقل الأموال من دون وجود رقابة، فضلاً عن السرعة الفائقة التي تخولها هذه التقنية في نقل الأموال، كما أن هذه التطبيقات توفر ضمانات عديدة للزبون، ولعل أهمها أن يكون حسابه محمي وآمن بواسطة رمز تعريف شخصي، كما يضمن للزبون أن تكون جميع العمليات مشفرة مما يُعقد من عملية تعقب الأموال القذرة[3].

ثانياً– الأعمال الـمصرفـية:

إن البنوك المصرفية أتاحت العديد من الخدمات التي تسهل للزبون إجراء أية عملية من دون التنقل، أو أن يكون في اتصال مباشر مع البنك الذي يتعامل معه، ومن بين هاته الخدمات:

1- خدمة تحويل الأموال بواسطة الهاتف النقال:

من بين الخدمات التي يوفرها الهاتف النقال خدمة تحويل الأموال، وتمثل هذه الخدمة ميزة سداد المدفوعات للآخرين عن طريق الهاتف النقال، وذلك عن طريق ما يعرف "محفظة المحمول"؛ والتي تعمل على تخزين القيمة قبل وبعد إتمام المعاملة، حيث يقوم الشخص المرسل للأموال بحفظها على ما يعرف بمحفظة المحمول، وذلك عن طريق الذهاب لـ: "وكيل" مسجل (وأحياناً وكيل مسجل وليس

1 محمود محمد محمود جابر، نفس المرجع، ص 224.

2 محمود محمد محمود جابر، نفس المرجع، ص 224.

3 محمود محمد محمود جابر، نفس المرجع، ص 226.

كثيراً من الأحيان)، وبعد ذلك يمكن للمرسل استخدام وسيلة آلية إلكترونية مؤمنة لتحويل الأموال، وبعدها يحق للمستلم إما تخزين الأموال في محفظته المحمولة من أجل الحصول على عدد من الأعمال المصرفية مستقبلاً، أو الذهاب إلى الوكيل لتحويل الأموال المحمولة إلى نقد[1].

ومن بين نماذج هذه المعاملات خدمة "إم. بيسا" التي قدمتها شركة "سفاريكوم"؛ والتي تملك شركة "فودافون" الأمريكية 40٪ من أسهمها، وهي تمثل أكثر شركات الاتصالات نجاحاً في هذا المجال، حيث استطاعت هذه الخدمة أن تجني أرباحاً تقدر بـ: 208 مليار، و3000 وكيل خلال 15 شهراً من دخولها للخدمة[2].

إن الأرقام التي تصدرها الهيئات الرسمية أو تصدرها هذه البنوك عن حجم تعاملاتها تثير الشبهة عن استغلال غاسلي الأموال لهذه الطريقة، حيث يقومون بإيداع أموالهم في البنوك ثم يقومون بتهريبها عن طريق استعمال البنوك الخلوية، وما يزيد الأمر سوء هو تقنية استعمال كلمة السر لمرة واحدة فقط، بحيث تُرسل للزبون عن طريق رسالة نصية قصيرة عند إبرام كل معاملة مما يزيد الأمر تعقيداً[3].

2- خدمـــة الدفع عـــبر الـــهاتف النـــقال:

1 الوكالة الأمريكية للتنمية الدولية وشركائها، بحث بعنوان: "استخدام خدمات تحويل الأموال والخدمات المصرفية عبر الهاتف المحمول لتطوير الزراعة في أفريقيا"، ص 1، متاح على الرابط، *http://www.findevgateway.org*، تاريخ الإطلاع: 2018/08/02.

2 الوكالة الأمريكية للتنمية الدولية وشركائها، نفس المرجع، ص 3.

3 في تقرير صادر عن وزارة الخارجية الأمريكية أن غسيل الأموال تضاعف بشكل صاروخي على مدى العقد السابق، إذ كان يبلغ حوالي 300-500 مليار دولار، حيث وصل حجم تجارة غسيل الأموال 3.61 تريليون دولار، وهو ما يعادل 5 في المائة من الناتج الإجمالي للاقتصاد العالمي، وأشار التقرير إلى أنه طبقاً لإحصائيات مؤسسات "وايرلس انتليجنس" فإن نصف سكان العالم البالغ وقتها 6.6 مليار نسمة يستخدم الهواتف الجوالة مع توقع ارتفاع هذه النسبة خلال عامين، وتابع التقرير قائلاً أن في بعض المناطق من العالم أصبحوا يقومون بإرسال وتلقي النقود أو الائتمان عن طرق الهواتف النقالة شائعاً ويساهم في تطور المجتمعات بشكل إيجابي، إلا أن هذا التطور رافقه استغلال من طرف الجماعات الإجرامية في أعمالها المحظورة. **انـــظر**: جريدة الشرق الأوسط السعودية، العدد 10708، بتاريخ 23 مارس 2008.

تمثل هذه الخدمة نوع من الخدمات التي يوفرها الهاتف النقال، وتعرف على أنها: "وسيلة من وسائل الدفع المختلفة عن طريق نقل الأموال بواسطة المحمول أو المحفظة النقالة بشكل عام، والتي تشير إلى خدمات الدفع التي تعمل تحت التنظيم المالي والأداء أو عبر جهاز محمول"[1].

وتوفر عملية الدفع بواسطة الهاتف النقال العديد من الخدمات لمن يستعمل هذه الوسيلة ومن بين هذه الخدامات التي تــوفرها:

- دفع الأقساط بواسطة الرسائل النصية.
- الدفع المباشر للفواتير بإضافة قارئ للبطاقات ملحق بأعلى الهاتف.
- الدفع عن طريق الشبكة بعيدة النطاق wap التي تستخدمها شبكة المحمول.
- الدفع عن طريق حقل الاتصالات قصيرة النطاق NFR وهو اختصار يعني: Near Field communication، والتي يمكن من خلالها للأجهزة التواصل مع بعضها البعض على مسافة قصيرة.

وعليه إن هذا النوع من المعاملات يتيح الفرصة لأصحاب الصفقات المشبوهة القيام به بعيداً عن أعين الرقابة، حيث يتمكن مستخدمي هذه الطريقة من الحصول على مقابل لسلعهم بطرق سرية وآمنة ومناسبة فيما يتعلق بالتحويلات النقدية، كما أن انتشار هكذا تعاملات يسهل من عملية نقل الأموال بطرق غير مشروعة، وتتسم هذه النظم بكفاءة عالية، فضلاً عن كونها فائقة السرعة.

3- خدمــة التــجارة الخلويــة:

تمثل التجارة الخلوية واجهة جديدة من أوجه التجارة الإلكترونية، والتي تعرف بأنها: "عملية البيع والشراء، أو تبادل المنتجات والخدمات والمعلومات باستخدام شبكات الحاسوب المختلفة بما فيها الإنترنت، كما تعني القيام بجميع مراحل التبادل بدءاً بالتزود بالمواد الأولية والتصنيع، مروراً بالتسويق والإعلان التجاري وبيع وتوزيع المنتجات إلى تبادل المعلومات داخل وخارج المؤسسة"[2].

---

1 عمار جبقجي، الدفع عن طريق الهاتف النقال، موقع إي بزنز، متاح على الرابط: *www.ibznz.com* ، تاريخ الإطلاع: 2018/07/09.

2 عماد أحمد أبو شنب، يسرى حرب، ووجدان أبو البصل، الخدمات الإلكترونية، ب. ط، دار الكتاب الثقافي، الأردن، 2011، ص 29.

وتعتمد التجارة الإلكترونية الخلوية نفس المزايا التي تقوم عليها التجارة الإلكترونية؛ سواءٌ فيما تعلق بعمليات البيع أو الشراء أو التسويق، ومختلف العمليات الأخرى المتعلقة بالتجارة الخلوية، والتي تعتمد على التعامل الإلكتروني باستخدام الشبكات اللاسلكية من خلال استعمال الهاتف الخلوي[1]، وتعمل بعض الهواتف الذكية بنفس الطريقة التي تعمل بها أجهزة الكمبيوتر من خلال ما تحتوي عليه هذه الهواتف من ميزات مساعدة وتكاملية، لها المقدرة على القيام بعديد الأعمال ذات الطابع الإلكتروني، كالبرمجيات، وأقراص الموسيقى والكتب وغيرها من الأنشطة الأخرى.

وتُقسمُ التجارة الخلوية إلى نفس الأنواع التي تقسم بها التجارة الإلكترونية، والتي تتمثل في[2]:

أ. **التجارة الإلكترونية بين المنظمات:** Business to Business (B2B) وتمثل جميع الجهات المشاركة في هذه الفئة من التجارة الإلكترونية منظمات أعمال.

ب. **التجارة الإلكترونية بين المنظمات والمستهلك:** Business to Consumer (B2C) ويشمل هذا النوع جميع مبيعات التجزئة الإلكترونية للمنتجات والخدمات من منظمات الأعمال إلى المستهلكين.

ج. **التجارة الإلكترونية بين المستهلكين:** Consumer to Consumer (C2C) يتم هذا النوع من البيوع بين المستهلكين فيما بعضهم البعض.

د. **تطبيقات التجارة الإلكترونية بين النظراء** Peer to Peer (P2P) هي عبارة عن تقنية تقوم على اقتسام المعلومات دون للجوء إلى وسيط، ومعالجة هذه المعلومات دون الحاجة إلى وجود أجهزة.

وتعتبر التجارة الإلكترونية من بين أهم الطرق التي يلجأ إليها غاسلي الأموال من أجل إضفاء الشرعية على أموالهم، وذلك من خلال استغلال النقود أو وسائل الدفع الإلكترونية المستخدمة في مثل هذا النوع من المعاملات.

الفـــرع الثالـــث: موقف التشريعات من جرائـــم غسيل الأموال.

سنتطرق من خلال هذا الفرع إلى موقف بعض التشريعات من جريمة غسيل الأموال، وذلك على النحو الآتي:

---

1 عماد أحمد أبوشنب، يسرى حرب، ووجدان أبو البصل، نفس المرجع، ص 36.

2 محمود محمد محمود جابر، المرجع السابق، ص 232.

أولاً– مــوقف المشرع الـمصري:

جرم المشرع المصري جريمة غسيل الأموال بموجب القانون رقم 80 لسنة 2002، بحيث لا يوجد نص مباشر في هذا القانون ينص على تجريم عمليات غسيل الأموال المرتكبة بواسطة الوسائل الإلكترونية أو الرقمية، إلا أنه بحسب بعض الباحثين المصريين[1]، هذا لا يعني إفلات الجاني من تطبيق العقوبة، حيث تطبق عليه الأحكام العامة للعقوبة بغض النظر عن الوسيلة.

ثانياً– موقــف المشرع الـجزائــري:

عرف المشرع الجزائري جريمة غسيل الأموال بموجب المادة 389 مكرر من ق.ع.ج والتي نصت على: "يعتبر تبييضا للأموال:

أ. تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

ب. إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها مع علم الفاعل أنها عائدات إجرامية.

ج. اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، أنها تشكل عائدات إجرامية.

د. المشاركة في ارتكاب أي من الجرائم المقررة وفقاً لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه[2]".

ويعتبر التشريع الجزائري من التشريعات التي أخذت بالمفهوم الواسع للتجريم بخصوص جريمة غسيل الأموال، وذلك يظهر من خلال نص المادة حتى لا يترك مجال لغاسلي الأموال لتملص من المساءلة القانونية والعقوبة، كما أن المشرع الجزائري نص من خلال المادة 4 من القانون 04-15 على نوع المال الذي يمكن أن يكون جزء أو عرضة لعملية غسيل الأموال، معترفاً ولو ضمنيا عن إمكانية غسيل الأموال بالطريقة الإلكترونية أو الرقمية.

---

1 طارق صادق عفيفي، المرجع السابق، ص 193.

2 القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر.ج.ج، ع 71، المؤرخة 10 نوفمبر 2004، ص 11.

الفصل الثاني:
جرائم الاختراق الإلكترونـــي بواسطة الهاتف النقال.

إن التطور السريع للهاتف النقال وبصورة غير طبيعية، ترتبت عنه عدة نتائج؛ منها ما هو إيجابي يتعلق بإتاحة التواصل بين الناس في كل أنحاء العالم بكل سهولة، فضلاً عن التكلفة القليلة التي تدفع لقاء هذه الخدمات، إلا أن هذا التطور الهائل واكبه كذلك استغلال سلبي ظهر في العديد من المجالات، سواءٌ من ناحية الهجمات التي يتعرض لها الهاتف النقال في حد ذاته عن طريق العديد من الفيروسات، والتي تعمل على الاعتداء على الوسائط التي تكون برمجة الهاتف، وهو ما يعرف بجرائم الإتلاف والاختراق الإلكتروني، والتي تعتمد على وجود ثغرات في نظم الهاتف، فتتم مهاجمته من خلال هذه الثغرة، ما يؤدي إلى تعطيل نظامه إما بشكل كلي أو جزئي.

كذلك ظهر مع هذا التطور التقني في مجالات الاتصالات عدة ظواهر أخرى قد تؤدي إلى تهديد سيادة الدول عن طريق بعض الجرائم الإلكترونية، مثل الإرهاب الإلكتروني الذي يمثل اليوم أحد أخطر الجرائم التي قد تهدد الدول عن طريق الاعتداء على نظامها المعلوماتي، والذي يشكل اليوم جزء كبير من حياة الدول أو ما يعرف الحكومة الإلكترونية، فضلاً عن عمليات عديدة خطيرة تتم عن طريق هذه الجريمة كتجنيد الشباب والنساء لصالح جماعات إرهابية متطرفة، وفضلاً عن ذلك، هناك ما يعرف كذلك بالتجسس الإلكتروني، والذي لا يقل خطورة عن الجريمة السابقة.

وانطلاقاً من هذه الخطورة قسمنا هذا الفصل إلى مبحثين تم التطرق فيه إلى مفهوم الاختراق الإلكتروني (المبحث الأول)، وجرائم الإرهاب والتجسس الإلكتروني بواسطة الهاتف النقال (المبحث الثاني).

المبحث الأول:
مفهوم الاختراق الإلكتروني.

صاحب التطور الذي وصل إليه الهاتف النقال عدة مخاطر بحيث أصبحت البيانات المخزنة في الهاتف النقال تشكل تهديداً خطيراً على أصحابها، وذلك من خلال الهجمات الإلكترونية التي قد يتعرض لها الهاتف النقال عن طريق ما يعرف بالهاكرز، وهو ما قد يهدد سلامة الهاتف والمعلومات المخزنة فيه، وظهر ذلك في صورة ما يعرف الاختراق الإلكتروني، لذلك قسمنا هذا المبحث إلى مطلبين؛ تناولنا فيه مفهوم الاختراق الإلكتروني وأسباب انتشاره (المطلب الأول)، ثم طرق الاختراق الإلكتروني (المطلب الثاني).

المطلب الأول: مفهوم الاختراق الإلكتروني وأسباب انتشاره.

يعتبر الاختراق الإلكتروني هو الوحدة الأساسية في ارتكاب الجاني لأي جريمة إلكترونية، بحيث لا يمكن للمجرم الولوج إلى موقع معين أو قرصنة ملفات ما، إلا بعد أن يقوم باختراق أنظمة الأمن لهذا الموقع، أو مكان حفظ هذه المعلومات، لذلك سنعالج من خلال هذا المطلب تعريف جريمة اختراق الهاتف النقال (الفرع الأول)، ثم أسباب الاختراق (الفرع الثاني).

الفرع الأول: تعريف جريمة اختراق الهاتف النقال.

يعرف الاختراق بصفة عامة على أنه: "القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف"[1]، وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوة دون رغبة منهم، وذلك وبغض النظر عن الأضرار التي قد يحدثها ذلك، سواءٌ الضرر المادي بأجهزتهم الشخصية، أو الضرر الأدبي والنفسي عند نسخ ملفات صور خاصة بالمستخدم دون علمه[2].

ومن خلال هذا المفهوم نستنتج أن الاختراق هو عبارة عن عملية سطو الكتروني غير مشروع بواسطة جهاز إلكتروني على جهاز آخر، بحيث يتتبع الثغرات الموجودة على هذا الجهاز، حتى يحقق

---

1 سعيدي سليمة، حجاز بلال، المرجع السابق، ص 96.

2 أشرف السعيد أحمد، القرصنة الإلكترونية، ب. ط، مطابع الشرطة، مصر، 2013، ص 16.

الهدف الذي في الغالب يكون ملفات أو صور خاصة بالمستخدم تكون مثبتة على جهازه، ويعتمد الاختراق على عملية السيطرة عن بعد، ولا يمكن أن يحدث اختراق إلا بتوفر شرطين أو عاملين أساسيين هما:

- البرنامج المسيطر: ويعرف هذا الجهاز بالعميل.
- الخادم: وهو البرنامج أو الجهاز الذي يسهل عملية الاختراق[1].

الـــفرع الثاني: أسباب الاختراق الإلكترونـــي.

هناك العديد من الأسباب التي قد تؤدي بالجاني إلى القيام بهذا النوع من العمليات، أهمها:

1- **أسباب فرديـــة:** قد يكون سبب الاختراق سبب شخصي متعلق بالمخترق اتجاه الضحية، حيث تحركه غريزة الانتقام منه، والأمثلة على ذلك كثيرة[2].

2- **حب التفوق على الآلـــة:** من الأسباب الوجيهة التي قد تدفع أي مخترق هو التغلب على الآلة وقهرها، بحيث لا يكون هدفه إيذاء الضحية بشكل مباشر، وإنما يكون هدفه برهنة مدى ذكاءه ومقدرته على التحكم في الأجهزة الإلكترونية، وفي الغالب تكون هذه الفئة من الشباب المراهقين أو المختصين في المجال الإلكتروني الذين يسعون ليثبتوا أنفسهم أمام أصدقاءهم[3].

3- **أسباب تجاريـــة:** بالنظر للمنافسة الكبيرة بين المعاملين الاقتصاديين الكبار، قد يؤدي هذا بأحدهم إلى اختراق النظام الخاص بهذه الشركة سواءٌ عن طريق استخدام جهاز الهاتف النقال في ذلك، أو اختراق أجهزة الهاتف الخاصة بالمتعاملين في الشركة من أجل الإضرار بسمعتها في السوق[4].

4- **الدافـع الســياسي:** يعتبر الدافع السياسي كذلك من أهم الأسباب التي تدفع إلى القيام بعملية اختراق سواء ،كعملية انتقام من المنافس أو حتى التمكن من الأسرار التي يمتلكها هذا السياسي من أجل استغلالها ضده[5].

---

1 سعيدي سليمة، حجاز بلال، نفس المرجع، ص 96.

2 نائلة عادل محمد فريد قورة، المرجع السابق، ص 57.

3 شمسان ناجي صالح الخيلي، المرجع السابق، ص 39.

4 محمد كمال محمود دسوقي، المرجع السابق، ص 26.

5 سعيدي سليمة، حجاز بلال، نفس المرجع، ص 101.

5- **أسباب عسكريـــة:** يتم اللجوء إلى هذا النوع من العمليات في الغالب بين الدول من أجل معرفة أهم التطورات التي وصلت إليها فيما يخص الشؤون العسكرية، فيكون ذلك أما عن طريق اختراق أجهزة الكمبيوتر التي يتم العمل بها في المنشآت العسكرية بواسطة الهاتف النقال، أو عن طريق اختراق أجهزة النقال الخاصة بالقيادات الكبيرة في الجيش[1].

6- **بـــهدف السرقـــة:** قد يكون الهدف من عملية الاختراق هو السرقة، بحيث يسعى المخترق من خلال عمله الحصول على أرقام خاصة ببطاقات الائتمان الخاصة بالضحية من أجل سرقة أموالـــه[2].

7- **بدافـــع ديـــني:** يرى البعض[3] أن التوجه الديني قد يكون سبب لعمليات الاختراق التي قد تتم ضد أنظمة أو مجموعات معينة من قبل أخرى، وذلك من خلال قرصنة حساب خاص بجهة معينة لمعرفة كيف تفكر، أو حتى لماذا تخطط، أو حتى من أجل إثبات التفوق على العدو، وخير مثال على ذلك الاختراقات التي يقوم بها الكيان الصهيوني من حين لآخر.

8- **عدم وجود الحمايـــة الكافية فـــي الجهاز:** معظم الأجهزة التي يتم اختراقها هي أجهزة لا تتوفر على الحماية الكافية سواء في ما يخص مضادات الفيروسات أو حتى كلمات السر المناسبة[4].

9- **بـــغرض الابـــتزاز:** من الأسباب الشائعة كذلك التي تؤدي إلى الاختراق هو ابتزاز الضحايا عن طريق استعمال الملفات والصور المتوصل إليها عن طريق الاختراق، سواء بنشرها أو بيعها، خاصة إذا كانت الشخصية المخترقة شخصية عامة، أو شركة تجارية تخشى على أسرارها المهنية من التسريب والانتشار[5].

---

1 سعيدي سليمة، حجاز بلال، نفس المرجع، ص 101.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص، ص 105-106.

3 ياسر الحركي، "لماذا يقوم الهاكرز باختراق المواقع وماذا يستفيدون من ذلك"، مقال متاح على الرابط الإلكتروني: *http://www.ebda2.net* تاريخ الإطلاع: 2018 /07/10.

4 محمد علاء حسين الحمامي، أسباب اختراق مواقع الويب وشبكات التواصل الاجتماعي"، مجلة الأيام، العدد 8765، نشرت بتاريخ 09 أفريل 2013، متاح على الرابط: *www.alayam.com*، تاريخ الاطلاع: 2018/07/11.

5 رجاء أحمد علي، أمن المعلومات وحمايتها من الاختراق، مقال متاح على الرابط الإلكتروني التالي: *www.sciences.uodiyala.edu.ik*، تاريخ الاطلاع: 2018/07/11.

المطلب الثاني: طــرق اخــتراق الهاتـــف النقال.

إن الطرق التي يتبعها الجناة من أجل اختراق أجهزة الهاتف النقال متعددة ومختلفة، وهي في معظمها تشكل تهديداً خطيراً على الهاتف النقال، وتتنوع هذه الأساليب بحسب الجهاز المراد اختراقه، فضلاً عن جودة هذا الجهاز وأهميته، كما أن وسائل الاختراق غير ثابتة فهي متطورة من وقت لآخر، ففي كل عام يتم صنع طرق جديدة تستهدف الأجهزة المحمولة الحديثة، بعضها عن طريق الفيروسات (الفرع الأول)، أو عن طريق وسائط تبادل المعلومات (الفرع الثاني)، أو عن طريق الإنترنت (الفرع الثالث)، وكذا عن طريق برامج التجسس الإلكتروني (الفرع الرابع).

الــفرع الأول: اختراق الهاتف النقال عن طريق الفيروسات.

تعتبر الفيروسات من أخطر وسائل الاختراق التي يعتمد عليها الجناة من أجل الولوج للهواتف النقالة، وتتنوع هذه الفيروسات باختلاف مصدرها والهجمات التي تريد تنفيذها، لذلك سوف نتطرق من خلال هذا الفرع إلى تحديد مفهوم الفيروسات، ثم أنواع الفيروسات التي تشكل ضرراً على الهاتف النقال.

أولاً– مفهوم الفيروسات:

تعرف الفيروسات على أنها: "عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد، وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى، وإعادة إنشاء نفسها حتى تبدو وكأنها تتكاثر وتتولد ذاتياً بالإضافة إلى قدرتها على الانتشار من نظام إلى آخر، إما بواسطة الأقراص الممغنطة أو عبر شبكات الاتصالات، بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى آخر في العالم"[1].

ويعرفها آخرون[2] على أنها: "برامج غير مرغوب فيها لها القدرة على الإنتشار وإعادة تكوين نفسها والالتصاق ببرامج أخرى، وتتمتع هذه البرامج بقدرات تدمير البرامج والمعلومات أو إصابة الأجهزة بالخلل، وذلك بمسح أو تغيير بعض ملفات التشغيل، ويظل خاملاً لفترة محددة، ثم ينشط فجأة في توقيت معين ليدمر البرنامج أو المعلومات المخزنة أو يتلفها جزئياً، بالخرق أو التعديل".

---

1 محمد عبدالله العوا، المرجع السابق، ص 247.

2 أشرف السعيد أحمد، المرجع السابق، ص 70.

وتعرف الفيروسات التي تخترق الهاتف النقال كذلك على أنها: "فيروسات حاسوبية، إلا أنها مصممة خصيصاً للعمل في بيئة الهاتف النقال والانتقال من هاتف إلى آخر، ويعد فيروس "كيبر" (Cabir) أول فيروس صمم ليعمل في الهواتف المحمولة، وصمم خصيصاً لاستهداف الهواتف التي تعمل بنظام "سمبيان" (symbain)، وتدعمه خاصية البلوتوث "Bluetooth"، فيقوم باستغلال هذه الخاصية لنشر نفسه بين الهواتف الأخرى"[1].

ومن خلال المفاهيم السابقة، نستنتج أن الفيروسات عبارة عن برامج ضارة صنعت خصيصاً من أجل الاعتداء على سلامة أجهزة الحاسوب والهاتف النقال، بحيث تتمتع بميزة الانتقال بين الأجهزة عبر الوسائط المتعددة، أو عن طريق الإنترنت، حيث تعمل هذه الفيروسات على الإتلاف الكلي أو الجزئي للجهاز، كما أنها تستطيع اختراق الملفات التي يخزنها الهاتف النقال من ملفات وصور، وهي في تطور مستمر بحيث كلما تطورت تقنيات الهاتف النقال كلما تطورت تقنيات اختراق هذه الأجهزة من قبل جماعة الهاكرز.

ثانياً– خـصائص فيروسات الـهاتف النـقال:

تمتاز فيروسات الهاتف النقال بالعديد من الخصائص، والتي تتمثل في:

1- القدرة على التخفي:

تعتبر هذه الخاصية من أهم الميزات التي تتمتع بها الفيروسات عموماً، وتتم عملية تخفي الفيروسات من خلال الارتباط ببرامج أخرى، أو عن طريق التمويه والتشبه ببرنامج معين يكون حسن الأداء ويعرض أشياء مثيرة، ثم عندما يبدأ التشغيل يعمل على تخريب النظام[2].

2- الـقدرة علـى الانـتـشار:

إن القدرة الفائقة للفيروسات على الانتقال من نهاية طرفية إلى باقي الأطراف الداخلة في الشبكة في ثوان معدودة بسبب التكاثر اللانهائي، هو ما يساعد على هذا الانتشار السريع، إضافة إلى التوافق في البرامج المستخدمة على نطاق واسع عبر دول العالم وشبكات المعلومات[3].

---

1 أريج الشيشاني، إزالة الفيروسات من الهاتف، مقال متاح على الرابط الإلكتروني التالي: *www.mawdoo3.com* ، تاريخ الإطلاع: 2018/07/04.

2 محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ب.ط، مركز الدراسات العربية ، ب.ب.ن، 2015، ص 52.

3 محمد نصر محمد، نفس المرجع، ص 52.

3- الـقدرة على الـتدمـــير:

إن الهدف الأساسي من أي عملية اختراق هي وصول الفيروسات إلى البرامج والنظم المعلوماتية والعمل على تعطيلها أو تخريبها[1].

ثالثاً- أنواع الفيروسات التـــي تـخترق الهاتف النقال:

هناك العديد من الفيروسات التي تخترق الهاتف النقال، أهمها:

1- فـــــيروس "ace":

يعمل هذا الفيروس على استهداف برامج الهاتف النقال، ثم يعمل على مسح جميع المعلومات التي تتوفر عليها ذاكرة الهاتف أو المعلومات الموجودة على خط الاتصال "SIMCARD" مما قد يجعل الهاتف غير صالح لأداء مهامه، حيث يصبح مجرد آلة معطلة لا تصلح للقيام بأي شيء، وعلامة اختراق هذا الفيروس للهاتف تكون من خلال ظهور كلمة "ace" على شاشته، وأول ظهور لهذا الفيروس كان في الولايات المتحدة الأمريكية، وسبّب في تعطيل ثلاثة (03) ملايين هاتف نقال[2].

2- فـــيروس كبـــير"cabir":

أول ظهور لهذا الفيروس كان سنة 2005 وينقسم إلى نوعان، "EPCC/CABIR" وفيروس "SYMBOS/CABIR" ينتشر هذا الفيروس عبر تقنية البلوتوث، بحيث يعمل على اقتحام جهاز الضحية من خلال ملف باسم: "CABIR SIS" بمجلد "Index"، وعند الضغط عليه لتشغيله يقوم هذا الفيروس بنسخ نفسه بنفسه داخل الجهاز أو أي جهاز آخر[3].

3- فـــيروس "SKULLS":

يعتبر هذا الفيروس من الفيروسات الخاصة التي تعمل على هواتف الهواتف النقالة طراز "نوكيا 7610" دون غيرها، وهو من الفيروسات الصعبة في طريقة عملها، وينتقل هذا الفيروس عن طريق اتصال الهاتف المحمول بأحد أجهزة الحاسوب المصابة بهذا النوع من الفيروسات، ويعمل هذا الفيروس على إبطال "Nokai Theme Manger" ليحول كل الصور التي يحتويها هذا التطبيق إلى جماجم ثم

---

1 محمد نصر محمد، نفس المرجع، ص 52.

2 منى المنجومي، دخول فيروس "ace" للسعودية شائعة، متاح على الرابط الإلكتروني: *http://ww.adslgate.com*، تاريخ الإطلاع: 2018/07/16.

3 طارق عفيفي صادق أحمد، المرجع السابق، ص 126.

يقوم بعدها بإبطال عمل الهاتف، بحيث يصبح عمل الهاتف النقال مقتصر على استقبال وإرسال المكالمات فقط، وتم تطوير هذا النوع من الفيروسات حتى أصبت لها المقدرة للانتقال من هاتف إلى هاتف عن طريق البلوتوث[1].

4- فـــيروس "IGear":

يعتبر هذا الفيروس أول فيروس يعمل على اختراق الهواتف الذكية، ويقوم هذا الفيروس بتعطيل برامج الحماية والأمن الخاصة بالهاتف، فضلاً عن التطبيقات المتعلقة بالإنترنت، ويتخفى هذا الفيروس عن طريق اسم لعبة شهيرة قابِلة للتشغيل على الهاتف وهي لعبة "IGear"، وفي الغالب ما يعمل هذا الفيروس رفقة فيروس "cabir"[2].

5- فـــيروس هامينغباد:

يعتبر هذا الفيروس من الفيروسات الحديثة التي توصل إليها قراصنة صينيون؛ حيث يعمل هذا الفيروس على اختراق الهواتف الذكية والحواسيب اللوحية التي تعمل بنظام "أندرويـد"، حيث يقوم بالتسلل إلى نظام الهاتف ثم يعمل على فتح خاصية الإدارة البرمجية مما يعطيه سيطرة تامة على نظام التشغيل، كما أن الهدف الأساسي من عمليات الاقتحام التي يقوم بها هذا الفيروس ليست الحصول على المعلومات الشخصية، وإنما استخدام الهواتف النقالة المصابة عن بعد، ودفعها للنقر على إعلانات معينة، وبحسب تقرير نشرته "تشك بوينت" لأمن المعلومات؛ فإن عدد الهواتف المتضررة من هذا الفيروس عشرة ملايين هاتف ذكي حول العالم[3].

6- فـــيروس"Lasco":

يظهر هذا الفيروس في شكل صغير الحجم يتيح له فرصة الانتقال إلى الهاتف النقال، وذلك بطريقة منفردة أو عن طريق الالتصاق بملفات أخرى، وهو أول فيروس يمتلك خاصية الانتقال بطريقتين مختلفتين، ويستخدم هذا الفيروس هواتف "symbain" ويلحق نفسه بملفات "sis"، ومن

---

1 طارق عفيفي صادق أحمد، نفس المرجع، ص 127.

2 طارق عفيفي صادق أحمد، نفس المرجع، ص 127.

3 دويتشه فيلله، فيروس يضرب ملايين الهواتف الذكية، موقع الجزيرة، مقال متاح على الرابط: *www.aljazeera.net* ، تم الإطلاع عليه بتاريخ: 2018/07/16.

الميزات الأخرى التي يمتاز بها هذا الفيروس أنه لا ينتشر بشكل مباشر إلا إذا قام الضحية بفتح الملفات أو محاولة فتحها[1].

الفرع الثانـــي: اختراق الهاتف النقال عن طريق وسائط تبادل المعلومات.

تعتبر وسائط تبادل المعلومات من بين أخطر الطرق التي يمكن أن يخترق الهاتف النقال من قبلها، وذلك لما تحتوي عليه هذه الوسائط من ثغرات أو ضعف في أمن المعلومات الخاصة بها، ومن بين هذه الوسائط:

أولاً– اختراق الهاتف النقال عن طريق تقنـية البلـوتـوث[2]:

تعرف هذه التقنية بأنها: "عبارة عن طريقة للاتصال اللاسلكي عبر موجات الراديو (RF) قصيرة المدى بين أجهزة تشكل شبكة شخصية محددة المسافة بحوالي 10 أمتار، وبالتالي أي جاهزين يتبعان نفس هذا المعيار يمكنهما الاتصال وتبادل البيانات فيما بينهما، ودون الحاجة إلى اتصال مباشر، والجهاز يمكن أن يكون هاتف محمول أو حاسب آلي أو كاميرا رقمية أو حتى طابعة"[3].

يعتبر البلوتوث من التقنيات التي تساعد على انتقال الفيروسات، وذلك من خلال تبادل المعلومات بصفة تلقائية بين الأجهزة أو من خلال إرسال ملفات أو صور، أو عن طريق استغلال تقنية البلوتوث إذا كانت مفتوحة، بحيث يعّمد الجاني إلى الدخول إلى ملفات الضحية ويأخذ منها ما يريد من بيانات ومعلومات، وتكثر هذه العمليات في الأماكن العامة والأسواق، كما قد يضاف إلى تقنية البلوتوث ما يعرف ببطاقات بلوتوث، وهي تشبه أقلام التخزين تباع بأسعار رخيصة، يمكن

---

1 طارق عفيفي صادق أحمد، المرجع السابق، ص 128.

2 عرفت تقنية البلوتوث على المستوى الشعبي في مطلع العام 1998م، عندما نشأت شركة بين عدد من الشركات العالمية : نوكيا، أي بي إم ، أريكسون، إنتل، وتوشيبا، والإعلان عن قيام مجموعة "The Bluetooth Specail Interest Group" والتي يرمز لها بالاختصار: "Bluetooth SIG " لتعتمد البلوتوث كخدمة أساسية في منتجاتها. **لمزيد من المعلومات انظر:** خالد المسيهيج، تقنية البلوتوث: ما بين تحقيق الفوائد وإساءة الاستخدام، مجلة الرياض، العدد 13621، تاريخ النشر 6 أكتوبر 2005، متاح على الرابط: *www.alriyadh.com* .

3 Ahmed A. Radhi, *Data Acquisition and Controlling System by Using Mobile phone Based Microcontroller via Bluetooth*, Journal of Al-Ma'mun College, The number 26, Al-Ma'mun University College, 2015, page323.

استخدامها للأجهزة المكتبية، أو الحواسيب المحمولة التي لا تتوفر فيها تقنية البلوتوث[1]، ومن أكثر الحوادث شيوعاً في هذا المجال ما يعرف بفيروس "زومبي" بحيث يعمل هذا الفيروس من خلال الإتحاد مع التطبيق الأمني للهاتف النقال، ثم ينقل تفاصيل بطاقة الهاتف النقال إلى أحد البرامج المركزية التي تسيطر عليها مجموعة معينة من القراصنة، وأكبر خسارة سجلها هذا الفيروس هو الاعتداء على أكثر من مليون جهاز هاتف محمول في الصين وحدها، وذلك يرجع إلى أن هذا النوع من الفيروسات لا يخترق إلا الهواتف الصينية الصنع[2].

ثانياً– اختراق الهاتف النقال عن طريق عن طريـــق البريـــد الإلكترونـــي:

يمثل البريد الإلكتروني أحد أهم وسائل التواصل الحديثة التي يتم استعمالها اليوم بين الناس، ويوفر البريد الإلكتروني العديد من الخدمات، ككتابة الرسائل وإرسال الصور والمستندات[3]. ويعد البريد الإلكتروني جزء ضروري في جميع الهواتف الذكية؛ وذلك حتى يتمكن أي عميل من الولوج لأي موقع أو الاستفادة من الخدمات التي تعرضها مختلف التطبيقات التي يتوفر عليها هذا النوع من الهواتف، هذا وقد يستعمل القراصنة البريد الإلكتروني من أجل اختراق الهاتف النقال، وذلك عن طريق بعث رسائل نصية تحتوي على فيروسات، من شأنها إما التجسس أو إتلاف الهاتف المحمول، بحيث تعمل هذه الفيروسات بمجرد فتح الرسائل الواردة عن طريق البريد الإلكتروني[4].

الـــفرع الثالث: اختراق الهاتـــف النقال عن طريـــق الإنترنت.

تمثل شبكة الإنترنت أخطر الوسائل التي يمكن أن يخترق من خلالها أي جهاز أياً كان نوعه وذلك من خلال الطرق التالية:

---

1 خضر عباس، أمن الاتصالات السلكية وللاسلكية، مدونة الدكتور خضر عباس، فلسطين، مقال متاح على الرابط الإلكتروني التالي: *http://drabbass.wordpress.com* ، تاريخ الإطلاع: 2018/07/14.

2 محمود محمد محمود جابر، المرجع السابق، ص 459.

3 على جعفر، المرجع السابق، ص 364.

4 يعرف هذا النوع من الرسائل الوارد على البريد الإلكتروني، برسائل الاقتحامية: "وهي مجموعة من الرسائل غير المرغوب فيها والتي ترسل بدون إذن مسبق بواسطة شركات التسويق والإعلانات في محاولة منهم للترويج لمنتجاتهم وخدماتهم. **راجع في ذلك:** لما عبد الرحمان الحسيني، إرشادات أمنية لمستخدمي الهواتف الذكية، موقع لها أون لاين، متاح على الرابط الإلكتروني التالي: *kenanaonline.com*، تاريخ الإطلاع: 2018/07/14.

أولاً– المواقع الـمشبوهة أو غـير المعروفـة:

تشكل المواقع المشبوهة وغير المعروفة بغض النظر عن محتواها أحد الأدوات الخطرة التي تستعمل من قبل القراصنة من أجل اختراق الهاتف النقال، بحيث سجل العلماء العديد من الفيروسات التي تنشط من خلال هذه المواقع، والتي قد تكون عواقبها وخيمة على المعلومات الموجودة في الجهاز، أو حتى على الجهاز في حد ذاته[1].

ثانياً– حصان طـــروادة[2]:

هو برامج يعمل على اختراق الأجهزة الإلكترونية، وهو من البرامج التي لها وجهان، أولها الزبون "Client" وثانيها هو الخادم "Serves" ينفصلان بإرسال الخادم إلى جهاز الغير (حاسوب أو هاتف نقال) بحيث يكون غير مقصود ويتم التعامل معه بعد ذلك، ويعتبر هذا البرنامج من قبيل البرمجيات الخداعة التي توهمك في بداية الأمر أنها تعمل بشكل مفيد وبناء من أجل خدمة الهاتف، إلا أنها في الحقيقة ضارة ومؤذية، ويقوم بعمله من خلال نسخ نفسه ذاتياً إلى الملفات الأخرى، ولا يمتنع من الدخول إلى الأماكن ذات الطبيعة السرية والمشفرة[3].

ويختلف حصان طروادة عن الفيروسات من حيث أنه لا يتكاثر ولا يلتصق بالملفات، حيث يؤدي عمله بطريقة منفردة، حيث يحمل ضمن برمجيته توقيت وأسلوب استيقاظه، ويعمل على تعديل البرامج وتزوير المعلومات، وقد تصل خطورته إلى تدمير النظام كله[4].

ثالثاً– برنامـــج الـــدودة:

يعرف برنامج الدودة على أنه: "مجموعة برامج صغيرة قائمة بذاتها، غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية، أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء

---

1 أسعد ضاهر، فيروس جديد قد يفجر هاتفك، موقع روسيا اليوم، متوفر على الرابط الإلكتروني التالي: *http://arabic.rt.com* تاريخ الإطلاع: 2018/07/14 .

2 يعود سبب تسمية فيروس حصان طروادة بهذا الاسم إلى المجسم الخشبي الذي اختبأ فيه عدد من الجنود اليونانيون وكانوا سبباً في فتح مدينة طروادة ، لهذا سمي هذا الفيروس بحصان طروادة لأنه يذكر بهذه القصة الشهيرة. ومعنى حصان طروادة: رمز الحصان يعني البرنامج، ورمز الجنود يعني الفيروس. **انـــظر:** أحمد حمدي: حصان طروادة: أسطورة بلا دليل، موقع قل ودل، متاح على الرابط الإلكتروني التالي: *www..qallwdalla.com* ، تاريخ الاطلاع: 2019/03/29.

3 محمد عبدالله العوَا، المرجع السابق، ص258، **وانظر كذلك:** على جعفر، مرجع سابق، ص 554.

4 محمد عبدالله العوَا، المرجع نفسه، ص 258.

تصفحهم الإنترنت، أو إلحاق الضرر بهم، أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظرًا لقدرتها الفائقة على التلون والتناسخ والمراوغة"[1].

وتعرف دودة الهاتف النقال بدودة الرسائل النصية القصيرة "Selfmite" وهي عبارة عن دودة من النوع النادر الذي يصيب أجهزة الأندرويد، حيث تعمل على إرسال رسائل نصية إلى أول عشرين اسم في جهات الاتصال التي تحتوي على "APK" خبيث في هاتف الضحية[2]، في بداية الأمر استطاع المختصون في أمن المعلومات السيطرة على هذا البرنامج إلا أنها عادات في نسخة متطورة تحت مسمى "Selfmite B"، بحيث يعمل هذا الفيروس بنفس الأسلوب السابق للفيروس الأول، إلا أنه أكثر عدوانية من قبل من حيث الانتشار، مما يجعله لا يقتصر على توجيه رسائل لـ: 20 شخص فقط، وإنما يقوم بإرسالها لجميع جهات الاتصالات على جهاز الأندرويد، ويتم تحميله من موقع خاص يحتوي على رسالة SMS الخبيثة مع رابط قصير من إحدى مواقع وخدمات تقصير الروابط المقدمة من "google" أو "goDaddy"، مع إرفاق الرسالة بباقي المعلومات النصية الأخرى، وتكون الرسائل التي ترسلها هذه الدودة مكتوبة على النحو التالي[3]:

Hi buddy, try this, its amazing u know.http://x.co/5***
Hey, try it, its very fine. http://x.co/5***

بالإضافة إلى طريقة الانتشار التي تمس بكل الأرقام المتواجدة في جهات الاتصال، فإن هذا الإصدار الجديد من الفيروس يعمل وفق النمط الحلقي الذي يتيح له فرصة إرسال العديد من الرسائل للهاتف الضحية، حتى ولو تم اكتشاف هذا الفيروس من قبل الشركة وتم التعامل معه، إلا أنه يبقى نشط، وبحسب تقرير فإن دودة "Selfmite" قامت بإرسال 150 ألف رسالة نصية فقط في مدة عشرة أيام لأكثر من 100 هاتف أندرويد على مستوى 16 عشر دولة منها أربعة دول عربية هي: (سوريا، العراق، المغرب، والسودان)، كما قد تسبب هذه الدودة في حجب رقم الهاتف المصاب وذلك بسبب

---

1 خالد أبو إبراهيم، ما هو الفيروس وما هو الديدان والترجان وسبل الوقاية منها، مقال متاح على الرابط على الرابط الإلكتروني التالي: *https://khaliid.com* ، تاريخ الاطلاع: 2019/03/21.

2 منة يحي، نسخة جديدة من دودة "Selfmite"، تهدد هواتف الأندرويد، موقع فيتو، مقال متاح على الرابط على الرابط الإلكتروني التالي: *www.vetogate.com* ، تاريخ الإطلاع: 2018/08/01.

3 الشريف د، دودة الرسائل النصية القصيرة "Selfmite" تعود لأندرويد وتصيب دول عربية، موقع كيونوتك أندرويد، مقال متاح على الرابط على الرابط الإلكتروني التالي: *www.cunotic.com*، تاريخ الاطلاع: 2018/08/01.

الكم الكبير لحركة مرور البيانات من الهاتف الواحد، وينتشر فيروس الدودة عن طريق إحدى الطرق الآتية:

1- أن تقوم الدودة بإنشاء أيقونات بأرقام أسماء مطابقة للأرقام الموجودة على الهاتف، ولكن لكل رقم رابط مختلف، حيث تكون الأيقونات والروابط الخاصة بها على الشكل التالي[1]:

Mobo Market ###
http://apx.rdkt.avazutracking.net/iclk/redirect.php?
Apxcod=115911&id=
$Mobigenie###
http://apx.rdkt.avazutracking.net/iclk/redirect.php?Apxcod=11591
1&id=

2- أما الطريقة الثانية التي تعمل بها دودة "Selfmite" فهي بواسطة استخدام Googel[+] على أن يكون مصاب ببرمجة تروجان الخبيثة، ما إن يبدأ جهاز الضحية بالعمل عن طريق هذا التطبيق حتى تحاول هي التشبث بأي تطبيق من متجر play، ويعتمد هذا الأمر على ملف التكوين الخاص بكل جهاز، وعند خروجه من المتجر وبطريقة تلقائية يتم فتح صفحة اشتراك مزعجة على متصفح الهاتف[2].

رابعاً- القنبلـة الـمعلومـاتيـة:

تعرف بأنها: "نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى"[3]، تظهر هذه القنبلة في شكل شفرة، بحيث تنقسم إلى مجموعة أجزاء صغيرة متفرقة حتى تستطيع التمويه والاختفاء، ثم تتجمع عند فترة زمنية معينة بحسب الأمر الذي تم إعطائه لها في زمن محدد، أو من أجل واقعة محددة، ويتعذر اكتشاف هذا النوع من البرامج لمدد قد تصل إلى الأعوام، وتعمل على إتلاف النظام بحيث لا تصبح له التشغيل أو أداء مهامه[4].

---

1 الشريف د، نفس المرجع.

2 الشريف د، نفس المرجع.

3 علي جعفر، المرجع السابق، ص 555.

4 هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ب.ط، دار النهضة العربية، القاهرة، 2000، ص103، **مشار إليه لدى:** على جعفر، المرجع السابق، ص 55.

وفي الغالب يعمل هذا البرنامج على إتلاف النظام والمعلومات التي يحتويها ويقسم هذا البرنامج إلى نوعين :

1- القنبلة الزمنية "Time Bome": يعمل هذا النوع من القنابل على هدف معين وفق زمن وساعة محددة ويوم محدد[1]، كأن يتم تحديد تاريخ الفيروس بـ: 2018/06/05 للقيام بمهمة معينة، فهو لا يقوم بهذا الهدف إلا وفقاً لهذا التوقيت.

2- القنبلة المنطقية "Logik Bome": على عكس النوع الأول يعمل هذا النوع استناداً على واقعة تحدث في النظام، كأن يقوم بالهجوم على النظام بمجرد التشغيل، أو عند قيام النظام بأمر معين[2].

الفرع الرابـــع: اخـــتراق الهاتـف النقال عـن طريـق برامج التجسـس الإلكترونـي.

تعد برامج التجسس الإلكتروني من بين أهم البرامج التي تستعمل لاختراق الأنظمة الإلكترونية من أجل السيطرة عليها ورصد معلومات وتحركات أصحابها، وتشمل هذه البرامج الأنواع الآتية:

أولاً- برنامـــج "Blue bug":

تم العمل على هذا الفيروس من قبل باحث ألماني، بحيث يمتلك هذا الفيروس المقدرة على التحكم على الأجهزة الخلوية عن طريق تقنية البلوتوث، والعمل على تحويلها إلى أجهزة تنصت عن بعد، كما يمتلك هذا البرنامج المقدرة على تسجيل جميع المكلمات التي يقوم بها الضحية مع الأشخاص الآخرين، بالإضافة إلى مقدرة هذا البرنامج على إرسال رسائل من هاتف الضحية إلى أشخاص آخرين دون علم هذا الأخير بذلك، كما أن هذا البرنامج له المقدرة على أن يخترق حتى

---

1 إبراهيم بدر محرز، جولة في أمن المعلومات مقالة، مجلة الحوار المتمدن، مقال متاح على الرابط الإلكتروني التالي: www.m.aher.org، تاريخ الاطلاع: 2018/07/18.

2 رغدة محمد هادي، وفاطمة حسن، البرامج الخبيثة تنتقل إلى جهاز المحمول، مجلة كلية التربية، العدد الأول، الجامعة المستنصرية، العراق، 2012، ص 522.

المحادثات التي تتم بجوار هاتف الضحية، وحتى لا يكشف أمره من خلال فاتورة الضحية يعمل الجاني على استعمال شريحة "SIM" مؤقتة حتى لا ينكشف شخصه في حال اكتشاف أمره[1].

ثانـياً– برنامج"Visible أو Discoverable":

إن ضبط الهواتف النقالة على وضعي "Visible أو Discoverable" يجعل من الهاتف في حالة مرئية لجميع الأجهزة الأخرى المتوافقة الموجودة في مجال اتصال هذا الهاتف، مما يوفر للأجهزة الاتصال فيما بينها وتبادل البيانات والمعلومات، وفي حال ما إذا توقف الضحية عن استعمال هذه الخاصية فإن الجاني يستطيع أن يهاجم الجهاز عن طريق استخدام بعض البرامج الأخرى المتخصصة المتوفرة على الإنترنت[2].

ثالثـــاً– برنامــج الـحشرة الجوالــة:

يعتبر برنامج الحشرة الجوالة من بين أهم برامج التجسس الحديثة التي تقوم باختراق الهاتف النقال، بحيث يعمل هذا البرنامج على تحويل الهاتف إلى ميكرفون بإمكانه أن ينقل ما يدور بين مستخدم الهاتف والأشخاص القريبين منه، وذلك عبر برنامج خاص يعمل على تشغيل ميكرفون الهاتف، ومن الخاصيات الأخرى التي يمتاز بها هذا البرامج قدرته على العمل في كل الظروف التي يكون فيها الهاتف النقال سواء يشتغل أم لا يشتغل، فمن خلال ميزة التحكم في الأجهزة عن بعد تستطيع هذه الحشرة أن تجعل الهاتف يُثبت الأصوات المحيطة به طوال الوقت دون استخدام الهاتف وخاصة الهواتف التي لا يمكن نزع بطاريتها[3].

---

1 خضر عباس، أمن الاتصالات السلكية وللاسلكية، مدونة الدكتور خضر عباس، فلسطين، مقال متاح على الرابط الإلكتروني التالي: *http://drabbass.wordpress.com*، تاريخ الإطلاع: 2018/07/14.

2 محمود محمد محمود جابر، المرجع السابق، ص 267.

3 ماجد. م، الحشرة الجوالة تقنية للتنصت على الخلوي وإن كان مقفلا، موقع طب نت، مقال متاح على الرابط الإلكتروني التالي: *www.tbeeb.net* تاريخ الإطلاع: 2018/07/18.

المبحث الثانـــي:
نـماذج مـن جرائــم اخـتراق الهاتــف النــقال.

من خلال المعلومات الواردة في المبحث السابق، تبين بأن هناك العديد من الطرق التي يتم من خلالها اختراق الهاتف النقال، لذا سنحاول من خلال هذا المبحث التطرق إلى بعض الجرائم التي يتم ارتكابها من خلال اختراق الهاتف النقال، وذلك عن طريق تقسيم هذا المبحث إلى ثلاثة مطالب، جرائم الإتلاف وتضخم البريد الإلكتروني (المطلب الأول)، ثم جرائم الإرهاب الإلكتروني بواسطة الهاتف النقال (المطلب الثاني)، ثم التجسس الإلكتروني (المطلب الثالث).

المطلب الأول: جرائـم الإتلاف وتضخم البريد الإلكترونـــي.

تعتبر جرائم الإتلاف وتضخم البريد الالكتروني من بين أهم الجرائم التي قد يتعرض لها الهاتف النقال، بحيث تكون ناتجة عن اختراق إلكتروني باستعمال إحدى الوسائل التي تم التطرق إليها سابقاً، لذلك سوف نقسم هذا المطلب إلى فرعين، جرائم الإتلاف (الفرع الأول)، جريمة تضخم البريد الإلكتروني (الفرع الثاني).

الفرع الأول: جرائـــم الإتـــلاف.

يشكل الإتلاف أحد صور الاعتداء على الهاتف النقال، بحيث يغير من طبيعة استعماله على النحو الذي كان مراد منه، ويعرف الإتلاف على أنه: "التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له"[1].

ويعرفه آخر[2] على أنه: "تغييب الشيء على نحو يفقده قيمته الكلية أو الجزئية، أو هو تخريب الشيء محل الجريمة بإتلافه والتقليل من قيمته، وذلك بجعله غير صالح للاستعمال أو تعطيله".

وعليه يتضح من التعريفين السابقين أن الإتلاف عبارة عن مساس بجوهر أو مادة الشيء، بحيث يقلل من قيمته الأساسية، إما عن طريق جعله غير صالح كلياً، أو أن يقلل من فعالية

---

1 جميل عبد الباقي الصعير، المرجع السابق، ص 128.

2 محمد إبراهيم سعد النادي، المرجع السابق، ص 67.

استعماله، أو أن يؤدي إلى تعطيله، ويعتبر الهاتف كغيره من الأشياء الذي قد يكون عرضة للإتلاف فيظهر ذلك في صورتين على النحو الآتـــي:

أولاً– الصورة الأولـى: جريـمة الإتـلاف الماديـة:

في هذه الحالة يكون الهاتف النقال في شكله المادي الخارجي عرضة للإتلاف، سواء هو بحد ذاته عن طريق الكسر الكلي، أو الجزئي، أو عن طريق الحرق أو غيرها من الوسائل الأخرى، وأن يتم الإتلاف عن طريق إتلاف أحد ملحقات الهاتف النقال كبطاقة SIM، أو بطاقة الذاكرة (carte mémoire)، ففي هذه الحالة لا يوجد اختلاف من الناحية الفقهية بخصوص النصوص المطبقة على هذه الجريمة أو حتى في تكييفها، فهي عبارة عن جريمة إتلاف مادي، ويطبق عليها النصوص الواردة بموجب إتلاف الأموال المنقولة والعقارية[1].

ونرى أن هذا النوع من الجرائم يخرج عن نطاق الجريمة المعلوماتية (الإلكترونية)، وذلك باعتبار أنه من الأفعال التي لا تمس بالبرمجة المتعلقة بالهاتف أو نظام المعالجة، وهذا ما يؤكد حتمية تطبيق النصوص التقليدية على هذا النوع من الأفعال.

ثانياً– الصورة الثانية: إتلاف المعلومات:

يعتبر إتلاف المعلومات من أهم الصور الحديثة للإعتداء على الهاتف النقال، وإن كانت هذه الصور تخلق إشكالات في النصوص المطبقة على هذه النوع من الإعتداءات، وسنتناول هذا الشق بنوع من التفصيل في الركن الخاص بالتجريم لهذه الجريمة[2].

1. تجريـم جريـمة الإتـــلاف:

إن الميزات الحديثة التي يتوفر عليها الهاتف النقال جعلته بنفس الإمكانيات التي يتوفر عليها الحاسب الآلي، كما أن هذا الميزات جعلت من الهاتف النقال عرضة لنفس المخاطر التي قد تصيب تلك الأجهزة، ومن بين هذه الجرائم جرائم الإتلاف، خاصة ما تعلق منها بمعلومات الهاتف النقال، وقد ثار جدل فقهي وقضائي كبير بشأن النصوص التي تطبق على جريمة الإتلاف في حال وقوعها، ونفصل في ذلك على النحو الآتي:

---

1 نائلة عادل محمد فريد قورة، المرجع السابق، ص 191.

2 شمسان ناجي صالح الخيلي، المرجع السابق، ص 222.

أ. **الإتــلاف غــير المـباشر للمعلومــات:** تتمثل هذه الحالة في أن يقوم أحدهم بالاعتداء على الجزئيات المعدنية المغناطيسية التي تتواجد على مستوى الوسيط المادي الذي يخزن هذه المعلومات، بحيث يتصور في هذه الحالة أن الاعتداء تم على عنصر مادي أُتلف عن طريق إرسال نبضات إلكترونية، في هذه الحالة لا يثور أي إشكال، حيث يتم تطبيق النصوص التقليدية على اعتبار أن ما تم الاعتداء عليه هو مال مادي مملوك للغير[1].

ب. **الإتــلاف المباشر للمعلومـــات:** في هذه الحالة يتم الاعتداء على المعلومات دون الدعامة المادية التي تحتوي هذه المعلومات أو البيانات[2]، ولقد أدت هذه الصورة إلى انقسام الفقه والقضاء إلى اتجاهين؛ كل منهم يستند إلى حجج معينة، ونستعرض هذه الاتجاهات على النحو التالـي:

1) **الاتــجاه المعارض:** يرى هذا الاتجاه بعدم إمكانية تطبيق النصوص التقليدية على هذه الحالة، ويستند في ذلك على الحجج الآتية[3]:

- انتفاء الصفة المادية عن النبضات الكهربائية التي تختزن البيانات والمعلومات، مما لا يجعلها تدخل ضمن المال المادي الذي قرر القانون حمايته معتمداً على قيمته الاقتصادية، على أن يبقى صالحًا لما صُنع من أجله.
- البيانات والبرامج لا يمكن اعتبارها مالاً في حد ذاتها باعتبار أنها غير قابلة للتملك، وأن الملكية لا تنصب إلا على الأشياء المادية ذات القيمة الاقتصادية.
- محو البيانات والبرامج يتم عن طريق التدخل في وظائف الجهاز، وهذا النشاط لا يعد من قبيل الإتلاف للدعامة المادية التي تحتوي البرامج والبيانات.

2) **الاتــجاه الـمؤيــد:** يرى هذا الاتجاه إمكانية تطبيق النصوص التقليدية على مثل هذا النوع من الاعتداءات، ويستند على الحجج الآتية: [4]

---

1 محمد عبيد الكعبي، المرجع السابق، ص 265.

2 أيمن عبد الله فكري، الجرائم المعلوماتية –دراسة مقارنة في التشريعات العربية والأجنبية–، ب. ط، مكتبة القانون والإقتصاد، الرياض، 2014، ص 294.

3 شمسان ناجي صالح الخيلي، المرجع السابق، ص 222-223.

4 على جعفر، المرجع السابق، ص 547-548.

- المعطيات الموجودة على الجهاز تشكل جزء من الكيان المادي للجهاز ما دامت مُثبتة عليه، كما قد تكون قيمة الجهاز من قيمة المعلومات المخزنة فيه.
- إن عدم الاعتراف بالصفة المادية للمكونات المنطقية للهاتف النقال من شأنه أن يحرره من الحماية الجنائية، مما يصعب عملية معاقبة من يقوم بإتلاف هذا النوع من الأجهزة.
- برامج وبيانات الهاتف النقال تعتبر من قَبيل الأموال لما لها من قيمة اقتصادية، ويرجع ذلك لخضوعها لكافة التصرفات القانونية التي ترد على حق الملكية، وبالتالي هي قابلة للتملك والاستحواذ عليها.
- برامج الهاتف النقال يمكن رؤيتها –ككيان مادي على شاشة الكمبيوتر، ويمكن ترجمته إلى أفكار، مما يستنتج منه أن له مصدر ومالك.[1]

2. الركـــن المادي لجريـــمة الإتـــلاف:

يتكون السلوك الإجرامي لجريمة الإتلاف من فعل الإتلاف، ووقوع الضرر وسنفصل في ذلك على النحو الآتي:

أ. فـــعل الإتلاف: يتحقق فعل الإتلاف بأن يأتي الجاني سلوك ايجابي أو سلبي يُشكل تعدياً على مال مملوك للغير، وذلك بصرف النظر عن وسيلته أو حجمه، ويتحقق الإتلاف المعلوماتي بعدة طرق؛ منها المحو والتعديل[2]، بحيث يُنقصُ هذا الفعل من صلاحية الجهاز المعتدى عليه، ويظهر السلوك الإجرامي لهذه الجريمة في الصور الآتية:

1) **التعديل غـــير المشروع للمعلومـــات:** تعتبر هذه الصورة من أكثر جرائم الإتلاف شيوعاً، وذلك من خلال التغيير غير المشروع للمعلومات والبرامج، ويتم عن طريق استخدام إحدى وظائف الهاتف النقال[3].

2) **تدمـــير الـمعلومـــات:** يعتبر تدمير المعلومات من صور الإتلاف التي قد تقع على الهاتف النقال، وتأخذ أثر أكبر من التعديل، وهناك العديد من التشريعات التي تعبر عن هذا

---

1 شمسان ناجي صالح الخيلي، المرجع السابق، ص 224.

2 عادة نصار، الإرهاب والجريمة الإلكترونية، ب. ط، العربي للنشر والتوزيع، القاهرة، 2017، ص 18.

3 نائلة عادل محمد فريد قورة، المرجع السابق، ص 217.

المصطلح بمصطلحات مغايرة كإخفاء المعلومات ومحوها، وإن كان البعض[1] يرى أن هذه المصطلحات لا يمكن أن تعبر بشكل مطلق عن التدمير، ومن أمثلة ذلك أنه لا يترتب على محو المعلومات التي تحتوي عليها ذاكرة الهاتف النقال أي تدمير، وإنما فقط لتعديل قائمة الملفات.

3) **الإدخال غير المشروع للمعلومات:** المقصود بالإدخال هو إدراج برنامج ما إلى كيان الهاتف النقال، وذلك من خلال إعطاء الهاتف تعليمات يسعى الجاني من خلالها إلى التمويه والتضليل في ارتكاب الجريمة فضلاً عن التغيير في الحقيقة[2].

ب. **وقـــوع الـــضرر:** يتمثل الضرر في جريمة الإتلاف في الأثر الذي يتركه الفعل، فلا يمكن أن يكون هناك إتلاف إذا لم يكن متبوع بضرر على الجهاز الذي تم إتلافه، بحيث يكيف على أنه من جرائم الضرر لا الخطر، بحيث يشترط المشرع لقيام هذا النوع من الجرائم أن تكون هناك نتيجة لهذا الفعل، ويشكل الضرر مفهوم عام مرن، بحيث يتغير ويختلف بحسب طبيعة الشيء وموضوعه، فقد يظهر الضرر في إنقاص لبعض المكونات الأساسية للجهاز، مما يؤثر على أداءه أو تكوينه، كما قد يكون الضرر على شكل إبطاء أداء الجهاز مما يعرقل أداءه لوظيفته، فالضرر متعدد ومختلف، وقد يقع بصور عديدة تختلف من وجهة نظر إلى أخرى[3].

3. الركـــن المعنوي لجريـــمة الإتلاف:

تعتبر جريمة الإتلاف من الجرائم العمدية التي تتطلب من أجل قيام المسؤولية ضد مرتكبها أن يكون هناك قصد جنائي عام فقط، وذلك من خلال علم الجاني علم تام بأنه يقوم بإتلاف ملك الغير بصورة تذهب بقيمته كلها أو بعضها دون سند شرعي، وينتفي العلم في حال ما إذا قام الجاني بفعل الإتلاف وهو يعتقد ملكيته لهذا المال، كأن يظن وارث المال أنه ملك لمورثه ويقوم بإتلافه، بالإضافة إلى علم الجاني يجب أن تتجه إرادته إلى القيام بهذا الفعل دون أن تكون مكرهة على ذلك، فإذا انتفت إرادة الجاني القيام بهذا الفعل ينتفي معها القصد الجنائي[4].

---

1 نائلة عادل محمد فريد قورة، المرجع نفسه، ص 218-219.

2 زيبحة زيدان، مرجع سابق، ص 54.

3 أسامة أحمد المناعسة، جلال محمد الزعبي، ، المرجع السابق، ص 121.

4 شمسان ناجي صالح الخيلي، المرجع السابق، المرجع السابق، ص 240.

4. موقف التشريــع الجزائــري والتشريعات المقارنة من جريمـــة الإتلاف:

نستعرض من خلال هذه النقطة موقف المشرع الجزائري، وبعض التشريعات المقارنة فيما يخص جريمة إتلاف المعلومات وذلك على النحو الآتـــي:

أ. التشريــع الجزائــري:

أضاف المشرع الجزائري القسم السابع مكرر وذلك بموجب القانون رقم 04-15 المؤرخ 10 نوفمبر 2004 والذي يعاقب على تجريم الاعتداءات المرتكبة ضد أنظمة المعالجة الآلية للمعطيات، وذلك في المواد من 394 مكرر إلى 394 مكرر7 من ق.ع.ج.

والواضح من هذه النصوص أن المشرع الجزائري حاول أن يتعامل مع هذا النوع من الجرائم بشكل موسع في سياسة تجريمها، حيث حاول الإلمام بكل الصور التي تشكل اعتداء على المعطيات سواء في صورة دخول أو بقاء أو تعديل أو إزالة أو تخريب أو تصميم أو نشر أو اتجار، مع أن المشرع لم يشر بصورة واضحة إلى جريمة الإتلاف، إلا أن ذلك من الممكن استنتاجه عن طريق بعض العبارات التي تدل على أن الإتلاف هو المقصود في نص المادة 394 مكرر1 من ق.ع.ج، والتي نصت على أن: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1].

ومن خلال هذه المادة نستنتج أن المشرع أشار إلى بعض العبارات التي تشكل الركن المادي لجريمة الإتلاف، والذي يحدث عن طريق الإدخال أو الإزالة أو التعديل، كما أن المشرع اعتبر هذه الجريمة جنحة كما هو واضح من العقوبة التي قررها لهذه الجريمة.

ويرى البعض[2] أن المشرع الجزائري تأثر بصفة كبيرة بالمشرع الفرنسي، خصوصاً في مدلول المادة 3/323 من قانون العقوبات[3]، والتي نصت على أن: "إدخال البيانات بطريقة احتيالية في نظام المعالجة

---

1 القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر.ج.ج، ع 71، المؤرخة 10 نوفمبر 2004، ص 12.

2 **نقلاً عـــــن:** زبيحة زيدان، المرجع السابق، ص 55.

3 Code pénal Francaise, Dernière modification le 25 novembre 2018 - Document généré le 09 janvier 2019; Article 323-3: *«Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier*

الآلي، استخراج، احتجاز أو إعادة إنتاج أو نقل أو حذف أو تعديل البيانات الواردة فيه يعاقب بالسجن لمدة خمس سنوات وغرامة قدرها 150.000 يورو".

ب. التـــشريـــع الأمـريـكي:

يعتبر التشريع الأمريكي من التشريعات السبّاقة في مجال تجريم المعلوماتية في جرائم الاعتداء على الحاسوب، أو على الإنترنت، وذلك وفقاً للقانون الصادر سنة 1986، والذي حمل اسم قانون جرائم الكمبيوتر الأمريكي، والذي حاول المشرع الأمريكي من خلاله مواجهة الإعتداء على الأموال الإلكترونية في القسم 18 منه، وهناك تشريع آخر، وهو التشريع الرئيس لجرائم الكمبيوتر والإنترنت[1] لعام 1994، والذي تم تعديله لمواجهة المشكلات الناشئة عن الشفرات الخبيثة[2].

وفي كل القوانين السابقة حاول المشرع الأمريكي حماية المصلحة العليا أو الدولة، ويظهر ذلك من خلال أحكام القوانين الصادرة في هذا المجال؛ ففي قانون سنة 1994م، جرمت المادة 1030/أ منه الإتلاف الذي يترتب عليه إعاقة الحكومة فقط، وهو ما لقي استهجان كبير مما أضطر الكونجرس الأمريكي إلى تعديل هذا القانون، وإضافة عدة فقرات أخرى لصور الإتلاف التي قد تصيب الأجهزة[3]، فتمثلت الصور المضافة في جريمة الإتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع للحكومة، إلا أنه يتم استخدامه من قبلها أو لصالحها أو إعاقة هذا الجهاز عن أداء مهامه المختلفة التي تباشرها الحكومة بواسطته، كما تم إضافة فقرة أخرى تقضي بحماية المعلومات وأنظمة الحاسب الآلية من أعمال الإتلاف، التي قد ترتكب بواسطة أشخاص غير مصرح لهم بالدخول إلى النظام وذلك في حالتين:

---

frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende».

1 هناك العديد من القوانين الأخرى التي صدرت في نفس المرحلة، والتي تهدف إلى مكافحة الجرائم المعلوماتية منها قانون أمن الحاسوب لسنة 1987م، والذي يقضي بإتخاذ الوكالات الفيدرالية خطوات ملائمة لتأمين وحماية حواسيبها، كما انفردت كل ولاية من الولايات بإصدار قانون خاص بها في هذا المجال، وحاولت تعديل قوانينها العقابية بما يتلاءم وهذا التعديل، انظر: محمود محمد جابر محمود، المرجع السابق ص 194.

2 نقلاً عـــن: محمد عبدالله العوا، المرجع السابق، ص 287- 288.

3 **See**: Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), *at; http://www.richmond.edu/jolt/v7i3/article2.html*. See also: American Bar Association Task Force on the Federalization of Criminal Law, *Report: Report on the Federalization of Criminal Law*, 1998 A.B.A. 2; *http://www.abanet.org/crimjust/fedreport.html.*

– أن يترتب على الإتلاف خسارة مادية تقدر بآلف الدولارات أو أكثر خلال عام واحد.

– أن تتعلق أعمال الإتلاف بمعلومات طبية دون اعتبار للخسائر المادية الناجمة عن ذلك[1].

الـفرع الثانـــي: جريـمة تضخم الـبريد الإلكترونـــي[2].

يمثل البريد الإلكتروني أحد أهم وسائل التواصل الحديثة وأكثرها شيوعاً في مجال المراسلات، ويرجع ذلك إلى العديد من الأسباب؛ من أهمها سهولة الإستخدام، فضلاً عن السرعة، بالإضافة إلى قلة التكلفة، وهذا ما جعل البريد الإلكتروني يتعرض للعديد من الهجمات التي تشكل جرائم في حال وقوعها، والتي من بينها جريمة تضخم البريد الإلكتروني، فما هي هذه الجريمة؟ وفيما تتمثل أحكامها ؟

أولاً– تعريف جريـمة تضخم البريـد الإلكترونـــي:

يعرف التضخم الإلكتروني على أنه: "تراسل نسخ مكررة بعدد كبير من نفس الرسائل عبر النظام التراسلي لبريد إلكتروني، بما يترتب عليه عدم انتظام سير النظام التقني المعلوماتي"[3]. ويعرفه آخر[4] على أنه: "استقبال عدد كبير من الرسائل الإلكترونية المزعجة".

ومن خلال المفهومين السابقين يتضح بأن التضخم الإلكتروني هو عبارة عن عدد لا متناهي من الرسائل المكررة، وفي الغالب ما تحمل هذه الرسائل إعلانات غير مرغوب فيها، أو عروض إباحية أو فيروسات، ويطلق على هذا البريد كذلك اسم البريد العشوائي، أو الرسائل العدائية أو التطفلية (Spam)، كما يمتاز هذا النوع من الرسائل في الغالب بخداع المتلقي عن طريق إغرائه والإلحاح عليه حتى يقوم بفعل عمل ما، كما قد تظهر هذه الرسائل من حين لآخر حتى أثناء فترة التشغيل للإعلان عن سلعة أو منتوج معين، كما وينصح المختصون في هذا المجال بعدم فتح هذه الرسائل أو إعادة

---

1 شمسان ناجي صالح الخيلي، المرجع السابق، ص 225.

2 يعرف البريد الإلكتروني على أنه: "استخدام شبكة الإنترنت كصندوق للبريد، بحيث يستطيع المستخدم إرسال الرسائل الإلكترونية إلى شخص أو عدة أشخاص من مستخدمين الإنترنت، وتتم هذه الخدمة في الغالب مجاناً ولا يستغرق إرسال الرسائل الإلكترونية أو استقبالها سوى بضعة ثوان، ويجب أن يكون لدى مستخدم الإنترنت برنامج للبريد الإلكتروني يُدرج ضمن البرامج التي يحتويها جهاز الكومبيوتر الخاص به". **انظر في ذلك:** عبد الله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2017، ص 67-68.

3 نبيل محمد عثمان عرعارة، المرجع السابق، ص 124.

4 خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات –دراسة مقارنة–، ب. ط، دار الفكر الجامعي، الإسكندرية، 2010، ص 139.

إرسالها لما قد تحتوي من أضرار ضد البريد الإلكتروني أو الجهاز في حد ذاته، كما يجب استخدام برامج خاصة تساعد في الحد من المتطفلين[1].

مما سبق ذكره يمكننا تعريف جريمة تضخم البريد الإلكتروني على أساس أنها: "ذلك الاعتداء الذي يستعمل فيه الجاني رسائل عشوائية أو تطفلية تحتوي على مضمون مضر بشكل كلي أو جزئي للبريد الإلكتروني على نحو يجعله غير صالح للاستعمال أو مزعج لمن يستخدمه".

ثانياً– طريقــة ارتكاب جريمــة التـضخم الإلكترونــي:

يتركب هذا الفعل من نقطتين أساسيتين وهما:

- **قيام الجاني بإرسال عدد لا محدود من الرسائل إلى بريد الضحية:** بحيث تكون هذه الرسائل في أغلب الحالات تفوق القدرة التخزينية لبريد الضحية، وذلك حتى يتمكن الجاني من خلال هذه الأفعال بالإضرار بجهاز الضحية، وذلك دونما استفادة من ذلك الفعل إلا إثباتاً للتفوق. ويستخدم في بعث هذه الرسائل برامج معدة خصيصاً لهذا الشأن، وفي أغلب الأحيان تكون برامج محظورة، وذلك باعتبارها تهديد لقواعد البيانات، وعادة ما يتم الحصول على عنوان البريد من خلال شبكة الإنترنت، وذلك من خلال استخدام برامج يمكنها تسجيل عناوين البريد الإلكتروني، مثل ما هو عليه الحال في غرف الدردشة، أو عن طريق برامج الاتصال المباشر، أو عن طريق الاشتراكات في مواقع الويب المختلفة[2].

- **كما أن الرسائل التي يقوم الجانــي بـعـثها في أغلب الأحيان تكون رسائل غير هادفـة:** ويكون القصد منها انتهاك الحرية الشخصية للأفراد، حيث تتنوع هذه الرسائل بين رسائل ترويجية للإعلانات المختلفة، أو أن تحتوي هذه الرسائل على مواد إباحية سواء أفلام أو صور، أو إعلان دعائي لمشروع من المشروعات الوهمية، والتي يصطلح عليها رسائل البريد البراقة[3].

ثالثاً– موقــف المشرع الجزائــري والتشريعات المقارنة من جريـمة تضخم البريــد الإلكتروني:

---

1 خالد ممدوح إبراهيم، نفس المرجع، ص 140.

2 خالد ممدوح إبراهيم، نفس المرجع، ص 142-143.

3 ما شاء الله الزاوي، المواجهة الجنائية للبريد الإلكتروني الدعائي المزعج أو المضلل، مداخلة تم إلقاءها في أعمال المؤتمر الدولي الربع عشر: الجريمة الإلكترونية، مركز جيل للبحث العلمي، طرابلس، 24-25 مارس 2017، لبنان، ص 9.

نستعرض من خلال هذه الجزئية موقف بعض التشريعات المقارنة من جريمة تضخم البريد الإلكتروني، وذلك على النحو الآتـــي:

1- موقف المشرع الفرنسي:

يرى البعض[1] أن هذا الفعل يدخل ضمن الاعتداء على نظام المعالجة الآلية للمعطيات، وأن المشرع عاقب عليه وفقاً للمادة 2/323 والتي تنص على أن: "الفعل الذي بمقتضاه يتم إعاقة عمل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس والغرامة"، ونحن بدورنا نؤيد هذا الرأي، وذلك لأن المعلومات التي يحتوي عليها البريد الإلكتروني تعتبر فعلاً من قبيل البيانات الخاصة والإعتداء عليها من دون إذن صاحبها يعتبر اعتداء على نظم البيانات.

2- موقف المشرع المصري:

يرى البعض[2] أن هذه الجريمة قابلة للعقاب من خلال تطبيق نص المادة (76) من قانون الاتصالات المصري رقم (10) لسنة 2003م، والتي جاء فيها: "يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تتجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين: ... 2- كل من تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات"، ومنه ينصرف مضمون هذه المادة إلى تكييف فعل تضخم البريد الإلكتروني على اعتباره أحد طرق الإزعاج الناتجة عن وسيلة اتصالات، كما أن المشرع المصري حدد نوع الوسيلة المرتكبة في تنفيذ الجريمة بقوله: "استعمال أجهزة اتصالات" وأحسن فعلاً عندما فعل ذلك، فضلاً عن جعله عقوبة الحبس غير محددة بحد أقصى، مما يجعلها خاضعة لجسامة الفعل.

3- الـمشرع الجزائــري:

لا يوجد نص صريح في التشريع الجزائري يجرم هذا النوع من الأفعال، وإن كنا نرى أن المشرع الجزائري ذهب في نفس مسلك المشرع الفرنسي في تجريم الاعتداء على نظم البيانات والمعطيات، فهذا يعني أن نفس الأحكام التي يطبقها المشرع الفرنسي من خلال معاقبته على هذا النوع من الجرائم قد يعمل بها، ويطبق على هذا النوع من الجرائم إذا ما وقعت في الجزائر.

---

1 CF.J. Predes & M.danli- Juan, droit pénal, t3, droit pénal spécial, Cujas, paris, 1995, p 205.

– **مشار إليه عند:** خالد ممدوح ابراهيم، المرجع السابق، ص 145.

2 طارق صادق عفيفي، المرجع السابق، ص 134.

رابعاً– طرق مكافحة جريـمة تضخم البريـد الإلكترونـي:

من أجل حماية البريد الإلكتروني من هذا النوع من الاختراق، على صاحب كل بريد إلكتروني ضرورة العمل بالأساليب الآتـية:

- الحذر من الرسائل التي يتم إرسالها من أشخاص غرباء أو غير موثوق فيهم، وذلك من خلال عدم النقر فوق الروابط، وعدم تنزيل المرفقات[1].
- المحافظة على تحديث برامج مكافحة الفيروسات، وذلك من أجل الحد من انتشار الفيروسات التي تنجم عن رسائل سبام (Spam)[2].
- الإبتعاد عن مسابقات الشبكة بمختلف أنواعها، بالإضافة إلى الاستطلاعات الغريبة التي قد تعترضك أثناء تصفحك لمواقع الإنترنت، بحيث لا تعد أكثر من أدوات استقطاب من أجل استغلال البريد الإلكتروني الخاص بك[3].
- الإشتراك في إحدى خدمات تصفية البريد الإلكتروني مما قد يضمن مقاومة هذا النوع من الرسائل، بحيث من خلال الاشتراك في هذا النوع من الخدمات توفر وسيطاً بينك وبين مزود خدمة الإنترنت وشركات إرسال سبام (Spam)، بحيث تستخدم أسلوباً خاصاً في اختيار جميع الرسائل الواردة والتأكد على أنها رسائل حقيقية[4].
- كما يجب عدم استعمال العنوان البريدي في جميع المواقع الخاصة وغرف الدردشة، بحيث ينصح باستخدام عنوان بريد إضافي لا يُستعمل من أجل العمل أو الأغراض الشخصية، حتى لا يؤثر على البيانات الشخصية المتوفرة ضمن البريد الخاص[5].

المطلب الثانـــي: جريـمة الإرهاب الإلكترونـي.

إن الثورة التكنولوجية ومتطلباتها الكثيرة خَلَقَت صراعاً كبيراً بين الدول على أصعدة مختلفة، جعلت كل جهة من الجهات تسعى إلى تطوير أنظمتها المعلوماتية، وخلق آلية دفاعية لا تسمح

---

1 أشرف السعيد أحمد، مرجع سابق، ص 58.

2 مجدي محمد أبو العطاء، أمن المعلومات والإنترنت، ط. الأولى، كمبيوساينس، مصر، 2016، ص 93.

3 مجدي محمد أبو العطاء، نفس المرجع، ص 92.

4 مجدي محمد أبو العطا، المرجع السابق، ص 90.

5 خالد ممدوح إبراهيم، المرجع السابق، ص ص 147-151.

للخصم سواء تمثل في مجموعة إرهابية، أو دولة غير صديقة في اختراق هذا النظام المعلوماتي، الذي قد يشكل كل أسرار الدولة السياسية والاقتصادية والاجتماعية، ولذلك من خلال هذا المطلب نتطرق إلى مفهوم الإرهاب الإلكتروني (الفرع الأول)، وصوره والأحكام المنظمة له (الفرع الثاني).

الفرع الأول مـــفهوم الإرهاب الإلكترونـــي[1].

من خلال هذا الفرع نتطرق لتعريف الإرهاب الإلكتروني (أولاً)، ثم بيان خصائصه (ثانياً)، فمخاطره (ثالثاً)، وذلك على النحو التالي:

أولاً– تعريـــف الإرهاب الإلكترونـــي[2]:

هناك العديد من المفاهيم الخاصة بالإرهاب الإلكتروني، والتي من بينها تعريف الباحث الأمريكي (بوليت مارك) الذي عرف الإرهاب الالكتروني على أنه: "هجمات ذات دوافع سياسية، اقتصادية، أو شخصية ضد المعلومات، ونظم الحاسوب وبرامجه، من قبل مجموعة إرهابية وعملاء سريين"[3].

وعرفته الباحثة "دوروثي دينينج" في قولها: "يجمع مصطلح الإرهاب الإلكتروني ما بين مفهوم الإرهاب والفضاء الإلكتروني، ومن ثمّ فهو يشير إلى الاعتداءات والتهديدات الموجهة لأجهزة الحاسب

---

1 كان أول ظهور لمصطلح الإرهاب الإلكتروني في الثمانينات من القرن العشرين، حيث لم يكن هذا المصطلح ذو صيت كبير في العالم، ليكتسب شهرته بعد عدة هجمات حيوية حدثت ضد مواقع إلكترونية حساسة في الولايات المتحدة الأمريكية، ليتم بعدها تقديم عدة دراسات في هذا الموضوع من طرف أكاديميون من أجل الوقوف على المصطلح، وإعادة النظر فيه بصورة أكاديمية، ولعل من بين أهم ما ساهم في انتشار الإرهاب الإلكتروني على نطاق واسع ترافقه مع شبكة الإنترنت، فضلاً عن ظهور عدد كبير من الجماعات الإرهابية التي عملت على الاستفادة من هذه الوسائل على نطاق واسع. **انـــظر**: أحمد محمد عبد الباقي، الإنترنت، التكنولوجيا وجرائم المستقبل، ط. الأولى، دار النهضة العربية، مصر، 2017، ص 23.

2 يقابل الإرهاب الإلكتروني ما يعرف بالإرهاب التقليدي والذي يعرف بأنه: "كل استخدام للقوة أو العنف أو التهديد أو الترويع، يلجأ إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي، بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، إذا كان من شأن ذلك إيذاء الأشخاص، أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بالاتصالات، أو المواصلات، أو بالأموال، أو بالمباني، أو بالأملاك العامة، أو الخاصة، أو احتلالها، أو الاستيلاء عليها، أو منع، أو عرقلة ممارسة السلطات العامة، أو دور العبادة، أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور أو القوانين أو اللوائح". **انـــظر**: مصطفى محمد موسى، الإرهاب الإلكتروني–دراسة قانونية، أمنية، نفسية، اجتماعية– ط. الأولى، مطابع الشرطة، مصر، 2009، ص 93–94.

3 **نقلاً عـــن**: نجاري بن الحاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الإلكتروني، مذكرة لنيل شهادة الماجستير، تخصص قانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2016، ص 24.

الآلي والشبكات الإلكترونية والمعلومات الموجودة عليها، بهدف إجبار الحكومات والمجتمعات على أفعال معينة لأغراض سياسية أو اجتماعية[1]".

وعرفه آخر[2] كذلك على أنه: "ذلك النشاط الذي يستخدم وسائل غير قانونية يقوم به شخص أو عدَّة أشخاص من خلال استخدام لكل وسائل العصر الرقمي الحديث، والمتمثل بتقنيات المعلومات والاتصالات لتحقيق أغراض محددة".

ومن خلال قراءة المفاهيم السابقة نستنتج أن المفهوم الأول اعتمد على الدوافع التي يتم من خلالها اللجوء إلى ارتكاب هذا النوع من الأفعال، وهي في معظمها دوافع ذات أبعاد تخص الدول أو المؤسسات الكبيرة أو أفراد ذو أهمية في المجتمع أكثر منها الأفراد العاديون، بينما ذهب المفهوم الثاني إلى تقديم فكرة عامة عن أصل المصطلح، ثم المخاطر التي يمكن أن تنتج عن هذه التهديدات، بينما حاول المفهوم الثالث الوقوف على البعد القانوني للجريمة بحيث أعطى تعريفاً قانونياً، يعتمد في البداية على عدم مشروعية الفعل ثم من يقوم بهذا الفعل، ثم الوسائل المستعملة لارتكاب هذا النوع من الجرائم، وحاول أن يختصر الهدف من هذه الجريمة في غرض محدد، بينما نجد أن المفهومين الأول والثاني يريان أن الهدف من الإرهاب الإلكتروني هو إلحاق الأذى بالمعلومات ونظم الحاسوب وبرامجه، وتضيف الدراسة الهاتف النقال وبرامجه، كما أشار المفهوم الأول إلى نوع الجناة الذين يرتكبون هذا النوع من الجرائم، حيث يمكن أن يكون هؤلاء الجناة جماعة إرهابية، وهذا أمر متوقع الحدوث خصوصاً بالنظر لما يشهده العصر الحالي من تكاثر لهذه الجماعات والتكوين العالي والفني لأفرادها، خاصة في مجال المعلوماتية وأجهزة الحاسوب والهاتف النقال، كما يمكن أن يكون الجناة عملاء سريون وهذا أيضاً أمر متوقع الحدوث بالنظر للسباق الذي تشهده محاور العالم الكبرى في شتى المجالات.

ومن خلال ما سبق يمكن تعريف الإرهاب الإلكتروني على أنه: "هجوم إلكتروني تقوم به جماعة إرهابية أو دولة أو عملاء سريون ضد الحواسب الآلية أو أجهزة الهاتف النقال، والتي تحتوي على معلومات ومعطيات سرية بالنسبة لدولة أخرى أو شركات أو أفراد، بهدف تدمير أو استغلال هذه المعلومات أو المعطيات في أغراض سياسية أو اجتماعية أو اقتصادية".

---

1 نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية – دراسة في أبعاد الأمن الإلكتروني- ب. ط، المكتب العربي للمعارف، القاهرة، 2018، ص 35.

2 حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، جامعة ديالى، عدد خاص، العراق، 2013، ص 222.

ثانياً– خصائص جريــمة الإرهاب الإلكترونــي:

كغيرها من الجرائم تمتاز جريمة الإرهاب الإلكتروني بعديد من الخصائص، والتي منها[1]:

- مقارنة بالإرهاب التقليدي لا يحتاج الإرهاب الإلكتروني إلى عنف وقوة من أجل تنفيذ الجريمة، وإنما يتطلب وجود وسيلة تكنولوجية متخصصة في هذا المجال (الهاتف النقال/الحاسوب الآلي)، بحيث يجب أن تكون هذه الوسيلة متصلة بشبكة الإنترنت ومزود ببعض البرامج اللازمة.
- يعتبر الإرهاب الإلكتروني من الجرائم العابرة للحدود، ويرجع ذلك لنمط الجريمة أو حتى الوسائل المستخدمة في ارتكاب الجريمة، مما يجعلها غير محصورة بنطاق إقليمي معين[2].
- تمتاز جريمة الإرهاب الإلكتروني بصعوبة اكتشافها، وذلك يرجع لعدة أسباب منها نقص الخبرة لدى الأجهزة الأمنية المختصة، فضلاً عن الفضاء الإلكتروني الذي تحدث فيه هذه الجريمة، والذي لا يتيح فرصة التبليغ عن الجريمة[3].
- تعتبر جريمة الإرهاب الإلكتروني من الجرائم الإلكترونية التي يصعب إثباتها، ويعود ذلك إلى طبيعة الدليل التقني الذي يتميز بسرعة طمسه والتخلص منه، فضلاً على المقدرة على إتلافه وتدميره[4].
- قد تكون جريمة الإرهاب الإلكتروني جريمة منظمة بحيث تتطلب أكثر من شخصان لارتكابها[5].

---

1 حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، ب. ط، دار فكر وفن للطباعة والنشر والتوزيع، مصر، 2015، ص 190.

2 ياسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، مداخلة علمية تم إلقاءها في الملتقى العلمي: "الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية"، خلال الفترة من 2-2014/09/4، كلية العلوم الإستراتيجية، عمان، ص 11.

3 ياسر محمد عطية، المرجع السابق، ص 11

4 حسنين شفيق، المرجع السابق، ص 190.

5 حسنين شفيق، نفس المرجع، ص 190.

- يتمتع مرتكب جريمة الإرهاب الإلكتروني بنوع من الذكاء الإلكتروني، الذي يمكن أن يرجع إلى كون الجاني مختص في المجال التقني المعلوماتي، أو أنه لديه خبرة ومعرفة في التعامل مع الوسائل التكنولوجية الفنية.

ثالثاً– أسباب انتشار جرائم الإرهاب الإلكترونـــي:

لقد ساهم في انتشار جرائم الإرهاب الإلكتروني العديد من الأسباب؛ سواء المتعلقة بتطور المعلوماتية وبالتكنولوجيا، أو المرتبطة بالوضع السياسي والاجتماعي والاقتصادي، وهو ما يتم التطرق له على النحو الآتـــي:

1- الأسباب السياسية والاجتماعية والاقتصادية:

تتمثل هذه الأسباب في ما يلي[1]:

- استبداد الأنظمة السياسية، وعدم مشاركة الشعب في صناعة القرارات، والقضايا المصيرية.
- اعتماد الدول أساليب قهرية أو غير إنسانية في التعامل مع شعوبها.
- عجز الحكومات عن توفير المتطلبات الأساسية لشعوبها.
- البطالة ودورها في غسل الأدمغة، والرغبة في الانتقام من الدولة ومؤسساتها.
- الأزمة الحضارية، وأزمة الهوية خاصة لدى الشباب.
- حب الظهور والشهرة لدى بعض الفئات الاجتماعية، مما يضطرهم للقيام بأعمال تخريبية وتدميرية.

2- الأسباب التكنولوجية:

هناك العديد من الأسباب التكنولوجية التي ساهمت في ظهور وتفشي جريمة الإرهاب الإلكتروني، ومن بين هذه الأسباب[2]:

---

1 إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني–دراسة مقارنة–، رسالة مقدمة من أجل نيل درجة الماجستير في القانون العام، جامعة ما بين النهرين، الموسم الجامعي 2013–2014، ص 30–33.

2 مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية –دراسة مقارنة بين التشريع الأردني والعراقي– رسالة مقدمة من أجل الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الموسم الجامعي: 2017/2016، الأردن، ص 22–23.

- سهولة استخدام شبكة المعلومات وقلة تكلفتها.
- الفراغ التنظيمي والقانوني في الجرائم الإلكترونية.
- ضعف بنية شبكات المعلومات المصممة من أجل أن تكون مفتوحة أمام الجميع، بشكل لا يسمح للحواجز الأمنية فرض رقابة عليها.
- وجود ثغرات كثيرة في شبكة المعلوماتية تتيح للجماعات الإرهابية في استغلالها من أجل ممارسة الأعمال التحضيرية والإرهابية.

رابعاً– مخاطر جريمـــة الإرهاب الإلكترونـــي:

ترتبط جريمة الإرهاب الإلكتروني ارتباطاً وثيقًا بالتطور التقني والتكنولوجي، لذلك تعتبر الدول المتطورة التي تعتمد على نظام الحكومة الإلكترونية "الإدارة الإلكترونية" من أكثر الدول تضرراً في هذا المجال، وهذا باعتبار أن هذه النوع من العمليات الإرهابية يكون سهل التنفيذ، كما أنه يوفر التأمينات السرية الكاملة لأعضاء المجموعات بعيداً عن الفوضى والإزعاج، بحيث تعتمد هذه العمليات على ضغطة زر من جهاز إلكتروني من أجل تدمير البنية المعلوماتية وتحقيق آثار تخريبية مخيفة[1]. ولعل من أخطر الهجمات التي تشنها هذه المجموعات شن هجوم إرهابي مدمر من أجل إغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة على الاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية[2].

إن مخاطر الإرهاب الإلكتروني تنبئ بجرائم مستقبلية خطيرة قد تفوق بأضرارها الجرائم التقليدية، من جميع النواحي هذا ما يحتم على الدول السرعة في توفير آليات تحارب هذه الظاهرة وتحد من أضرارها ومخاطرها.

الفرع الثانـــي: موقف التشريعات المقارنـــة من جريـــمة الإرهاب الإلكتروني.

---

1 حسن تركي عمير، سلام جاسم عبد الله، المرجع السابق، ص 329.

2 عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني، مداخلة مقدمة إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 2-4 جوان 2008، ص 30.

نتطرق من خلال هذا الفرع إلى موقف بعض التشريعات فيما يخص جريمة الإرهاب الإلكتروني؛ وذلك من حيث عملية التجريم والقواعد الإجرامية التي تم إسناد الجريمة إليها، سواء تعلق الأمر بقواعد إجرامية خاصة بالإرهاب، أو القواعد المتعلقة بالجريمة الإلكترونية، باعتبار أن جريمة الإرهاب الإلكتروني هي جريمة إلكترونية.

أولاً– التشريع الفرنسي:

يُعتبر التشريع الفرنسي من بين أهم التشريعات التي سعت إلى مكافحة هذا النوع من الجرائم، حيث واجه المشرع الفرنسي جريمة الإرهاب بصفة عامة ضمن الباب الثاني من الكتاب الرابع من قانون العقوبات الفرنسي، تحت عنوان: "جرائم ضد الأمة والدولة والسلم العام"، وذلك ضمن المواد 1/421 إلى 7/422 من ق.ع.ف[1].

هذا وقد نصت المادة 1/421 من قانون العقوبات الفرنسي على الجرائم التي تصنف أعمالاً إرهابية، والتي تكون ذات صلة بمشروع فردي أو جماعي، ويكون الغرض منها الإخلال بالنظام العام بشكل خطير، وذلك باستخدام الجناة للتخويف والترغيب من أجل القيام بأفعالهم هذه، ومن بين هذه الجرائم التي أوردها المشرع الفرنسي في هذا الباب الجرائم الآتية:

- الهجمات المعتدية على الحياة (الاغتيالات) والاعتداء على السلامة الجسدية والخطف، وخطف السفن والطائرات، أو وسيلة نقل أخرى، على النحو المحدد في الكتاب الثاني من هذا القانون.
- السرقة والابتزاز، والتدمير، والإتلاف، فضلاً عن جرائم المعلومات على النحو المحدد في الكتاب الثالث من هذا القانون[2].

---

1 محمود محمد محمود جابر، المرجع السابق، ص 307.

2 Art 421-1:" Constituent de actes de terrorisme, lorsqu' elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes:

1° Les atteintes volontaires à la vie, les atteintes volontaires à l' intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre ll du présent code;

2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre lll du présent code; Modifié par la Loi n°2011-266 du mars 2011-art,18.

يتضح من نص المادة السابقة أن المشرع الفرنسي قد أدرج جريمة الإرهاب الإلكتروني ضمن جرائم الإرهاب التقليدية، وذلك بإيراده لفظ "جرائم المعلومات" ضمن الفقرة الثانية من المادة 1/421، وإن كان قد حدد الأفعال المكونة للجريمة بموجب الكتاب الثالث من قانون العقوبات الفرنسي، والتي تخص بالتجريم العدوان على أنظمة المعالجة الآلية للبيانات، سواء تم ارتكاب هذه الجرائم عن طريق الحاسب الآلي أو الهاتف النقال، بصفة فردية أو جماعية على أن يترتب على ارتكابها إخلال بالنظام العام.

ثانياً– موقف الـمشرع الـمصري:

عالج المشرع ظاهرة الإرهاب بصفة عامة ضمن القانون 94 لسنة 2015 والمتعلق بمكافحة الإرهاب، وضمَّن المشرع هذا القانون العديد من الأحكام الموضوعية منها ما هو متعلق بالجماعة الإرهابية وتعريفها[1]، كما عرف المقصود من الإرهابي أو من يعتبر إرهابي في مفهوم هذا القانون، فضلاً عن تعريف الجريمة الإرهابية والعمل الإرهابي، وفي هذا التفصيل حرص المشرع المصري من أجل الإلمام بكافة الأفعال التي يكمن أن تضر بالأمن العام والسلامة العامة للمجتمع المصري، وهذا واضح من نص المادة 2 من هذا القانون، والتي عرفت العمل الإرهابي على أنه: "كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج، بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر، أو إيذاء الأفراد أو إلقاء الرعب بينهم، أو تعريض حياتهم، أو حرياتهم، أو حقوقهم العامة، أو الخاصة، أو أمنهم للخطر، أو غيرها من الحريات والحقوق التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي أو الأمن القومي، أو إلحاق الضرر بالبيئة أو بالموارد الطبيعية أو بالآثار أو بالأموال، أو المباني، أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة، أو الجهات، أو الهيئات القضائية، أو مصالح الحكومة، أو الوحدات المحلية، أو دور العبادة، أو المستشفيات، أو مؤسسات ومعاهد العلم، أو الدبلوماسية القنصلية، أو المنظمات والهيئات الإقليمية الدولية في مصر، من القيام بعملها أو ممارستها لكل أو بعض أنشطتها، أو مقاومتها، أو تعطيل تطبيق أي من أحكام الدستور أو القوانين، أو

---

1 عرف المشرع المصري الجماعة الإرهابية في الفقرة أ من المادة الأولى بقوله: "كل جماعة أو جمعية أو هيئة أو منظمة أو عصابة مؤلفة من ثلاثة أشخاص على الأقل أو غيرها أو كيان تثبت له هذه الصفة، أياً كان شكلها القانوني أو الواقعي سواءٌ أكانت داخل البلاد أو خارجها، وأيًا كانت جنسيتها أو جنسية من ينتسب إليها، تهدف إلى ارتكاب واحدة أو أكثر من جرائم الإرهاب، أو كان الإرهاب من الوسائل التي تستخدمها لتحقيق أو تنفيذ أغراضها الإجرامية".

اللوائح. وكذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة بالفقرة الأولى من هذه المادة، أو الإعداد لها، أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات، أو بالنظم المعلوماتية، أو النظم المالية، أو البنكية، أو بالاقتصاد الوطني، أو مخزون الطاقة، أو بالمخزون الأمني من السلع، والمواد الغذائية والمياه، أو بسلامتها، أو بالخدمات الطبية في الكوارث والأزمات"[1].

وبالرغم من طول هذه المادة، إلا أن المشرع المصري حاول التفصيل في ذكر الأعمال التي يمكن أن تشكل اعتداء إرهابي، حيث كان توجهه واضحاً عندما ذكر الاعتداءات التي يمكن أن تشكل خرقاً لنظم الاتصالات والمعلوماتية، فهو بذلك يكون قد أقر بوجود عمل إرهابي قد يستهدف هذه الطائفة من المصالح الحيوية للدولة أو حتى للأفراد. وفضلاً عن هذا النص هناك نصوص أخرى مباشرة أشار فيها المشرع المصري إلى الأعمال التي يمكن أن تشكل اعتداء إرهابي على نظم الاتصالات والمعلوماتية ونذكر منها:

ما نصت عليه المادة 12 من قانون مكافحة الإرهاب، والتي نصت على أن: "يعاقب بالإعدام أو السجن المؤبد كل من أنشأ أو أسس أو نظَم أو أدار جماعة إرهابية أو شارك فيها بأي صورة مع علمه بأغراضها، وتكون العقوبة السجن المشدد الذي لا تقل مدته عن عشر (10) سنوات إذا تلقى الجاني تدريبات عسكرية أو أمنية أو تقنية لدى الجماعة الإرهابية لتحقيق أغراضها، أو كان الجاني من أفراد القوات المسلحة أو الشرطة".

ومن خلال هذه المادة نلاحظ أن هناك العديد من الإشارات التي لها علاقة بنظم الاتصالات والمعلومات، وذلك ما يمكن استنتاجه من خلال لفظ "تقنية"؛ والذي يفسر بالضرورة على وجود مهارة فنية متعلقة بأنظمة الحاسوب والهاتف النقال، وكيفية استعمالها في أعمال تخريبية.

كما أشارت المادة 15 من نفس القانون بشكل مباشر على الوسائل التي يمكن اعتمادها من طرف الجماعات الإرهابية، وذلك من خلال تدريب أعضاء الجماعة على استعمال وسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية، أو أي وسيلة تقنية أخرى من أجل تنفيذ أغراضهم الإجرامية[2].

---

1 القانون رقم 93 المتعلق بمكافحة الإرهاب، المؤرخ في 30 شوال 1439 الموافق لـ: 15 أغسطس 2015، ج.ر.ج.م، ع 33 مكرر، ص 6.

2 نصت المادة 15 من قانون مكافحة الإرهاب على أن: "يعاقب بالسجن المؤبد أو السجن المشدد الذي لا تقل مدته عن عشر سنين، كل من قام بأي طريقة مباشرة أو غير مباشرة، أو بقصد ارتكاب جريمة إرهابية في الداخل أو الخارج، بإعداد أو تدريب أفراد على صنع أو استعمال الأسلحة التقليدية أو غير التقليدية، أو وسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية ، أو

ثالثاً– موقـف الـمشرع الجزائـري:

يمكن أن نستنتج موقف المشرع الجزائري من جريمة الإرهاب الإلكتروني من خلال استقراء المادة 87 مكرر من قانون العقوبات، والتي ضمنها المشرع الأعمال الموصوفة بأفعال إرهابية وتخريبية، فمن خلال هذه المادة أورد المشرع العديد من الأفعال والتي كان من بينها: "... تخريب أو إتلاف وسائل الاتصال"[1]، فهذه الجملة تحمل مدلول واسع لكل الأفعال التي يمكن أن ترتكب ضد هذه الوسائل، وإن كان يعاب على المشرع الجزائري عدم التفصيل في هذه المسألة على غرار ما ذهب إليه المشرع المصري؛ لأن إيراد اللفظ على عمومه يفتح باب الاجتهاد في الأفعال التي يمكن أن يتضمنها هذا النوع من الجرائم والأفعال التي يمكن أن تستثنى من ذلك، أو حتى وسائل الاتصال التي يقصدها المشرع.

أما النص الثاني فيتجسد في أحكام المادة 394 مكرر من ق.ع.ج والتي تضمنت العديد من الأحكام المتعلقة بالاعتداء في مجال المعلوماتية، والتي يمكن أن تندرج ضمنها جريمة الإرهاب الإلكتروني، حيث نصت المادة 394 مكرر على أن: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50000 دج إلى 100000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50000 دج إلى 150000 دج".

ومن خلال النص السابق أشار المشرع الجزائري إلى بعض الأفعال التي يمكن أن تشكل جزء من صور الإرهاب الإلكتروني، وخصوصاً عندما أورد المشرع مصطلحات مثل: الدخول، الحذف التغيير، والتخريب، فكل هذه المصطلحات قد تدخل في إطار السلوك الإجرامي لهذه الجريمة.

أي وسيلة تقنية أخرى، أو قام بتعليم فنون حربية أو أساليب قتالية أو تقنية، أو مهارات، أو حيل، أو غيرها من الوسائل، أي كان شكلها لاستخدامها في ارتكاب جريمة إرهابية، أو حرض على شيء مما ذكر".

1 المادة 87 مكرر من الأمر رقم 95-11 المؤرخ 25 رمضان 1415 الموافق 25 فبراير 1995 المعدل والمتمم للأمر 66-156 المؤرخ 18 صفر 1386 الموافق 8 يونيو 1966م المتضمن قانون العقوبات، ج.ر.ج.ج، ع 11، المؤرخة 1 مارس 1995، ص 8.

كما أنه نص في المادة 394 مكرر 2 الفقرة الثانية كذلك على صورة أخرى من صور الإرهاب الإلكتروني، حيث جاءت فقرة هذه المادة على الشكل التالي: "...حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم". كذلك من خلال هذه الفقرة يمكن أن نستنتج إمكانية حصول مجموعة إرهابية على معلومات ذات طابع سري تخص أمن الدولة وسلامة أفرادها، أو حتى تساهم في نشر معلومات قد تضر باقتصاد الدولة أو غيرها من الأفعال الأخرى المضرة.

كما أن نص المادة 394 مكرر 3 تضمن استهداف الجريمة للدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، فهذا إن دل على شيء فهو يدل على خطورة المنشآت المستهدفة وسريتها، أو حتى خصوصية المؤسسة، بحيث مجرد التلاعب بمعلومات المواطنين الخاصة من أوراق شخصية وغيرها عن طريق إتلافها أو تخريبها، فهذا يعتبر إرهاب إلكتروني، خاصة مع توجه الدولة الحديث في تبني الإدارة الإلكترونية ومحاولة تعميمها على جميع القطاعات[1].

ومن خلال نص المادة 394 مكرر 5 أشار المشرع إلى إمكانية حدوث الجريمة بطريقة منظمة عن طريق اتفاق مسبق بين جماعة معينة في المشاركة في ارتكاب هذه الجريمة، بشرط أن يكون التحضير لهذه الجريمة مجسد بفعل أو أفعال مادية، كما أن إيراد مصطلح مجموعة قد ينصرف إلى مجموعة ذات طابع إرهابي يكون هدفها التخريب.

وعليه بالرغم من النصوص السالفة الذكر، إلا أن موقف المشرع الجزائري لم يكن واضحاً بما يكفي فيما يخص هذا النوع من الجرائم الخطيرة؛ سواء من خلال النصوص التقليدية التي جرمت الأفعال الموصوفة بأعمال إرهابية أو تخريبية، أو حتى من خلال النصوص المتعلقة بالجريمة المعلوماتية، حيث وجب على المشرع الجزائري أن يسلك نهج المشرع المصري وإيضاح الفكرة حول هذا النوع من الجرائم.

الـمطلب الثالث: جريـمة التجسس الإلكترونـي.

تعتبر جريمة التجسس الإلكتروني من بين أكثر الجرائم وقوعًا وانتشارًا بين الأشخاص سواء العامة أو الخاصة، خصوصاً بعد التطور الهائل في مجال التكنولوجيا واستخداماتها العديدة، حيث

1 المادة 394 مكرر 3: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

شكل الهاتف النقال أحد الوسائل الحديثة التي تُـنبأ بعصر جديد من الجوسسة والإختراق، وهناك العديد من الأمثلة التي تدل على خطورة التجسس الإلكتروني، لذلك نتطرق من خلال هذا المطلب إلى مفهوم جريمة التجسس الإلكتروني (الفرع الأول)، وموقف التشريعات منها (الفرع الثاني).

الفرع الأول: مفهوم جريـــمة التجســس الإلكتروني.

سنتناول من خلال هذا الفرع تعريف جريمة التجسس، وبيان خصائصها والأحكام المنظمة لها، وبيان ذلك على النحو التالــي:

أولاً- تعريف التجســس الإلكترونــي:

يعرف التجسس بصفة عامة بأنه: "فعل إيجابي قوامه الكشف واستظهار الحقائق المخفية، ولكنه كشف واستظهار غير مشروع، إن كان بوسائله أو بغايته أو بأحدهما، وهو بذلك فعل لا يقره الشارع ويفرد لمرتكبه العقوبة الجزائية الرادعة دون تهاون، انسجاماً مع روح التشريع، وإدراكاً لعظم خطورة هذا السلوك"[1].

ومن خلال هذا التعريف نستنتج أن التجسس عبارة عن تتبع حقيقة معينة من أجل كشفها وذلك باستعمال طرق غير مشروعة، مما يجعل هذا الفعل محظوراً ويقر له القانون عقوبات صارمة.

أما بالنسبة للتجسس الإلكتروني فيعرف بأنه: "استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول والحكومات والتنصت عليها، بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، وتشمل جميع أنواع المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية والاجتماعية"[2].

ويعرفه آخرون[3] على أنه: "طرق مختلفة لاختراق المواقع الالكترونية وسرقة بعض المعلومات التي تكون ذات أهمية وخطورة للطرف المتلقي والمسروق".

وعليه، من خلال المفاهيم السابقة يتضح أن التجسس الإلكتروني عبارة عمليات خطيرة تستهدف خصوصية الأشخاص والدول من خلال استغلال التكنولوجيا الحديثة في جمع معلومات

---

1 أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص 299.

2 على جعفر، المرجع السابق، ص 569.

3 أحمد محمد عبد الباقي، المرجع السابق، ص 117.

عنهم، وعن أعمالهم وحياتهم بطريقة تتيح استعمالها ضدهم، وتتنوع هذه المعلومات وتختلف باختلاف الجهة المخترقة والمعلومات التي تمتلكها.

ثانياً– أنــواع التجســـس:

تختلف عمليات التجسس باختلاف الجهة المستهدفة بعملية الإختراق، أو الهدف المراد من عملية التجسس، وفيما يلي يتم التطرق لأهم أنواع عمليات التجسس على النحو التالي:

1- أنواع التجسس بحسب الجهة المستهدفة بعملية الإخـــتراق:

في هذه الحالة يقسم التجسس إلى الأنواع الآتيـــة:

أ- **التجسس على الأفراد:** في هذه الحالة قد يتم التجسس على شخصية ما، إما أن تكون شخصية عامة، أو شخصية عادية[1].

ب- **التجسس على الحكومات:** ويعتبر هذا النوع من أكبر عمليات التجسس الشائعة بين الدول، خاصة الدول المتطورة التي تلجأ إلى هذا النوع، من أجل تحقيق غرض اقتصادي أو سياسي أو عسكري[2].

2- أنواع التجسس بحسب الهدف المخـــترق: ينقسم التجسس من خلال هذا التصنيف إلى عدة أشكال وهي:

أ. **التجسس على المعلومات العسكرية:** يتعلق هذا النوع من التجسس بكل ما اتصل بالمعلومات العسكرية، سواءٌ خطط عسكرية أو أسلحة أو صواريخ، أو خطط استراتيجية، ويعتبر هذا النوع من أكثر أنواع التجسس حساسية وسرية[3].

---

1 ومن أمثلة هذه الحادثة ما وقع مع المستشارة الألمانية "أنجيلا ميركل" التي تم اختراق هاتفها الشخصي، وهو الخبر الذي نقله بيان من موقع "ويكيليكس" والذي كشف عن 3 عمليات تنصت لوكالة الأمن القومي الأمريكية على محادثات لميركل وبيانات تشمل أرقام هواتف المستشارة الأمريكية، ومساعديها، وطاقم مكتبها، وحتى رقم جهاز الفاكس، كما أن نفس التقرير أوضح أن هناك مستشارين سابقين على أنجيلا ميركل تم التجسس عليهم، وهم كل من: "غيرهارد شرودر" و"هيلموت كول"، **انـــظر في ذلك:** موقع روسيا اليوم، مقالة بعنوان: "ويكيليكس: وكالة الأمن القومي تتجسس على ألمانيا منذ عقود"، متاح على الرابط الإلكتروني التالي: *https://arabic.rt.com/news/788206* ، تاريخ الإطلاع: 2018/08/10.

2 علي جعفر، المرجع السابق، ص 270.

3 رشاد خالد عمر، المرجع السابق، ص 42.

ب. **التجسس على المعلومات الاقتصادية:** تعتبر هذه المعلومات ذات أهمية كبيرة، لما لها من دور بالنسبة للدول من حيث التنمية والمنافسة العلمية[1].

ج. **التجسس على المعلومات العلمية:** تتعلق هذه المعلومات بالأبحاث والدراسات والاختراعات العلمية، بجميع أنواعها العسكرية أو الصناعية، وتعتبر هذه المعلومات ذات قيمة كبيرة، بحيث يمكن أن تكون عرضة للتجسس من أجل السرقة، أو من أجل صناعة مضاد لها[2].

الفرع الثانـــي: موقف التشريعات المقارنة من جريمة التجسس.

نستعرض من خلال هذا الفرع موقف بعض التشريعات من جريمة التجسس الإلكتروني، بدءاً بالمشرع الفرنسي (أولاً)، فالمشرع المصري (ثانياً)، ثم موقف المشرع الجزائري (ثالثاً)، وذلك على النحو التالـــي:

أولاً– موقـــف المشرع الفرنسي من جريمة التجسس:

إن موقف المشرع الفرنسي لم يكن واضح بما يكفي فيما يخص جرائم التجسس الإلكتروني سواء عبر الهاتف النقال أو غيرها من الوسائل الإلكترونية الأخرى، وهذا ما سنحاول أن نبينه من خلال عرض النصوص التي جرم من خلالها المشرع الفرنسي جريمة التجسس، والتي جاءت في الباب الأول ضمن الكتاب الرابع من ق.ع.ف، وخاصة في الفصل الأول الذي جاء معنون بـــــ: "الخيانة والتجسس".

تنص المادة 5/411 من ق.ع.ف على أن: "يعاقب على التخابر مع دولة أجنبية أو مؤسسة أو منظمة أجنبية، أو عملاء لهم، على نحو يؤدي إلى الإضرار بالمصالح الأساسية للأمة، بالسجن لمدة 10 سنوات وغرامة 150.000 يورو"، ويتبين من نص هذه المادة أن المشرع الفرنسي تطرق إلى التخابر بصفة عامة مشيراً إلى الأشخاص الذين يتم التخابر لصالحهم، والمصالح التي قد تكون عرضة للتخابر، والتي عبر عنها بمصطلح "تؤدي إلى الإضرار بمصالح الأمة"، فهو بذلك يكون قد ترك المجال واسع لتحديد المصلحة التي تكون عرضة للتجسس.

وفضلاً عن المادة السابقة نجد أن المشرع الفرنسي في نص المادة 6/411 من ق.ع.ف قد بَيّـن الوسائل التي قد يقدمها العميل لمن يعمل لأجله، والتي تتمثل في معلومات، أو أشياء أو وثائق، أو

---

1 علي جعفر، المرجع نفسه، ص 517.

2 على جعفر، المرجع نفسه، ص 570.

بيانات إلكترونية، أو ملفات للقاءات، أو اجتماعات تضر بمصالح الأمة، كما عاقب المشرع الفرنسي في النص السابق على التقديم والإتاحة، ومن أجل الحرص أكثر على المعاقبة على هذه الجريمة أضاف المشرع في المادة 7/411 مصطلح التسليم، بحيث تتحقق الجريمة في الصور الآتية: "التقديم، الإتاحة، والتسليم"[1].

ثانياً– موقف المشرع المصري من جريمة التجســـس:

رغم أن المشرع المصري لم يعطِ دلالات واضحة فيما يخص التجريم لسلوك "التجسس الإلكتروني"، إلا أن هناك العديد من المواد التي تنص وبصفة غير مباشرة على إمكانية المعاقبة على هذا النوع من الجرائم، ومن أمثلة ذلك ما ذهب إليه المشرع في المادة 80 الفقرة أ من ق.ع.م، والتي جاء فيها: "يعاقب بالحبس مدة لا تقل عن ستة (06) أشهر ولا تزيد عن خمس (05) سنوات، وبغرامة لا تقل عن 100 جنيه ولا تتجاوز 500 جنيه:

- كل من حصل– بأي وسيلة غير مشروعة – على سر من أسرار الدفاع عن البلاد، ولم يقصد تسليمه، أو إفشاءه لدولة أجنبية، أو لأحد ممن يعملون لمصلحتها.
- كل من أذاع –بأي طريقة– سراً من أسرار الدفاع عن البلاد.
- كل من نظم أو استعمل أي وسيلة من وسائل التراسل، بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته،

وتكون العقوبة السجن إذا وقعت الجريمة في زمن الحرب".

ومن خلال نص المادة يتضح أن المشرع المصري جرم التجسس الذي يهدد مصلحة الدفاع عن البلاد بصفة عامة، وهو ما عبر عنه بلفظ "سر من أسرار الدفاع عن البلاد"، كما يلاحظ أن المشرع المصري في نص المادة 85 من نفس القانون، حاول التفصيل في المجالات التي تندرج ضمن أسرار الدفاع.

---

1 Art 411-7:"Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étranger, à une entreprise étrangère ou sous contrôle étranger ou leurs agents, des renseignements, procèdes, objets, documents, données informatisées ou fichiers dont l' exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d' emprisonnement et de 150000 euros d'amende". Modifié par Ordonnance n°2000-916 du 19 septembre2000.

والملاحظ كذلك أنه أشار في البند 3 إلى استعمال وسائل التراسل في تنفيذ هذه العملية، مما يجعل وسيلة الهاتف النقال تندرج ضمن هذه الوسائل، ويمكن أن تستخدم في الاختراق والتخابر لجهة ما.

ثالثاً– موقف المشرع الجزائــري من جريمة التجســس:

جرم المشرع الجزائري جريمة التجسس ضمن القسم الأول من الفصل الأول من الكتاب الثالث، من ق ع ج، والذي عُنون بـ: "جرائم الخيانة والتجسس"، وجرمت هذه النصوص بصفة عامة كل الاعتداءات التي تندرج تحت طائلة الخيانة والتجسس، وتضر بالدفاع الوطني والاقتصاد الوطني، ومن أمثلة ذلك ما نص عليه المشرع في المادة 61 من ق.ع.ج، والتي جاء فيها: "...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 بأي طريقة أخرى"[1].

كما أشار المشرع كذلك إلى التجسس في الفقرة 02 من المادة 62 من قانون العقوبات حيث نص على أن: "...القيام بالتخابر مع دولة أجنبية أو مع أحد عملاءها بقصد معاونة هذه الدولة في خططها ضد الجزائر".

ومن خلال قراءة النصوص السابقة يتضح بأن المشرع الجزائري سلك نفس النهج الذي اعتمده المشرع الفرنسي وكذا المصري في تجريم التجسس الإلكتروني، بحيث لا توجد نصوص صريحة أو فعلية تنص على تجريم هذا النوع من الأفعال أو تعاقب على ذلك، مما يوجب على المشرع الجزائري إعادة النظر في مثل هذا النوع من الجرائم، من خلال وضع نصوص خاصة بها، أو إدراجها ضمن القواعد التقليدية، مع وضع قواعد خاصة بتجريم مثل هذا النوع من الأفعال.

1 القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156 المؤرخ 18 صفر 1386 الموافق 8 يونيو 1966م المتضمن قانون العقوبات، ج.ر.ج.ج، ع 84، 24 ديسمبر 2004، ص 19.

ملخص الــباب الأول:

قدمت التكنولوجيا للإنسان عدَّة امتيازات جعلت من حياته أكثر سهولة ورفاهية، إلا أن هذا الأسلوب الجديد في الحياة صاحبه العديد من المشكلات والأضرار التي في الغالب تكون مصاحبة للاستعمال السلبي لهذه الأدوات، سواءٌ من قبل صانعيها، أو حتى من قبل مستخدميها، وعليه فقد حاولنا من خلال هذا الباب تسليط الضوء على بعض الجوانب السلبية لهذه التكنولوجيا، خاصة تكنولوجيا الهاتف النقال، وذلك من خلال تقديم عرض مفصل عن تكنولوجيا الهاتف النقال، وعن هذه التقنيات الخطيرة التي تتركَّب منها هذه التكنولوجيا.

وفي ظل هذه الدراسة، تم إلقاء الضوء على الإعتداءات الخطيرة التي نتجت عن الاستعمال الخاطئ لهذه التكنولوجيا، والتي تنوعت بتنوع النشاط الإجرامي المستخدم فيه هذه الوسيلة، بين جرائم أشخاص، وجرائم أموال، والتي في معظمها تهدد المصالح الخاصة، كما قد تهدد المصلحة العامة أيضاً، ومما يزيد الأمر خطورة هو أن هذه الظواهر الإجرامية في تزايد مستمر، وفي تطور دائم وموازٍ لتطور التقنيات والتحسينات المضافة إلى الهاتف النقال.

وفضلاً عن الجرائم السابقة، ساهمت تكنولوجيا الهاتف النقال بشكل كبير في ارتكاب الجرائم الإلكترونية، والتي تشكل إجرام موازي للإجرام التقليدي في بعض الحالات، أو أداة مساعدة في حالات أخرى، ومن بين أخطر هذه الجرائم جريمتي التجسس والإرهاب الإلكتروني، اللتان تهددان النظم الإلكترونية التي تعتمد عليها الدول في مختلف القطاعات، فضلاً عن كونها تهدد مصالح الأفراد بشكل يمس بأسرار تخص أمن الدولة، من خلال اختراق هواتف شخصيات أو هيئات سيادية في الدولة، وعن طريق التنصت والتجسس على أفراد عاديين على نحو يمس بحرمة الحياة الخاصة التي تكفلها الدساتير، وتحميها القوانين الجزائية.

الباب الثاني:
الحماية الإجرائية من الجرائم المرتكبة بواسطة الهاتف النقال

الباب الثاني:

الحماية الإجرائيــة من الجرائـم المرتكبة بواسطة الهاتــف النــقال.

يشكل الشق الإجرائي في الدعاوي القضائية بمختلف أنواعها جانباً هاماً، وذلك على اعتبار أن الدعوى القضائية لا تتصل بهيئة الحكم للفصل فيها إلا بعد مراعاة عدة إجراءات تنظمها القوانين الإجرائية بحسب كل قانون ومتطلباته، فهناك القوانين الإجرائية المتعلقة بالمنازعات المدنية والإدارية وهو يطلق علية بقانون الإجراءات المدنية والإدارية، وهناك القوانين المتعلقة بالإجراءات الجنائية، وهي ما يطلق عليها الإجراءات الجزائية بحسب ما هو معمول به في القانون الجزائري.

وتشكل الإجراءات الجزائية المرشد الرئيسي في عملية تقصي الدعاوي الجنائية، والبحث عن مرتكبها، فلذلك نجد أن جل التشريعات الوطنية تحاول من خلال تقنينها الإجرائي أن توازي بين عدة مصالح، قد يظهر في الوهلة الأولى أنها متعارضة مع بعضها البعض، إلا أن المتطلع على هذا القانون سوف يجد عكس ذلك؛ بحيث تعمل القوانين الإجرائية على البحث في آثار الجريمة ومرتكبها من أجل تحقيق العدالة من جهة، وبين توفير ضمانات للأشخاص المعنيين من جهة أخرى.

وكما أسلفنا سابقاً فالقوانين الإجرائية تتضمن العديد من المواد التي تنظم العديد من الإجراءات؛ والتي من بينها الجهاز المكلف بالبحث والتحري عن الجرائم، والجهات المختصة بالتحقيق، فضلاً عن هيئات الحكم التي تفصل في الموضوع وتشكيلتها، أضف لذلك فإن القانون الإجرائي يتضمن طرق البحث عن الأدلة الجنائية، والشروط الشكلية التي يجب مراعاتها في جمع هذه الأدلة، حتى يتسنى للقاضي المختص الأخذ بها دون أن يصطدم بقاعدة المشروعية واستبعاد الأدلة غير المشروعة.

وبناء على ما ذكر، نتطرق من خلال هذا الباب إلى الآليات الإجرائية المتبعة في البحث عن الجرائم المرتكبة بواسطة الهاتف النقال والجهات المختصة (الفصل الأول)، ثم طرق جمع الأدلة الجنائية الواجب توفرها لإثبات هذا النوع من الجرائم (الفصل الثاني).

الفـــصل الأول:

آلـيات البحث والتـحري عـن الجرائــم المرتكبــة بواسطـة الهاتـف النـقال.

تعتبر عملية البحث في الجريمة من أصعب المراحل التي تمر بها الدعوى الجنائية، بحيث يجب على رجال القضاء المرور بعدة إجراءات تقتضي منهم التنقل بين مسارح الجريمة إذا كانت متعددة، أو التحفظ على الأجهزة والبحث عنها إذا كانت الجريمة ذات طابع إلكتروني، لذلك نجد أن المشرع الجزائري من أجل تسهيل هذه العملية، ومن أجل تقصي الحقيقة بأسرع وقت، عمل على تقسيم هذه المهام من خلال وضع عدة أجهزة تعمل على البحث على الجريمة، وذلك من خلال العمل المشترك الذي يقوم به رجال القضاء سواء مع رجال الدرك، أو رجال الشرطة، أو غيرهم من الجهات الأخرى التي نص عليها المشرع الجزائري وغيره من التشريعات المقارنة الأخرى، بموجب قانون الإجراءات الجزائية أو غيرها من القوانين ذات الطابع الخاص.

من جانب آخر، شكلت الجريمة الإلكترونية بصفة عامة، وجرائم الهاتف النقال بصفة خاصة، ظاهرة من الظواهر التي هددت المجتمع بصورة فجة، مما استدعى تدخل المشرع في تجريم هذا النوع من الجرائم وفرض عقوبات على مرتكبها، وهو ما يستدعي بالضرورة وجود آليات وأشخاص على نفس التكوين والكفاءة التي يعمل بها هذا النوع من المجرمين، ولذلك حاولت التشريعات المقارنة مراعاة هذا النوع من الجرائم، من خلال تكوين رجال الضبطية القضائية والعمل على استحداث وحدات وفرق بحثية خاصة بالبحث والتحري عن الجرائم ذات الطابع الإلكتروني وجرائم الاتصال.

ولتوضيح هذا الأمر، نتطرق من خلال هذا الفصل إلى السلطات المختصة في التحري والتحقيق عن الجرائم المرتكبة بواسطة الهاتف النقال (المبحث الأول)، ثم طرق البحث والتحري عن الجرائم المرتكبة بواسطة الهاتف النقال (المبحث الثاني)، وتفصيل ذلك على النحو التالي:

المبحث الأول:

السلطات المختصة فـي التحري والتحقيق عن الجرائم المرتكبـة بواسطة الهاتف النـقال

تصنف جرائم الهاتف النقال ضمن الجرائم الإلكترونية التي أخذت طابع خاص واستثنائي على المستوى العالمي؛ وذلك فيما يتعلق بالبحث والتحري عنها، ولذلك يتم التطرق من خلال هذا المبحث إلى السلطات المكلفة بجمع الاستدلالات في هذا النوع من الجرائم، سواءٌ في القانون الجزائري أو القوانين المقارنة، فضلاً عن الجهات المكلفة بالتحقيق في هذا النوع من الجرائم، ولذلك يتم التطرق إلى إجراءات تحريك الدعوى العمومية في الجرائم المرتكبة بواسطة الهاتف النقال (المطلب الأول)، ثم التطرق إلى السلطات المختصة في التحري وجمع الاستدلالات في هذا النوع من الجرائم (المطلب الثاني)، وصولاً إلى السلطات المختصة بالتحقيق (المطلب الثالث).

المطلب الأول: تحريك الدعوى العموميــة في الجرائم المرتكبة بواسطة الهاتف النقال.

حدد المشرع الجزائري عمل النيابة العامة وفق المبادئ الأساسية التي سطرتها نصوص قانون الإجراءات الجزائية، خاصة المادة الأولى منه، إلا أن ذلك لا يلغي النصوص الاستثنائية التي أقرها المشرع فيما يخص بعض الجرائم الخطيرة، حيث عمل على توسيع سلطات وكيل الجمهورية فيما يخص هذه الجرائم، ويظهر ذلك جلياً من خـــلال:

1- توسيع الاختصاص المكانـــي لوكيل الجمهوريــة:

بحيث يصبح لوكيل الجمهورية اختصاص وطني فيما يتعلق بالجرائم الست المذكورة بموجب المادة 2/37 من القانون 04-14 المعدل لقانون الإجراءات الجزائية الجزائري[1]، والتي نصت على أن: "يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص، حتى ولو حصل هذا القبض لسبب آخر. يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

---

1 القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-155 المؤرخ في صفر عام 1386 الموافق 8 يونيه سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 71، ص 5.

2- التوســيع من مــجال صلاحيات النيابــة العامـة:

ويتعلق الأمر بمجال إصدار الإذن بالتفتيش، والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وذلك طبقاً لما نصت عليه المادة 65 مكرر 5 من قانون الإجراءات الجزائية، والتي جاء فيها: "...يجوز لوكيل الجمهورية المختص أن يأذن بما يأتــي:

- اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرق شخص أو عدة أشخاص يتواجدون في مكان خاص".

3- إجبار النـيابة على تـحريك الدعـوى العمومية بشكل تلقائي في جرائم المعلوماتية:

وذلك بحسب ما هو منصوص عليه في المادة 144 مكرر، والمادة 144 مكرر 1، والمادة 144 مكرر 2، وذلك فيما يتعلق بجرائم القذف الإلكتروني الذي تمس بشخص الرسول صلى الله عليه وسلم، أو المعلوم من الدين، أو رئيس الجمهورية[1].

والملاحظ أن المشرع الجزائري لم يؤسس نيابة خاصة فيما يتعلق بالجرائم الإلكترونية على عكس ما هو معمول في بعض التشريعات، كالتشريع الأمريكي الذي عمل على إنشاء جهاز للنيابة مختص بمكافحة الجريمة الإلكترونية في عام 1995م، وذلك تحت مسمى (CTC)، حيث كان ذلك استجابة للمخاوف المتزايدة من جرائم الحاسوب، وفي العام 2004 تم تغيير اسم هذا الجهاز إلى "نيابة الملكية الفكرية والقرصنة الإلكترونية"(CHIP)، ويدخل ضمن هذه النيابة عدد من الخبراء ذو الخبرة التقنية الذين تم تدريبهم خصيصاً لمواجهة الجرائم الإلكترونية وجرائم الإتصالات، كما تعمل هذه الأجهزة على جمع الأدلة الإلكترونية والرقمية، والتي تساعد في الكشف عن هذا النوع من الجرائم[2].

المطلب الثانــي: السلطات المختصة بالتحري وجــمع الاستدلالات.

كلف المشرع الجزائري جهاز الضبطية القضائية بعملية البحث والتحري عن الجرائم التي ترتكب في الإقليم الوطني، وذلك وفق ما يعرف بضوابط الاختصاص الشخصي والنوعي والإقليمي،

---

1 زبيحة زيدان، المرجع السابق، ص 113.

2 محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات) – دراسة مقارنة التشريع المصري والفرنسي والأمريكي والاتفاقيات الدولية والإقليمية–، ط. الأولى، المكتب الجامعي الحديث، الإسكندرية، 2018، ص 55.

وعرف بهذه الفئات في مواد الفصل الأول من الباب الأول من قانون الإجراءات الجزائية الذي جاء معنون بـ: "في البحث والتحري عن الجرائم"، وقسمهم إلى عدة فئات؛ منها ذات الاختصاص العام، وفئات ذات اختصاص خاص.

وبناء عليه، يتم التطرق إلى الضبطية القضائية ذات الاختصاص العام (الفرع الأول)، ثم الضبطية القضائية ذات الاختصاص الخاص (الفرع الثاني)، وهذا فيما يخص البحث والتحري عن الجرائم ذات الطابع الإلكتروني.

الـفرع الأول: الضبطية القضائـية ذات الاختصاص الــعام.

قبل أن نشير إلى هذه الفئة من رجال الضبط القضائي، لا بد من الإشارة إلى الاختصاص المكاني الذي يحكم عمل رجال الضبط القضائي، والذي أشارت إليه المادة 16 من قانون الإجراءات الجزائية، والذي حدد مكان ممارسة هذه الفئة لوظائفهم المعتادة مع إمكانية تمديد الاختصاص، في حال إذا كان هناك ظرف استعجالي يقتضي ذلك، على أن تكون ممارسة هذا الاختصاص الاستثنائي في دائرة المجلس القضائي الملحقين به، مع جواز امتداد اختصاصهم إلى كافة التراب الوطني إذا ما طُلب منهم ذلك من القاضي المختص[1]، وهناك إشارة واضحة في قانون الإجراءات الجزائية تخول أن يمتد فيها الإختصاص إلى كامل التراب الوطني، والتي حددها المشرع في جرائم المخدرات، والجريمة المنظمة، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، وهذا ما نصت عليه المادة 16 في فقرتها 7 والتي جاء فيها: "...غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات، والجريمة المنظمة العابرة للحدود، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال، والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يـمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

---

1 تنص المادة 16 من القانون رقم 06-22 على أن: "يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة. إلا أنه يجوز لهم، في حالة الاستعجال أن يباشروا مهمتهم في كافة دائرة الاختصاص المجلس القضائي الملحقين به. ويجوز لهم أيضاً في حالة الاستعجال، أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونًا، وبجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية. وفي الحالات المنصوص عليها في الفقرتين السابقتين، يتعين عليهم أن يخبروا مسبقًا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة اختصاصه".

وتتكون الضبطية القضائية من الفئات التي نصت عليها المادة 15 من الأمر 15-02 والتي تـشمل:

- رؤساء المجالس الشعبية والبلدية.
- ضباط الدرك الوطني.
- الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني.
- ذوو الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك الدرك الوطني ثلاث سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة.
- الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث سنوات على الأقل بهذه الصفة، والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة خاصة من لجنة خاصة.
- ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصاً بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل.[1]

ويتنوع الإختصاص النوعي لهذه الفئة بتنوع المرحلة التي تمر بها الدعوى الجنائية، حيث يكون لهم دور فعال في مرحلة الاستدلال قبل اتصال الدعوى الجنائية بالقضاء، حيث أناط بهم المشرع مهمة جمع الأدلة والبحث عن مرتكبي الجريمة، فضلاً عن تلقي البلاغات والشكاوي، وهذا باستثناء ما نص عليه المشرع في المادة 15 مكرر من قانون 17-07 والتي تضمنت الآتـي: "تنحصر مهمة الشرطة القضائية لضباط وضباط الصف التابعة للمصالح العسكرية للأمن في الجرائم الماسة بأمن الدولة المنصوص والمعاقب عليها في قانون العقوبات..."[2]، ولكن هذا الدور يتقلص تدريجياً باتصال

---

1 الأمر رقم 15-02 المؤرخ 07 شوال 1436هـ الموافق 23 يوليو 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيه سنة 1966، المتضمن قانون الإجراءات الجزئية ، ج ر ج ج ، ع 40، المؤرخة في 23 يوليو 2015، ص 29.

2 القانون رقم 17-07 المؤرخ في 28 جمادي الثانية 1438 الموافق لـ27 مارس 2017 المعدل والمتمم للأمر رقم 66- 155 المؤرخ في صفر عام 1386 الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزائية ، ج ر ج ج، ع 20، المؤرخة 29 مارس 2017، ص 6.

الدعوى بالقضاء، بحيث ينحصر دور الضبطية القضائية في تنفيذ أوامر قاضي التحقيق، وهذا ما نصت عليه المادة 12 في فقرتها الثالثة، والتي جاء فيها: "...ويناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها التحقيق القضائي"[1]، بينما نصت المادة 13 من نفس القانون على دور الضبطية القضائية بعد فتح التحقيق الذي ينحصر في تنفيذ تفويضات جهات التحقيق وتنفيذ طلباتها[2] .

ومما يجب الإشارة إليه في هذا الصدد أن المشرع الجزائري وفي ظل القانون رقم 17-07 أضاف كذلك نص المادة 15 مكرر1، والتي اشترطت تأهيل ضباط الشرطة القضائية عن طريق مقرر يصدره النائب العام للمجلس القضائي الذي يتبع له جهاز الضبطية القضائية، كما ويتم تأهيل ضباط الشرطة التابعين للمصالح العسكرية على مستوى مجلس قضاء الجزائر وبنفس الطريقة، ويستثنى من هذا التأهيل رؤساء المجالس الشعبية [3].

بالإضافة إلى ضباط الشرطة القضائية هناك أعوان نصت عليهم المادة 19 من قانون الإجراءات الجزئية، وهم كل موظفو مصالح الشرطة وذوو الرتب في الدرك الوطني، ورجال الدرك، ومستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية، وتعمل هذه الفئة من رجال الضبطية القضائية على معاونة ضباط الشرطة القضائية في مباشرة وظائفهم، حيث يعملون على إثبات الجرائم المقررة في قانون العقوبات، وذلك من خلال امتثال أوامر رؤسائهم، وجمع كافة المعلومات التي تساعد على الكشف عن مرتكبي تلك الجرائم[4] .

---

1 الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو 1966 المعدل والمتمم، المتضمن قانون الإجراءات الجزائية، ج ر ج ج ، ع 48، المؤرخة 9 يونيو 1966، ص 23.

2 المادة 13 من قانون الإجراءات الجزائية تنص: "إذا ما افتتح التحقيق القضائي فإن على الضبط القضائي تنفيذ تفويضات جهات التحقيق وتلبية طلباتها".

3 تنص المادة 15 مكرر: "باستثناء رؤساء المجالس الشعبية البلدية، لا يمكن لضباط الشرطة القضائية الممارسة الفعلية لصلاحيات التي تخولها لهم هذه الصفة، إلا بعد تأهيلهم بموجب مقرر من النائب العام لدى المجلس القضائي الذي يوجد بإقليم اختصاصه مقرهم المهني بناءً على اقتراح السلطة الإدارية التي يتبعونها. ويتم تأهيل ضباط الشرطة القضائية التابعين للمصالح العسكرية للأمن من طرف النائب العام لدى مجلس قضاء الجزائر وفقاً للكيفيات المحددة في الفقرة الأولى من هذه المادة".

4 تنص المادة 20 من قانون الإجراءات الجزائية على أن: "يقوم أعوان الضبط القضائي الذين ليست لهم صفة ضابط الشرطة القضائية بمعاونة ضباط الشرطة القضائية في مباشرة وظائفهم ويثبتون الجرائم المقررة في قانون العقوبات ممتثلين في ذلك لأوامر رؤسائهم مع الخضوع لنظام الهيئة التي ينتمون إليها، ويقومون بجمع كافة المعلومات الكاشفة عن مرتكبي تلك الجرائم".

وبناءً عليه يمثل ما سبق ذكره الاختصاص العام للضبطية القضائية في جميع الجرائم بمختلف أنواعها، إلا أن القانون والتنظيم قد شمل الجرائم ذات الطابع الإلكتروني بفئات خاصة فيما تعلق بالبحث والتحري عن الجرائم من هذا النوع، وهو ما ستتناوله في الفرع الثاني.

الفرع الثانـــي: الضبط القضائي المختص في الجرائم الإلكترونية.

يمكن تناول هذه النقطة من وجهين أساسيين، الوجه الأول يتمثل في الفروع التي تم تأسيسها على مستوى جهات الدرك الوطني والأمن الوطني، والوجه الثاني الهيئات الخاصة التي تم إنشاءها بموجب قوانين خاصة وذلك على النحو الآتـــي:

أولاً– الفرق الـــخاصة:

شكلت الجريمة الإلكترونية سابقة فيما يخص ارتكابها، أو حتى البحث عنها، مما جعل التشريعات الغربية والعربية تحاول استحداث طرق جديدة للتعامل مع هذا النوع من الجرائم، وظهر ذلك بشكل مباشر في المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين الذي انعقد في هافانا من 27 أغسطس إلى 7 سبتمبر 1990، والذي شدد على توجه المجتمع الدولي نحو تعيين أعضاء النيابة العامة من الفئات التي تكون لها المقدرة على التحقيق في الجرائم ذات الطبيعة الإلكترونية[1]، لذلك نجد أن العديد من التشريعات السباقة سعت لتنفيذ هذه التوصيات؛ وخصوصاً التي شهدت ضرر من هذا النوع من الجرائم، حيث عمل التشريع الأمريكي على استحداث وحدة شرطية تكون متخصصة ومؤهلة للبحث والتحري عن الجرائم ذات الطابع الإلكتروني، على أن تكون هذه الوحدة تابعة لجهاز FBI، وفضلاً عن هذه الوحدة عملت الولايات المتحدة الأمريكية كذلك على إنشاء مركز لحماية الشبكات، والذي يهدف إلى الرقابة على جميع المواقع التي تعتبر استراتيجية وقد تهدد المصالح العليا للدولة، مثل الدفاع والكهرباء وغيرها من القطاعات الأخرى الحساسة، بالإضافة لما سبق، عملت الحكومة الأمريكية كذلك على إنشاء مركز للمعلومات، والذي يعمل على رصد كافة التهديدات التي قد تمس بأنظمة المعلومات الصناعية، ومن الأجهزة الأخرى التي عملت الحكومة الأمريكية على استحداثها ما يعرف بمكتب التحقيقات الفيدرالية، وهو مكتب مختص في تلقي شكاوي الاحتيال عبر الإنترنت[2].

---

1 محمود عمر محمود، المرجع السابق، ص 126.

2 محمود محمد محمود جابر، المرجع السابق، ص 19- 20.

وفي ذات السياق سار المشرع الفرنسي على نفس خطى المشرع الأمريكي، حيث عمل على استحداث عدة وحدات تكون متخصصة في الجريمة الإلكترونية، ويظهر ذلك جلياً من خلال إنشاء الديوان الوطني المركزي لمكافحة الإجرام المرتبط بتكنولوجيا الإعلام والاتصال (O.C.L.C.T.I.C) بحيث يتبع هذا الديوان للقطب الثاني المتخصص في مكافحة الإجرام المالي وحماية الملكية، والذي بدوره يتبع للمديرية الفرعية المختصة بمكافحة الجريمة المنظمة والإجرام المالي، وأُنشأ هذا الديوان سنة 2000م، وذلك تطبيقاً للقانون رقم 88-19 المتعلق بالمعلوماتية[1]، والذي يقضي بتجريم الاعتداء على أنظمة المعالجة الآلية للمعطيات، ومن الوحدات المتخصصة كذلك، الفرقة المركزية لمكافحة الإجرام المعلوماتي، والتي تم تأسيسها سنة 1994م، وكذلك فرقة الأبحاث لجرائم تكنولوجيا الإعلام وغيرها من الوحدات المتخصصة في هذا الشأن[2].

أما على المستوى العربي، فقد عمل المشرع المصري على استحداث وحدة تعرف بـ: "إدارة مكافحة جرائم الحاسبات وشبكات المعلومات"، وذلك وفقاً للقرار رقم: 13507 لسنة 2002م بحيث تتبع هذه الوحدة للإدارة العامة للمعلومات والتوثيق، ويتولى الإشراف عليها مدير الإدارة العامة بينما يتولى الاختصاص الفني مصلحة الأمن العام، وتختص هذه الإدارة في مكافحة الجرائم التي تقع باستخدام الحواسيب في مجال نظم المعلومات وشبكات قواعد البيانات[3]، فضلاً عن هذه الوحدة أعطى المشرع المصري لفئات أخرى مهمة الضبط فيما يتعلق بالجرائم الخاصة بالاتصالات، وهو ما نصت عليه المادة 69 من قانون الاتصالات المصري لسنة 2003م، والتي جاء فيها: "يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص تخويل العاملين الذين يحددهم الجهاز والقوات المسلحة وأجهزة الأمن القومي صفة مأمور الضبط القضائي بالنسبة إلى الجرائم التي تقع مخالفة لأحكام هذا القانون وتكون متعلقة بأعمال وظائفهم"[4].

وبالنسبة للمشرع الجزائري الذي حاول أن يواكب هذا النقلة النوعية في مجال الجريمة من خلال العمل على تأهيل وتكوين رجال الضبطية القضائية، خاصة رجال الدرك الوطني، وذلك من خلال

---

1 Loi n°88-19 du janvier 1988 relative à l'informatique, JORF du 06 janvair1988, (LOI GODFRAIN0).

2 **نقلاً عــن:** بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة ، السنة القضائية 2011/2010، ص 3-4.

3 محمود محمد محمود جابر، المرجع السابق، ص 22.

4 طارق عفيفي صادق أحمد، المرجع السابق، ص 210.

التكوينات الخارجية التي استفادت منها هذه الفئة في جامعات كبرى، مثل سويسرا، كندا، والولايات المتحدة الأمريكية، وذلك في كل ما يتعلق بالمجال التقني والحاسب الآلي، وفضلاً عن التكوين الخارجي يتلقى رجال الضبطية القضائية تكوينات داخلية تشرف عليها هيئات وطنية، مثل التكوين الذي يتم على مستوى مركز الدراسات والبحوث في الإعلام العلمي والتقني، كما تساهم هذه الفئة في الملتقيات الدولية منها والوطنية، المنعقدة على مستوى الجامعات[1]، هذا ولقد عمل التنظيم الداخلي للدرك الوطني والأمن الوطني على استحداث أجهزة خاصة بمكافحة الجريمة المعلوماتية، تتمثل هذه الأجهزة في:

1- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني (CPLCIC/GN):

ويعمل هذا المركز على محاربة الجريمة الالكترونية من خلال العناصر الأساسية التالية:[2]

- **الوقاية:** تظهر الوقاية من خلال عمليات التحسيس والتوعية التي يشرف عليها جهاز الدرك الوطني، بالتعاون مع وزارة التضامن والأسرة وقضايا المرأة، فضلاً عن عديد الملتقيات الوطنية والأيام الدراسية الموجهة للشباب أو غيرها من الفئات الأخرى.
- **اليقظة:** تظهر اليقظة من خلال الدورات السيبرانية التي تعتمد على جمع المعلومات وتوثيقها، لا سيما ما تعلق بالجريمة والأمن العمومي.
- المكافحة والأمن الرقمي.

2- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني (INCC/GN):

يمثل هذا المعهد مؤسسة عمومية ذات طابع إداري تتبع للوصاية المباشرة لوزير الدفاع الوطني وتضطلع بالمهام الآتية[3]:

---

1 أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، جامعة قاصدي مرباح ورقلة، الموسم الجامعي 2012-2013، ص 47.

2 **نقلاً عن:** سهام بوعموشة، الوقاية واليقظة والأمن الرقمي: استراتيجية الدرك في مكافحة الجريمة الإلكترونية ، جريدة يومية الشعب، متاح على الرابط: *http://www.echchaab.com*، تاريخ الإطلاع: 15 أكتوبر 2018.

3 لمزيد من المعلومات بخصوص هذا المعهد والمهام المنوطة به، يرجى زيارة الموقع الرسمي لصفحة الدرك الوطني على الرابط: *https://www.mdn.dz/site_cgn/index.php?L=ar#undefined* ، تاريخ الاطلاع 03 نوفمبر 2018.

- العمل على إجراء الخبرات والفحوص العلمية في مرحلة جمع الاستدلال ومرحلة التحقيقات القضائية فيما يتعلق بالجنح والجنايات،
- يعمل هذا الجهاز على ضمان تقديم المساعدة العلمية الضرورية أثناء القيام بالتحريات، خاصة المعقدة منها عن طريق استخدام مناهج الشرطة العلمية،
- تصميم وانجاز بنوك المعطيات،
- العمل على المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام،
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة،
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي،
- المشاركة في كل الملتقيات والمحاضرات أو الندوات على الصعيدين الوطني والدولي لتطوير مستوى مستخدمي المعهد.

ويحتوي المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني على العديد من الأقسام والمصالح المختصة، والتي من بينها مصلحة الإعلام الآلي، والتي تعمل على رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية، فضلاً عن اكتشاف المعلومات المسروقة وتفكيك البرامج.

3- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني (SCLCTIC):

تعمل هذه المصلحة على مواكبة الجريمة الإلكترونية من خلال العمل على التوعية على خطورة هذا النوع من الجرائم، من خلال المشاركة في الملتقيات والندوات والأيام الدراسية، كما أكدت هذه المصلحة على عضويتها ودورها الفعال في جهاز الشرطة الدولية "الإنتربول"، وذلك باعتبار هذه الجريمة تأخذ بعد محلي ودولي كذلك[1].

ثانياً- الهيئة الوطنية للوقاية من الجرائم المتصلة بجرائم تكنولوجيا الإعلام والاتصال ومكافحتها:

1 فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة علمية مقدمة للمشاركة في أعمال المؤتمر الدولي الربع عشر للجريمة الإلكترونية، المنعقد بتاريخ 24-25 مارس، جامعة طرابلس، لبنان، ص 133.

نص المشرع الجزائري على إنشاء هذه الهيئة بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009، حيث جاء في نص المادة 13 منه: "تنشأ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحته. وتحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"[1]. وفي نفس القانون نص المشرع على بعض المهام التي تتولى فيها هذه الهيئة مهمة الضبط القضائي، حيث جاء في نص المادة 14 الفقرة "ب" ما يلي: "...مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية".

وفي ضوء المرسوم الرئاسي رقم: 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، نتطرق لتشكيلة ومهام وطريقة عمل هذه الهيئة، وذلك على النحو الآتــي:

1- تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

نص الفصل الثاني من المرسوم رقم: 15-261 على تشكيلة هذه الهيئة؛ بحيث تتكون من لجنة ومديريات وأعضاء، فأما اللجنة والمديريات فقد نصت عليهم المادة 6، ويمكن حصرهم في:

- لجنة مديرة،
- مديرية عامة،
- مديرية للمراقبة الوقائية واليقظة الإلكترونية،
- مركز للعمليات التقنية،
- ملحقات جهوية.

بينما حددت الأعضاء المادة 7 من نفس المرسوم الرئاسي، وهم:

---

1 القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ: 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الأعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، المؤرخة 16 عشت 2009، ص 9.

2 المرسوم الرئاسي رقم 15-256 المؤرخ في 14 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج،ع 53، المؤرخة في 8 أكتوبر 2015.

- الوزير المكلف بالعدل: رئيس اللجنة،
- الوزير المكلف بالداخلية،
- الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال،
- قائد الدرك الوطني،
- المدير العام للأمن الوطني،
- ممثل عن رئاسة الجمهورية،
- ممثل عن وزارة الدفاع الوطني،
- قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

2- طـرق سـير الـهيئة الوطنيــة للوقـاية مـن الجرائـم المتصلـة بتكنـولوجـيا الإعلام والاتـصال ومكافحتـها:

تعمل الهيئة المديرة من خلال الدورات التي تجمع أعضائها، وذلك بناءً على استدعاء من رئيسها، أو بطلب من أحد أعضائها[1]، كما يتوجب على الهيئة وضع نظام داخلي يسيرها مع المصادقة عليه، وهو ما نصت عليه المادة 7 من المرسوم 15-261 السالف الذكر.

ونصت المادة 18 من نفس المرسوم على إمكانية تزويد الهيئة بقضاة، وذلك مع مراعاة الشروط المعمول بها في التشريع، كما تزود بضباط شرطة قضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني على أن يحدد عدد هذه الفئة بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع الوطني والداخلية وفقاً لما ورد في المادة 2/18 من المرسوم 15-261.

كما تزود الهيئة بمستخدمي الدعم التقني على أن تجلب هذه الفئة من المستخدمين المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني وفقاً للمادة 3/18، ويجوز للهيئة أن تستعين بأي شخص من غير أفراد الهيئة، بحيث يكون صاحب خبرة في مجال من المجالات التي تحتاج إليها الهيئة في تسيير عملها، وهو ما نصت عليه المادة 19 بقولها: "يمكن أن تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها".

---

1 تنص المادة 16 من المرسوم 15-261 على أن: "تجتمع الهيئة المديرة بناءً على استدعاء من رئيسها أو بناء على طلب أحد أعضائها".

3- مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تضطلع الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال بالعديد من المهام، يأتــي في مقدمتها:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال طبقاً للمادة 2/11 من المرسوم 15-261.
- إرسال المعلومات المحصل عليها عن طريق المراقبة الوقائية إلى الجهات المختصة (السلطات القضائية المختصة، وجهاز الشرطة القضائية المختصة)، وذلك طبقًا للمادة 3/11 من نفس المرسوم.
- تنفيذ طلبات المساعدة القضائية الأجنبية وتبادل المعلومات معها، وذلك فيما يدخل في مهام الهيئة من خلال العمل على تحديد مكان تواجد مرتكبي الجريمة وجمع المعلومات المتعلقة بهم وفقاً لما تنص عليه المادة 6/11 من نفس المرسوم.
- العمل على التنظيم أو المشاركة في عمليات التوعية من مخاطر استعمال التكنولوجيا على الأمن العام والأفراد طبقاً للمادة 6/11 من نفس المرسوم.
- مساعدة السلطات القضائية في التحريات التي تجريها، وفي إنجاز الخبرات القضائية حسب ما ورد في المادة 14 الفقرة "ج" من القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الأعلام والاتصال ومكافحتها السالف الذكر.
- تكوين قاعدة معطيات تحليلية تشمل كل ما يتعلق بالإجرام المتصل بتكنولوجيات الإعلام والاتصال.
- العمل على إعداد إحصائيات وطنية دورية فيما يتعلق بجرائم تكنولوجيات الإعلام والاتصال حسبما ورد في المادة 3/12 من المرسوم 15-261 السالف الذكر.
- مراقبة الاتصالات الإلكترونية والعمل على تجميع وتسجيل محتواها في حينها، وذلك فيما يتعلق بالجرائم الموصوفة بأنها جرائم الإرهاب والتخريب والمساس بأمن الدولة وفقاً للمادة 22 من نفس المرسوم.

- القيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية تحت سلطة قاضي مختص وفقًا لما هو معمول به في القانون رقم 09-04 السالف الذكر.

المطلب الـثالث: السلطات المختصة بالتحقيق في الجرائم المرتكبة بواسطة الهاتف النقال.

يمثل التحقيق إجراء جوهري من إجراءات الدعوى الجنائية فيما يتعلق بالجرائم التي تتطلب ذلك، باعتباره يمثل ضمانة من الضمانات التي يكفلها الدستور والاتفاقيات الدولية، على أن تقوم بذلك سلطة مختصة، وتتمتع بالاستقلالية عن سلطة الإتهام في النظام القضائي الذي يعتمد معيار ازدواج سلطة الاتهام والتحقيق، وينقسم التحقيق عموماً إلى تحقيق ابتدائي (الفرع الأول) وتحقيق نهائي (الفرع الثاني).

الفرع الأول: التـحقـيق الابـتدائي.

يمثل التحقيق الابتدائي أحد أهم الشروط الإجرائية في مسار الدعاوى الجنائية التي تتطلب التحقيق، وذلك في النظام القضائي الذي يعتمد فصل سلطة الاتهام عن سلطة التحقيق، وتُسند هذه المهمة إلى قاضي التحقيق، والذي يعين بمقتضى قرار من وزير العدل بعد استشارة المجلس الأعلى للقضاء في الجزائر، وذلك وفقاً لما نص عليه القانون العضوي رقم: 04-11 المتضمن القانون الأساسي للقضاء[1] في المادة 50 منه[2]، على أن يتصل قاضي التحقيق بالدعوى العمومية وفق

---

1 القانون العضوي رقم 04-11 المؤرخ في 21 رجب 1425 الموافق 6 سبتمبر 2004، يتضمن ، ج.ر.ج.ج ، المؤرخة في 8 سبتمبر 2004، ع 57.

2 تنص المادة 50 من القانون العضوي 04-11 على أن: "يتم التعيين بعد استشارة المجلس الأعلى للقضاء في الوظائف القضائية النوعية الآتية:

- نائب رئيس المحكمة العليا،
- نائب رئيس مجلس الدولة،
- نائب عام مساعد لدى المحكمة العليا،
- نائب محافظ الدولة لدى مجلس الدولة،
- رئيس عرفة بالمحكمة العليا،
- رئيس غرفة بمجلس الدولة،
- نائب رئيس مجلس قضائي،
- نائب رئيس محكمة إدارية،

إجراءات معينة نظمها قانون الإجراءات الجزائية[1]، ولكن السؤال المطروح هل نفس الجهات التي تعمل على التحقيق في الجرائم التقليدية مكلفة بالتحقيق في الجرائم ذات الطبيعة الإلكترونية ؟

لمعرفة هذا الأمر، لا بد من التطرق لتحديد مفهوم التحقيق الإبتدائي (أولاً)، ثم تمديد الاختصاص المكاني لقاضي التحقيق (ثانياً)، فالتعاون القضائي الدولي في التحقيق القضائي (ثالثاً)، ثم الخبرة القضائية (رابعاً)، فأسلوب التحقيق في الجرائم المرتكبة بواسطة الهاتف النقال (خامساً).

أولاً– مفهوم التحقيق الابتدائي:

هناك العديد من المفاهيم الفقهية للتحقيق الابتدائي، من بينها ما عرف به التحقيق الإبتدائي على أنه: "مجموعات الإجراءات التي تهدف إلى البحث عن الأدلة بشأن جريمة وقعت وتجميعها، ومن ثم تقديرها لتحديد كفايتها لإحالة المتهم إلى المحكمة المختصة"[2].

ومن خلال التعريف السابق يتضح أن التحقيق الابتدائي يهدف إلى جمع الأدلة وتقديرها بالإضافة إلى العمل على تأكيد الإتهام من عدمه.

- رئيس غرفة بمجلس قضائي،
- رئيس غرفة بمحكمة إدارية،
- النائب العام المساعد الأول لدى مجلس قضائي،
- محافظ مساعد الدولة المساعدة لدى المحكمة الإدارية،
- قاضي تطبيق العقوبات،
- رئيس المحكمة،
- وكيل الجمهورية،
- قاضي التحقيق."

1 تنص المادة 3/38 من قانون الإجراءات الجزائية على أن: "...ويختص بالتحقيق في الحادث بناءً على طلب من وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و73".

2 على حمزة عسل الخفاجي، التحقيق الابتدائي، مجلة العلوم الإنسانية، المجلد 23، العدد الأول، كلية التربية والعلوم الإنسانية، جامعة بابل، العراق، آذار 2015، ص 419.

وللتحقيق الابتدائي في الجريمة الإلكترونية العديد من الخصائص، وذلك بالنظر إلى طبيعة هذا النوع من الجرائم، وهو ما يمكن استنتاجه من خلال النصوص الواردة في قانون الإجراءات الجزائية، أو من خلال الاتفاقيات التي صادقت عليها الجزائر.

ثانياً– تمديد الاختصاص المكاني لقاضي التحقيق (الاختصاص الوطني):

عمل المشرع الجزائري على مواكبة التشريعات العالمية من خلال المصادقة على الإتفاقيات الدولية والإقليمية التي تنظم مكافحة الإجرام الإلكتروني وغيرها من الجرائم الخطيرة، مما انعكس إيجاباً على اختصاص قاضي التحقيق، وهذا ما ظهر جلياً في نص المادة 40 من قانون الإجراءات الجزائية والتي نصت على أن: "يتحدد اختصاص قاضي التحقيق محلياً بمكان وقوع الجريمة، أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص حتى لو كان هذا القبض قد حصل لسبب آخر. ويجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات، والجريمة المنظمة العابرة للحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف"[1].

من خلال هذه المادة يتضح أن المشرع وسع بشكل عام فيما يخص اختصاص قاضي التحقيق، إلا أنه أضاف استثناءً آخر على التوسيع فيما يخص الجرائم المذكورة، وحَسن ما فعل بالنظر للخطورة التي يشكلها هذا النوع من الجرائم، كما عرف قاضي التحقيق تمديداً آخر لاختصاصه فيما يعرف بنظام الأقطاب المتخصصة، والتي عملت الدولة على إنشاءها من أجل محاربة الجرائم المذكورة آنفاً[2].

ثالثاً– التعاون القضائي الدولي في التحقيق القضائي:

نصت على هذا الاختصاص العديد من الإتفاقيات الدولية المُنظم لهذا الشأن وذلك فيما يعرف بالتعاون القانوني والقضائي، حيث جاء في نص المادة 30 من الإتفاقية العربية لمكافحة جرائم

---

1 القانون رقم 04-14 المؤرخ في 17 ذي الحجة الموافق لـ: 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزائية ، ج ر ج ج، ع 5، المؤرخة في: 10 نوفمبر 2004، ص 5.

2 **نقلاً عــن:** محمد بكرارشوش، الإختصاص الإقليمي الموسع في المادة الجزئية في التشريع الجزائري، دفاتر السياسة والقانون، العدد الرابع عشر، جامعة قاصدي مرباح ورقلة، جانفي 2016، ص 321.

تقنية المعلومات ما نصه: "1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية، وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:

- في إقليم الدولة الطرف،
- على متن سفينة تحمل علم الدولة الطرف،
- على متن طائرة مسجلة تحت قوانين الدولة الطرف،
- من قبل أحد مواطني الدولة الطرف، إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها، أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة،
- إذا كانت الجريمة تمس أحد المصالح العليا للدولة..."[1].

وهناك اتفاقيات أخرى عديدة صادق عليها المشرع الجزائري، وإن كانت ذات طابع عام، إلا أنه يمكن أن تشمل هذا النوع من الجرائم، والتي من بينها إتفاقية باليرمو لمكافحة الجريمة المنظمة، وخصوصاً أن الهاتف النقال قد يستعمل في ارتكاب جرائم ذات طابع منظم وعابر للحدود كما تم التطرق إليه في الباب الأول من هذه الدراسة.

ثالـثاً- الـخبرة القضائـية:

تمثل الخبرة إحدى الوسائل القضائية التي يلجأ إليها المحقق القضائي في حالة ما إذا كان النزاع الذي أمامه نزاع تقني أو طبي يحتاج إلى معرفة فنية من مختص، وتلعب الخبرة دوراً كبيراً في التحقيق في الجرائم المرتكبة بواسطة الهاتف النقال أو في الجريمة الإلكترونية بصفة عامة، بحيث يتوجب على المحقق العمل وفق المعطيات التي يمده بها الخبير، وأن تكون الأسئلة مبنية على العمل المشترك بين الخبير والمحقق، وذلك وفق الإجراءات التالية[2]:

أ. قيام الخبير بتوضيح كافة المصطلحات ذات الطبيعة التقنية في الموضوع المعروض عليه، مع إمكانية استخدامها أثناء مجريات التحقيق مع بيان معانيها.

---

1 صادقت الجزائر على هذه الإتفاقية بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة 1435 الموافق لـ 8 سبتمبر 2014، ج ر ج ج، ع 57، المؤرخة في 28 سبتمبر 2014، ص 4.

2 محمود محمد محمود جابر، المرجع السابق، ص 58.

ب. أن تتم عملية استجواب المتهمين وأخذ أقوال الشهود بوجود الخبير المعلوماتي والتقني، مع إمكانية توجيه هذا الأخير أسئلة فرعية أثناء الاستجواب، على أن يتم الإتفاق مسبقاً بينه وبين قاضي التحقيق على الصلاحيات وحدود التدخل المسموح له به.

ج. مراعاة النظام القانوني الوطني فيما يتعلق بتنظيم سلطات قاضي التحقيق، والمدى المسموح به للخبير في مشاركة التحقيق وحضور الاستجواب.

د. أن تكون السلطة النهائية في مجريات التحقيق لقاضي التحقيق، وذلك على ضوء المعطيات المتوفرة عنده وسلطته التقديرية، وما يقرره القانون في النزاع المعروض أمامه.

وقد أوكل المشرع الجزائري مهمة إعداد الخبرة فيما يخص الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال للهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والإتصال، وذلك حسب ما هو وارد في المادة 14/ب من القانون 09-04 السالف الذكر[1]، وهو نفس ما نصت عليه المادة 12 من المرسوم الرئاسي والتي جاء فيها: "...إنجاز الخبرات القضائية في مجال اختصاص الهيئة".

رابعاً– أسلوب التحقيق في الجرائم المرتكبة بواسطة الهاتف النقال[2]:

---

1 تنص المادة 14 من القانون 09-04 على أن: "...ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية".

2 فضلاً عن الأسلوب الخاص الذي يجب على قاضي التحقيق مراعاته وهو بصدد البحث والتحقيق عن الجريمة الإلكترونية بصفة عامة والجريمة المرتكبة بواسطة الهاتف النقال بصفة خاصة، فإن البعض يرى وجوب توفر مواصفات نفسية وعلمية في قاضي التحقيق بجانب المعرفة القانونية والمهارة في إدارة التحقيق ومن بين هذه المواصفات:

1- **المواصفات الحسية:** وتشمل هذه الموصفات أو ما يعرف بالقدرات العديد من المميزات، والتي تتمثل في القدرة على التصور المكاني، القدرة على السرعة في إدراك التفاصيل، القدرة التذكرية، القدرة على الابتكار والتجديد.

2- **المواصفات التعبيرية:** وتشمل المقدرة الطلاقة الأمنية، والتي تظهر من خلال الطلاقة الفكرية للمحقق، فضلاً عن الطلاقة اللفظية، والصفة الثانية في المواصفات التعبيرية هي مقدرة المرونة الأمنية، والتي تظهر من خلال قدرة المحقق على التكيف مع الظروف التي تعترض التحقيق، فضلاً على مقدرته على إعادة تفسير المعلومات والمرونة الأمنية التلقائية.

3- **المواصفات الخاصة:** تعتبر هذه القدرات من هم الميزات التي يجب توفرها في المحقق الذي يكلف بالتحقيق في الجرائم ذات الطبيعة الإلكترونية وتتمثل في:

– **القراءة السريعة والتصورية:** وتتمثل في مقدرة المحقق على استيعاب قدر كبير من المعلومات مع فهمه معظمها والاحتفاظ بها لمدة زمنية معينة.

نظراً للأداة التي ترتكب هذه الجريمة ومسرح ارتكابها، يفترض في المحقق التعامل بمرونة أكثر مع هذه الجرائم مقارنة بباقي الجرائم التقليدية، حيث يتوجب على المحقق مراعاة الوقت كعامل جوهري في الكشف عن الجريمة؛ وذلك من خلال العمل على[1]:

- السرعة في البحث عن الدليل والحفاظ عليه باعتبار المسرح الإلكتروني سريع لا يمكن أن يكون متاح إلا لفترة قصيرة، فضلاً عن سرعة طمس الدليل والقضاء عليه[2].
- أن الجريمة التي يجري التحقيق بشأنها قد تكون مجرد غطاء لجريمة أخرى، مما يوجب على المحقق أن يكون أكثر دقة، والتثبت من الجريمة ونمط ارتكابها، والتقنية المستخدمة فيها، فضلاً عن الجاني أو الجناة المشتبه بهم في ارتكابها، الأسباب والدوافع التي تكون محتملة في ارتكابها، الاستدلال على الشهود في حالة ووجودهم، وطبيعة الأدلة الجنائية ومصادرها[3].
- التأكد من طبيعة الجريمة ومعرفة نوعها من حيث إذا كانت مستمرة أو مؤقتة، فضلاً عن الوقوف على نتائج تنفيذها[4].

الــفرع الثانــي: التحـقيق النهائــي.

يأخذ التحقيق النهائي صفة خاصة من بين المراحل التي تمر بها الدعوى العمومية، وذلك بالنظر إلى الضمانات العديدة التي يوفرها قانون الإجراءات الجزئية أو الإتفاقيات الدولية في هذا الصدد، ولذلك يتم التطرق من خلال هذا الفرع إلى تقديم لمحة عامة عن تطوُّر المنظومة القضائية وأثر ذلك على تنفيذ الأحكام الصادر عنها (أولاً)، فضلًا عن المشاكل التي قد تثار فيما يتعلق بالجريمة المرتكبة بواسطة الهاتف النقال أو الجريمة الإلكترونية بصفة عامة (ثانياً).

- **الذكاء الإلكتروني الرقمي**: وحتى يتمتع المحقق بالذكاء الإلكتروني الرقمي لا بد أن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، المقدرة على تحليل وتصميم البرامج وأنظمة التشغيل، أن يؤمن بوجود أشخاص مثله لديهم مقدرة على اختراق الشبكات.

لمعلومات أكثر انظر: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط. الأولى، مطابع الشرطة، مصر، 2009، ص ص 256-264.

1 محمود محمد محمود جابر، المرجع السابق، ص 58.

2 محمود محمد محمود جابر، نفس المرجع، ص 58.

3 محمود محمد محمود جابر، نفس المرجع، ص 58.

4 محمود محمد محمود جابر، نفس المرجع، ص 58.

أولاً– القضاء الجنائي فـــي الجزائر:

عرف القضاء الجنائي في الجزائر نقلة نوعية، وذلك تبعاً للسياسة الجنائية التي تشهدها البلاد، والتي تسعى من خلالها إلى الموازنة بين حقوق الإنسان من جهة، وتحقيق العدالة من جهة أخرى، وقد تجلى هذا الأمر من خلال تعديل قانون الإجراءات الجزائية سنة 2017، ومن النقاط الجوهرية التي استحدثها هذا القانون نذكـــر:

1– العمل على استحداث محكمة جنايات استئنافية من أجل تفعيل مبدأ التقاضي على درجتين في مادة الجنايات على غرار ما هو معمول به بالنسبة لمادة الجنح والمخالفات، وهذا وفقاً لما نصت عليه المادة 248 من القانون 17-07، والتي جاء نصها: "يوجد بمقر كل مجلس قضائي، محكمة جنايات ومحكمة جنايات استئنافية، تختص بالأفعال الموصوفة جنايات وكذا الجنح والمخالفات المرتبطة بها"[1].

2– رفع عدد المحلفين من اثنين إلى أربعة محلفين، وهذا من أجل تأكيد الطابع الشعبي لمحكمة الجنايات، واستثني من ذلك الجرائم المتعلقة بالإرهاب والمخدرات والتهريب[2]، وعليه فالمشرع أحسن عندما استثنى الجرائم المذكورة أنفًا من الطابع الشعبي، وإن كنا نرى أن المجال واسع فيما يخص جرائم الإرهاب حيث أنها تتضمن الجرائم الإرهابية ذات الطابع الإلكتروني، وذلك فيما يعرف بالهجمات الإلكترونية أو التجنيد الإلكتروني الذي انتشر مؤخراً بصورة واسعة، كما نرى أنه حبذا لو أن المشرع اشترط في اختيار المحلفين التخصص، بحيث يكون المحلفين منتقين بحسب القضية وهذا متاح، فالجزائر تزخر اليوم بكفاءات في مختلف المجالات يمكن الاستفادة منها في تحسين مرفق العدالة.

---

1 القانون رقم 17-07 المؤرخ 28 جمادي الثانية 1438 الموافق 27 مارس 2017، 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 20، المؤرخة 29 مارس 2017، ص 8.

2 تنص المادة 258 من القانون 07/17 على أن: "تتشكل محكمة الجنايات الابتدائية من قاض برتبة مستشار بالمجلس القضائي على الأقل، رئيساً ومن قاضيين مساعدين، وأربعة محلفين. تتشكل محكمة الجنايات الاستئنافية من قاضٍ برتبة غرفة على الأقل، رئيسًا، ومن قاضيين مساعدين وأربعة محلفين. وتتشكل محكمة الجنايات الابتدائية ومحكمة الجنايات الاستئنافية، عند الفصل في الجنايات المتعلقة بالإرهاب والمخدرات والتهريب من القضاة فقط".

وبذلك تعتبر النقاط المذكورة سابقاً من بين أهم النقاط التي أشار إليها القانون 17-07 المعدل والمتمم لقانون الإجراءات الجزائية.

ثانــياً- الاختصاص العالــمي للقضاء الجنائي فــي الجرائم المرتكبة بواسطة الهاتف النقال:

إن المبدأ الذي يحكم تطبيق القانون الجنائي هو مبدأ إقليمية القانون، وذلك بغض النظر عن مرتكب الجريمة سواء كان من مواطني تلك الدولة أو أجنبي، وذلك بالنظر لعدة اعتبارات منها مبدأ سيادة الدولة، والذي تقرره المواثيق والأعراف الدولية، فضلاً عن سهولة تتبع الأدلة والمحافظة عليها[1]، ومن التطبيقات القضائية فيما يتعلق بجرائم الهاتف النقال ما صدر عن محكمة باريس والتي قضت باختصاص المحاكم الفرنسية في القضايا التي يكون فيها جهاز البث موجوداً خارج الأراضي الفرنسية، بينما تظهر الرسائل التي يقوم ببثها في فرنسا: "تعتبر الجريمة مرتكبة في كل مكان تظهر فيه الرسائل المؤثمة محل البث"[2]. كما أن المشرع الفرنسي ذهب أبعد من ذلك حيث يطبق نفس العقوبة التي قد تصدر بحكم أجنبي على شريك في جريمة وقعت خارج أراضيها، وذلك في حال ما إذا كان هذا الفعل مجرم بموجب القانون الفرنسي والقانون الأجنبي، بالإضافة إلى صدور حكم نهائي من جهات القضاء الأجنبي في مرتكب الفعل الأصلي في الخارج، وهذا ما نصت عليه المادة 5/113 من ق.ع.ف، والتي جاء فيها: "يطبق القانون الفرنسي على كل من ارتكب فعلاً في إقليم الجمهورية يجعله شريكاً في جناية أو جنحة وقعت في الخارج، إذا كانت الجناية أو الجنحة معاقباً عليها في القانون الفرنسي والقانون الأجنبي، وكانت ثابتة بمقتضى حكم نهائي من القضاء الأجنبي".

المشرع الجزائري بدوره نص على امتداد الاختصاص الإقليمي للجهاز القضائي الجزائري خارج الوطن، وذلك بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، إذ نصت المادة 15 منه على أن: "زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

---

1 محمود محمد محمود جابر، المرجع السابق، ص 83-84.

2 **نقلاً عــن:** محمود محمد محمود جابر، نفس المرجع، ص 83.

ومن خلال نص المادة السابقة يتضح أن المشرع الجزائري يشترط لامتداد الاختصاص الإقليمي في الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، والمرتكبة من شخص أجنبي أو خارج الأراضي الجزائرية أن تكون الجريمة من الجرائم التي تمس بـــ:

- مؤسسات الدولة الجزائرية.
- الدفاع الوطني.
- المصالح الإستراتيجية للاقتصاد الوطني.

وبالإضافة إلى ما سبق، فالمشرع الجزائري بموجب القانون رقم: 09-04 قد أقر العديد من الإجراءات التي تساعد القضاء في هذا الصدد، منها تبادل المعلومات التي تفيد في التعرُّف على مرتكب الجريمة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1].

ومن النقاط التي تثار على المستوى الفقهي هو مبدأ عالمية القانون الجنائي[2] فيما يتعلق بجرائم الهاتف النقال خاصة، والجريمة الإلكترونية عامة، وذلك بالنظر إلى العديد من الأسباب التقنية والقانونية التي تحتم مثل هذا المبدأ على هذا النوع من الجرائم، والتي نذكر منها[3]:

- التطور الهائل في تكنولوجيا المعلومات والذي لا يحدد بمكان معين.
- أعمال القرصنة والبث والنسخ غير المشروع للعديد من المواد التي تعتبر ذات ملكية فكرية.
- نص اتفاقية بودابست على هذا المبدأ في مادتها 1/22 البند 1 والتي جاءت فيها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية، أو أية إجراءات أخرى يرى أنها ضرورية من أجل تقرير اختصاصه بالنسبة لكل جريمة جنائية محددة وفقاً للمواد 2-11 من هذه الاتفاقية حينما يتم

---

1 زيبحة زيدان، المرجع السابق، ص 176.

2 تعرف عالمية القانون بأنها: "أن يكون لكل دولة ولاية القضاء في أية جريمة بصرف النظر عن مكان وقوعها أو مساسها بمصالحها أو جنسية مرتكبها أو المجني عليه فيها". انـــظر: أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط. السابعة عشرة، دار هومة، الجزائر، 2018، ص 111.

3 محمود محمد محمود جابر، المرجع السابق، ص 96.

ارتكاب الجريمة[1]: د- ... عن طريق أحد مواطنيه، إذا كانت الجريمة المرتكبة معاقب عليها جنائياً في قانونه، أو كانت لا تخضع لأي اختصاص إقليمي لأية دولة أخرى".

ومما تجدر الإشارة إليه أن الإتفاقية العربية لمكافحة جرائم التقنية عملت على إقرار نفس المبدأ، وذلك في المادة 30 منها، والتي جاء في الفقرة "د" منها ما نصه: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في هذه الاتفاقية، وذلك: (د)- ...إذا ارتكبت خارج الاختصاص القضائي الإقليمي لأي دولة".

11 هلالي عبد اللاه أحمد، كيفية المواجهة الجنائية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، ب. ط، دار النهضة العربية، القاهرة 2011، ص 232.

الـمبحث الثانــي:

طـرق البحث عـن الـجرائم الـمرتكبة بواسطة الـهاتف النـقال.

تمثل أدوات البحث عن الجريمة أهم شروط التحري الجنائي الناجح، بحيث يلتزم المحقق أو ضابط الشرطة القضائية بأساليب معينة حددها القانون الإجرائي، وذلك وفق ضوابط وأساليب قد تختلف من نظام إجرائي إلى آخر، ومن بين أساليب البحث عن الأدلة الجنائية التفتيش، المعاينة، المراقبة الإلكترونية، والتسرب، فكل هذه الأساليب قد نظمها قانون الإجراءات الجزائية أو قوانين خاصة تنظم الجريمة الإلكترونية.

لذلك، ومن خلال هذا المبحث يتم التطرق إلى هذه الأساليب بدءاً بأدوات التحري والتحقيق التقليدية (المطلب الأول)، وصولاً لأدوات التحري والتحقيق المستحدثة (المطلب الثاني).

المطلب الأول: أدوات التحري والتحقـيق التقليديـة.

تعتبر إجراءات التفتيش والمعاينة والضبط من أقدم الإجراءات المعمول بها في القوانين الإجرائية في البحث والتحري عن الجرائم، وفي الغالب ما تأتي هذه الطرق بنتائج إيجابية فيما يخص الكشف عن دليل أو أثر من الآثار التي يخلفها الجناة، والسؤال الذي يُطرح في هذا الصدد؛ يتعلق بالبحث عن الخصوصية التي تمتاز بها هذه الإجراءات في الجريمة الإلكترونية عامة، والجريمة المرتكبة بواسطة الهاتف النقال خاصة ؟

وللإجابة عن هذا السؤال يتم التطرق في هذا المطلب إلى إجراء التفتيش (الفرع الأول)، ثم المعاينة (الفرع الثاني)، وصولاً إلى إجراء الضبط (الفرع الثالث)، وذلك على النحو التالي:

الـــفرع الأول: التفتيش.

من خلال هذا الفرع نتطرق إلى الأحكام التي تتعلق بإجراء التفتيش وذلك على النحو الآتـي:

أولاً– مفهـــوم التفـتـيش:

هناك العديد من المفاهيم الخاصة بإجراء التفتيش؛ حيث يعرفه البعض[1] بأنه: "إجراء من إجراءات التحقيق يقوم به موظف مختص، طبقًا للإجراءات المقررة قانونًا، في محل يتمتع بحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم".

---

1 عوض محمد عوض، قانون الإجراءات الجنائي ج 1، ب. ط، مؤسسة الثقافة الجامعية، مصر، 1989، ص 478.

ويعرفه البعض[1] الآخر بأنه: "هو إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة في شأنها".

كما يعرف بأنه: "إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، ويستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بعض النظر عن إرادة صاحبه"[2].

ومن خلال المفاهيم السابقة يتضح أن التفتيش هو عبارة عن إجراء من الإجراءات التي يقوم بها رجال القضاء الموكل إليهم مهمة البحث والتحقيق في الجرائم، بحيث يهدف هذا الإجراء إلى الكشف عن الأشياء المخفية أو الجناة الهاربين من العدالة، وذلك من خلال تتبع وضبط الأدلة التي قد يتركها الجناة خلفهم في مسرح الجريمة، وتتنوع هذه الأدلة بتنوع الجرائم، فالتفتيش في حد ذاته لا يمكن اعتباره دليل، وإنما هو عبارة عن إجراء من أجل تقصي الدليل الذي قد يفضي إلى إثبات التهمة على المتهم أو نفيها عنه.

ثانياً– آليات تـفتيش الهواتـف النـقالـة:

نميز في تفتيش الهاتف النقال بين عدة حالات، لكل حالة خصوصيتها، والطريقة الخاصة التي تعتمد في تفتشيها، ولذلك قسمنا هذا العنصر إلى ما يلـــي:

1- تـفتـيش المكونـات المـاديـة للهاتـف النقال:

تتمثل المكونات المادية للهاتف النقال من جميع المكونات المادية سواء في شكلها الخارجي؛ والذي يمكن رؤيته بالعين المجرد، والذي يظهر في الغطاء الخارجي للجهاز، وشاشة العرض، وبطارية الهاتف، وغيرها من الوسائل الأخرى التي ترتبط بالهاتف من الناحية الخارجية[3]، أو المكونات المادية الداخلية، والتي يحتاج إليها الهاتف من أجل التشغيل؛ وهي عبارة عن مجموعة من المقاومات، والمكثفات المترابطة مع بعضها البعض من خلال خيوط النحاس، كما تعتبر التطبيقات أو البرامج

1 زبيخة زيدان، المرجع السابق، ص 130.

2 محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، بدون طبعة، أكاديمية الشرطة، مصر، 2016، ص 139.

3 طارق عفيفي صادق أحمد، المرجع السابق، ص 16.

جزء من المكونات المادية باعتبارها مرتبطة ارتباطاً وثيقاً بالهاتف النقال، ولا يمكن له أن يشتغل من دونها، وتختلف مكونات الهاتف النقال باختلاف الجيل الذي ينتمي إليه[1].

وفي هذه الحالة تتفق جل التشريعات على أن تفتيش الأجزاء المادية للهاتف لا يثير أي إشكال، ويطبق عليها نفس أحكام التفتيش العادية، ويشترط فيها نفس الإجراءات التي يجب مراعاتها في أحكام التفتيش العادية، من مراعاة للتوقيت، والإذن، ومكان تواجد الهاتف النقال. وهناك العديد من التشريعات التي أشارت إلى هذه النقطة وبصفة مباشرة، منها التشريع الإجرائي اليوناني في المادة 251 منه، والمادة 487 من قانون الإجراءات الكندي، قياساً على حكم تفتيش الحاسوب[2].

2- تفتيش الكيان الـمنطقي للهاتــف النــقال:

قبل أن نخوض في بيان جواز تفتيش الكيان المنطقي للهاتف النقال، وجب توضيح بعض النقاط الجوهرية فيما يخص هذا الكيان الذي يأخذ نفس حكم جهاز الحاسب الآلي (الكمبيوتر)؛ وذلك باعتبار الهاتف النقال الذكي عبارة عن حاسوب متنقل بحجم صغير، بحيث يتكون من نفس المميزات والتطبيقات التي يتكون منها الحاسوب.

ومن جانب آخر، يجب توضيح الفرق بين المعلومات والبيانات فيما يتعلق بالكيان المنطقي للهاتف النقال، حيث يميز البعض[3] المعلومات عن البيانات من حيث القدرة على الإسترداد، ذلك أن المعلومة المخزنة في الهاتف النقال ينطبق عليها مفهوم المعلومة في ذاكرة الإنسان، والتي في الغالب ما يتم استرجاعها بشكل ناقص وخاص بالموضوع المراد استرجاعه، وهذا على خلاف البيانات، والتي تسترجع بشكل عام، لذلك يطلق عليها البيانات المخزنة في الهاتف النقال لا المعلومات.

ويُعتبر المشرع الجزائري من بين التشريعات التي أجازت تفتيش المنظومة المعلوماتية من أجل البحث عن الأدلة، وذلك وفقاً لما نصت عليه المادة 5 من القانون 09-04 والتي نصت على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش، ولو عن بعد، إلى:

- منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها.

---

1 أحمد الجابري، دروس بعنوان شرح الهاتف المحمول خطوة بخطوة، منتدى نجم الإبداع، مقال متاح على الرابط الإلكتروني التالي: *http:// ngmelabdaa.own0.com/t138-topic*، تاريخ الإطلاع: 2018/11/05.

2 **نقلاً عـــن:** محمود محمد محمود جابر، المرجع السابق، ص 165.

3 محمود عمر محمود، المرجع السابق، ص 129.

– منظومة تخزين معلوماتية...".

وهذه إشارة واضحة من المشرع الجزائري عن إمكانية تفتيش المنظومة المعلوماتية، ولكن الإشكال ليس في هذه النقطة بقدر ما هو في عملية الاسترداد، بحيث أن إجراء التفتيش في المنظومة يستهدف البيانات، ما يعني استرداد جميع البيانات المخزنة في الهاتف النقال، والتي لا يمكن فصلها عن بعضها البعض، مما يجعل المتحري أو المحقق يخلط بين ما هو مشروع وغير مشروع، ما قد يؤدي إلى بطلان إجراء التفتيش عملاً بمبدأ المشروعية، كما أن هذه النقطة تنتج عنها عديد الإشكالات المتمثلة في[1]:

أ- **عدم وجود منهج بـحث يفرز الدليل الجنائـي:** من الإشكالات التي قد يقع فيها المكلف بالتفتيش هو عدم وجود منهج لمحرك البحث يمكن الإستعانة به للحصول على الدليل الرقمي، مما أدى بالقضاء الأمريكي إلى رفض الإقرار بأن التفتيش ينصب على الموقع، بل ممكن أن يكون من الموقع، مما ينتج عنه بطلان التفتيش عملاً بمبدأ تجاوز الغاية، إلا أن الفكر القانوني قد وجد الحل لهذه النقطة عن طريق فكرة الضبط العرضي[2].

ب- **أن التفـتيش الرقمي قد يكون اعـتداء على الـملكية الفكرية:** إن الاسترداد الكلي للبيانات يثير إشكالية الإعتداء على حقوق المؤلف، والتي كفلتها نصوص دستورية ومواثيق دولية[3].

3- تـفـتيش الهاتف النـقال عـن بُعد:

من الإشكالات الأخرى المطروحة بخصوص تفتيش الهاتف النقال؛ هو أن يكون الهاتف بعيد، وتتم عملية التفتيش في بياناته دون إذن صاحبه، أو أن صاحبه الذي قام بتخزين المعلومات على أراضي أجنبية[4]، فما مدى إمكانية تفتيش هذا الهاتف النقال في مثل هذه الحالة ؟

يمكننا التمييز في هذه الحالة بين فرضيتن، وذلك على النحو الآتي:

---

1 محمود عمر محمود، نفس المرجع، ص 130.

2 نقلاً عــن: محمود عمر محمود، نفس المرجع، ص 130.

3 محمود عمر محمود، نفس المرجع، ص 130.

4 رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة بوبكر بلقايد –تلمسان–، الموسم الجامعي: 2017-2018، ص ص 283- 285.

أ- قيام الجانـي بـتخزين الـمعلومات فـي مكان آخر داخل الدولـة:

في هذه الحالة لا تثور أية إشكالية باعتبار القوانين الإجرائية الداخلية للدول، أو حتى المواثيق الدولية حاولت الوقوف على هذه النقطة ومعالجتها، وهذا ما ظهر جلياً في المادة 5 من القانون المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال بالنسبة للمشرع الجزائري، حيث مكنت هذه المادة السلطات القضائية المختصة وضباط الشرطة القضائية من تفتيش المنظومة المعلوماتية، وذلك يرجع إلى تفطن المشرع الجزائري بارتباط الأنظمة المعلوماتية ببعضها البعض عن ما يعرف بالشبكة المحلية، أو خطوط الهاتف، أو بواسطة الأقمار الصناعية[1].

كما أن المادة 2/26 من الإتفاقية العربية لمكافحة الجريمة الإلكترونية عملت على تكريس هذا المبدأ، حيث نصت على أن: "... الدول الأطراف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها، إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية المعلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومة قابلة للوصول أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى". وتعنـــى الجزائر بأحكام هذه الإتفاقية، على اعتبار أنها قد صادقت عليها[2].

ب- قـيام الـمتهم بـتخزيـن بـياناتـه داخـل نظام معلوماتـي خارج حـدود الدولة:

نص المشرع الجزائري على هذه الحالة بموجب الفقرة 3 من المادة 5 من القانون 09-04 والتي نصت على أنه: "...إذا تبين مسبقاً بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات المختصة طبقاً للإتفاقيات الدولية ذات الصلة، ووفقاً لمبدأ المعاملة

---

1 زبيحة زيدان، المرجع السابق، ص 139.

2 وبخلاف التشريع الجزائري هناك العديد من التشريعات الأخرى التي عملت على النص على مثل هذا الإجراء ضمن قوانينها الإجرائية؛ فقد نص على ذلك القانون المصري بموجب المادة 206 من القانون الإجرائي المصري، والمادة 57-1 من قانون الإجراءات الجنائية الفرنسي والتي نصت على أن: "- عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش فيها- على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، مادامت هذه البيانات متصلة في شبكة واحدة في النظام الرئيسي، أو يتم الدخول إليها، أو تكون متاحة ابتداء من النظام الرئيسي"، كما يعتبر القانون الكندي كذلك من القوانين التي نصت على اتخاذ مثل هذا الإجراء في مثل هذه الحالة، ومن المواثيق الدولية التي نصت على هذا الإجراء اتفاقية بودابست المتعلقة بالجريمة الإلكترونية وذلك طبقا للمادة 2/19 من هذه الاتفاقية، **انـظر في ذلك:** محمود محمد محمود جابر، المرجع السابق، ص 171-172.

بالمثل"، ويتضح من نص هذه الفقرة أن المشرع أجاز التفتيش في حال إذا كانت المعطيات المبحوث عنها قد خزنت في نظام معلوماتي خارج الإقليم، ولكن قيد ذلك بشروط أساسية تتمثل فـــي:

- أن يكون الإجراء وفقاً لمساعدة السلطات المختصة في ذلك البلد.
- أن يتم التفتيش وفقاً للشروط المعمول بها في الإتفاقيات الدولية ومبدأ المعاملة بالمثل.

وفضلاً عن هذه المادة، فقد نصت المادة 40 من الإتفاقية العربية لمكافحة الجريمة الإلكترونية على هذا الإجراء، حيث جاء فيها: "يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخـــــرى:

- أن تصل إلى معلومات تقنية المعلومات المتوفرة (مصدر مفتوح)، بغض النظر عن الموقع الجغرافي للمعلومات.
- أن تصل أو تستقبل – من خلال تقنية معلومات في إقليمها- المعلومات الموجودة لدى الدولة الطرف الأخرى، وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة."

وكما هو واضح من نص هذه المادة، فهي تجيز إمكانية البحث والتفتيش في المنظومة المعلوماتية لدولة أجنبية، في حال إذا ارتكب فيها الفعل، ولكن تحدد ذلك بالشروط الآتية:

- أن تكون الدولتان طرف في الإتفاقية العربية لمكافحة الإجرام الإلكتروني.
- الحصول على موافقة طوعية وقانونية من الشخص صاحب المعلومات[1].

وعلاوة على ذلك، يتبين من خلال نص المادة أن الإتفاقية قد ميزت بين الموقع المفتوح الذي يمكن الولوج إليه من دون شروط أو قيود، بل ويمكن تفتيشه حتى دون علم أو أخذ إذن من الدولة

---

1 يعتبر هذا الإجراء نفس ما نصت عليه اتفاقية بودابست لمكافحة الإجرام المنظم، حيث جاء في نص المادة 32 منها: "يجوز إمكانية الدخول بغرض التفتيش والضبط في نظام المعلوماتي تابع لدولة أخرى بدون إذن منها في إحدى الحالتين:

- إذا كانت البيانات مخزنة علناً (أي مباحة للجمهور)
- في حالة موافقة الشخص –صاحب أو حائز البيانات – على التفتيش."

الأخرى، وبين المواقع الخاصة أو المغلقة التي يشترط فيها موافقة الدولة الأخرى عن طريق سلطاتها المختصة.

وعمل المشرع الجزائري على تجسيد تنفيذ هذا الإجراء عن طريق ما يعرف بالإنابة الفضائية، وهو ما نصت عليه المادة 16 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي جاء فيها: "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني. ويمكن في حالة الاستعجال ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة أعلاه، وإذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها".

وعليه من خلال نص هذه المادة، يمكن أن نستنتج عدة أمور أساسية فيما يتعلق بالمساعدة القضائية، والتي ربطها المشرع كما هو موضح في نص المادة بشروط عدة؛ كوجود اتفاقية دولية عامة أو خاصة تنظم هذا المجال، بالإضافة إلى تفعيل مبدأ المعاملة بالمثل في مثل هذا النوع من الإجراءات، كما أن الجانب الجزائري ملزم بتنفيذ المساعدة القضائية على وجه السرعة في حال ما إذا وردت عن إحدى وسائل الاتصال الحديثة، مع ووجوب التأكد من صحة مصدرها.

ومن جانب آخر، لم يأخذ المشرع الجزائري بالمساعدة القضائية على إطلاقها، حيث قيدها بشرطين هــما:

- إذا كان فيها مساس بالسيادة الوطنية.
- إذا كانت ماسة بالنظام العام.

ثالــثاً- ضوابــط إجــراءات التفتــيش:

حتى يكون إجراء التفتيش صحيح وجب على السلطات القضائية المختصة بالتحقيق، وضباط الشرطة القضائية التزام القواعد والضمانات التي حددتها القوانين الإجرائية، والتي يمكن أن نجملها في:

1- وجود إذن من السلطات المختصة بإصداره:

يعتبر هذا الإجراء من بين الإجراءات الضرورية في القيام بعملية التفتيش، ونص المشرع الجزائري على ذلك بموجب المادة 44 من قانون الإجراءات الجزائية، ويجب أن يتضمن هذا الإذن جميع

الشروط الشكلية المتعلقة بعملية التفتيش، على أن توصف بطريقة دقيقة، وإلا كانت نتائج التفتيش معرضة للبطلان[1].

2- أن يتم التفتيش بحضور المتهم أو المشتبه فيه:

من الضمانات الأساسية التي تفرضها القواعد الإجرائية، هو أن يتم التفتيش بحضور المراد تفتيشه، وفي حال تعذر حضور التفتيش يتوجب على ضابط الشرطة القضائية أن يلزمه بتعيين ممثلاً ينوب عنه في حضور عملية التفتيش، وفي حالة امتناعه، أو كان في حالة فرار استدعى ضابط الشرطة القضائية شاهدين لحضور عملية التفتيش، من دون أن يكون خاضعين لسلطته[2]، غير أن المشرع الجزائري استثنى من هذا الشرط بعض الجرائم الخاصة، حيث جاء في نص الفقرة الأخيرة من المادة 45 أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني، وكذا جرد الأشياء، وحجز المستندات المذكورة أعلاه". وكما هو واضح من هذه الفقرة فإن المشرع قد استثنى الجرائم الماسة بالمعطيات من هذا الإجراء، وذلك بالنظر لخطورة هذه الجريمة، فضلاً عن سرعة التخلص من الدليل، مما يوجب التدخل السريع من السلطات المختصة في الحصول عليه قبل طمسه وإتلافه، وقد حسن ما فعل.

3- احـــترام مـواعيد التفتـيش:

من بين الضوابط العامة في التفتيش هو مراعاة الأوقات التي يجب أن يتم فيها التفتيش، والتي حددها المشرع الجزائري طبقاً للمادة 47 من القانون 06-22 والتي جاء في فقرتها الأولى: "لا يجوز

---

1 تنص المادة 44 من قانون الإجراءات الجزائية على أنه: "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقاً أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش، إلا بإذن مكتوب صادر من وكيل الجمهورية، أو قاضي التحقيق، مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش. ويكون الأمر كذلك في حالة التحري في الجنحة الملتبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون. يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل، وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان. تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها، والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون. إذا اكتشف أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببًا لبطلان الإجراءات العارضة."

2 انــظر المادة 45 من القانون رقم 06-22 المتضمن ق.إ.ج.ج المعدل والمتمم.

البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحاً، ولا بعد الساعة الثامنة (8) مساءً، إلا بإذن طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الأحوال الاستثنائية المقررة قانوناً"، وتتعلق هذه القاعدة بتفتيش الأماكن الخاصة، والتي راعى فيها المشرع الظروف الخاصة بحرمة المسكن والحياة الخاصة، وهو نفس الشيء الذي يطبق في حالة تفتيش الهاتف النقال، غير أن المشرع وضع لهذه القاعدة عدّة استثناءات، تتمثل فـي:

- الجرائم المعاقب عليها في المواد 342 إلى 348[1].
- جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال، والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، وفي هذا النوع من الجرائم يجوز لقاضي التحقيق إجراء التفتيش في أي وقت وفي أي مكان على امتداد التراب الوطني، أو أن يأمر ضباط الشرطة القضائية القيام بذلك وفقاً لما نصت عليه المادة 3/47.

4- سريــة إجــراءات التفتـيش فيما يـتعلق بالـسر المهنـي:

تعتبر سرية إجراءات التفتيش من بين أهم الضوابط التي يتوجب على ضابط الشرطة القضائية أن يحرص عليها، ويكون ذلك من خلال اتخاذ جميع التدابير اللازمة لضمان احترام ذلك السر.

رابـعاً- طريقـة تـفتيش الـهاتـف النـقال:

إن خصوصية تفتيش الهاتف النقال تفرض ضرورة اتباع الإجراءات والمراحل التالية في ذلك[2]:

- تفتيش المنظومة المعلوماتية (للهاتف أو الحاسوب)، وطبع نسخة ورقية وإلكترونية من ملفات معينة في ذات الوقت،
- عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة،
- ضبط الجهاز، وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

---

1 جاءت هذه المواد ضمن القسم الرابع من قانون العقوبات، تحت عنوان "تحريض القصر على الفسق والدعارة".

2 محمود محمد محمود جابر، المرجع السابق، ص 191.

الفرع الثانـــي: المعايــنة.

تمثل المعاينة أحد الأساليب التي يلجأ إليها ضباط الشرطة القضائية وسلطات القضاء من أجل البحث عن الأدلة وتتبع أثر الجناة، لذلك سنتطرق من خلال هذا الفرع إلى التفصيل فيها من خلال النقاط الآتية:

أولاً– مفهوم المعاينــة:

هناك العديد من المفاهيم التي تعرف المعاينة، حيث عرفت بأنها: "إثبات مباشر ومادي للآثار التي خلفها ارتكاب الجريمة، عن طريق رؤيتها أو فحصها فحصاص مباشراً بهدف المحافظة عليها خوفاً من إتلافها أو محوها أو تعديلها"[1].

ويعرفها آخر[2] بأنها: "إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وهي تتطلب أن ينتقل مأمور الضبط القضائي إلى مكان ما لمباشرتها لإثبات حالته، وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء".

وعليه من خلال هذه المفاهيم نستنتج أن المعاينة عبارة عن تقصي للآثار المادية التي قد يخلفها الجناة في مسرح الجريمة، وذلك من خلال رؤيتها بالعين المجردة، أو عن طريق استخدام أدوات مخصصة في رفع هذه الآثار، وقد يباشر هذا الإجراء عن طريق ضباط الشرطة القضائية، وذلك بتكليف من السلطات المختصة، أو عن طريق قاضي التحقيق في مرحلة التحقيق الابتدائي، وبالرغم من أهمية المعاينة في الجرائم التقليدية، إلا أن هذا ينتفي والجرائم ذات الطابع الإلكتروني، وذلك بالنظر لخصوصية مثل هذه الجرائم من حيث مسرح الجريمة والأدوات المرتكبة فيها، خاصة إذا كانت تمس بالنظام المعلوماتي سواءٌ الهاتف النقال أو الحاسب الآلي.

---

1 صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري– تيزي وزو–، الموسم الجامعي 2012-2013، ص 83.

2 محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجريمة المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، أعمال الملتقى الوطني: آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، بالجزائر العاصمة، مركز جيل للبحث العلمي، بتاريخ: 29 مارس 2017، ص 60.

ثانيــاً– معايــنة الـهاتف النــقال:

لا تشكل معاينة الهاتف النقال من الناحية المادية أي إشكال بالنسبة للمحققين أو حتى ضباط الشرطة القضائية، وذلك بالنظر إلى تركيبة هذه المواد التي تقبل المعاينة، ولكن الصعوبة تثار إذا كان محل المعاينة النظام المعلوماتي للهاتف النقال، وتظهر هذه الصعوبة نظراً للأسباب التالية:

- انعدام الآثار المادية الناتجة عن هذا النوع من الجرائم مقارنة بالجرائم التقليدية، والتي في معظم الأحيان تدل دلالة واضحة على وقوع الجريمة ونسبتها لشخص ما، وهو ما يلعب دور إيجابي في عملية البحث أو التحقيق[1].
- العبث بأدلة النقال: تعتبر الجريمة المرتكبة بواسطة الهاتف النقال من الجرائم التي يسهل طمس أدلتها، وذلك بالنظر إلى عملية التجوال الناتجة عن الاستعمال الكثير للهاتف النقال[2].
- عدم احتفاظ بعض الضحايا بتسجيلات الدخول، أو عدم اكتشافهم للأنشطة الإجرامية التي تعرضوا لها، إلا بعد مدة يصعب فيها على مقدم الخدمة أن يزودهم فيها بتسجيلات[3].
- عمل القراصنة على تغيير تسجيلات الدخول غير المشروع، حتى تتاح لهم الفرصة لإخفاء الأدلة على أفعالهم الإجرامية[4].

ثالــثاً– كيفيــة معايــنة الـهاتف النــقال:

نظراً للطبيعة الخاصة للهاتف النقال كمسرح جريمة، أو أداة لتنفيذ الجريمة، وجب التعامل معه بطريقة دقيقة؛ وذلك من خلال الاستعانة بأصحاب الاختصاص والخبرة في هذا المجال من رجال التحقيق أو ضباط الشرطة القضائية، وأن يتم التعامل مع جهاز الهاتف النقال الذي تم استخدامه في الجريمة بكل دقة، ومن مختلف جوانبه وسائر ملحقاته، كما يعمل القائم بالمعاينة بإثبات الحالة التي تكون عليها توصيلات الهاتف والمتصلة بمكونات النظام الخاصة به، كما يتوجب على القائم بالمعاينة حفظ ذاكرة الهاتف من أجل معرفة الصفحات التي ولــج إليها مستخدمه[5].

---

1 محمود عمر محمود، المرجع السابق، ص 141.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 223.

3 محمود محمد محمود جابر، المرجع السابق، ص 155.

4 محمود محمد محمود جابر، نفس المرجع، ص 155.

5 طارق عفيفي صادق أحمد، المرجع السابق، ص 223. **وانظر كذلك:** محمود محمد محمود جابر، المرجع السابق، ص 161.

الــفرع الثالث: الضـبط فــي الـجرائم المرتكبة بواسطـة الهاتف النقال.

غلب على الفقه الجنائي اعتبار الضبط القضائي نتيجة لإجراء التفتيش أو المعاينة، وذلك على اعتبار أنه في الغالب ما ينتج عن هذا النوع من الإجراءات، لذلك وقبل التطرق باستفاضة لأحكام الضبط في الجرائم المرتكبة بواسطة الهاتف النقال، يتوجب بداية التطرق لمفهوم الضبط القضائي (أولاً)، ثم بيان صور هذا النوع من الضبط (ثانياً)، على نحو يتبين من خلاله بيان خصوصية إجراءات الضبط في هذا النوع من الجرائم.

أولاً– مفهــوم الضبـط القضائـي:

يعرف الضبط القضائي بأنه: "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق"[1]. ويعرفه آخر[2] بأنه: "العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوفر نفس القواعد التي تنطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط".

ومن خلال هذه المفاهيم، نستنتج أن الضبط القضائي هو عبارة عن إجراء من إجراءات المتابعة في الدعوى الجنائية، بحيث قد يتصل هذا الإجراء بمرحلة الاستدلال، كما قد يتصل بمرحلة التحقيق، والإجراءات التي أشار إليها المفهوم الثاني دون الأول تعتبر اقتصار إجراء الضبط على ما ينتج عن التفتيش، وهو منطق غير مقبول على الإطلاق، حيث قد يكون الضبط نتيجة للتفتيش كما قد يكون نتيجة للمعاينة، وتتحدد طبيعة إجراء الضبط بحسب الطريقة التي يتم وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص، واقتضى الأمر تجريده من حيازته؛ كان الضبط بمثابة إجراء تحقيق، أما إذا كان الاستيلاء عليه دون الاعتداء على حيازة قائمة؛ فإنه يكون بمثابة إجراء استدلال[3].

---

1 محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، ب. ط، مطابع الشرطة، مصر، 2016، ص 162.

2 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط. الأولى، مطابع الشرطة، مصر 2008، ص 208.

3 محمد عبد الله إبراهيم، المرجع السابق، ص 163.

ثانــياً- صور الضبط الـمتعلق بالـهاتف النقال:

يمكن تمييز ثلاث حالات فيما يتعلق بالضبط القضائي في مجال الهاتف النقال، تتضمن هذه الحالات:

1- الضبط الــمادي لمكونات الهاتف النقال:

تناولت الدراسة التركيبة المادية للهاتف النقال سواء في الباب الأول منها، أو حتى من خلال إجراء التفتيش، لذلك يتم الإكتفاء بالتعليق على هذه النقطة دون توضيح لهذه المكونات المادية، مع الإشارة أنه لا يوجد خلاف حول إمكانية الضبط المادي للهاتف النقال أو أحد عناصره المادية، وذلك باعتبار أنها تقبل الضبط بطبيعتها، ويجب أن تتوفر كل الضمانات التي يجب توفرها في إجراء التفتيش أو المعاينة، وإلا كان هذا الإجراء باطل، ومن بين هاته الضمانات؛ ما نص عليه المشرع الجزائري بموجب المادة 64 من ق.إ.ج.ج والتي جاء فيها: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة إلى رضاه. وتطبق فضلاً عن ذلك أحكام المواد من 44 إلى 47 من هذا القانون. غير أنه عندما يتعلق الأمر بتحقيق في إحدى الجرائم المذكورة في المادة 47 (الفقرة 3) من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر".

ومنه يتضح من خلال المادة السابقة أن المشرع الجزائري وفّر نفس الضمانات لعملية الضبط التي يستوجب توافرها في كل من إجراءات التفتيش والمعاينة. ومن عمليات الضبط في هذا النوع ما تم في قضية المغنية اللبنانية "س ت" ورجل الأعمال والسياسي المشهور المصري والتي قرر الحكم أنه: (قدم المتهم للضابط هاتفين محمولين أولهما ماركة HTC وعليه الشريحة رقم: ...، والثاني عليه الشريحة رقم: ....، مسجل على الهاتف الأول سبع رسائل نصية مرسلة إلى تليفون المتهم الثاني رقم: ...، وخمس مكالمات صوتية متبادلة بين المتهمين ومسجل على الهاتف الثاني ست رسائل نصية مرسلة إلى ذات تليفون المتهم الثاني المذكور رقمه، تدور حول التخطيط للجريمة وكيفية ارتكابها سواء من لندن أو في دبي، وقد ثبت من خطابات شركتي "موبينيل" و"فودافون"، وكذا كشوف المكالمات والرسائل الصادرة والواردة من وإلى تليفون المتهم الأول وتليفون المتهم الثاني، أنهما تبادلا العديد من المكالمات الصوتية

والرسائل النصية؛ منها المكالمات والرسائل المسجلة على تليفون المتهم الأول وأنها وصلت إليه، ومن هذه الرسائل رسالة بتاريخ 2008/5/11 يطلب فيها المتهم الأول من المتهم الثاني أن يرسل له عنوان "س ت"، مما أكد أن جميع هذه الرسائل والمكالمات كان موضوعها قتل المجني عليها "س ت")[1].

2- ضبط الـمعلومات التي يتضمنها الـهاتف النــقال:

يعتبر ضبط المعلومات من الأمور التي تثير عديد الإشكالات، وذلك بالنظر إلى نوع هذه المعلومات ذات الطبيعة المعنوية، ولكن بالرغم من هذه الصعوبة، إلا أن المشرع الجزائري وغيره من التشريعات الأخرى المقارنة، حاول معالجة هذه المشكلة عن طريق اقتراح آليات للضبط أو الحجز تتلاءم وطبيعة هذه المعلومات التي تم ضبطها، ومن أمثلة ذلك ما نص عليه المشرع الجزائري بموجب المادة 6 من قانون مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي جاء فيها: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز، وفقاً للقواعد المقررة في قانون الإجراءات الجزائية..."، فالمشرع الجزائري يرى بإمكانية ضبط وحجز المعلومات، وذلك عن طريق النسخ على شكل أوراق أو التخزين على دعامة خارجية، كما أن المشرع الجزائري يذهب أبعد من ذلك؛ حيث يقر بإمكانية تشكيل المعطيات من جديد، من أجل جعلها قابلة للإستعمال في التحقيق، وذلك عن طريق استعمال الوسائل التقنية الضرورية ودون المساس بمحتوى المعطيات، وهذا ما نصت عليه الفقرة 3 من المادة السادسة من نفس القانون السابق.

الـمطلب الثانــي: أدوات التحري والتحقيق المستحدثــة.

إن تطور أساليب ارتكاب الجريمة والأدوات المستعملة فيها فرض على التشريعات مسايرة هذا النوع من الأدوات واستخدامها في الكشف عن هذا النوع من الجرائم، وهو ما سايره التشريع الجزائري من خلال المادة 65 مكرر 5 وما يليها في ق إ ج ج، أو ما تم إدراجه بموجب قوانين خاصة، وهو نفس الشيء المعمول به فيما يتعلق بالتشريعات المقارنة.

---

1 **نقلاً عـــن**: محمود عمر محمود، المرجع السابق، ص 142.

لذلك، ومن خلال هذا المطلب يتم التطرق إلى بعض الطرق التي قد يتم اللجوء إليها من أجل البحث والتحقيق في جرائم الهاتف النقال، والتي من بينها مراقبة الإتصالات (الفرع الأول)، والتسرب (الفرع الثاني)، ثم الإستعانة بمزود الخدمات (الفرع الثالث).

الــفرع الأول: مراقبة اتصالات الــهاتف النقال.

تعتبر مراقبة الهواتف النقالة أحد الأشكال المستحدثة في البحث والتحري عن الجرائم التقليدية والحديثة، إلا أن هذه الوسيلة لقيت اعتراضاً كبيراً على المستوى الدولي، وذلك باعتبار أنها تمس بخصوصية الإنسان وحرمة حياة الخاصة، لذلك نجد أن بعض التشريعات ربطت هذا الأسلوب في التحري والتحقيق عن الجرائم بعدة شروط وإجراءات، وهو ما يتم التطرق إليه بالتفصيل من خلال العناصر التالية:

أولاً– مــفهوم الـمراقبــة:

هناك العديد من المفاهيم المحددة لمصطلح المراقبة، والتي تعرف بأنها: "الالتقاط السمعي أو أي التقاط لمحتويات أي اتصال سلكي أو الكتروني أو شفوي باستخدام أي جهاز الكتروني، أو ميكانيكي أو أي جهاز آخر"[1]. ويعرفها البعض[2] كذلك بأنها: "تعمد الإنصات والتسجيل، ومحلها المحادثات الخاصة، سواءٌ أكانت مباشرة أو غير مباشرة، أي سواءٌ كانت مما يتبادله الناس في مواجهة بعضهم البعض، أو عن طريق وسائل الاتصال السلكية واللاسلكية، أما الأحاديث العامة فلا قيد على مراقبتها وتسجيلها، سواءٌ علم بذلك أطرافها ووافقوا أو اعترضوا أجهلوا أصلاً، لأنه ليس في مراقبتها أو تسجيلها مساس بحق ولا انتهاك الحرمة".

ويتضح من هذين المفهومين أن المراقبة هي تنصت على الأمور الخاصة بالفرد فيما يتعلق بالاتصالات، سواء تعلق ذلك بالمحادثات العادية، كالبرقية والرسائل، أو إلكترونية كمراقبة المكالمات ورسائل الهاتف والبريد الإلكتروني، وإن كان البعض يميز بين المراقبة التي تستهدف الهاتف والأخرى التي تستهدف شبكات الإنترنت، حيث يطلق على الحالة الأولى تنصت إذا ما تمت عن طريق الهاتف

---

1 عبد الله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2017، ص 94.

2 محمود محمد محمود جابر، المرجع السابق، ص 217.

النقال، ويطلق على الحالة الثانية مراقبة إلكترونية إذا كان المستهدف منها البريد الإلكتروني والشات[1]، وتعد المراقبة من الطرق المعمول بها في أغلب التشريعات العربية كالمصري والجزائري، وكذلك التشريعات الأجنبية، كالتشريع الفرنسي والأمريكي والبلجيكي، وذلك وفقًا لظروف وقواعد خاصة[2].

ثانياً– شروط مراقبــة الاتصالات الإلكترونــية[3]:

حدد المشرع عدة شروط حتى يستطيع المحقق أن يلجأ لهذه الطريقة في الكشف عن الجريمة ويمكن حصر هذه الشروط في:[4]

1– أن يلجأ للمراقبة الإلكترونية للاتصالات في حال ما إذا كانت الجريمة موصوفة بجرائم إرهاب، أو تخريب، أو أنها تمس بأمن الدولة، أو الاقتصاد الوطني، أو أن تكون الجريمة تشكل اعتداء على المنظومة المعلوماتية، على نحو قد يمس بالنظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني.

2– أن تكون مراقبة الإتصالات هي السبيل الوحيد للوصول إلى نتيجة فيما يتعلق بالتحريات والتحقيقات القضائية.

3– تنفيذًا لمقتضيات طلب المساعدة القضائية الدولية المتبادلة.

---

1 عبد الله جعفر كوفلي، المرجع السابق، ص 94.

2 من بين أكثر المعيقات التي تجعل من المراقبة أو التنصت محل نقد وجدل في الفقه الأجنبي والعربي هي قواعد المشروعية؛ هذا النوع من الأفعال في البحث عن الأدلة، وفي خضم هذا النقاش حول هذا الموضوع، يرى البعض ضرورة تفعيل الآليات القانونية لحماية الخصوصية من الانتهاكات التي قد تلحقها من خلال هذا الإجراء، وذلك من خلال استخدام الأدوات التالية:

أ– **الخصوصية التقليدية:** من الضوابط التي يتوجب احترامها في حال اللجوء إلى إجراء المراقبة هو ضابط الخصوصية بمفهومها التقليدي، وإن كان هذا المفهوم غير متفق عليه في الفقه ويختلف من بيئة إلى أخرى.

ب– **الخصوصية الحديثة:** تمثل الخصوصية الحديثة نوع متطور من التصور الفكري لحياة الإنسان الخاص، فنحن هنا نتكلم عن الخصوصية في واقع افتراضي يشكل امتداد لحياة الإنسان في الواقع، ويظهر ذلك من خلال البيانات الشخصية، البريد الإلكتروني، والحسابات البنكية، والصور الشخصية.

لمزيد من التفاصيل انــظر: فؤاد أمين السيد محمد، جرائم مراقبة المراسلات الإلكترونية، الطبعة الأولى، دار النهضة العربية، مصر، 2016، ص 38-39.

3 عرفت الفقرة "و" من المادة 2 من القانون 09-04 الاتصالات الإلكترونية على أنها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

4 المادة 6 من القانون رقن: 09-04 السالف الذكر.

4- أن تكون مراقبة الاتصالات الإلكترونية "بإذن" يصدر من السلطات القضائية المخولة بذلك، ويشترط في هذا الإذن أن يستوفي عدة شروط، حتى لا تتعرض النتائج المترتبة عنه للبطلان، وتتمثل هذه الشروط فـــي[1]:

- أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة وطبيعتها (سكنية أو غيرها).
- الجريمة التي تبرر اللجوء إلى هذا التدبير ومدتها.
- أن يسلم الإذن مكتوب لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، ويستثنى من هذه الحالة الجرائم الموصوفة بجرائم الإرهاب، أو التخريب، أو الماسة بأمن الدولة، والتي يصدر إذن المراقبة الخاص بها من قبل النائب العام لدى مجلس قضاء الجزائر، والذي يختص بمنح الإذن لضباط الشرطة القضائية المنتمين لهيئة الوقاية من جرائم تكنولوجيا الإعلام والاتصال، حيث تكون مدة هذا الإذن ستة (6) أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

5- تحرير محضر بالعمليات وآليات وضع الترتيبات التقنية التي تسمح المراقبة، ويكون ذلك من طرف ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص وفقاً لما نصت عليه المادة 65 مكرر9.

وفي حال احترام هذه الشروط تكون المراقبة كإجراء صحيحة، ولكن هل هناك حالات يمكن أن يُلجأ فيها لأحد طرق المراقبة دون أخد إذن من السلطات المختصة ؟ أو بدون إذن ؟

إن ما هو معمول به في التشريع الجزائري استحالة هذا الأمر؛ باعتبار الإذن يحقق ضمانات أساسية لصحة الإجراء ولحماية خصوصية الأفراد المحمية وفقاً للدستور، ولكن في بعض التشريعات المقارنة يمكن ذلك تطبيقاً للاستثناءات التالية[2]:

---

1 تنص المادة 65 مكرر 7 من القانون 06-22 على: "يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر للجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوب لمدة أقصاها أربعة (4) شهور قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية".

2 محمود محمد محمود جابر، المرجع السابق، ص ص 231-235.

أ. **المراقبة المعتادة لعمل الشبكة من قبل مزود الخدمة:** تلجأ بعض التشريعات إلى العمل بهذا الاستثناء تحسباً لأي طارئ أو ضرر قد يصيب أنظمتهم المعلوماتية أو الاتصالية، ومن بين هذه التشريعات؛ التشريع الأمريكي الذي يسمح لمشغل لوحة التحويل، أو مدير، أو موظف، أو وكيل لدى مزود خدمة الاتصالات السلكية أو الإلكترونية إمكانية استخدام نقل اتصال سلكي، أو إلكتروني، أو اللجوء إلى مراقبة وكشف استخدام أي اتصال في السياق العادي لوظيفته، بحيث يكون ذلك ضروري للقيام بعمله أو لحماية حق ملكية مزود الخدمة[1].

ب. **المراقبة بناءً على شكوك المشترك:** من بين الإستثناءات التي نص عليها القانون الأمريكي هو المراقبة بناءً على شكوك المشترك، ويخص هذا الاستثناء ضحايا الهجوم على الحاسوب، وقرر ذلك بتوافر الشروط الآتية:

- سماح مالك أو مشغل الحاسوب بأن تتم عملية مراقبة الاتصالات.
- أن يكون الشخص الذي يتولى مراقبة الاتصال عضواً في التحقيق وبشكل قانوني.
- توفر أسباب معقولة عند الشخص الذي يقوم بمراقبة محتويات منتهك الحاسوب ذو الصلة بالتحقيق.
- أن لا تتطرق المراقبة لغير الاتصالات التي تم بثها من قبل المنتهك.

ج. **المراقبة بناءً على موافقة أحد أطراف الاتصال:** تعتبر هذه الصورة كذلك من بين الاستثناءات التي قررها المشرع الأمريكي في مراقبة الاتصالات وذلك بناءً على موافقة أحد الأطراف.

---

1 ومن الأمثلة هذه الحالة قضية تتلخص وقائعها في أن رجال الضبط القضائي كانوا يتقصون جريمة اختطاف، وقد لجأ المختطف في قضية الحال إلى استخدام خط هاتف نقال مقلد، مما أدى برجال الضبط القضائي إلى الاستعانة بمزود خدمات الاتصالات السلكية من أجل مراقبة الخط استناداً إلى أن القانون يسمح بذلك في حالة الاعتداء على حقوق المزودين لتلك الخدمات، وفي صدد حكم المحكمة في هذه القضية أقرت أنه وفقاً للقسم *USC§2511(2) (a) i18* يجب أن تبدأ مبادرة مراقبة الخط من طرف مزود الخدمة بمناسبة أداءهم لعملهم، ومن ثم تبليغ رجال الضبط وليس العكس، كما أقرت المحكمة أنه يجوز لمزود الخدمة أن يقوم بالمراقبة في إطار مكافحة الغش والسرقة على الخدمات التي يقدمونها، ويتضح من هذه القضية أن المشرع الأمريكي ضبط دور مزود الخدمات بدون إذن بالشروط الآتيـة:

- أن يكون مزود الخدمات ضحية جريمة، ويعمل على مراقبة الاتصال من أجل حماية حقوقه وممتلكاته.
- تأكد السلطات من أن مزود الخدمات عمد إلى المراقبة من أجل حماية حقوقه وممتلكاته.
- بأن لا تكون المراقبة تمت وفقًا لتوجيه من السلطات لأي غرض كان،

انـــظر: محمود محمد محمود جابر، المرجع نفسه ص 232.

ثالــثاً– صور الــمراقبة باستخدام الهاتــف النقال:

هناك العديد من الحالات التي يُمكن تصور مراقبة الهاتف النقال من خلالها، وتتمثل هذه الصور في:

1- التقاط المحادثات التــي تتم بجوار الهاتف النقال:

تعتبر هذه الميزة من أكثر الوسائل وأكثر استخداماً؛ حيث تتم عن طريق تشغيل ميكرفون الهاتف النقال عن بعد، واستخدامه في استراق السمع على ما يدور بالقرب منه، وتتوفر هذه الخدمة في جميع الحالات التي يكون عليها الهاتف سواء كان مفتوحاً أو مغلقاً، ومن بين أكثر الدول استخداماً لهذا الطريقة الولايات المتحدة الأمريكية، خصوصاً فيما يتعلق بالجريمة المنظمة[1].

2- تشغيل كاميرا الهاتف المحمول دون علم صاحـــبها:

تمثل هذه الطريقة واحد من أهم الطرق التي قد يلجأ إليها في المراقبة عن طريق الهاتف النقال، حيث تعتمد هذه الميزة على التحكم في الكاميرا الملحقة بالجهاز التي تعمل على التقاط كل ما يدور حولها، بغض النظر عن الوضعية التي يكون عليها الهاتف النقال (مفتوح/مغلق)، ولعل بعكس الطريقة السابقة لم يلق هذا الأسلوب من المراقبة استحساناً من قبل جهات التحقيق والقضاء، مما جعل استخدامه مقصور على الفئات الإجرامية دون غيرها[2].

3- تــتبع حائز جهاز الهاتف ومعرفة أمــاكن تواجده:

من بين أهم الميزات التي تتيحها الهواتف النقال هي خدمة الموقع والتي ساهمت في كثير من الحالات في تقفي أثر الجناة والقبض عليهم، كما تتيح الشريحة الموصولة بالهاتف النقال إمكانية العمل بهذه الميزة وذلك عن طريق التعاون مع الشركة التي تقدم خدمة الاتصال، وذلك من خلال تتبع المكالمات التي قام المشبه فيه أو المتهم بالقيام بها[3].

---

1 أشرف توفيق شمس الدين، المراقبة والتنصت من خلال الهاتف المحمول في التحقيق الجنائي، دراسة مقدمة إلى مؤتمر الجوانب القانونية والاقتصادية للهاتف المحمول الذي تعقده كلية الحقوق بجامعة بنها، 2010، ص 427.

2 أشرف توفيق شمس الدين، نفس المرجع، ص: 428.

3 أشرف توفيق شمس الدين، نفس المرجع، ص: 429.

4- التحكم فــي الهاتف النقال عن طريق برنامج تجســـسي يرسل إليه:

من بين أكثر الصور خطورة هي هذه الصورة، بحيث تعتمد على إرسال برنامج خبيث عن طريق رسالة نصية، أو عن طريق البريد الإلكتروني، وتجعل من الهاتف النقال تحت سيطرة هذا البرنامج، وبالتالي مراقبة كل المهام التي يقوم بها هذا الهاتف.

الـفرع الثانـــي: إجراء التـــسرب.

يمثل التسرب أحد الإجراءات الحديثة التي نص عليها المشرع بموجب القانون رقم 06-22 في المواد من 65 مكرر11 إلى المواد 65 مكرر 18 في ق إ ج ج، ومن خلال هذا الفرع يتم التطرق إلى مفهوم إجراء التسرب (أولاً)، وإلى الشروط التي يجب توفرها في هذه العملية (ثانياً) على النحو التالي:

أولاً– مفهوم إجــراء التسرب:

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية، والتي نصت على أن: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. يسمح لضابط أو عون الشرطة القضائية أن يستعمل، لهذا الغرض، هوية مستعارة، وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم".

وعليه نستنتج من خلال التعريف السابق أن التسرب هو نوع من أنواع المراقبة يعتمد على تسخير أحد أفراد الضبطية القضائية، وذلك تحت إشراف ضابط يسمى بمنسق العملية، على أن يقوم المتسرب بمراقبة المشتبه فيهم عن طريق العمل معهم، باعتباره فاعل أصلي أو شريك أو مجرد خاف، مع إمكانية استعمال هوية مستعارة حتى يحمي نفسه أو عائلته من أي تهديد قد يلحق به، كما منع المشرع المتسرب من تحريض المشتبه فيهم على ارتكاب الجريمة تحت طائلة بطلان، وأتاح المشرع للمتسرب أن يرتكب بعض الأفعال المنصوص عليها في المادة 65 مكرر 14، والتي نصت على أنه: "يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عمليات التسرب والأشخاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جزائياً القيام بما يأتــي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو ضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال".

ثانيـاً– شروط إجـــراء التـسرب:

حتى يكون التسرب إجراءً صحيحاً وغير معرض للبطلان، يجب أن تتوفر فيه الشروط الآتــية:

1- أن يكون بتكليف من السلطات القضائية المختصة، سواء من طرف النيابة العامة أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
2- أن يكون في إحدى الجرائم المنصوص عليها في المادة 65 مكرر 5 من قانون الإجراءات الجزائية[1].
3- أن يكون التسرب بإذن من السلطات المختصة، ويشمل هذا الإذن المواصفات الآتية:

- أن يسلم الإذن عملاً بمقتضيات التحري والتحقيق، تطبيقاً لنص المادة 65 مكرر 11، وإلا كان الإذن باطلاً،
- أن يكون الإذن مكتوب تحت طائلة البطلان،
- أن يكون مُسبباً تحت طائلة البطلان،
- أن يذكر في الإذن طبيعة الجريمة التي ينصب عليها الإذن، حيث نصت الفقرة 2 من المادة 65 مكرر 15 على أن: "تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء..."،
- ذكر هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته،
- تحديد مدة الإذن، والتي في الغالب لا تتجاوز الأربعة (04) أشهر مع إمكانية تجديدها كل ما اقتضت ضرورة التحريات التحقيق ذلك، وفقاً لنفس الشروط الشكلية والزمنية.

---

1 تنص المادة 65 مكرر 11 على: "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه".

ثالـثاً– طرق مـمارسة إجراء التسرب فـي الـجرائم الإلكتـرونيـة:

إن أول سؤال يتبادر إلى الذهن هو مدى ملائمة إجراء التسرب، كوسيلة للبحث والتحري عن الجرائم التقليدية، مع الجرائم ذات الطبيعة الإلكترونية بصفة عامة، والجرائم المرتكبة بواسطة الهاتف النقال بصفة خاصة، ومن المعلوم أن التكنولوجيا فرضت عالم افتراضي موازي للعالم الواقعي الذي نعيشه اليوم، هذا العالم يحمل في طياته جميع الخصائص التي يعتمد عليها العالم الواقعي، مما يجعل التسرب يتم عن طريق انضمام المتسرب لصفحات ومواقع يكون مشتبه فيها، أو أن تكون هناك دلائل قوية تشير إلى تخطيط هؤلاء الجناة إلى ارتكاب جريمة ما، خاصة فيما يتعلق بالجريمة المنظمة العابرة للحدود، فيضطر المتسرب إلى الإنضمام لمثل هذه المجموعات والصفحات الإلكترونية بهوية وهمية، قاصداً من وراء ذلك الحصول على معلومات تمكنه من الإطاحة بعناصر هذه المجموعة[1].

الفرع الثالث: الإستعانــة مــزود الخدمــات.

يعتبر إجراء الإستعانة بمزود الخدمات من بين الطرق التي استعانت بها التشريعات، فيما يتعلق بالجرائم المرتكبة بواسطة وسائل الإتصال، ويلعب هذا المزود دور كبير سواء في الوقاية من الجريمة قبل ارتكابها، أو حتى في المساعدة في الكشف عن مرتكب الجريمة.

ونظراً لأهمية هذا الإجراء، يتم التطرق لتحديد مفهوم مقدم الخدمات (أولاً)، ثم للإلتزامات المفروضة عليه (ثانياً)، وبيان ذلك على النحو التالــي:

أولاً– تـعريـف مـقدم الـخدمـات:

عرف المشرع الجزائري مقدم الخدمات في الفقرة "د" من المادة الثانية، والتي جاء فيها: "1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات. 2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية، لفائدة خدمة الإتصال المذكورة أو لمستعمليها"[2].

---

1 رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص 434.

2 تتقارب هذه المادة مع الفقرة "ج" من المادة الأولى من الاتفاقية المتعلقة بالجريمة الإلكترونية المنعقدة في بودابست، والتي نصت على: "يقصد بمقدم الخدمات "1- أي كيان عام أو خاص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق

وعرفته الإتفاقية العربية لمكافحة تقنية المعلومات في مادتها الثانية (02) في الفقرة الثانية منها على أنه: "أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".

ومن التعريفات الأخرى كذلك تعريف قانون الإتصالات المصري الذي عرفه بأنه: "أي شخص طبيعي أو اعتباري، مرخص له من الجهاز بتقديم خدمة أو أكثر من خدمات الإتصالات للغير"[1].

وعليه من خلال المفاهيم السابقة يتضح لنا أن مقدمي الخدمات في التشريع المصري عبارة عن أشخاص، قد يحملون الصفة المعنوية أو الطبيعية، وهذا على خلاف القانون الجزائري الذي يتضح من نص المادة السابقة أنه أشار بلفظ "أي كيان عام أو خاص"؛ بما يوحي أن اللفظ قد ينصرف إلى الأشخاص المعنوية دون الأشخاص الطبيعية، وهذا على عكس ما أشير إليه في تعريف الإتفاقية العربية لمكافحة تقنية المعلومات، والتي ذكرت الكيان الطبيعي والمعنوي متبوع بعام أو خاص، والتي تنصرف على الأخير دون الأول، مما يجعل تعريفها الأكثر دقة، كما نلاحظ من خلال المفاهيم السابقة أن مقدم الخدمة يضطلع بمهام مختلفة كتقديم الخدمات المعلوماتية، وتزويد بخدمة الاتصالات، فضلاً على القيام بمعالجة أو تخزين معطيات معلوماتية، مما يلعب دوراً كبيراً في الكشف عن الجرائم المرتكب بواسطة وسائل الاتصالات.

ثانـــياً– التـزامـات مقدمـي الخدمـات:

حددت المادة 10 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بعض الإلتزامات التي يجب على مقدمي الخدمات مراعاتها أثناء أداءهم لمهامهم، وتمثلت هذه الالتزامات فـي:

1– تقديم المساعدة للسلطات المكلفة بالتحريات القضائية، وذلك من خلال تسهيل تسجيل المعطيات ذات الصلة بمحتوى الاتصالات في وقتها.

نظام معلوماتي. 2- وأي كيان آخر يقوم بمعالجة بيانات المعلومات أو تخزينها، نيابة عن خدمة الاتصالات المذكورة أو مستخدمي هذه الخدمة".

1 المادة الأولى فقرة 07 من القانون المصري رقم (10) لسنة 2003 المتعلق بتنظيم الإتصالات، الصادر في 03 من ذي الحجة سنة 1423هـ، الموافق لـ: 04 من فبراير سنة 2003 م، الجريدة الرسمية العدد رقم 5 مكرر لسنة 2003.

2- كتمان سرية عمليات التحقيق التي يتم انجازها عن طريق تكليف صادر من سلطات التحقيق تحت طائلة عقوبات جنائية في حال إفشاءها[1].

3- حفظ المعلومات المتعلقة بالسير.

وفضلاً عن الإلتزامات السابقة، أناط المشرع الجزائري بمقدم الخدمات حفظ المعلومات المتعلقة بالسير، وذلك من خلال الإحتفاظ بـــ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،
- المعطيات التي تسمح بالتعرف على المرسل إليه، أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.

والواضح من نص المادة 11 أن المشرع شدد على حفظ معلومات الهاتف؛ خاصة ما تعلق منها بالتعرف على مستعملي الخدمة، وتلك التي تسمح بالتعرف على معطيات المرسل والمرسل إليه، فضلاً عن ذلك، حدد المشرع مدة حفظ هذه المعلومات بسنة، وذلك بدءً من تاريخ التسجيل، وشدد المشرع على عدم احترام الالتزامات السابقة بفرض عقوبات إدارية وجزائية على المخالف لتلك الإلتزامات؛ حيث نص في الفقرة الأخيرة من المادة 11 على: "...دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى (5) سنوات، وبغرامة من 50.000 دج إلى 500.000 دج. يعاقب الشخص المعنوي بالغرامة وفقاً للقواعد المقررة في قانون العقوبات".

---

1 تنص المادة 10 على: "في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها يطلب من المحققين، وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

الفصل الثانـــي:
أدلــة الإثــبات فــي الـجرائم الـمرتكبــة بواسطــة الهاتـف النــقال

تعتبر الأدلة الجنائية من بين أكثر الأمور التي يسعى رجال الضبط القضائي والتحقيق البحث عنها، فهي الجوهر الأساسي الذي يُعتمد عليه في وجود متابعة جنائية من عدمها، وبها تتحدد نسبة الجريمة إلى الفاعل، ويتحدد مركزه القانوني كمتهم، ويعمل رجال القضاء من خلال الأدوات السابقة الذكر على العمل على تحصيل هذه الأدلة.

وتتنوع الأدلة الجنائية التي حددها المشرع بموجب قانون الإجراءات الجزائية؛ بين أدلة قولية كالاعتراف والشهادة، وفنية كالخبرة، وعلمية كالدليل التقني، وتعتبر هذه الأدلة في وجهة نظر القاضي الجنائي ذات قوة وحجية متساوية، وتخضع في جميع الحالات إلى السلطة التقديرية للقاضي فهو يأخذ منها ما يشاء ويطرح ما يشاء.

من جانب آخر، وبصدد معالجة الجريمة المرتكبة بواسطة الهاتف النقال ذات الطبيعة الإلكترونية، تطرح إشكالية البحث عن الأدلة التي يتحقق بها الكشف عن هذا النوع من الجرائم ؟ فهل جميع الأدلة تصلح لأن تكون دليلاً لإثبات هذه الجريمة ؟

بناء على هذه التساؤلات، ومن أجل الإجابة عنها يتم في هذا الفصل تحديد مسار الأدلة التي يتوجب تقصيها في البحث عن هذا النوع من الجرائم، كما يتم حصر هذه الأدلة في تلك التي تكون أكثر وقعاً وتجانساً مع الجرائم التي ترتكب بواسطة الهاتف النقال، وتحمل الطبيعة الإلكترونية.

لذلك، وبناء على ما ذكر، يتم التطرق في هذا الفصل إلى الشهادة والخبرة ودورها في الكشف عن الجرائم المرتكبة بواسطة الهاتف النقال (المبحث الأول)، ثم التطرق إلى الدليل الرقمي وأهميته في الكشف عن مثل هذا النوع من الجرائم (المبحث الثاني).

المبحث الأول:

الشـــهادة والـخـبرة في الجرائم الـمرتكبة بواسطة الهاتــف النقال.

تعتبر الشهادة والخبرة أحد أهم الأدلة التي يعتمد عليها القضاء في الوصول إلى الحقيقة، وكشف هوية مرتكب الفعل الإجرامي، لذلك ومن خلال هذا المبحث، يتم تسليط الضوء على دور الشهادة والخبرة في الكشف عن الجرائم المرتكبة بواسطة الهاتف النقال، وعن الميزات التي تختلف فيها الشهادة والخبرة فيما يتعلق بالجرائم الإلكترونية عن غيرها من الجرائم الأخرى.

يتم التطرق إلى الشهادة كدليل إثبات في الجرائم المرتكبة بواسطة الهاتف النقال (المطلب الأول)، ثم إلى إجراء الخبرة (المطلب الثاني).

الـمطلب الأول: الشهادة في الجرائم الـمرتكبة بواسطة الهاتــف النقال.

تعتبر الشهادة من بين أكثر الأدلة الجنائية[1] قدماً، عرفتها معظم التشريعات القانونية القديمة منها والحديثة، وتتخذ الشهادة صورة نمطية تعتمد على إقامة الدليل على أحدهم، بالاعتماد على ما شهده شخص آخر أثناء ارتكاب المتهم للفعل الذي يحظره القانون، لذلك سوف يتم التطرق من خلال هذا المطلب لمفهوم الشهادة (الفرع الأول)، ثم للشاهد المعلوماتي (الفرع الثاني).

الفرع الأول: مفهـــوم الشهادة.

ونتطرق في هذا الفرع لتعريف الشهادة (أولاً)، ثم التزامات الشاهد القانونية (ثانياً)، على النحو التالي:

---

1 يعرف الدليل على أنه: "الوسيلة الإثباتية المشروعة التي تسهم في تحقيق حالة اليقين لدى القاضي بطريقة سائغة يطمئن إليها، وأن تؤدي عقلاً إلى ما رتبه عليها من أحكام"، فيما يمكن تعريف الدليل الجنائي من خلال وجهة النظر الأولى على مستوى التحقيق، ويعرف بأنه: "الحجية المحدودة التي تستخلص من ظاهرة أو واقعة أو تصرف مادي أو معنوي، يولد اقتناعًا بوقوع جريمة أو أحد وقائعها بالقدر الكافي لإسنادها إلى المشتبه فيه أو نفيها عنه، وبما يخول اتخاذ بعض الإجراءات الماسة بحرية المشتبه فيه"، أما على مستوى مرحلة التحقيق فهو يعرف على أنه: "الحجية القضائية الناشئة في نفس القاضي ووجدانه، والتي تستخلص من واقعة أو ظاهرة حقيقية أو مادية أو معنوية متعلقة بالجريمة، تقوده إلى الحقيقة الإجرائية، بحيث يولد على ظهورها على ساحة الإثبات لدى القاضي الاقتناع القضائي بوقوع الجريمة بأركانها القانونية، أو واقعة من وقائعها أو أمر مرتبط بها، أو متصل بها، وإسنادها إلى متهم معين بذاته أو نفي ذلك". انـــظر: محمد حمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود "دراسة مقارنة"، رسالة مقدمة للحصول على درجة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة القاهرة، الموسم الجامعي 2012-2013، ص 190-191.

أولاً– تـعريـف الشـــهادة:

يعرف البعض[1] الشهادة بأنها: "وسيلة إثبات بمقتضاها يدلي الشاهد بمعلومات عما شاهده أو سمعه أو أدركه بحواسه عن طريق واقعة معينة أو ظروف خاصة بالجريمة أو عن الجريمة برمتها أمام سلطة التحقيق أو الحكم"، ويعرفها آخر[2] بأنها: "ما يقر به الشخص أمام المحكمة عن وقائع قد يكون رآها أو سمع بها وتكون مرتبطة بالجريمة التي فتح من أجل التحقيق فيها".

يتبين من ذلك بأن الشهادة عبارة عن إدلاء أو إقرار يقوم به شخص معين بصفته حضر واقعة معينة، وذلك عن طريق الرؤية، بحيث يحضر جميع وقائع هذه الجريمة حال ارتكابها، وتتكون لديه صورة عامة حول هذه الجريمة، أو عن طريق السماع، وإن كان يعاب على المفاهيم السابقة تحديد المقصود بالسماع بدقة، حيث أن ما يتبادر إلى الذهن هو السماع بصفة عامة، وإن كان في نظرنا المقصود منه هو سماع المجريات التي تمت وقت ارتكاب الجريمة، ومما يذكر كذلك أن المفهوم الأول كان مفصلاً حيث حدد جميع الصور التي يمكن أن يُعد بصاحبها كشاهد.

ومما سبق يمكن أن نعرف الشهادة على أنها إقرار قضائي يقوم به شخص يدعى الشاهد أمام هيئة التحقيق أو الحكم عن وقائع أو مجريات متعلقة بجريمة ما.

ثانـــياً– التزامات الشاهـــد:

تفرض الشهادة على الشاهد العديد من الالتزامات، والتي تم النص عليها بموجب قانون الإجراءات الجزائية، والتي نوردها على النحو التالي:

1- الالتـــزام بالـحضور:

يُعد من أهم النقاط التي تم النص عليها بموجب قانون الإجراءات الجزائية الجزائري، أو حتى في القوانين المقارنة، حيث أمر المشرع الجزائري بإحضار الشاهد بصفة رضائية طواعية، أو عن طريق

1 مصطفي يوسف، الحماية القانونية للشاهد، ب. ط، دار النهضة العربية، القاهرة، 2011، ص 32.

2 ماينو جيلالي، الحماية القانونية لأمن الشهود في التشريعات المغاربية: دراسة في التشريع الجزائري والمغربي والتونسي، مجلة دفاتر السياسة والقانون، العدد الربع عشر، جامعة قاصدي مرباح –ورقلة–، جانفي 2016، ص 16.

تسخير القوات العمومية مع إمكانية تسليط عقوبات عليه، وهذا ما نصت عليه المادتان 88 و89 من قانون الإجراءات الجزائية[1].

2- أداء اليمـين:

من الالتزامات المهمة التي تقع على عاتق الشاهد هو أداء اليمين، بشرط أن يكون هذا الشاهد بالغاً من العمر ستة عشر فما فوق، وهو ما يتضح في نص المادة 2/93 من قانون الإجراءات الجزائية الجزائري، والتي نصت: "وتسمع شهادة القصر إلى سن السادسة عشر بغير خلف يمين".

3- أداء الشـــهادة:

تعتبر هذه النقطة من النقاط الجوهرية فيما يتعلق بالشهادة، حيث لا يجوز للشاهد الامتناع أمام القاضي عن شهادته، خاصة إذا ما وصل إلى علم القاضي معرفة الشاهد بمرتكب الجناية، أو الجنحة، مما قد يؤدي إلى تطبيق عقوبات جزائية تتمثل في الحبس من شهر إلى سنة والغرامة من 1000 إلى 10.000 دج أو تطبيق أحدى هاتين العقوبتين[2].

الفرع الثانـــي: الشاهد المعلوماتي.

من خلال هذا الفرع سنتطرق إلى تعريف الشاهد المعلوماتي، وذكر أهم الفئات التي تدخل في هذا النوع من الشهود، فضلاً عن ذكر الإلتزامات التي تقع على عاتق هذا الشاهد، وذلك على النحو الآتـــي:

أولاً- تـعريـف الشاهـد المعلوماتـي:

يعرف الشاهد المعلوماتي بأنه: "الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب، الذي تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات Système de traitement

---

1 نصت المادة 88 من قانون الإجراءات الجزائية الجزائري على طرق التي يعلم بها الشاهد من أجل المثول أمام قاضي التحقيق وسماع شهادته، وجاءت على الشكل التالي: "يستدعي القاضي أمامه بواسطة أحد أعوان القوة العمومية كل شخص يرى الفائدة من سماعه. وتسلم نسخة من طلب الاستدعاء إلى الشخص المطلوب حضوره، كما يجوز استدعاء الشهود أيضاً بكتاب عادي موصى عليه أو بالطريق الإداري، ولهؤلاء الأشخاص المطلوب سماعهم فضلاً عن ذلك الحضور طواعية". أما نص المادة 89 فقد تحدثت عن إمكانية تعرض الشخص لعقوبة في حال تخلفه عن أداء الشهادة في إحالة صريحة لنص المادة 97 من نفس القانون، وجاء نصها على الشكل التالي: "يتعين على كل شخص استدعى بواسطة أحد أعوان القوة العمومية لسماع شهادته أن يحضر ويؤدي اليمين عند الاقتضاء ويدلي بشهادته وإلا عوقب بمقتضى نص المادة 97...".

2 انظر المادة 98 من ق.إ.ج.ج.

informatique إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله"[1]. ويعرف أيضاً بأنه: "ذلك الشخص صاحب الدراية الفنية بنظم المعلومات والاتصالات، والذي تكون لديه معلومات أساسية وجوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للمعطيات أو البيانات"[2].

ومن خلال هذين المفهومين يتبين بأن التعريف الأول وصف الشاهد المعلوماتي بأنه الشخص الذي يملك معلومات عن جريمة تم ارتكابها بواسطة الحاسب الآلي، بالرغم من أن ذلك لا يختلف كثيراً عن الجانب المراد الحديث عنه فيما يتعلق بالجرائم المتعلقة بالهاتف النقال من حيث التركيبة المعلوماتية، ومن الملاحظ كذلك على هذا التعريف أنه حصر الشاهد المعلوماتي في نطاق محدد؛ وهو "الفني صاحب الخبرة"، وإن كنا نرى أن هذا الوصف ينصرف إلى الخبير أكثر منه إلى الشاهد، بينما نرى أن التعريف الثاني عرف الشاهد المعلوماتي فيما يقارب الجرائم المرتكبة بواسطة الهاتف النقال، فضلاً على أنه لم يحدد صفة لهذا الشاهد، غير أنه صاحب دراية بمجال التقنية فيما يتعلق بالهاتف النقال.

ومن خلال ما سبق ذكره يمكن القول بأن الشاهد المعلوماتي هو كل شخص ذو مقدرة على التعامل مع الهاتف النقال، وتكون لديه معلومات أو معطيات تدل على ارتكاب جريمة في النظام والبيانات الخاصة بجهاز هاتف نقال، وضد شخص ما بواسطة هاتف نقال يعود لملكية شخص ما.

ثانياً– أنـواع الشهود فـي مـجال الـمعلوماتية:

هناك فئات عدة يمكن أن تدرج في قائمة الشهود المعلوماتيون، ويمكن إجمال هذه الفئات في:

1- مشــغلي الأجــهزة:

تتمثل هذه الفئة في كل الأشخاص المسئولون عن تشغيل الأجهزة والأدوات المتصلة بها، ويشترط فيهم أن يكونوا على دراية تامة بطرق تشغيل هذه الأجهزة، فضلاً عن الذكاء الإلكتروني المتطلب في التعامل مع هذا النوع من الأجهزة[3].

---

1 هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية (دراسة مقارنة)، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008، ص 23.

2 محمود محمد محمود جابر، المرجع السابقة، ص 245.

3 هلالي عبد اللاه أحمد، المرجع السابق، ص 23.

2- خـــبراء البـرمـجة:

يطلق لفظ خبراء البرمجة على مخططو البرامج والذين يكلفون بكتابة أوامر البرامج، وينقسم هؤلاء الخبراء إلى مخططو برامج التطبيقات ومخططو برامج النظم[1].

3- الـمحللون:

يتمثل المحللون في الفئة التي تعمل على تجميع بيانات نظام ما، ثم تقوم بتحليل هذا النظام، وذلك من خلال تقسيمه إلى وحدات منفصلة، واستنتاج العلاقات الوظيفية التي قد تجمع بين هذه الوحدات، كما تعمل هذه الفئة على تتبع البيانات داخل النظام في إطار ما يعرف بمخطط تدفق البيانات[2].

4- مهندسو الصيانة والاتصالات:

يدخل في هذه الفئة كل الأشخاص الذين توكل لهم أعمال الصيانة الخاصة بالهاتف النقال سواء بمكوناتها، أو شبكات الاتصال المتعلقة بها[3].

5- مديـــرو النظم:

وهم جميع الأشخاص الذين تُوكل لهم مهمة تسيير أعمال الإدارة المتعلقة بالنظام المعلوماتي[4].

ثالثاً- التــزام الشاهد المعلوماتــي بالإعلام:

من بين أهم النقاط الجوهرية التي قد تثار فيما يتعلق بالشهادة في الجريمة الإلكترونية هو التزام الشاهد بالإعلام، والذي يقصد به: "التزام الشاهد المعلوماتي حائز المعلومات الجوهرية اللازمة لاختراق نظام المعالجة الآلية للبيانات، بحثاً عن أدلة الجريمة التي تتطلبها مصلحة التحقيق والتحري، وهو مطالب بأن يُعلم بها سلطات التحقيق والتحري على سبيل الإلزام، وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك"[5].

---

1 هلالي عبد اللاه أحمد، نفس المرجع، ص 23.

2 عبد العال الديربي، ومحمد صادق إسماعيل، الجريمة الإلكترونية، ب.ط، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 323.

3 على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، ب. ط، المكتب الجامعي الحديث، الإسكندرية، 2012، ص 63.

4 مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 221.

5 هلالي عبد اللاه أحمد، المرجع السابق، ص 25.

ويتضح من خلال هذا المفهوم أن الإلتزام بالإعلام في الجرائم الإلكترونية يرتبط بامتلاك الشاهد لمعلومات، قد تكون عبارة عن شفرة أو نظام أو برنامج، ما يساعد في كشف الجريمة.

ولقد أثار الإلتزام بالإعلام جدلاً واسعاً بين من يرى ضرورة قيام الشاهد المعلوماتي بالإعلام، وبين من يرفض ذلك، تبعاً لأسباب معينة قد تحُول دون قيام الشاهد المعلوماتي بهذا الواجب، ولذلك نستعرض وجهة نظر كلا الفريقين على الشكل الآتـي:

1- الإتـجاه المـعارض:

ينطلق هذا الإتجاه من فرضية أن الالتزامات التي فرضها المشرع على الشاهد المعلوماتي لا تتضمن مثل هذا النوع من الالتزام، لذلك لا يتوجب عليه القيام بذلك[1]، بحيث لا يفرض عليه الإفصاح عن كلمة المرور التي تسمح بالولوج للنظام، كما لا يتعين عليه طباعة الملفات المسترجعة من ذاكرة نظام معلوماتي[2].

2- الإتـجاه المؤيــد:

بخلاف الاتجاه السابق، هذا الاتجاه يؤكد ضرورة الالتزام بالإعلام ويحتجون بالأسباب التالية:

- العمل على إدراج هذا المبدأ ضمن المواد القانونية المنظمة لهذا الشأن، وذلك حتى يسهل على رجال التحري والتحقيق من أداء مهامهم، وفي نفس الوقت حماية للشاهد من خرق سر المهنة[3].
- الإلتزام بالإعلام مبدأ وقائي؛ بحيث يرى البعض من أنصار هذا الاتجاه أن الالتزام بالإعلام يشكل وقاية، ويحول دون ضبط الجهاز بأكمله، أو الأجهزة الممتدة التابعة له في التفتيش والمعاينة[4].

ومن خلال ما سبق عرضه نذهب إلى ترجيح الرأي الثاني، وذلك باعتبار أن التزام الشاهد المعلوماتي بالإعلام ضروري وفعال من جميع النواحي، سواء القانونية والتي يتوجب على المكلفين بهذه

---

1 على عدنان الفيل، المرجع السابق، ص 64.

2 رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، ب. ط، المكتب الجامعي الحديث، الإسكندرية، 2018، ص 152.

3 هلالي عبد اللاه أحمد، المرجع السابق، ص 26.

4 رشاد خالد عمر، المرجع السابق، ص 152.

المهام وضع نصوص صريحة تحمي التقني والمهني، والذي قد يكشف سر من أسرار وظيفته وجب عليه كتمانه، وكذلك مساعدة المكلف بالتحري والتحقيق الذي قد يثقل بمهام كبيرة في التفتيش والمعاينة في مجال الجريمة المعلوماتية، والذي يكون واسع ومتشعب في كثير من الحالات، بالإضافة إلى تفعيل الجانب الوقائي الذي يعد ضرورة في مثل هذا النوع من الجرائم.

رابعاً– أنــواع الشهادة المتصلة بـجرائم الهاتف النقال:

هناك عدة طرق يمكن للشاهد أن يعبر من خلالها عن شهادته، نذكر من بينها:

1- الشهادة الفوريــة:

تمثل هذه الصورة أحد الأنواع الشهادة التي قد يدلي بها الشاهد، بحيث تكون هذه الشهادة بصورة فورية أمام قاضي الجلسة، وذلك عن طريق استعمال الشاهد لأحد الميزات الاتصالية الحديثة التي تتيح تواجده بشكل افتراضي، بواسطة خدمة المكالمة المرئية أو عبر خدمات الإنترنت المتصلة بالهاتف النقال، ولقيت هذا النوع من الإدلاء بالشهادة قبول لدى الفقه، وذلك على اعتبار أن الشاهد يحقق تواجد تام أمام المحكمة، وقد تكون هذه الطريقة مساعدة بشكل كبير في تفعيل حماية الشهود، ومن بين الدول التي تأخذ بهذا النوع الشهادة القضاء الأمريكي وذلك في حال ما رأى القاضي أن القضية المعروضة عليه تستلزم ذلك[1].

2- الشهادة المكتوبة كتابــة إلكترونيــة:

تعتبر هذه الصورة أحد الطرق التي قد يلجأ إليها الشاهد في الإدلاء بشهادته، وذلك عبر رسائل SMS أو E-MAIL أو BBM، وتعتبر هذه الوسيلة من الوسائل التي لم يشر إليها المشرع الجزائري في قانون الإجراءات الجزائية كوسيلة للشهادة، غير أنه يمكن أن يستعين بفحوى هذه الرسائل على اعتبار أنها مستندات، وهو ما نص عليه المشرع كاستثناء على مبدأ الشفوية بموجب المادة 2/233 من قانون الإجراءات الجزائية الجزائري[2]، وهو نفس ما ذهب إليه المشرع المصري الذي أخذ بها كاستثناء يجوز الاستعانة بها في حال ما أذنت المحكمة، أو القاضي المنتدب بذلك، وهو ما

---

1 محمود محمد محمود جابر، المرجع السابق، ص 244.

2 تنص المادة 2/233 على أن: "...غير أنه يجوز لهم بصفة استثنائية الاستعانة بمستندات بتصريح من الرئيس...".

نصت عليه المادة 90 من قانون الإثبات المصري، ويرجع ذلك إلى اعتبار أن الشفاهية أحد المبادئ الأساسية التي تقوم عليها الشهادة[1].

3- الشهادة المسجلة عــن طريــق الهاتف النقال:

تمثل هذه الصورة أحد الأشكال التي قد تصنف على أنها شهادة من خلال الهاتف النقال، بحيث تعتمد على التسجيل في وقت سابق للمحاكمة، ثم يحتفظ بهذا التسجيل إلى أن يعرض على محكمة الموضوع، والتي بدورها تعرضه على الجاني، وتواجهه بما ورد فيه، وقد يكون هذا الدليل عبارة عن تسجيل صوتي أو فيديو أو رسالة مكتوبة[2].

وعليه من خلال عرض الصور السابقة للطرق التي قد تؤدى بها الشهادة في مجال جرائم الهاتف النقال، نرى أن خصوصية هذه الجرائم، أو حتى عصرنة قطاع العدالة لمواكبة هذا النوع من الأدوات قد تفرضه ظروف معينة لجرائم يتعين حماية الشهود فيها، إلا أن هذا يجعلنا نتحفظ على قبول الصورة الثانية والثالثة بالخصوص كنوع من أنواع الشهادة، وذلك لعدة اعتبارات نوردها في الآتي:

- مخالفة شرط جوهري من شروط الشهادة؛ وهو الشفوية، والتي تساهم بشكل كبير في تكوين الاقتناع لدى القاضي.
- المناقشة: إن مناقشة الدليل تعتبر من بين الضمانات التي تفرضها المحاكمة العادلة.
- تبرير البعض للمسألة كونها استثناء نص عليه قانون الإجراءات الجزائية لا يمكن الأخذ به على الإطلاق، وحمله للقياس على هذا النوع من الصور ما لم يوجد نص صريح على ذلك.
- الخلط بين الشهادة والاعتراف، حيث نرى أن إرسال الجاني رسالة نصية، أو أن يسجل له فيديو، أو تسجيل صوتي، قد تدخل في باب الإعتراف أكثر منها الشهادة.

---

1 محمود عمر محمود، المرجع السابق، ص 164.

2 أمل فاضل عبد خشان، وأحمد حمد الله، الإثبات الجنائي في جرائم إساءة استعمال الهاتف النقال، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد الرابع، العدد الثاني عشر، ج 1، جامعة كركوك، بتاريخ: 2015/02/01، ص 332.

الـمطلب الثانـــي: الـخـبـرة في الجرائم الـمرتكبة بواسطة الهاتــف النقال.

تمثل الخبرة أحد الأساليب القضائية التي يلجأ إليها القضاء في الكشف عن الجريمة، وإثبات وقوعها ونسبتها إلى شخص، وتشغل الخبرة حيزاً كبيراً في الجرائم ذات الطبيعة العلمية والفنية، لذلك يتم اللجوء إليها بنسبة كبيرة في الجريمة المعلوماتية، ولتوضيح أحكامها فيما يتعلق بالجرائم المرتكبة بواسطة الهاتف النقال، نتطرق لمفهوم الخبرة (الفرع الأول)، ثم للخبرة التقنية (الفرع الثاني).

الـفرع الأول: مـفهوم الـــخبرة.

من خلال هذا الفرع يتم التطرق إلى تعريف الخبرة (أولاً)، والشروط المتطلبة فيها (ثانياً)، وذلك على النحو التالي:

أولاً– تعريــف الــخبرة:

تعرف الخبرة بأنها: "إبداء رأي فني من شخص مختص فنياً في شأن واقعة ذات أهمية في الدعوى الجنائية"[1]. وتعرف أيضاً بأنها: "معرفة فنية خاصة بأمور معينة تتجاوز اختصاص المحقق"[2].

يتضح من خلال هذين المفهومين أن الخبرة عبارة عن رأي يصدر من مختص في مجال من المجالات التي تتطلب دراية واسعة من الشخص المكلف، بحيث يكون المختص في متابعة الدعوى والتحقيق فيها قليل العلم والدراية في هذا المجال.

ثانياً– الضوابـط التي تحكم عملية الـخبرة:

تعتبر الخبرة من الأعمال القضائية التي ضبطها المشرع بعدة شروط، وذلك حتى يتحقق الهدف المراد منها، وسنتطرق لهذه الضوابط على الشكل الآتي:

1- نــدب الـخبــير:

تعتبر عملية ندب الخبير من بين أهم الأمور التي قام القانون بتنظيمها، حيث نجد أن القانون الجزائري نص على مثل هذا الإجراء بموجب المادة 143 من ق.إ.ج.ج، والتي نصت على أن: "لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءً على طلب النيابة العامة، وإما من تلقاء نفسها أو من الخصوم. وإذا رأى قاضي التحقيق أنه لا موجب

---

1 شريف أحمد الطباخ، الإثبات الجنائي في ضوء الفقه والقضاء، ط. الأولى، دار الفكر والقانون، المنصورة، 2015، ص 198.

2 فوزية عبد الستار، شرح قانون الإجراءات الجنائية ج 1، ط. الثانية، دار النهضة العربية، القاهرة، 2010، ص 345.

للاستجابة لطلب الخبرة فعليه، أن يصدر في ذلك أمراً مسبباً في أجل ثلاثين (30) يومًا من تاريخ استلامه الطلب. وإذا لم يبت قاضي التحقيق في الأجل المذكور، يمكن الطرف المعني إخطار غرفة الاتهام مباشرة خلال (10) أيام، ولهذه الأخيرة أجل (30) يوماً للفصل في الطلب تسري من تاريخ إخطارها. ويكون قرارها غير قابل لأي طعن. ويقوم الخبراء بأداء مهامهم تحت مراقبة قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية التي أمرت بإجراء الخبرة."

ومن خلال هذه المادة يتضح أن الخبير يتم انتدابه إما بناءً على طلب من النيابة العامة، أو جهات التحقيق، أو الحكم أو الخصوم، والملاحظ كذلك أن سلطة انتداب الخبير من عدمها أوكلها المشرع لقاضي التحقيق، الذي يجوز له البت في انتداب الخبير من عدمه في مدة لا تتجاوز (30) يوم على أن يصدر قرار مسبب في حالة الرفض، مع إمكانية إخطار المتضرر لغرفة الاتهام في حالة عدم بت قاضي التحقيق في الطلب في المدة القانونية الممنوحة له، ويمارس الخبراء مهامهم تحت رقابة قاضي التحقيق، أو أي قاضي آخر تنتدبه الجهة القضائية التي أمرت بالخبرة.

2- حــلف اليــمين:

من الشروط التي يجب على الخبير القيام بها قبل البدء في عمله أداء اليمين، وذلك في حالتين؛ الأولى أن يكون الخبير ضمن الجدول المعد مسبقاً للخبراء الذين عينهم المجلس القضائي مسبقاً، ففي هذه الحالة يُكتفى باليمين الذي أداه الخبير مسبقاً، والحالة الثانية أن يكون الخبير من خارج الجدول، ففي هذه الحالة يتعين عليه أداء اليمين قبل أداء مأموريته أمام الجهات القضائية المختصة، وهو ما نصت عليه المادة 145 من قانون الإجراءات الجزائية الجزائري[1].

---

1 تنص المادة 145 من قانون الإجراءات الجزائية الجزائري على: "يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا، أمام ذلك المجلس بالصيغة الآتي بيانها: أحلف بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال".

هذا، ولا يجدد هذا القسم ما دام الخبير مقيداً في الجدول، ويؤدي الخبير الذي يختاره من خارج الجدول قبل مباشرته مهمته اليمين السابق بيانها أمام قاضي التحقيق، أو القاضي المعين من الجهة القضائية. ويوقع على محضر أداء اليمين من القاضي المختص والخبير والكاتب."

انــظر: مصطفى مجدي هرجة، ندب الخبراء في المجالين الجنائي والمدني، ط. الأولى، دار محمود للنشر والتوزيع، القاهرة، 2016، ص 14.

3- قــرار نــدب الخبير:

يعتبر قرار ندب الخبير من أهم الشروط الشكلية التي يجب مراعاتها حتى يكون تقرير الخبرة صحيح، وغير معرض للنقض، ويشمل قرار الندب الآتــي:

أ- مــهمة الـخبير:

من أهم الشروط التي يجب أن يتضمنها قرار ندب الخبير هي المهمة المكلف بها الخبير، والتي لا يجب أن تخرج عن نطاق الأعمال التي تتطلب وجود خبرة فنية أو تقنية[1].

ب- مــهلة الإنــجاز:

من بين الشروط التي شدد عليها المشرع فيما يتعلق بالخبرة هو المهلة الممنوحة للخبير في إنجاز العمل المناط به، مع إمكانية تمديد المهلة بناءً على طلب الخبير في حال ما كانت الضرورة تستدعي ذلك، على أن يكون ذلك بقرار مسبب من القاضي، أو الجهة التي ندبتهم، وفي حال لم يسلم الخبير تقريره في الأجل المحدد يجوز أن يُستبدل بغيره، على أن يقدم كل ما توصل إليها من نتائج للأبحاث التي أشرف عليها، فضلاً عن رد جميع الأشياء، والأوراق، والوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز المهمة، وذلك في مدة لا تتجاوز ثمان وأربعون ساعة، مع إمكانية تعرضهم لعقوبات تأديبية قد تصل لحذف أسمائهم من جدول الخبراء المنصوص عليه بموجب المادة 144 من قانون الإجراءات الجزائية[2].

الـفرع الثانــي: الـخبرة التقنية فــي الـجرائم الـمرتكبة بواسطة الـهاتف النقال.

نتطرق من خلال هذا الفرع إلى الخبرة فيما يتعلق بالجرائم المرتكبة بواسطة الهاتف النقال، والدور الذي تلعبه الخبرة التقنية في الكشف على مثل هذا النوع من الجرائم، وذلك من خلال تحديد مفهوم الخبرة التقنية (أولاً)، ثم بيان الصعوبات التي تواجه الخبرة التقنية (ثانياً)، وصولاً للخبرة في مجال جرائم الهاتف النقال (ثالثاً)، فأساليب عمل الخبير التقني (رابعاً)، ختاماً بسلطة القاضي في تقدير الخبرة (خامساً).

---

1 انظر المادة 146 من ق.إ.ج.ج.

2 انظر المادتين: 144 و148 من ق.إ.ج.ج.

أولاً– تعريف الــخبرة التقنية:

تعرف الخبرة التقنية على أنها: "إبداء الرأي الفني من أحد المتخصصَين في شأن واقعة ذات أهمية في دعوى متعلقة بإحدى الجرائم الإلكترونية"[1]، وبالتالي فالخبرة الفنية لا تختلف كثيراً عن الخبرة في مختلف المجالات الأخرى في شكل أو جزء منها، إلا أنها متعلقة بالجرائم ذات الطابع الإلكتروني، وتتخذ الخبرة التقنية ثلاث صور، وذلك على النحو الآتــي:

1- الــخبرة الخاصة:

يظهر هذا الشكل من الخبرة في مظهرين أساسيين؛ الأول في ما تقوم به الشركات الكبرى الناشطة في المجال التكنولوجي من توظيف وتعاقد مع كفاءات أثبت تمكنهم من مجال الإلكتروني بمختلف أنواعه، مما يحذ ببعض الشركات إلى تعيين العصاة للقانون الذين أثبتوا مهارتهم في المجال التكنولوجي، وذلك من منطلق اقتصادي بحت، أما المظهر الثاني فيتمثل في الخبرة الخاصة الفردية والتي تشغل حيزاً كبيراً، وأثبتت مهارة عالية في الجانب التكنولوجي، سواء عن طريق التكوين أو الموهبة، وإن كانت هذه الأخيرة أكثر تحققاً بالنظر للجرائم الإلكترونية التي تحدث في الغالب، ومن فئات لا علاقة لها بالتكوين أو الدراسة في هذا المجال[2].

2- **المؤســسات التعلـيـمـية:**

يعتمد هذا النوع من الخبرة الرقمية على الكفاءات التي يتم تكوينها في المجال التكنولوجي من طرف المؤسسات التعليمية، حيث قامت عدة مؤسسات كبيرة مثل جامعة "ستانفورد"، وجامعة "كاليفورنيا" على العمل على تكوين خبراء في هذا المجال، وذلك من أجل رصد مثل هذا النوع من الجرائم، وعن طريق منهج علمي غير تجاري[3].

3- جــهات الضبط القضائي:

تظهر هذه الصورة من خلال ما عملت عليه بعض الدول المتطورة مثل الولايات المتحدة، وغيرها من الدول الغربية الأخرى، على تأسيس أجهزة أمنية متخصصة في البحث عن مثل هذا النوع من الجرائم، بحيث تكون هذه الأجهزة مدربة على مستوى عالٍ مع توفير جميع التقنيات التي

---

1 محمود محمد محمود جابر، المرجع السابق، ص 257.

2 عمر محمد بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، ب. ط، مؤسسة أدم للنشر والتوزيع، مالطا، 2008، ص 114.

3 محمود محمد محمود جابر، المرجع نفسه، ص 258.

تساعدهم على أداء مهامهم، ومن أمثلة ذلك الفرع التابع لــ FBI الأمريكي والمسمى: "المعمل الإقليمي الشرعي للحاسوب"[1].

ثانياً– الصعوبات التـي تواجــه الــخبرة التقنية:

بالرغم من التكوين العالي للخبير في مجال التقنية، إلا أنه قد يواجه عدة صعوبات في إطار الخبرة التقنية، ويمكن إجمال هذه الصعوبات في الآتـــي[2]:

- فقدان جزء كبير من المعلومات والأوامر، والتي تشكل جزء هام من التوصل للحقيقية، أو مساعدة الخبير، وذلك عند الإتلاف، أو المحو، أو غيرها من الآليات التي قد يلجأ إليها الجاني في الجرائم الإلكترونية.
- قيام الجاني بتهيئة الجهاز محل المعاينة بأدوات قابلة للتفجير بمجرد تشغيل الجهاز.
- اتساع مسرح الجريمة الإلكترونية الذي يكون في بعض الحالات متعدد بين عدة دول، مما يسبب في تعقيد الإجراءات بالنظر إلى الاختلافات الواقعة بين التشريعات في بعض الدول، فضلاً عن سرعة حركة البيانات الرقمية عبر الشبكات مع المقدرة الهائلة للمجرم المعلوماتي للتخلص من هذه البيانات.
- تعمد الجاني إخفاء هويته حتى لا يتمكن الخبير أو السلطات من التوصل إليه، وذلك عن طريق الاستعانة ببعض التطبيقات والبرامج المخصصة لذلك.
- إخفاء المعلومات: إذ من الأساليب الأخرى التي يعمل الجناة في الجريمة الإلكترونية إلى الاستعانة بها هي إخفاء المعلومات، وذلك عن طريق استخدام بعض البرامج، والتطبيقات التي تساعد على إيجاد ملفات آمنة عبر استخدام الشبكة العالمية، مما يجعل العمل على استعادة هذه الملفات أو إعادة تركيبها مهمة صعبة أمام المحقق والخبير.

ثالـثاً– الــخبرة فـي مجال جرائم الهاتف النقال:

ينطبق على الخبرة في مجال الهاتف النقال نفس المعيار الذي ينطبق على الخبرة في الجريمة الإلكترونية، إلا أن الخبير عليه أن يراعي المسائل التقنية الآتــية:

---

1 عمر محمد بن يونس، المرجع السابق، ص 117.

2 حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط. الأولى، دار النهضة الغربية، القاهرة، 2017، ص 66-67.

1- أن يكون الخبير على دراية كبيرة بالهواتف النقالة من حيث النوعية والصناعة ونظام التشغيل الرئيسي والفرعي، فضلاً عن كلمات المرور والتشفير، وغيرها من البيانات الأخرى التي تساعده على أداء مهامه[1].

2- القيام بتقديم وصف لطبيعة الهاتف النقال والشبكة، وذلك من حيث تنظيم ومدى تركيز أو توزيع المعالجة الآلية، فضلاً عن تقديم وصف لنمط وسائل الإتصالات، وتردد موجات البث، وأمكنة اختراقها، مع الإشارة إلى المَواطن التي قد تتواجد فيها الأدلة والشكل والهيئة الذي قد تكون عليه[2].

3- على الخبير نقل الأدلة المستخلصة من الهاتف النقال بصورة غير مرئية إلى شكل مرئي دون أن يلحق أي ضرر بذلك الجهاز[3].

4- العمل على عزل النظام المعلوماتي للهاتف دون أن يشكل ذلك أي ضرر على الهاتف[4].

رابعاً- أساليب عمل الخبير التقني:

يعتبر أسلوب تعامل الخبير التقني مع الهاتف النقال هو المحدد الرئيس لمعيار نجاحه في الكشف عن الأدلة الجنائية التي يتوفر عليها هذا الهاتف، وتنقسم هذا الأساليب إلى نوعين يتمثلان في:

- الأسلوب الأول: التحلـــيل الرقمي للهاتف النقال.

يقوم هذا الأسلوب على تحليل جرائم الهاتف النقل معتمداً على "كارت سيم" الملحقة بالهاتف النقال، وذلك من خلال عمل تحليل عام لجميع الاتصالات والرسائل والأرقام التي تواصل معها الجاني أو التي تم حذفها، فضلاً عن تحليل الأرقام السرية للبطاقة (كود PIN وPUK)، ومعرفة إذا ما تم التلاعب بها، وفي الغالب ما يتم استخدام هذا الأسلوب في جرائم التهديد المرتكبة بواسطة الهاتف النقال، فضلاً عن تحليل كارت سيم قد يلجأ الخبير إلى تحليل ذاكرة الهاتف النقال، والتي تحتوي في أغلب الأحيان على أسرار كثيرة قد تتعلق بالجريمة، أو حتى بالجاني سواء عن طريق الصور أو

---

1 أمل فاضل عبد خشان، أحمد حمد الله، المرجع السابق، ص 337.

2 ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة مقدمة استكمالًا لمتطلبات الماجستير تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الموسم الجامعي: 2011-2012، ص 112.

3 ثنيان ناصر آل ثنيان، المرجع نفسه، ص 337.

4 محمود محمد محمود جابر، المرجع السابق، ص 259.

الفيديوهات، والتسجيلات التي قد يحتوي عليها الجهاز، وهناك العديد من البرامج التي قد تساعد على استرجاع هذه الملفات[1].

– الأسلوب الثانــي: تتبع المواقع الإلكترونية التي تشكل جزءاً مــن الجريـمة الـمرتكبة بواسطة الهاتف النقال.

يمثل هذا الأسلوب طريقة غير مباشرة للكشف عن الجرائم المرتكبة بواسطة الهاتف النقال، كأن يقوم الخبير بتتبع حركة بروتوكول IP لموقع إلكتروني معين، ثم يتوصل إلى الهاتف النقال الذي ارتكبت الجريمة من خلاله[2].

خامساً– سلطة القاضي فــي تقدير الـخبرة:

بالرغم من اليقين العلمي التام الذي قد تقوم عليه الخبرة فيما يصل إليه الخبير من نتائج، إلا أن سلطة القاضي أو المحكمة تبقى هي السلطة الأخيرة في تحديد مدى قبولها لهذا الدليل من عدمه، ذلك أن للقاضي كل السلطة التقديرية بأن يأخذ منها ما يشاء ويطرح ما يشاء، شأنها شأن الأدلة الأخرى، وهذا ما نص عليه المشرع الجزائري بموجب المادة 212 من ق.إ.ج.ج، والتي جاء فيها: "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعًا لاقتناعه الخاص".

وفي نفس الإتجاه ذهبت محكمة النقض المصرية والتي قررت: "محكمة الموضوع هي الخبير الأعلى في كل ما يستدعي خبرة فنية"، وقررت أيضاً: "رأي الخبير الاستشاري للمحقق أو المحكمة إن شاء أخذ به وإن شاء طرحه جانباً"[3].

---

1 طارق عفيفي صادق أحمد، المرجع السابق، ص 268؛ **وانظر كذلك:** محمود محمد محمود جابر، المرجع نفسه، ص 260.

2 طارق عفيفي صادق أحمد، المرجع نفسه، ص 268.

3 **نقلاً عــن:** محمود عمر محمود، المرجع السابق، ص 202.

المبحث الثاني:

الـــدليل الإلكـــتروني.

يمثل الدليل الإلكتروني أحد أهم الأدوات التي يعتمد عليها في البحث والتحقيق في الجرائم ذات الطابع الإلكتروني، ويرجع ذلك في الأساس إلى خصوصية الجريمة المرتكبة في الوسط الافتراضي سواء بواسطة جهاز الحاسب الآلي، أو الهاتف النقال.

لذلك ونظراً لأهمية هذا الدليل الإلكتروني؛ يتم التطرق لتحديد مفهومه (المطلب الأول)، ثم بيان أنواع الأدلة الإلكترونية المستمدة من الهاتف النقال (المطلب الثاني)، وصولاً لحجية الدليل الإلكتروني (المطلب الثالث).

المطلب الأول: مفهوم الدلـــيل الإلكترونـــي.

يطلق على الدليل الإلكتروني العديد من التسميات، وهي تصب في نفس المفهوم؛ منها "الدليل التقني"، و"الدليل الرقمي"، ولذلك عندما نتكلم عن مفهوم الدليل الإلكتروني فإننا نقصد المفهوم الشامل الذي تندرج تحته كل هذه المفاهيم.

لذلك، يتم التطرق من خلال هذا المطلب لتعريف الدليل الإلكتروني (الفرع الأول)، وكذا لخصائص الدليل الإلكتروني (الفرع الثاني).

الـفرع الأول: تعريف الدليل الإلكترونـــي.

هناك العديد من المفاهيم الفقهية للدليل الإلكتروني والتي سوف نقف على البعض منها مع التعليق، ومن بين هذه المفاهيم يرى البعض[1] بأن الدليل الإلكتروني هو: "ذلك الدليل الذي يجد أساسًا له في العالم الافتراضي ويقود إلى الجريمة، فهو كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني، بحيث تمكن الحاسوب من إنجاز مهمة ما".

ويتضح من خلال هذا التعريف أنه كيّـف الدليل الإلكتروني على أنه الدليل المستمد من الجرائم التي تقع في الأماكن الافتراضية، والذي يعتمد على البيانات والمعلومات التي تم إعدادها من أجل التخزين في جهاز الحاسب الآلي، ويعتبر هذا الأمر من بين أهم الانتقادات التي يمكن أن توجه لهذا

---

1 عمر محمد بن يونس ،المرجع السابق، ص 25، وانظر كذلك: خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط. الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 229.

التعريف، بحيث لا يمكن حصر الدليل الإلكتروني في الوسائل المادية والمعنوية المستمدة من جهاز الحاسب الآلي فقط، بحيث يشمل كذلك الأدلة المستمدة من آلة التصوير الرقمية، والهاتف النقال، وخاصة الهاتف الذكي الذي يمتاز بكل المواصفات التي يمتاز بها الحاسوب.

من جانب آخر هناك من يرى بأن الدليل الإلكتروني هو: "الدليل المأخوذ من أجهزة الكمبيوتر بحيث يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجمعيها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة، مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون"[1].

إن ما يُستنتج من هذا التعريف أنه حاول تقديم شرح وافٍ للدليل الإلكتروني، وذلك من خلال وصف الآليات التي يكون عليها هذا الدليل، والذي يظهر في شكل نبضات مغناطيسية أو كهربائية، والتي يتم جمعها وتحليلها عن طريق تطبيقات معد خصيصًا لهذه المهام ليظهر بعدها في عدة مخرجات مختلفة. ولا يسلم هذا التعريف من النقد الموجه للتعريف السابق، بحيث حَصر كذلك الدليل الرقمي في الدليل المستمد من جهاز الكمبيوتر فقط.

وبين هذا وذاك، يرى البعض الآخر بأن الدليل الإلكتروني هو: "ذلك الدليل الذي يتكون من بيانات ومعلومات الكترونية غير ملموسة، ويتطلب إدراكها الاستعانة بأجهزة وبرامج معينة، ويقدم معلومات في شكل نصوص مكتوبة أو صور أو أصوات، أو أشكال أو رسوم، عن طريق ترجمة البيانات الرقمية المخزنة في أجهزة الكومبيوتر وشبكات الاتصال، لإثبات واقعة معينة ونسبتها إلى شخص معين"[2].

---

1 على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول لأكاديمية شرطة دبي المنعقد في الفترة 26-4 إلى 28-4-2003، ص 259؛ **وانـــظر كذلك**: أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها (دراسة مقارنة للتشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2016، ص 287.

2 بهاء المري، المرجع السابق، ص 396.

إن المفهوم الأخير عمل على تعريف الدليل الإلكتروني من خلال التركيز على آليات عمل الدليل الإلكتروني، بالإضافة إلى عرض الأشكال التي قد يظهر من خلالها، مع إضافة بسيطة؛ وهي إضافة عنصر شبكات الاتصال، واعتبارها كأحد الأدوات التي يُستمد منها الدليل الإلكتروني.

ومن خلال ما سبق يمكننا أن نعرف الدليل الإلكتروني على أنه جميع المعلومات المستمدة من العالم الافتراضي، والتي تدل على وقوع جريمة ونسبتها لشخص ما، سواء تم الحصول عليها عن طريق المعلومات والبيانات المخزنة في الهاتف النقال أو الحاسب الآلي، أو الكاميرا الرقمية.

الـفرع الثانـي: خصائص الدلـيل الإلكـترونـي.

يمتاز الدليل الإلكتروني بالعديد من الخصائص، والتي تجعله يختلف عن الدليل التقليدي وتتمثل هذه الخصائص في الآتــي:

أولاً– الدلـيل الإلكترونــي دليل علمي:

من أهم الميزات التي يتمتع بها الدليل الإلكتروني هو كونه دليل علمي، وهذا يرجع إلى الأساس الذي يقوم عليه هذا الدليل، والواقعة الإجرامية التي يهدف إلى إثبات وقوعها، وتظهر هذه الخاصية من خلال العوامل الآتية:[1]

– الجريمة المراد إثباتها جريمة افتراضية تحكمها بيئة المعلومات والبيانات، والتي تتميز بالتطور والتعدد.

– الحصول على هذا النوع من الأدلة لا يمكن إلا عن طريق استخدام الأدوات العلمية التي يجب أن تحقق نتائج مطابقة مع الحقيقة، على اعتبار العلم مسعاه الحقيقة.

– مسألة حفظ الدليل تعتبر من أهم الميزات التي تثير الجانب المتعلق بالصفة العلمية المتعلقة بهذا الدليل، والتي يراعى فيها الجانب الفني والتقني، والذي يحافظ على سلامة الدليل من الإتلاف.

ثانياً– الدلـيل الإلكترونــي ذو طبـيعة معنويــة:

من أهم الميزات التي يتميز بها الدليل الإلكتروني هو كونه دليل ذو طبيعة معنوية، ويرجع ذلك إلى المجال الذي يستمد منه هذا الدليل، والذي يظهر في شكل موجات مغناطيسية وكهربائية، والتي تترجم بعدها في شكل مادي ملموس[2].

---

1 حازم محمد حنفي، المرجع السابق ، ص 16-17.

2 خالد عياد الحلبي، المرجع السابق، ص 231.

ثالثاً– الدلــيل الإلكترونــي دليل تقني:

تبعاً لخاصية العلم الثابت بمجال لا يقبل النفي فيما يتعلق بالدليل الإلكتروني، فهذا يثبت خاصية أخرى تعتبر تابعة لصفة العلم وهي صفة التقنية، ويفرض هذه الخاصية صفة الآلة المتعامل معها في البحث عن الدليل، سواء كان الهاتف النقال، أو جهاز الحاسب الآلي، فتركيبة هذه النوع من الأجهزة يجب أن يتعامل معه بمنطقها وتركيبتها، وهذا يستدعي وجود سلطات في الضبط والتحقيق تكون على دراية بهذا النوع من الآلات، وذلك بعيدًا عن الخبرة[1]، ويبنى على هذه الصفة توفر الضوابط التالية في الدليل الإلكتروني:

- وجود توافق بين الدليل المتحصل عليه، والبيئة المستمدة منها بطريقة لا تقبل التضاد.
- العمل على تطوير الأدوات التي يتم من خلالها البحث عن هذه الأدلة، وذلك من أجل مواكبة التطور المستمر في التقنيات الحديثة[2].

رابعاً– الدليل الإلكترونــي يصعب التــخلص منه:

لعل من بين أهم الميزات التي يتمتع بها الدليل الإلكتروني بالمقارنة مع الدليل التقليدي هي صعوبة التخلص منه، ويرجع ذلك للأسباب التاليــة:

1- صعوبــة مـحو الدليل الإلكتروني:

لعل نظام التخزين والحماية الذي تتمتع به الوسائل الإلكترونية تجعل من مهمة محو المعلومات المخزنة فيها صعبة في بعض الحالات، مع إمكانية استرجاع هذه المعلومات.

2- إمكانية إظهاره بــعد إخفائــه:

نظراً للتطور التقني في مجال الثورة المعلوماتية هناك العديد من التطبيقات التي تتيح فرصة إعادة كافة الملفات والمعلومات المخزنة سواء في الهاتف النقال، أو جهاز الحاسب الآلــي[1].

---

1 عمر محمد بن يونس، المرجع السابق، ص 43.

2 من الأمثلة التي نضربها في هذا الصدد هو ما تعمل عليه بعض الدول الغربية مثل الولايات المتحدة الأمريكية وألمانيا، التي عملت على إيجاد عناصر في مرحلة الاستدلال والتحقيق يتمتعون بخبرة عالية في مجال التقنية، وفي هذا فصل بين الخبرة وبين هذه السلطات، وذلك بالاعتماد على معيار التكوين في التعيين في مثل هذه المناصب، وهو ما أسهم بشكل كبير في مساعدة هذه الفئات في كل من الولايات المتحدة الأمريكية وألمانيا في تطوير تكنولوجيا المعلومات، **للمزيــد انــظر**: عمر محمد بن يونس، نفس المرجع، ص 43.

خامساً– الدليل الإلكترونـــي دليل متنوع ومتطور:

يفهم من هذه الخاصية أن الدليل الرقمي متنوع القنوات والمصادر، بحيث يمكن أن يظهر في شكل بيانات غير مقروءة، أو أن يظهر في شكل ملفات معدة بنظام المعالجة الآلية للكلمات، أو عن طريق البريد الإلكتروني، أو عن طريق عمليات التشفير التي قد تستخدم للحد من عمليات العدوان على حقوق المؤلف، وغيرها من العمليات الأخرى[2].

سادساً– الدليل الإلكتروني قابل للنسخ:

من بين الخصائص التي يمتاز بها الدليل الإلكتروني هي المقدرة على نسخ هذا الدليل، وذلك بميزات تتيح نفس الموصفات الأصلية للدليل الحقيقي، وهذا ما لا يتوفر في الدليل التقليدي، وتشكل هذه الخاصية ضمانة ذات فاعلية ضد تلف أو فقدان الدليل[3].

سابعاً– تقديــم معلومات عن الجانــي:

بالمقارنة بالأدلة المادية نجد أن الدليل الإلكتروني له مقدرة كبيرة على تقديم صورة واضحة عن الجاني، ويظهر هذا في بعض العلامات ذات الدلالة العامة التي قد تساعد في الكشف عن هوية الجاني، بحيث يساعد الدليل الإلكتروني في بعض الحالات على تسجيل حركات الفرد، وهذا يتضح جلياً في خدمات الموقع التي تقدمها الهواتف الذكية أو بعض مواقع التواصل الاجتماعي[4].

ثامناً– الدليل الإلكترونــي ذا طابع ديـناميكي:

من بين أهم الميزات التي يتمتع بها الدليل الإلكتروني هو مقدرته على الانتشار بسرعة فائقة عابراً عائق الزمان والمكان، ويظهر هذا جلياً في جرائم نشر الفيروسات والمواد الإباحية عبر البلوتوث أو الإنترنت، أو غيرها من وسائل التواصل الأخرى[5].

---

1 عذارى سعود عبد المحسن، الضبط والتفتيش في جرائم الحاسب الآلي، رسالة مقدمة لنيل الماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2016، ص 12؛ **وانظر:** فؤاد أمين السيد، مرجع سابق، ص 112؛ **انــظر أيضاً:** نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي–دراسة تحليلية– مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد 1، العدد 19، جامعة تكريت، 2013، ص 186.

2 حازم محمد حنفي، المرجع السابق، ص 20.

3 عذارى سعود عبد المحسن، المرجع السابق، ص 25.

4 عذارى سعود عبد المحسن، نفس المرجع، ص 25.

5 طارق عفيفي صادق أحمد، نظرية الحق، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2016، ص 310.

الفرع الثالث: معيقـــات اكتشاف الدليل الإلكترونـــي.

بالرغم من الميزات التي يتمتع بها الدليل الإلكتروني بالمقارنة بالدليل التقليدي، إلا أن عملية اكتشاف الدليل الإلكتروني قد تعترضها عدة معيقات تحول دون اكتشافه، لذلك نتطرق من خلال هذا الفرع أهم المعيقات التي قد تحول دون اكتشاف هذا الدليل، بدءاً بالصعوبات المتعلقة بالجاني (أولاً)، ثم انتحال الصفة الإفتراضية (ثانياً)، ثم الطبيعة العالمية للجريمة الإلكترونية (ثالثاً)، وكذا غياب الخبرة الكافية في التعامل مع الدليل الإلكتروني من طرف السلطات المختصة (رابعاً)، وختاماً بضخامة حجم البيانات الإلكترونية (خامساً)، وذلك على النحو الآتي:

أولاً– صعـوبات مـتعلقـة بالجانـي:

كما أوردنا في الباب الأول من هذه الدراسة، فالمجرم المعلوماتي يتميز بذكاء كبير ومهارة عالية في التكنولوجيات الحديثة، ومعرفة كل التقنيات المتعلقة بها، فهذه الصفات التي يتميز بها المجرم المعلوماتي قد تحول دون التوصل إلى اكتشاف الجريمة، فضلاً عن التوصل إلى دليل يثبت ارتكابها، فأول شيء يفكر فيه المجرم المعلوماتي بعد ارتكاب جريمته هو التخلص من الدليل؛ سواء عن طريق المحو أو الإتلاف، وهذا أمر ميسر في مثل هذا النوع من الجرائم، ومن أمثلة هذه الحالة؛ قيام أحد الجناة من مهربي الأسلحة في دولة النمسا، والذي عمد إلى إدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة الإلكترونية، والذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه، بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة مفاتيحه محو وتدمير كافة البيانات[1].

ثانياً– انـتحال صفـة الإفـتراضـية:

من أبرز المعيقات التي تحول دون كشف المجرم في الجرائم الإلكترونية أو الوصول إلى دليل ما، هو لجوء مرتكبي هذا النوع من الجرائم إلى انتحال شخصيات وهمية تساعدهم على التخفي، وارتكاب أفعالهم الإجرامية بمنأى عن دراية السلطات المعنية بمكافحة مثل هذا النوع من الجرائم[2].

---

1 علي عدنان الفيل، المرجع السابق، ص 80.

2 طارق عفيفي صادق أحمد، المرجع السابق، ص 279.

ثالثاً– صفـة العالـمية فــي الجريـمة الإلكترونية:

من بين الميزات التي تتميز بها الجريمة المعلوماتية هو كونها جريمة ذات طبيعة عالمية عابرة للحدود، مما قد يشكل عوائق قانونية تحول دون التمكن من تتبع هذه الجريمة، وتتبع الجناة الذين قاموا بارتكابها[1]، خاصة في حال عدم وجود اتفاقيات تقضي بتبادل المعلومات والمساعدة القضائية بين الدولة المعتدى عليه، والدولة مرتكبة الجريمة، مما يجعلنا في هذه الحالة ننبه إلى ضرورة تفعيل المساعدة الأمنية والقضائية بين جميع الدول، فيما يخص مثل هذا النوع من الجرائم.

رابعاً– غـياب الخبرة الكافية في التعامل مع الدليل الإلكتروني من طرف السلطات المختصة:

من بين أهم الصعوبات التي تحول دون اكتشاف الجريمة المرتكبة بواسطة الأدوات التكنولوجية الحديثة، وهو عدم وجود أشخاص ذو مؤهل عالي، وقدرة عالية في التحكم في الأدوات التكنولوجية سواء في مرحلة الاستدلال أو مرحلة التحقيق[2]، وإن كنا نلمس في السنوات الأخيرة الاهتمام الكبير من السلطات في السعي إلى اكتساب معرفة بهذا النوع من الأدوات، من خلال تفاعل هذه السلطات مع الملتقيات والندوات التي تنعقد على مستوى مؤسسات التعليم العالي، فضلاً عن التكوينات الخارجية التي تحرص الدولة على إمداد مثل هذه الفئات بها.

خامساً– ضخامــة حـجم البـيانات:

ومن بين الصعوبات الأخرى كذلك التي تحول دون التوصل إلى الأدلة في مثل هذا النوع من الجرائم، هو حجم المعلومات محل الفحص، والذي قد يتطلب وقتاً كبيراً في الوصول إليه، مما يجعل العمل عليه صعب ومرهق سواءٌ في مرحلة جمع الإستدلالات أو التحقيق[3].

الـمطلب الثانـي: أنواع الأدلــة الإلكترونيــة المستمدة من الـهاتف النقال.

إن الهاتف النقال بما يتمتع به من قدرات تكنولوجية عالية أدى إلى المساعدة في ارتكاب جرائم إلكترونية عديدة، مما يستدعي أن يستخرج الدليل من خلاله، لذلك ومن خلال هذا المطلب

---

1 عبد الناصر محمد محمود فرغلي، ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية – دراسة تطبيقية مقارنة–، مداخلة مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد 12-2007/11/14، جامعة نايف للعلوم الأمنية، الرياض، ص 10.

2 جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، العدد 12، جامعة ذي قار، 2016، ص 21.

3 صغير يوسف، المرجع السابق، ص 129.

نتطرق لأهم الأدلة التي يمكن استنباطها من خلال الهاتف النقال، بدءاً بالدليل الناتج عن فحص مسار وبروتوكول الهاتف النقال (الفرع الأول)، ثم الدليل الناتج عن النظام المادي والمعلوماتي للهاتف النقال (الفرع الثاني).

الــفرع الأول: الدلـيل الناتــج عن فحص مسار وبروتوكول الــهاتف النــقال.

إن ربط الهاتف النقال بشبكة الإتصال وشبكة الانترنت ساعد بشكل كبير في تقصي الجرائم التي قد تركب بواسطة الهاتف النقال، وذلك عن طريق الاستعانة بهذه الوسائل في التوصل إلى الدلائل التي تثبت ارتكاب الجريمة ومرتكبها.

ونظراً لأهمية هذه الوسائل، نتطرق في هذا الفرع للدليل الإلكتروني الناتج عن فحص مسار الإنترنت (أولاً)، ثم الدليل الإلكتروني الناتج عن فحص بروتوكول الأنترنت (ثانياً).

أولاً– الدلـيل الإلكترونــي الناتج عن فحص مسار الأنترنـت:

يعرف مسار الإنترنت على أنه الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فالهاتف النقال بمجرد أن يتعرف على المسار يقوم تلقائياً باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وتتم عملية تتبع مسار الإنترنت عن طريق نظام الفحص الإلكتروني، والذي يعرف بعلم البصمات المعاصرة، والذي يعمل على تتبع الحركة العكسية لمسارات الإنترنت.

جدير بالذكر أن هناك اختلاف فيما يتعلق بقبول هذه الرأي من عدمه، فيذهب البعض[1] إلى إنكار إمكانية تحديد مسار الجريمة، باعتبار أن الإنترنت مرنة بطبيعتها، ولو افترضنا وقوع ذلك، فهذا الدليل سوف يكون قاصراً على أن يكون أداة للإثبات لوحده باعتبار أنه سوف يحتاج إلى أدلة أخرى تؤيده، كما أن في حال التوصل إلى هذا الدليل إنما يتوصل إلى عنوان IP[2]، وهذا لا يمكن الأخذ به كدليل تام يكفي لنسبة الجريمة لهذا الشخص، إذن قد يكون الهاتف مسروق أو استعمال الإنترنت مسروق أو مؤجر، ويذهب الرأي الثاني إلى إمكانية تتبع مسار الإنترنت، وبالتالي إمكانية

---

1 عمر محمد بن يونس، المرجع السابق، ص 63.

2 يعرف IP بأنه عنوان رقمي مميز خاص بكل جهاز اتصال عند اتصاله بشبكة الإنترنت – سواء كان هذا الجهاز حاسب آلي أو خادم هاتف محمول، راوتر، طابعة– بحيث لا يمكن أن يتكرر هذا العنوان الرقمي في أي وقت على أكثر من جهاز واحد مطلقاً. **للمزيــد انظر:** حازم محمد حفني، المرجع السابق، ص 86.

التوصل من خلاله إلى مرتكب الفعل الإجرامي، وتزعمت هذا الرأي محكمة باريس، ولها العديد من الأحكام التي تؤيد هذه الوجه مثل قضية الموقع ياهو (Yahoo)[1].

ثانياً– الدليـل الإلكترونـي الناتـج عـن فحص بروتوكول الأنترنت:

من العمليات التقنية التي يعتمد عليها في البحث عن الدليل الإلكتروني، هو ما يعرف بروتوكول الإنترنت، أو رقم الهاتف النقال، حيث يتيح بروتوكول الإنترنت الحرية لأي شخص إمكانية الولوج للإنترنت، والاستفادة من خدماتها والتنقل بين المواقع التي تتوفر فيها كما يشاء، وتتم عملية البحث في قواعد البيانات المسجلة على بروتوكول الإنترنت ليست بالأمر الصعب، بحيث يمكن لأي شخص القيام بذلك عن طريق البحث في قواعد البيانات الخاصة بالمسجلين[2].

---

1 هي عبارة عن قضية تم عرضها على محكمة باريس في شهر أبريل من سنة 2000، وتتلخص وقائعها في أن الموقع الشهير ياهو (Yahoo) قام بنشر وإجراء مزاد لكل المواد والمستحضرات (أفلام، ملابس، خناجر، رسومات، ميداليات) المتعلقة بالفترة النازية في ألمانيا، فضلاً عن نشر صور للزعيم النازي أدلف هتلر ولبعض الشعارات النازية، وهو ما دفع بعض الطلبة اليهود ممثلين في اتحاد الطلبة اليهود في فرنسا، في إقامة دعوى ضد هذه الشركة على أساس قيام هذه الأخيرة من التقليل من محرقة الهولوكوست، وطلب اتحاد الطلاب اليهود من المحكمة أن تقوم "ياهو" بإزالة كل هذه المواد من موقعها في فرنسا، إلا أن الشركة دفعت بعدم اختصاص القضاء الفرنسي بهذه الدعوى باعتبار أن شركة "ياهو" تحمل الجنسية الأمريكية، لكن اتحاد الطلبة الفرنسي عمل على متابعة "ياهو" الفرنسية من أجل منع الشركة الأم من الدفع بالجنسية الأم للشركة، مما جعل القضاء الفرنسي يحكم باختصاص القضاء الفرنسي بهذه القضية، إلا أن الشركة عادت ودفعت بأنها لم تكن تنوي تعظيم النازية، أو دعم المعتقدات التي تدعو إليها عن طريق ما تتم نشره على الموقع الخاص بها، كما أقرت بأنها لا تقدم أي دعم للولوج لمثل هذه الموضوعات غير المشروعة، إلا أن هذا لم يمنع القضاء الفرنسي من إصدار حكم يقضي بمنع كل ملفات الإنترنت الفرنسية التي تمكن من الولوج إلى خدمات المزاد التي تقدم هذه الخدمات المتعلقة بالفترة النازية، كما أمر القضاء بإزالة الرابط التصفحي المتعلق بياهو العالمية، وبث تحذيرات عبر ملفات "ياهو" فرنسا حول أنشطة "ياهو" العالمية غير المشروعة، فضلاً عما سبق أمر كذلك القضاء الفرنسي شركة "ياهو" بفرعها الفرنسي والعالمي بدفع عشرة الآلف فرنك فرنسي لكل من ليكرا واتحاد الطلبة اليهود، إلا أن القضاء الفرنسي لم يحدد الطريقة التي يتوجب على موقع "ياهو" إزالة هذه الملفات بها، إلا أن شركة "ياهو" دفعت بعدم تنفيذ الحكم بشقه التقني باعتبار عدم وجود برامج وآليات تساعد على ذلك، مما دفع الإدعاء باتهام "ياهو" بعدم تنفيذ قرار المحكمة، وطلب من القضاء بتشكيل لجنة من الخبراء للبث في إمكانية التخلص من الملفات من عدمه، وهو ما استجاب له القضاء بتاريخ 11 أغسطس 2000، حيث تم تشكيل لجنة من جنسيات مختلفة متخصصة في المجال التقني، وفي 6 من نوفمبر 2000 أصدرت لجنة الخبراء تقريرها النهائي بإمكانية القيام بتنفيذ الحكم، وبوجود تقنيات تسمح بمنع مستخدمي الانترنت في فرنسا من الولوج لهذا الموقع، كما قررت لجنة الخبراء أن استخدام وسائل الفلترة أو التصفية يمكن أن يحقق الهدف بنسبة 80 %، وفي تاريخ 20 من نوفمبر 2000 أصدر القضاء الفرنسي حكمه بإلزام موقع "ياهو" بفلترة مسارها، لكي لا يتم بث ما يمكن أن يتعارض مع القانون الجنائي. **انـــظر في ذلك:** محمود عمر محمود، المرجع السابق، ص 205.

2 عمر محمد بن يونس، المرجع السابق، ص 69.

الــفرع الثانــي: الدلــيل الناتــج عـن النظام الـمادي والـمعلوماتــي للهاتف النقال.

من الميزات التي يوفرها الهاتف النقال هو إمكانية استخلاص أدلة النفي أو الإثبات من خلال الهاتف ذاته، وذلك عن طريق التركيبة المادية له، أو عن طريق النظام المعلوماتي الذي يشغل هذا الهاتف، وهذا ما يتم التطرق له تبعاً من خلال دراسة الدليل الناتج عن النظام المادي للهاتف النقال (أولاً)، ثم دراسة الدليل الناتج عن النظام المعلوماتي للهاتف النقال (ثانياً).

أولاً– الدلــيل الناتــج عن النظام الـمادي للهاتف النقال:

سبق وأن تم التطرق في هذه الدراسة إلى الجوانب المادية للهاتف النقال، والتي تتمثل في العناصر الملموسة للهاتف كالكاميرا، والشاشة والبطارية، والسماعة، وبطاقة الذاكرة، وغيرها من الوسائل الأخرى، فهذه الوسائل يمكن أن تكون مصدر لدليل ينفي أو يثبت واقعة إجرامية تم فيها استخدام الهاتف النقال لارتكابها، ولعل بطاقة الذاكرة من بين أهم هذه الوسائل التي يمكن أن يتم الحصول منها على معلومات، باعتبار أن معظم الملفات المصورة والمكتوبة توجد على مستوى هذه البطاقة[1].

ثانياً– الدلــيل الناتج عن النظام الـمعلوماتــي للهاتف النـقال:

تتم هذه العملية عن طريق فحص النظام المعلوماتي للهاتف النقال، واسترداد كافة المعلومات التي يحتوي عليها، والقيام بضبطها على أن تكون هذه المعلومات مخزنة في File بغض النظر عن الحالة التي تكون عليها، وعلى شرط أن تكون هذه المعلومات محل جريمة، ويعتمد تخزين هذه المعلومات على عدة طرق، منها ما يعرف بالتشفير، أو نظام إخفاء المعلومات[2].

الـمطلب الثالث: حـجيــة الدلــيل الإلكترونــي.

بالرغم من الدور الكبير الذي يلعبه الدليل الإلكتروني في الإثبات إلا أن هذا لا يجعله استثناء عن باقي الأدلة الأخرى، حيث يخضع الدليل الإلكتروني لنفس الآليات التي تخضع لها الأدلة التقليدية، ولتوضيح هذا الأمر نتطرق من خلال هذا المطلب إلى شروط قبول الدليل الإلكتروني (الفرع الأول)، ثم نتطرق بعد ذلك إلى سلطة القاضي في تقدير الدليل الإلكتروني (الفرع الثاني).

---

1 أمل فاضل عبد خشان، أحمد حمد الله، المرجع السابق، ص 355.

2 محمود عمر محمود، المرجع السابق، ص 206.

الـفرع الأول: شروط قبـول الدليل الإلكترونــي.

إن معيار قبول الدليل الإلكتروني كأداة لإثبات أو نفي جريمة ما، يخضع لشروط معينة يجب أن تتوفر حين استخلاص هذا الدليل، وإلا كان باطلًا، وتتمثل هذه الشروط في مشروعية الدليل الإلكتروني (أولاً)، ثم مناقشة هذا الدليل (ثانياً)، على ألا يكون هذا الدليل قائماً على التخمين والظن (ثالثاً).

أولاً– مشروعية الدليل الإلكترونــي:

تستلزم مشروعية الدليل الإلكتروني النظر إليه من ناحيتين؛ ناحية الوجود، وناحية التحصيل، وتفصيل ذلك على النحو الآتــي:

1- **مشروعية الوجود:** تعني مشروعية الوجود أن يكون هذا الدليل معترف به من الناحية القانونية ومسموح للقاضي أن يستند إليه في أحكامه، والتي تصدر عنه في مثل هذه القضايا التي تحتاج مثل هذا الدليل[1].

2- **مشروعية الحصول على الدليل:** ويقصد بمشروعية الحصول على الدليل الإلكتروني أن تتم عملية البحث عنه من طرف السلطات المختصة، وبطريقة قانونية وقفاً للقواعد والإجراءات المعدَّة لذلك[2]، إذ يجب أن يكون هذا الدليل صادقاً في مضمونه، فضلاً عن التوصل إليه بطريقة سليمة ونزيهة[3].

---

1 صابرين يوسف عبدالله، دور الأدلة المرئية في الإثبات الجزائي، مجلة كلية الحقوق، المجلد 19، العدد الثاني، جامعة النهرين، العراق، 2017، ص 264.

2 براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري –تيزي وزو، الموسم الجامعي: 2018/2017، ص 144.

3 هناك العديد من القضايا التي استند فيها القضاء إلى دليل إلكتروني؛ ومن أمثلتها قضية اشتهرت باسم "عماد الكبير" وهي عبارة عن قضية تتلخص وقائعها في قيام ضابط مباحث من قسم بولاق الدكرور في مصر بتاريخ: 20 يناير من العام 2006 بتعذيب وهتك عرض "عماد الكبير"، وذلك من أجل أن يجبره على الإعتراف بجرم ما، ثم قام بعدها بتصويره بكاميرا تليفون محمول لتكون وسيلة ضغط عليه من أجل فضحه أمام زملائه السائقين، ولكن تم تسريب الفيديو وتم تبادله بين العامة عبر تقنية البلوتوث على هواتفهم المحمولة، ما أدى إلى نشر القضية بواسطة إحدى الصحف، ليقدم الفيديو بعدها إلى جهات التحقيق، وإحالة ضابط الشرطة إلى محكمة الجنايات، والتي اطمأنت إلى الدليل الإلكتروني المقدم إليها، وقضت بمعاقبة المتهم بالسجن لمدة ثلاث سنوات. **للمزيـد انظر:** بهاء المر، المرجع السابق، ص 372.

إن مشروعية الدليل الإلكتروني ترتبط بالعديد من الحقوق التي قد نص عليها الدستور أو القوانين الجنائية التي تعد تكريساً لضمانات المحاكمة العدالة، فمن بين الدساتير نجد أن الدستور الجزائري نص في المادة 46 منه على ضرورة حماية الحياة الخاصة للمواطن بالمعنى الواسع لهذه الحماية، حيث جاء نص هذه المادة على النحو التالي: "لا يجوز انتهاك حرمة الحياة الخاصة للمواطن، وحرمة شرفه يحميها القانون. سرية المرسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل من الأشكال المساس بهذه الحقوق دون أمر معلل من السلطات القضائية ويعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"[1].

من خلال هذا النص يظهر مدى حرص المشرع الجزائري على حماية الحريات الخاصة المتعلقة بالأفراد، ونرى أنه شدد فيما يتعلق بالمراسلات والاتصالات والمعطيات الشخصية، خصوصاً ونحن نتكلم عن الدليل الرقمي، والذي في الغالب يتم الحصول عليه عن طريق تتبع هذه الوسائل، وإن كان الإستثناء الوحيد في هذه المسألة هو ما تطرق إليه المشرع بموجب المادة 65 مكرر5 من ق.إ.ج.ج ويرجع هذا الاستثناء إلى خطورة هذا النوع من الجرائم[2]، وإلى ضرورة تفعيل مثل هذه الآليات في الكشف عنها، إلا أن المشرع رغم الاعتماد على هذا النوع من الوسائل قد ضبطها بالعديد من الشروط والضمانات كوجود إذن، وأن تتم في المواعيد المحددة في المادة 47 من ق.إ.ج.ج، وأن تتم تحت الرقابة المباشرة لوكيل الجمهورية، أو قاضي التحقيق[3].

ومن النصوص الأخرى التي شددت على حماية خصوصية الأفراد والعمل على تقصي المشروعية في الحصول على الدليل ما جاء في المادة 135 من ق.ع.ج، والتي تنص على أن: "كل موظف في السلك الإداري أو القضائي وكل ضابط شرطة وكل قائد أو أحد رجال القوة العمومية دخل بصفته

---

1 القانون رقم 16-01، المؤرخ في 26 جمادي الأول عام 1437هـ الموافق لـ: 6 مارس 2016، المعدل والمتمم للدستور 1996، المؤرخ في 26 رجب 1417 الموافق 7 ديسمبر 1996، المتضمن الدستور، ج.ر.ج.ج، ع 14، المؤرخة 7 مارس 2016، ص 11.

2 عدد المشرع هذه الجرائم في نص المادة 65 مكرر 5 كالآتي: "رائم المخدرات، الجريمة المنظمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد".

3 انظر المادة 65 مكرر 5 من ق.إ.ج.ج.

المذكورة منزل أحد المواطنين يغبر رضاه، وفي غير الحالات المقررة في القانون وبغير الإجراءات المنصوص عليها فيه، يعاقب بالحبس من شهرين إلى سنة وبغرامة من 20.000 إلى 100.000 دج دون الإخلال بتطبيق المادة 107"[1].

ويبنى على مشروعية الدليل استبعاد كل الأدلة التي تم التحصل عليها بطريقة غير مشروعة، وذلك من باب تحقيق الوظيفة التربوية والأخلاقية لبناء عدالة جنائية سوية، فضلاً عن أن استبعاد الدليل غير المشروع يضمن كفالة الاحترام والهيبة اللازمين للسلطات القضائية، ومن شأنه كذلك أن يزيد من الثقة بين القاضي والمجتمع، فالطرق التي يجرمها القانون لا يمكن أن يعتمد عليها في تحصيل الأدلة وإلا كان القضاء أعرج[2].

ثانياً– مـناقشـة الـدلـيل الإلكترونـي:

يمثل هذا المبدأ أحد أهم المبادئ التي تقوم عليها المحاكمة العادلة، والذي ينشأ عن شفوية المرافعة والحق في الدفاع، وهو ما يقرر مواجهة المتهم بالوقائع المنسوبة إليه والأدلة المؤيدة، حتى يتسنى له الحق في الرد، والتوضيح، والدفاع عن نفسه[3].

وهو نفس المبدأ المطبق على الأدلة الناتجة عن الوسائل الإلكترونية؛ إذ يتوجب على القاضي عرضها أياً كانت طبيعتها؛ صورة، أو فيديو، أو تسجيل، أو أشرطة، أو أوراق منسوخة لمستخرجات إلكترونية على المتهم، ومناقشتها بحضوره والسماح له بإبداء رأيه فيها وتفنيدها، كما على الخبير الحضور للجلسة، وتقديم كل ما توصل إليه في تقرير الخبرة ومناقشته أمام القاضي والمتهم والحضور[4].

ثالـثاً– ألا يكـون الدلـيل قائماً على التخمين والـظن:

حتى يكون الدليل الإلكتروني صحيح وقابل للاستناد عليه في إصدار الحكم، سواء في الإدانة أو البراءة، وجب أن يكون هذا الدليل حقيقي وواقعي قدر المستطاع، وأن لا يلتبس بالظنون

---

1 جاء نص المادة 107 من قانون العقوبات الجزائري على الشكل التالي: "يعاقب الموظف بالسجن المؤقت من خمس (05) إلى عشر (10) سنوات إذا أمر بعمل تحكمي أو ماس سواء بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر".

2 سربار نظام عثمان، الجريمة الجنائية الناشئة عن إساءة استخدام الهواتف النقالة، رسالة مقدمة للحصول على درجة الماجستير في الحقوق، كلية الحقوق، جامعة المنصورة، الموسم الجامعي، 2013-2014، ص 190-191.

3 عمار بوضياف، المحاكمة العادلة في النظام الجنائي الإسلامي والمواثيق الدولية (دراسة مقارنة)، ط. الأولى، جسور للنشر والتوزيع، الجزائر، 2010، ص 46.

4 صابرين يوسف عبدالله، المرجع السابق، ص 265.

والتخمينات، ويستند القاضي في معرفة ذلك إما عن طريق المعرفة الحسية التي تدركها الحواس، من خلال الوقوف على معاينة المخرجات المستمدة من الدليل الإلكتروني، وإما عن طريق المعرفة العقلية بما يقوم به من تحليل واستنتاج ليصل إلى الحقيقة، ويجب أن يصدر حكمه استناداً عليها[1].

الفرع الثانـي: سلطة القاضي في تقدير الدليل الإلكترونـي.

تتحدد سلطة تقدير الدليل من طرف القاضي بحسب نظام الإثبات المعتمد من طرف قضاء كل دولة، ونظراً لهذا التباين، نتطرق في هذا الفرع لبيان أنظمة الإثبات (أولاً)، ثم دراسة أسباب تفعيل هذا المبدأ في الدليل الإلكتروني (ثانياً)، فأسباب العمل بقاعدة سلطة القاضي في تقدير الأدلة مع الأدلة الإلكترونية (ثالثاً)، وصولاً لموقف المشرع الجزائري منها (رابعاً).

أولاً– أنـظمة الإثـبات:

تنقسم نظم الإثبات إلى ثلاث نظم مختلفة تتأسس كل واحدة منها على مبادئ معينة، وتتمثل هذه النظم في الصور التالية:

1- نظام الإثـبات المقيد:

يعتمد هذا النظام على التحديد المسبق لأدلة الإثبات وقيمتها الإثباتية، ولا يجوز للقاضي أن يأخذ بغير هذه الأدلة، فالقاضي في هذا النوع من أنظمة الإثبات مجرد مطبق للقانون، والإقتناع الشخصي للمشرع، ومن بين القوانين التي تعمل بهذا النظام؛ القانون الأمريكي، والإنجليزي[2].

2- نظام الإثـبات الـحر:

بخلاف النظام المقيد يعتمد النظام الحر على عدم تحديد الأدلة التي يتوجب على القاضي الأخذ بها في حكمه، بحيث يترك حرية واسعة للقاضي في أن يأخذ ما يشاء من الأدلة، ويطرح ما يشاء، وذلك بالنظر إلى القضية المعروضة عليه، وملابساتها، والأوضاع التي تمت فيها، ولا يطلب في هذا النظام من القاضي إلا تبيان الأسباب التي استند عليها في إصدار حكمه، ومن النظم القانونية التي تأخذ بهذا النظام؛ نظام فرنسا[3].

---

1 محمد حمد عمر الغياثين، المرجع السابق، ص 208.

2 محمود محمد محمود جابر، المرجع السابق، ص 126.

3 صابرين يوسف عبدالله، المرجع السابق، ص 270.

3- نـظام الإثـبات الـمختلط:

يمثل النظام المختلط الإتجاه التوفيقي الذي يجمع بين المزايا الإيجابية في النظام الحر والأخرى في النظام المقيد، بحيث يعتمد هذا النظام على تحديد الأدلة التي يتوجب على القاضي أن يأخذ بها في الإثبات، ويترك له متسع من الحرية في أخذ ما يريد منها، أو أن يكمل منها ما نقص، مما هو معروض عليه في الجلسة، وتتفاوت الأنظمة القانونية في العمل بهذا النظام بين دول توسع في الشروط وأخرى تقلل منها، ومن بين الدول التي تأخذ بهذا النظام؛ سوريا ومصر[1].

ثانيـاً- أسـباب تفعيل السلطة التقديـريـة للقاضـي:

إن الطبيعة الخاصة للدعاوى الجنائية فرضت التعامل معها بمنطق مغاير لما هو معمول به في القضاء المدني، فالقاضي المدني ينحصر دوره في الترجيح بين الأدلة والأخذ بأكثرها قوة، بينما للقاضي الجنائي دور إيجابي بدرجة كبيرة؛ فهو كذلك موكل إليه جمع الأدلة والتأكد منها، فعبء الإثبات في القضاء الجنائي لا يتوقف عند الضحية والجاني، وإنما يمتد حتى للقاضي باعتباره ممثل المجتمع، ومن الاعتبارات التي تقرر إلزامية العمل بهذا المبدأ، نذكـــر:

1- صعوبـــة الإثبات في الـمواد الـجنائيـة:

يتميز القضاء الجنائي بصعوبة الإثبات، ويرجع ذلك إلى قيام المجرم بطمس كل الأدلة التي قد تساعد في العثور عليه، أو اكتشاف هويته[2].

2- طبـيعة الـمصالـح التي يـحميها القانون الـجنائي:

يمثل القانون الجنائي العصا الحديدية التي تكفل بها الدول حماية الحريات والمصالح الاقتصادية والاجتماعية سواء العامة أو الخاصة.

3- الطبيعة الـخاصة لنظام الـمحلفـين:

من أهم الخصائص التي يمتاز بها القضاء الجنائي؛ الاستعانة ببعض الفئات الشعبية في القضايا ذات الطبيعة الجنائية، ومن الأكيد أن هذه الفئات لا تكون بنفس التكوين والمهارة التي يكون عليها

---

1 منار عبد المحسن عبد الغني العبيدي، عواد حسين ياسين، حجية الإثبات بالوسائل المرئية الحديثة وموقف القضاء منها (كاميرات المراقبة، وكاميرات الهاتف النقال)، مجلة جامعة تكريت للحقوق، المجلد الأول، العدد الأول، الجزء الأول، جامعة تكريت، سبتمبر 2016، ص 185.

2 طواهري اسماعيل، الاقتناع الشخصي للقاضي في المواد الجنائية في القانون المقارن، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة الجزائر 1، الموسم الجامعي 2013-2014، ص 104-106.

القاضي، سواء في فهم القانون، أو الأدلة المعروضة للمناقشة، فضلاً عن أن هذه الفئات غير ثابتة وتختار عن طريق القرعة[1].

4- مـبدأ قرينـة الـــبراءة:

من أكثر المبادئ التي يتوجب على القاضي الجنائي مراعاتها؛ مبدأ قرينة البراءة، والذي يشكل ضمانة أساسية من ضمانات المحاكمة العادلة، حيث أن عدم افتراض البراءة في المتهم، سوف ينتج عنها استحالة تقديم دليل منطقي ومقبول، مما يجعله عير قادر على إثبات براءته، والتسليم بأنه هو مرتكب الجريمة[2].

رابعاً- أسباب العمل بقاعدة سلطة القاضي فـي تقدير الأدلة مع الأدلــة الإلكترونيــة:

من الأمور التي حازت الإجماع من الناحية العلمية، أو حتى القضائية، هو اليقين الثابت الذي تحققه الأدلة العلمية، فهي أدلة تصل إلى درجة لا يمكن معها للقاضي أن يمارس سلطته التقديرية في تأكيد أو نفي المسائل التي يشير إليها هذا الدليل، ولكن هذا لا يلغي نسبة الشك التي تتولد لدى القاضي من الدليل الإلكتروني، والتي يمكن نسبتها إلى الأسباب التاليـــة:[3]

1- خـضوع الدليل الإلكتروني للعبث بشكل يـخالف ما هو عليه فــي الواقع:

فقد يعبر الدليل عن وقائع غير تلك التي يراد إثباتها، على نحو يجعل غير المختص غير قادر على التمييز بين صحة هذا الدليل من عدمها.

2- الـخطأ فــي الدليل الإلكترونــي:

رغم اليقين التام الذي يحوزه الدليل لإلكتروني، إلا أن هذا لا يجعله يسلم من الخطأ في بعض الحالات، ولو بنسب ضئيلة، وهذا يمكن أن يرجع إلى الأسباب الآتـــية:

- الخطأ في استخدام الأداة التي يتم استخلاص الدليل من خلالها، وذلك باستخدام شيفرات غير صحيحة، أو مواصفات خاطئة.

---

1 طواهري اسماعيل، نفس المرجع، ص 106.

2 عمار بوضياف، المرجع السابق، ص 41.

3 ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد الثاني، جامعة النهرين، جانفي 2016، ص 243-244.

- استخدام أدوات تقل نسبة الوصول للحقيقة فيها عن 10 %، وهو ما يحدث غالباً مع وسائل اختزال البيانات، أو عن طريق معالجتها بطريقة غير التي يجب أن تتم بها عملية التقييم.

وعليه من خلال ما سبق بيانه، يتضح أن الشك الذي يتصل بالدليل الإلكتروني ليس متصل الدليل بذاته، فهو قد يطابق الحقيقة والواقع، إلا أن العوامل المحيطة بظروف جمعه أو التأكد من صحته هي التي تثير الشك لدى القاضي، وتجعله حائزاً على نفس القيمة الإثباتية للأدلة الجنائية التقليدية الأخرى.

خامساً– مـوقف المشرع الـجزائري من الدلـيل الإلكـترونـي:

إن المشرع الجزائري من بين التشريعات التي أخذت بقبول الدليل الإلكتروني في الإثبات، وذلك واضح بشكل جلي في الوسائل الثبوتية التي تمت إضافتها بمقتضى تعديل قانون الإجراءات الجزائية لسنة 2006، وبالرغم من أن هذه الوسائل وردت على سبيل الحصر فيما يتعلق ببعض الجرائم الخطيرة وفقاً لظروف مشددة، إلا أن المشرع أكد على ذلك بصورة أكثر وضوح في القانون رقم: 09-04 المتعلق الوقاية من الجرائم المتصلة بتكنولوجيا الاتصال والإعلام، إذ بموجب هذا القانون بَيّـن الآليات التي يجب العمل بها من أجل مكافحة الجريمة الإلكترونية، وطرق البحث عن أدلتها.

هذا ويأخذ الدليل الإلكتروني نفس القوة الاثباتية للأدلة الأخرى، وذلك عملاً بنص المادة 212 والتي تركت للقاضي حرية الإثبات بكافة الوسائل، فضلاً عن سلطته الكاملة في تكوين اقتناعه الشخصي الذي يجب أن يبنى على الأدلة المقدمة في معرض المرافعات، والتي حصلت المناقشة فيها حضورياً وأمامه[1]، كما أن القانون لا يحاسب القاضي على الطريقة التي توصل إليها في بناء قناعته، وإنما يأمره بتسبيب الحكم فقط[2].

---

1 تنص المادة 212 من ق.إ.ج.ج على: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص. ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات التي حصلت المناقشة فيها حضورياً أمامه".

2 تنص المادة 307 من ق.إ.ج.ج على أن: "يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تتعلق فضلاً عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة: "إن القانون لا يطلب من القضاة أن يقدموا حساباً عن الوسائل التي بها وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم وفي صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة

ملخــص الــباب الـثاني:

يعتبر الجانب الإجرائي في القضايا الجنائية جانب مهم وحساس، فهو يلعب دوراً كبيراً في تحريك الدعوى الجنائية، والبحث عنها، وكشف غموضها، والوصول إلى حقيقية مرتكبها، والدوافع التي أدت بهم إلى القيام بتلك الأفعال، ففي جميع التشريعات المقارنة يكفل القانون الإجرائي الضمانات التي تحقق العدالة بطريقة لا يطال فيها الدعوى أي إجراء باطل، ولا يمس فيها أي شخص تعسفاً.

ومن خلال ما سبق عرضه في هذا الباب يظهر الدور الكبير الذي يلعبه قانون الإجراءات الجزائية بصفة عامة، والقوانين المتعلقة بجرائم التكنولوجيا بصفة خاصة، في محاربة الجريمة الإلكترونية من الناحية الإجرائية، فبموجب هذه القوانين حاول المشرع الجزائري مواكبة التطور التقني والاستفادة منه بشكل إيجابي في البحث عن بعض الجرائم؛ خاصة الخطيرة منها، وذلك عن طريق إضافة باب خامس بعنوان –في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور–.

وفضلاً عما جاء في قانون الإجراءات الجزائية، ضَمّن المشرع الجزائري القانون 09-04 العديد من الإجراءات الأخرى الخاصة بالجريمة الإلكترونية بصفة خاصة، وحاول تبيان جميع الإجراءات المتعلقة بها والسلطات المختصة في البحث والتحري عنها، وآليات التعامل مع الدليل الإلكتروني وأهميته في مثل هذه الجرائم.

ومن خلال هذا الباب أيضاً، حاولنا الوقوف على بعض الأدلة التي يتم استعمالها في إثبات الجرائم المركبة بوسائط إلكترونية، وكيف تنوعت هذه الأدلة بين أدلة تقليدية مثل: الشهادة والخبرة وكيف تغير مدلولها في هذا النوع من الجرائم، ثم تطرقنا إلى الدليل الإلكتروني والدور الكبير والجوهري الذي يلعبه في الكشف عن الجرائم الإلكترونية بصفة عامة، والجرائم المرتكبة بواسطة الهاتف النقال بصفة خاصة، كما حاولنا من خلال هذا الباب التطرق إلى القيمة الإثباتية له، لنصل في الأخير إلى نتيجة مفادها أن الدليل الإلكتروني مثله مثل باقي الأدلة يخضع لنفس الشروط، ويأخذ نفس القوة في التأثير على يقين القاضي.

المسندة إلى المتهم، وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق وجباتهم: هل لديكم اقتناع شخصي ؟"

الخاتمـــــــــة

الـخاتمـــــة:

تطرقنا فيما تَقَدَّمَ من هذه الدراسة، إلى الاستخدامات غير المشروعة للهاتف النقال في ارتكاب بعض الجرائم؛ إما باعتباره أداة مساعدة لتنفيذ الجريمة أو محلاً لارتكابها، وذلك من خلال منظور شامل، اعْتُمِدَ فيه على تحليل النصوص القانونية المتعلقة بمختلف أنماط الجرائم ذات الطبيعة الإلكترونية، مع اسْتِجْلَاء موقف المشرع الجزائري من هذا النوع المستحدث من الجرائم، خاصة تلك التي ترتكب بواسطة الهاتف النقال، وآليات التحري عنها. كما تم العمل على إيضاح الجرائم التي قد ترتكب بواسطة الهاتف النقال؛ وذلك من خلال التطرق إلى بعض الأنماط الإجرامية ذات الطبيعة التقليدية، وأيضاً الإلكترونية، كما بَيَّنا أساليب البحث عن الجرائم المرتكبة بواسطة الهاتف النقال، والسلطات المختصة في ذلك، معتمدين في ذلك بشكل كبير على القانون الجزائري، مقارناً ببعض التشريعات ذات السبق في مكافحة هذا النوع من الجرائم. وهو ما أفضى بنا إلى رصد مجموعة من النتائج والملاحظات نوردها كما يلي:

أولاً– ما يـتعلق بالطبـيعة الفنية والتقنية للهاتــف النقال:

شهد الهاتف النقال تدريجياً تطوراً كبيراً، بحيث لم يعد مجرد وسيلة اتصال لنقل الكلام والرسائل بين الناس، وإنما أصبح شاملاً للعديد من المميزات الفنية والتقنية المتطورة والحديثة، والتي قد تشكل تهديداً مباشراً على بعض جوانب الحياة الخاصة للأفراد، دون أن يكون هناك أي وازع أخلاقي أو قانوني رادعاً لهذا التهديد.

ثانــياً– خصوصية التكييف فيما يتعلق بجرائم الهاتف النقال:

خلصنا من خلال هذه الدراسة إلى اتساع التكيف القانوني للجرائم المرتكبة بواسطة الهاتف النقال؛ ويرجع ذلك إلى العديد من الأسباب؛ من بينها سهولة استعمال الهاتف النقال، المميزات التقنية التي يحتوي عليها والتي قد توفر العديد من الخدمات بشكل سهل وبسيط كالخدمات المالية أو الشخصية، إضافة إلى اتصال معظم الهواتف النقالة بشبكة الإنترنت، فضلاً عن ميزة التجوال.

ثالــثاً– بخصوص التكيف وتداخل الأنـماط الإجرامـية:

نظراً لخصوصية الجرائم المرتكبة بواسطة الهاتف النقال؛ توصلنا إلى وجود العديد من الإشكالات القانونية والقضائية التي تقع بمناسبة تكييف جرائم الأشخاص المرتكبة بواسطة الهاتف النقال؛ خاصة

ما تعلق منها بالاعتداء على خصوصية الأفراد، إذ هناك العديد من الجرائم التي قد تندرج ضمن الاعتداء على الحياة الخاصة للأفراد، بينما تغيب عنها بعض الشروط المُهِمَّة لِتُكَيَّف ضمن نطاق هذه الجريمة، وهو ينتج عدالة معاقة وقاصرة؛ وذلك بسبب عدم وجود نصوص قانونية خاصة تطبق على هذا النوع من الجرائم المستحدثة، أو اللجوء إلى تطبيق نصوص تقليدية غير ملائمة.

رابـــعاً- الفراغ التشريعي لمواجهة الجريمة الإلكترونية المرتكبة بواسطة الهاتف النقال:

أَثْبَتَتْ هذه الدراسة وجود فراغي تشريعي كبير فيما يخص مكافحة الجريمة الإلكترونية، بصفة عامة، وتلك المرتكبة بواسطة الهاتف النقال بصفة خاصة، والسبب في ذلك أن جل التشريعات المقارنة تحصر طرق ارتكاب الجريمة الإلكترونية في تلك الجرائم المرتكبة بواسطة الحاسوب أو عن طريق شبكة الإنترنت، بالرغم من أن الأداة الأكثر استخدماً في هذا النوع من الجرائم في وقتنا الحالي هو الهاتف النقال.

خامـــساً- صعوبات البحث والتحري عن الجرائم المرتكبة بواسطة الهاتف النقال:

توصلنا من خلال هذه الدراسة إلى وجود العديد من الصعوبات في عملية البحث التحري عن الجرائم المرتكبة بواسطة الهاتف النقال، ويرجع ذلك إلى العديد من الأسباب؛ والتي من بينها إحجام الضحايا التبليغ عن الجريمة خوفاً من الفضيحة، أو نتيجة لعدم اكتشافهم لها، وقد يرجع السبب في بعض الأحيان نتيجة لنقص تأهيل المكلفون بعمليات البحث والتحري بمثل هذا النوع من الجرائم.

سادســاً- صعوبة استخلاص الأدلة خاصة فيما يتعلق بالجريمة ذات الطابع الإلكتروني:

توصلنا من خلال هذه الدراسة إلى الصعوبات التي قد تعيق السلطات القضائية في الوصول إلى الأدلة التي تثبت الجرائم المرتكبة بواسطة الهاتف النقال نتيجة لطبيعة مسرح الجريمة، وكذلك بسبب سهولة طمس الدليل المرتبط بها أيضاً.

سابــعاً- بخصوص دور مزود الخدمات في الكشف عن الجرائم المرتكبة بواسطة الهاتف النقال:

خلصنا من خلال هذه الدراسة إلى أن مزود الخدمات له دور كبير في الكشف عن الجرائم المرتكبة بواسطة الهاتف النقال، وذلك انطلاقا من الخدمات التي يقدمها للجمهور سواء من ناحية الاتصالات أو تقديم خدمات الإنترنت، مما يجعله ملزم بحفظ البيانات والمعلومات التي تتم عن طريق الخادم المرتبط به، وبالتالي الاستعانة به في حال كانت الضرورة تستدعي ذلك.

وتماشيا مع ما تمَّ التوصل إليه في هذه الدراسة من نتائج وملاحظات، نورد فيما يلي بمجموعة من التوصيات التي قد تساهم في تيسير مكافحة الجرائم المرتكبة بواسطة الهاتف النقال، أهمها:

أولاً– العمل على إعادة النظر في تكييف بعض الجرائم ذات الطبيعة التقليدية، وذلك بطريقة تتماشى مع الظروف المستجدة والتطورات التكنولوجية الراهنة التي أصبحت تفرض وقائع إجرامية مستحدثة ومغاير لما هو متعارف عليه من أنماط إجرامية.

ثانـياً– ضرورة استحداث نصوص قانونية خاصة تهدف بشكل صريح ومباشر إلى تجريم الأنماط المستجدة من الجرائم المرتكبة بواسطة الهاتف النقال، وعدم الإكتفاء بالنصوص التقليدية القائمة، والتي لا تتلاءم وخصوصية الجرائم المستحدثة المرتكبة بواسطة الهاتف النقال.

ثالـــثاً– يجب فرض رقابة فائقة على العمليات المالية التي تتم عن طريق الهواتف النقالة؛ نظراً لما لها من دور كبير في ارتكاب عمليات غسيل الأموال، وذلك من خلال استحداث برامج رقابية تسمح بالإطلاع على كافة العمليات المالية التي تتم بواسطة الهواتف النقالة، وإمكانية تتبع القائمين بمثل هذا النوع من المعاملات المالية غير المشروعة.

رابـــعاً– ضرورة إيجاد وحدات شرطية وقضائية مختصة في محاربة الجريمة الإلكترونية، فضلاً عن تفعيل دور الهيئة الوطنية لمكافحة الجريمة الإلكترونية، والفروع المتواجدة على مستوى الدرك، والأمن الوطني، والعمل على القيام بدورات وتكوينات دورية تمكنهم من الإطلاع على أحدث الأنماط الإجرامية الإلكترونية، بما في ذلك تلك التي ترتكب بواسطة الهاتف النقال، وتمكينهم من الطرق والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

خامـــساً– ضرورة إعادة النظر في العقوبات المقررة لجرائم الاتصال والمعلومات أو الجرائم المتصلة بها، مع العمل على تشديدها، حيث لاحظنا أن أغلب العقوبات المقررة لهذه الجرائم لا تحقق الردع الكافي، مما لا يؤدي إلى استخدام آمن لتكنولوجيا المعلومات والاتصال.

سادســاً– العمل على استحداث نظام وقائي يعمل على مكافحة الجرائم الإلكترونية قبل ارتكابها سواء في شكل تطبيقات مخصصة لذلك أو في شكل حكومة إلكترونية.

سابـــعاً: الحرص على تفعيل الأحكام والقواعد الواردة في البنود الدولية التي صادقت عليها الجزائر، والمتعلقة بالمساعدة القضائية الدولية، مع السعي نحو إبرام اتفاقيات ثنائية أو جماعية تتعلق بالجريمة الإلكترونية بصفة عامة والجرائم المرتكبة بواسطة الهاتف النقال بصفة خاصة.

قائمـــــة المراجـــــع

قائمـــــة المراجـع:

- القرآن الكريم

أولاً– الكتب العامـــة:

1- أديبة محمد صالح، الجريمة المنظمة دراسة قانونية مقارنة، ب. ط، منشورات كردستان للدراسات الإستراتيجية، السليمانية، العراق، 2009.

2- أحمد إبراهيم الزعارير، مدخل إلى علم الجريمة، ط. الأولى، دار البيروني للنشر والتوزيع، عمان، 2015.

3- أحمد عبد اللاه المراغي، الظاهرة الإجرامية–دراسة تحليلية تأصيلية مقارنة لأسباب الجريمة–، ب. ط، مركز الدراسات العربية للنشر والتوزيع، مصر، 2018.

4- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط. السابعة عشرة، دار هومة، الجزائر، 2018.

5- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص ج1، ط. العشرون، دار هومه، الجزائر، 2018.

6- باسل عبدالله الضمَّور، غسيل الأموال في المصارف–دراسة مقارنة–، ط. الأولى، مكتبة القانون والاقتصاد، الرياض، 2013.

7- هيثم عبد الرحمن البقلي، غسيل الأموال –كإحدى صور الجريمة المنظمة بين الشريعة والقانون المقارن–، ب. ط، دار العلوم، مصر، 2010.

8- طارق عفيفي صادق أحمد، نظرية الحق، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2016.

9- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، ب. ط، دار النهضة العربية، مصر 2005.

10- مصطفى مجدي هرجة، ندب الخبراء في المجالين الجنائي والمدني، ط. الأولى، دار محمود للنشر والتوزيع، القاهرة، 2016.

11- مريوان سليمان، القذف في نطاق النقد الصحفي –دراسة مقارنة–، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2014.

12- نويري عبد العزيز، الحماية الجزائية للحياة الخاصة في القانون الجزائري والفرنسي – دراسة مقارنة، ط. الثانية، دار هومة، الجزائر، 2016.

13- عبد الله الزمامي، غسيل الأموال في المملكة العربية السعودية، ب. ط، مكتبة القانون والاقتصاد، الرياض، 2010.

14- عوض محمد عوض، قانون الإجراءات الجنائي ج1، ب. ط، مؤسسة الثقافة الجامعية، مصر، 1989.

15- فوزية عبد الستار، شرح قانون الإجراءات الجنائية ج1، ط. الثانية، دار النهضة العربية، القاهرة، 2010.

16- شلبي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، ب. ط، دار هومة، الجزائر، 2013.

17- شريف أحمد الطباخ، الإثبات الجنائي في ضوء الفقه والقضاء، ط. الأولى، دار الفكر والقانون، المنصورة، 2015.

18- خالد أقيس، استراتيجيات وطرق التدريس العامة والإلكترونية، ط. الأولى، مركز الكتاب للنشر، القاهرة، 2016.

ثانيًا– الـمراجع الـمتخصصة:

19- أيمن بن ناصر بن حمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الإجتماعي: دراسة مقارنة، ط. الأولى، مكتبة القانون والإقتصاد، الرياض، 2015.

20- أيمن عبد الله فكري، الجرائم المعلوماتية –دراسة مقارنة في التشريعات العربية والأجنبية–، ب. ط، مكتبة القانون والإقتصاد، الرياض 2014.

21- أحمد محمد عبد الباقي، الإنترنت؛ التكنولوجيا وجرائم المستقبل، ط. الأولى، دار النهضة العربية، مصر، 2017.

22- أحمد محمد عبد الرؤوف المنيفي، السرقة الإلكترونية وحكمها في الإسلام، ط. الثانية، واد أي كتب، لندن، 2018.

23- أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها (دراسة مقارنة للتشريعات العربية والأجنبية)، ط. الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2016.

24- أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية(دراسة مقارنة)، ط. الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2014.

25- أسد الدين التميمي، مصطلحات الإنترنت والحاسوب: أول معجم شامل بكل مصطلحات الإنترنت متداولة وفي العالم وتعريفاتها، ط. الأولى، دار أسامة للنشر والتوزيع، عمان، الأردن، 2009.

26- أشرف السعيد أحمد، القرصنة الإلكترونية، ب. ط، مطابع الشرطة ، مصر، 2013.

27- بهاء المري، جرائم المحمول والإنترنت، ب. ط، منشأة المعارف، الإسكندرية، 2017.

28- جميل إطيمزي، أنظمة وأدوات التعليم الإلكتروني، ب. ط، دار فليس فليسونغ، الولايات المتحدة، 2010.

29- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، ط. الثانية، دار النهضة الحديثة، القاهرة، 2012.

30- هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية (دراسة مقارنة)، ط. الثانية، دار النهضة العربية، القاهرة، 2008.

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

32- هشام محمد شريف عروبكي، نظم الاتصالات الخلوية، ط. الأولى، دار الكتاب العالمية، بيروت، 2015.

33- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري وفي التشريع الدولي، ب. ط، دار الهدى، الجزائر، 2011.

34- حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط. الأولى، دار النهضة العربية، القاهرة، 2017.

35- حسن إبراهيم خليل، تطبيقات قضائية على جريمة الإزعاج المعتمد عن طريق وسائل الاتصالات الحديثة، ط. الأولى، دار الفكر والقانون للنشر والتوزيع، مصر، 2015.

36- طارق إبراهيم الدسوقي عطية،، الأمن المعلوماتي – النظام القانوني لحماية المعلوماتي- دار الجامعة الحديثة، القاهرة، 2009.

37- طارق عفيفي صادق أحمد، الجرائم الإلكترونية (جرائم الهاتف المحمول)، ط. الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.

38- طلعت الشهاوي، المسؤولية الجنائية عن جرائم الاتصالات –دراسة مقارنة-، ط. الأولى، دار النهضة العربية، مصر، 2017.

39- مجدي محمد أبو العطاء، أمن المعلومات والإنترنت، ط. الأولى، كمبيوساينس، مصر، 2016.

40- مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، ب. ط، دار النهضة العربية، القاهرة، 2000.

41- محمود محمد محمود جابر، الجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، ط. الأولى، المكتب الجامعي الحديث، الإسكندرية، 2017.

42- محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات) –دراسة مقارنة التشريع المصري والفرنسي والأمريكي والإتفاقيات الدولية والإقليمية-، ط. الأولى، المكتب الجامعي الحديث، الإسكندرية، 2018.

43- محمد أديب عنيمي، مستقبل الحاسبات، ط. الأولى، المكتبة الأكاديمية، مصر، 2001.

44- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، ط. الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2004.

45- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية –دراسة مقارنة- ط. الأولى، دار الفكر والقانون، المنصورة، مصر 2017.

46- محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ب. ط، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015.

47- محمد عبدالله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، ب. ط، أكاديمية الشرطة، مصر، 2016.

48- محمد عبد الله العوَا، جرائم الأموال عبر الإنترنت، ط. الأولى، دار الفتح للطباعة والنشر، الإسكندرية، 2013.

49- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، ط. الثانية، دار النهضة العربية، مصر، 2009.

50- مصطفي يوسف، الحماية القانونية للشاهد، ب. ط، دار النهضة العربية، القاهرة، 2011.

51- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط. الأولى، مطابع الشرطة، مصر، 2008.

52- مصطفى محمد موسى، الإرهاب الإلكتروني-دراسة قانونية، أمنية، نفسية، اجتماعية- ط. الأولى، مطابع الشرطة، مصر، 2009.

53- نائله عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية –دراسة نظرية تطبيقية، ط. الأولى، منشورات الحلبي الحقوقية، لبنان، 2005.

54- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية –دراسة في أبعاد الأمن الإلكتروني-، ب. ط، المكتب العربي للمعارف، القاهرة، 2018.

55- عمر محمد بن يونس، ب. ط، مؤسسة أدم للنشر والتوزيع، مالطا، 2008.

56- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة-دراسة مقارنة-، ط. الأولى، منشورات زين الحقوقية، بيروت، 2013.

57- على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)، ب. ط، المكتب الجامعي الحديث، الإسكندرية، 2012.

58- عماد أحمد أبو شنب، ويسرى حرب، ووجدان أبو البصل، الخدمات الإلكترونية، ب. ط، دار الكتاب الثقافي، الأردن، دون سنة النشر.

59- عبدالله جعفر كوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2017.

60- عبد العال الديربي، الجريمة الإلكترونية، ط. الأولى، المركز القومي للإصدارات القانونية، مصر، 2012.

61- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجي الاتصالات الحديثة، ط. الأولى، منشأة المعارف، الإسكندرية، 2009.

62- عبدالفتاح بيومي حجازي، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، 2010.

63- عبد الله سيف الكيتوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، ب. ط، دار النهضة العربية، القاهرة، 2013.

64- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، ب. ط، المكتب الجامعي الحديث، الإسكندرية، 2018.

65- سعيدي سليمة، وحجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، ط. الأولى، دار الفكر الجامعي، الإسكندرية، 2017.

66- شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت-دراسة مقارنة- ب. ط، دار النهضة العربية، مصر، 2009.

67- خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات —دراسة مقارنة-، ب. ط، دار الفكر الجامعي، الإسكندرية، 2010.

68- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط. الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011.

69- غادة نصار، الإرهاب والجريمة الإلكترونية، ب. ط، العربي للنشر والتوزيع، القاهرة، 2017.

ثالـثًا- الـمجلات العلميـة:

70- أحمد حمد الله أحمد، جريمة السرقة المرتكبة بواسطة الهاتف النقال، مجلة كلية الحقوق، المجلد 16، العدد 1، جامعة النهرين، 2014،

71- أمل فاضل عبد خشان، أحمد حمد الله، الإثبات الجنائي في جرائم إساءة استعمال الهاتف النقال، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد الرابع، العدد الثاني عشر، ج 1، جامعة كركوك، بتاريخ: 2015/02/01.

72- انسام سمير طاهر الحجامي، جريمتي القذف والسب عبر الإنترنت، مجلة رسالة الحقوق، العدد الثاني، جامعة كربلاء، 2015.

73- الجمال سمير حامد عبد العزيز، المشكلات القانونية لاستخدام الهاتف النقال، مجلة الفكر القانوني والاقتصادي، المجلد 1، العدد 2، جامعة بنها، 2010.

74- باخويا دريس، جريمة تبييض الأموال (المكافحة والعوائق) ، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد الأول، يناير 2012، المركز الجامعي تمنراست.

75- جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، العدد 12، جامعة ذي قار، 2016.

76- زين العابدين عواد كاظم، جريمة سرقة الهاتف في القانون العراقي والمقارن، مجلة الكوفة للعلوم القانونية والسياسية، جامعة الكوفة، العدد 6، 2010.

77- حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، 2013.

78- طارق كاظم عجيل، جريمة غسيل الأموال (دراسة في ماهيتها والعقوبة المقررة لها)، مجلة النزاهة والشفافية للبحوث والدراسات، العدد 1، كلية القانون، جامعة ذي قار، 2009..

79- ماينو جيلالي، الحماية القانونية لأمن الشهود في التشريعات المغاربية دراسة في التشريع الجزائري والمغربي والتونسي، مجلة دفاتر السياسة والقانون، العدد الربع عشر، جامعة قاصدي مرباح – ورقلة–، جانفي 2016.

80- محمد بكرارشوش، الاختصاص الإقليمي الموسع في المادة الجزئية في التشريع الجزائري، دفاتر السياسة والقانون، العدد الرابع عشر، جامعة قاصدي مرباح ورقلة، جانفي 2016.

81- ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد الثاني، جامعة النهرين، جانفي 2016.

82- منار عبد المحسن عبد الغني العبيدي، عواد حسين ياسين، حجية الإثبات بالوسائل المرئية الحديثة وموقف القضاء منها (كاميرات المراقبة، وكاميرات الهاتف النقال)، مجلة جامعة تكريت للحقوق، المجلد الأول، العدد الأول، الجزء الأول، سبتمبر 2016.

83- نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي–دراسة تحليلية– مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد 1، العدد 19، جامعة تكريت، 2013.

84- صالح أحمد محمد أللهيبي، علاقة السببية في المسؤولية المدنية عن أضرار الهاتف النقال –دراسة تحليلية–، مجلة الفكر القانوني والاقتصادي، المجلد 1، العدد 2، جامعة بنها، 2010.

85- صابرين يوسف عبدالله، دور الأدلة المرئية في الإثبات الجزائي، مجلة كلية الحقوق، المجلد 13 العدد الثاني، جامعة النهرين، 2017.

86- على حمزة عسل الخفاجي، التحقيق الابتدائي، مجلة العلوم الإنسانية، المجلد 23، العدد الأول، كلية التربية والعلوم الإنسانية، جامعة بابل، آذار 2015.

87- علاء عبد المحسن جبر السيلاوي، الجريمة المنظمة وأثرها في انتشار الفساد الإداري، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 1، العدد 2، جامعة الكوفة، 2009 .

88- فريدة علواش، جريمة غسيل الأموال (المراحل والأساليب)، مجلة العلوم الإنسانية، العدد الثاني عشر، جامعة بسكرة، نوفمبر 2007.

89- فتيحة محمد قوراري، المسؤولية الجنائية عن الإيذاء المبهج –دراسة تحليلية مقارنة لجرائم مستحدثة تتعلق بالهواتف النقالة–، مجلة الشريعة والقانون، المجلد 24، العدد 42، جامعة الشارقة، 2010.

90- رزان محمد ياسر العلبي، صفاء أوتاني، حق الإنسان في سرية مراسلاته البريدية واتصالاته السلكية واللاسلكية، مجلة جامعة البعث، المجلد 38، العدد 7، جامعة البعث، سوريا 2016.

91- رغدة محمد هادي، فاطمة حسن، البرامج الخبيثة تنتقل إلى جهاز المحمول، مجلة كلية التربية، العدد الأول، الجامعة المستنصرية، 2012.

92- شادية أحمد، الصرافة الخلوية تتيح لك أن تحمل البنك في جيبك، مجلة آفاق المستقبل، العدد 24، مركز الإمارات للدراسات والبحوث الإستراتيجية ، الإمارات، ديسمبر 2014.

93- شنة زواوي، الحماية الجنائية لحق الشخص على صورته، دفاتر السياسة والقانون، العدد الثالث عشر، جامعة قاصدي مرباح ورقلة، جوان 2015.

رابـــعاً– الرسائـل العلمـية:

(01) أطـروحات الدكـتوراه:

94- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري –تيزي وزو، الموسم الجامعي: 2018/2017.

95- طواهري اسماعيل، الاقتناع الشخصي للقاضي في المواد الجنائية في القانون المقارن، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة الجزائر 1، الموسم الجامعي: 2013-2014.

96- محمود عمر محمود، المسؤولية الجنائية الناتجة عن جرائم المحمول (دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية)، رسالة مقدمة لنيل درجة الدكتوراه، جامعة عين شمس، 2011.

97- معاذ سليمان راشد محمد الملا، المسؤولية الجنائية عن إساءة استعمال الهاتف المحمول (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، جامعة عين شمس، الموسم الجامعي: 2013/2012.

98- محمد بن عبد العزيز بن صالح المحمود، المسؤولية الجنائية عن إساءة استخدام مواقع التواصل الاجتماعي الحديثة (دارسة تأصيلية تطبيقية)، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الدكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.

99- محمد حمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود "دراسة مقارنة"، رسالة مقدمة للحصول على درجة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة القاهرة، الموسم الجامعي: 2012-2013.

100- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزئية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد –تلمسان–، الموسم الجامعي: 2017-2018.

(02) رسائـــل الماجستير:

101- إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني–دراسة مقارنة–، رسالة مقدمة من أجل نيل درجة الماجستير، جامعة ما بين النهرين، الموسم الجامعي 2013-2014.

102- كعرار سفيان، الجريمة المنظمة عبر الوطنية وأثرها على الأمن الإنساني، مذكرة مقدمة لاستكمال متطلبات الماجستير، جامعة سطيف، الموسم الجامعي: 2014/2013.

103- محمد فوزي صالح، الجريمة المنظمة وأثرها على حقوق الإنسان، مذكرة مقدمة لنيل شهادة الماجستير في القانون الدولي الإنسان، جامعة يحي فارس المدية، الموسم الجامعي: 2008-2009.

104-مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية –دراسة مقارنة بين التشريع الأردني والعراقي- رسالة مقدمة من أجل الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الموسم الجامعي: 2017/2016.

105-مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، رسالة الماجستير، جامعة قاصدي مرباح ورقلة، الموسم الجامعي: 2012-2013.

106-نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المرسلات عبر البريد الإلكتروني، رسالة مقدمة لنيل درجة الماجستير في الحقوق، جامعة القاهرة، 2017.

107-نجاري بن الحاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الإلكتروني، مذكرة لنيل شهادة الماجستير، تخصص قانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، 2016.

108-صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري- تيزي وزو-، الموسم الجامعي: 2012-2013.

109-عذارى سعود عبد المحسن، الضبط والتفتيش في جرائم الحاسب الآلي، رسالة مقدمة لنيل الماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2016.

110-سائد سعيد محمد رضوان، اعتماد الشباب الفلسطيني على صحافة الهاتف المحمول كمصدر للأخبار وقت الأزمات- دراسة ميدانية- رسالة مقدمة استكمالا للحصول على درجة الماجستير في الصحافة، كلية الآداب، الجامعة الإسلامية، غزة، الموسم الجامعي: 2016-2017.

111-سربار نظام عثمان، الجريمة الجنائية الناشئة عن إساءة استخدام الهواتف النقالة، رسالة الماجستير في الحقوق، كلية الحقوق، جامعة المنصورة، الموسم الجامعي: 2013، 2014.

112-ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة ماجستير تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، 2011-2012.

خامساً- بـحوث مؤتمرات ونـدوات:

113-أشرف توفيق شمس الدين، المراقبة والتنصت من خلال الهاتف المحمول في التحقيق الجنائي، دراسة مقدمة إلى مؤتمر الجوانب القانونية والاقتصادية للهاتف المحمول الذي تعقده كلية الحقوق بجامعة بنها، 2010.

114- بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في طار التكوين المحلي المستمر للقضاء، مجلس قضاء قسنطينة، السنة القضائية 2011/2010.

115- ياسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، مداخلة علمية تم إلقاءها في الملتقى العلمي: "الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، خلال الفترة: 2-2014/09/4، كلية العلوم الإستراتيجية، عمان.

116- ما شاء الله الزاوي، المواجهة الجنائية للبريد الإلكتروني الدعائي المزعج أو المضلل، مداخلة تم إلقاءها في أعمال المؤتمر الدولي الرابع عشر: الجريمة الإلكترونية، مركز جيل للبحث العلمي، 24-25 مارس 2017، طرابلس، لبنان.

117- محمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجريمة المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، أعمال الملتقى الوطني آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، بالجزائر العاصمة، مركز جيل للبحث العلمي، بتاريخ 29 مارس 2017.

118- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني، مداخلة مقدمة إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، المنعقد في القاهرة في المدة من: 2 إلى 4 جوان 2008.

119- عبد الناصر محمد محمود فرغلي، ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية –دراسة تطبيقية مقارنة، مداخلة مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد بتاريخ: 12-2007/11/14، جامعة نايف للعلوم الأمنية، الرياض.

120- على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول لأكاديمية شرطة دبي المنعقد في الفترة 26-4 إلى 28-4-2003.

121- عمر علي عذاب، تأثير الهاتف النقال على صحة الإنسان، مداخلة تم إلقائها في المؤتمر الوطني للتحديات البيئية: الواقع والطموح، المعهد التقني في كلارا، العراق، 2018.

122-فتيحة محمد قوراري، أحكام جرائم الإيذاء المبهج –دراسة تحليلية مقارنة لجرائم مستحدثة تتعلق بالهواتف النقالة–، مداخلة مقدمة لمؤتمر الجوانب القانونية والاقتصادية للهاتف المحمول، المنعقد بتاريخ 27-2010/04/28، في كلية الحقوق، جامعة بنها.

123-فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة علمية مقدمة للمشاركة في أعمال المؤتمر الدولي الربع عشر للجريمة الإلكترونية، المنعقد بتاريخ 24-25 مارس، جامعة طرابلس، لبنان.

124-طبيعة الإرهاب الإلكتروني، مداخلة مقدمة إلى المؤتمر الإسلامي العالمي لمكافحة الإرهاب، المنظم من طرف رابطة العالم الإسلامي، بتاريخ 22-25 فبراير 2015م.

سادساً– النصوص القانونيـــة والتنظيمية:

(1) فـــي القانون الجزائري:

125-القانون رقم 16-01، المؤرخ في 26 جمادي الأول عام 1437هـ الموافق لـ: 6 مارس 2016، المتضمن الدستور، ج.ر.ج.ج، العدد 14، المؤرخة 07 مارس 2016.

126-الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو 1966 المعدل والمتمم، المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 48، المؤرخة 9 يونيو 1966.

127-القانون رقم 82-04 المؤرخ في 13 فيفري 1982، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات المعدل والمتمم، ج.ر.ج.ج، ع 7، المؤرخة في 16 فبراير 1982.

128-الأمر رقم 95-11 المؤرخ 25 رمضان 1415 الموافق 25 فبراير 1995 المعدل والمتمم للأمر 66-156، المتضمن قانون العقوبات، ج.ر.ج.ج، ع 11، المؤرخة في 1 مارس 1995.

129-القانون رقم 04-14 المؤرخ في 17 ذي الحجة الموافق لـ: 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386، الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 5، المؤرخة 10 نوفمبر 2004.

130-القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في صفر عام 1386 الموافق 8 يونيه سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 71، المؤرخة 10 نوفمبر 2004.

131-القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج، العدد 71، المؤرخة 10 نوفمبر 2004 .

132-القانون رقم 06-23 المؤرخ في 04 ذي الحجة 1427 الموافق 20 ديسمبر 2006، المتضمن قانون العقوبات المعدل والمتم للأمر 66-156، ج.ر.ج.ج، العدد 84، المؤرخة 24 ديسمبر 2004.

133-القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ: 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الأعلام والاتصال ومكافحتها، ج ر ج ج، ع 47، المؤرخة 16 غشت 2009.

134-القانون رقم 11-14 المؤرخ في 2 أوت 2011 المعدل والمتمم للقانون 66-156 المتعلق بقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 44.

135-الأمر رقم 15-02 المؤرخ 07 شوال 1436هـ الموافق 23 يوليو 2015 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزئية، ج ر ج ج ، ع 40، المؤرخة 23 يوليو 2015.

136-القانون رقم 17-07 المؤرخ 28 جمادي الثانية 1438 الموافق 27 مارس 2017، المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيه سنة 1966 المتضمن قانون الإجراءات الجزائية، ج ر ج ج، ع 20، المؤرخة 29 مارس 2017.

137-القانون العضوي رقم 04-11 المؤرخ في 21 رجب 1425 الموافق 6 سبتمبر 2004، يتضمن القانون الأساسي للقضاء، ج.ر.ج.ج، ع 57، المؤرخة 8 سبتمبر 2004.

138-المرسوم الرئاسي رقم 15-256 المؤرخ في 14 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج، ع 53، المؤرخة 8 أكتوبر 2015.

(2) القوانـــين الفرنســـية:

139-قانون العقوبات الفرنسي المعدل والمتمم.

140-قانون الإجراءات الجزائية الفرنسي.

(3) القوانــين المصريــة:

141-القانون 95 الصادر بتاريخ 1969/06/30 المتعلق بقانون العقوبات المعدل والمتمم، الجريدة الرسمية لجمهورية مصر العربية، العدد 25.

142-القانون رقم 93 المؤرخ 1995/05/28 المتعلق بقانون العقوبات، الجريدة الرسمية للجهورية المصرية، العدد 21 مكرر.

143-القانون رقم 95 المؤرخ في 1996/06/30 المتعلق بقانون العقوبات، الجريدة الرسمية للجمهورية المصرية، العدد رقم 25 مكرر.

144-القانون رقم 148 المؤرخ في 2006/07/15، المتعلق بقانون العقوبات، الجريدة الرسمية للجمهورية المصرية، العدد 28 مكرر.

(4) القوانــين الإماراتــية:

145-قانون العقوبات الاتحادي الاماراتي رقم 2005/34 المعدل والمتمم للقانون 1987/03.

سابعاً– المواثيق والاتفاقيات الدوليــة.

146-اتفاقية بودابست.

147-الاتفاقية العربية لمكافحة الجريمة المعلوماتية.

ثامناً– الأحكام والــقرارات القضائية.

148-قرار محكمة النقض المصرية رقم 69/1155 ق، الجلسة 2000/01/02، غير منشور.

تاسعاً– الــمعاجم والقواميــس.

149-ابن منظور، لسان العرب، ج 15، ط. الثالثة، دار إحياء التراث، بيروت.

150-مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية، مصر، 2004.

عاشراً– الــمراجع الأجنبيــة.

(1) LES REVUES :

151- Ahmed A. Radhi, Data Acquisition and Controlling System by Using Mobile phone Based Microcontroller via Bluetooth, Journal of Al-Ma'mun College, The number 26, Al-Ma'mun University College, 2015.

152- Mohammed Meraj, Sumit Kumar, Evolution of Mobile Wireless Technology from 0G to 5G, International Journal of computer Science and Technologies, Vol 6 (3) 2015

(2) LES LOIS:

153- Loi n°88-19 du janvier 1988, relative à l'informatique, JORF du 06 janvair1988. (LOI GODFRAIN0)

154- Loi n° 2007-297 du 05 mars 2007 relative à la prévention de la délinquance, JORF du 7 mars 2007.

155- Loi n° 2011-267 du 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité intérieure, JORF du 15 mars 2011.

(3) DECISIONS JUDICIAIRES:

156- Cass. Crim. 29 avril 1986,J.C.P, 1987,ll, 20788.N° 5.

157- Cass. Crim 20Janvier 1992, no90-86. 604: juris-Date no 1992- 002462.

إحدى عشر– مـواقع الإنـترنـت.

158- http://www.ebda2.net

159- www.alayam.com

160- www.sciences.uodiyala.edu.ik

161- www.mawdoo3.com

162- http://ww.adslgate.com

163- www.aljazeera.net

164- www.alriyadh.com

165- http://drabbass.wordpress.com

166- kenanaonline.com

167- http://arabic.rt.com

168- www..qallwdalla.com

169- https://khaliid.com

170- www.vetogate.com

171- www.cunotic.com

172- www.m.aher.org

173- www.tbeeb.net

174- http://arabic.com

175- http://www.echchaab.com

176- https://www.facebook.com/algerie.gendarmerie.dz/posts

177- http:// ngmelabdaa.own0.com/t138-topic

178- www.cojss.com/vb/showthead.php?16746

179- http://m.hespress.com

180- archive. Aawsat.com

181- http:// ngmelabdaa.own0.com/t138-topic

182- www.dbaasco.com/vb/showthread.php?t=1127

183- dtarabia.blogspct.com

184- http://www.alriyadh.com

185- https://www.who.int

186- https://www.sehatok.com

187- http://zedni.com

188- www.citc.gov.sa

189- www.djelfa.info/vb/showthread.php?t=571344

190- https://www.sudaress.com/alkharlahza/121

191- http://www.tootshamy.com

192- : http://www.mof.gov.iq

193- http://www.findevgateway.org

194- http://www.almarsal.com

195- www.ibznz.com

فهرس المحتويـــــات

فــهرس المحتويــات

العـــنوان	الصفحـــة
إهـــــــداء	/
شكر وعـــــــرفان	/
قائمـــة المختصرات	/
مقدمـــــــة	01
الفصل التمهيدي: **الأحكام العامة للجرائم المرتكبة بواسطة الهاتف النقال**	06
المبحث الأول: **الـمضامين الـمفاهيمية لتكنولوجـيا الهاتــف النقال**	08
المطلب الأول: مفهوم الهاتف النقال.	08
الفرع الأول: نشأة الهاتف النقال.	08
الفرع الثاني: تعريف الهاتف النقال.	09
الفرع الثالث: مكونات الهاتف النقال.	11
المطلب الثاني: تقنيات وشبكات الهاتف النقال.	12
الفرع الأول: تقنيات الهاتف النقال.	13
الفرع الثاني: شبكات الهاتف النقال.	15
المطلب الثالث: أضرار الهاتف النقال.	16
الفرع الأول: الأضرار الكهرومغناطيسية.	17
الفرع الثاني: أضرار الهاتف النقال الأمنية.	19
الفرع الثالث: الأضرار العلمية.	20

الفرع الرابع: الأضرار البيئية:	20
المبحث الثاني: **مفهوم الجريمة المرتكبة بواسطة الهاتف النقال.**	21
المطلب الأول: مفهوم جرائم الهاتف النقال وخصائصها.	21
الفرع الأول: تعريف جرائم الهاتف النقال.	21
الفرع الثاني: خصائص الجرائم المرتكبة عبر الهاتف النقال.	22
المطلب الثاني: طبيعة جرائم الهاتف النقال.	25
الفرع الأول: جرائم الهاتف النقال جرائم أشخاص.	25
الفرع الثاني: جرائم الهاتف النقال جرائم أموال.	25
الفرع الثالث: جرائم الهاتف النقال الماسة بأمن الدولة والآداب العامة.	25
البـــاب الأول : **الحماية الموضوعية من الجرائم المرتكبة بواسطة الهاتف النقال**	27
الفصل الأول: **جرائم الهاتف النقال الماسة بالأشخاص والأموال.**	29
المبحث الأول: **جرائم الأشخاص المرتكبة بواسطة الهاتف النقال.**	30
المطلب الأول: جرائم الإيذاء المبهج.	30
الفرع الأول: مفهوم جرائم الإيذاء المبهج.	30
الفرع الثاني: مكافحة جريمة الإيذاء المبهج في التشريع الفرنسي.	39
الفرع الثالث: العقوبة المقررة لجريمة الإيذاء المبهج.	42
الفرع الرابع: تقييم المشرع الفرنسي في تجريم جرائم الإيذاء المبهج.	44
الفرع الخامس: موقف المشرع الجزائري من جرائم الإيذاء المبهج.	46

المطلب الثاني: جرائم الاعتداء على الخصوصية باستخدام الهاتف النقال.	46
الفرع الأول: جرائم التقاط الصورة الخاصة وتسجيل المكالمات.	46
الفرع الثاني: جريمة القذف بواسطة الهاتف النقال.	52
الفرع الثالث: جريمة السب بواسطة الهاتف النقال.	56
الفرع الرابع: جريمة التشهير عبر الهاتف النقال.	59
المبحث الثانـــي: **جرائم الأموال المرتكبة بواسطة الهاتف النقال.**	62
المطلب الأول: جرائم السرقة والنصب بواسطة الهاتف النقال.	62
الفرع الأول: جريمة السرقة بواسطة الهاتف النقال.	62
الفرع الثاني: جريمة النصب بواسطة الهاتف النقال.	68
المطلب الثاني: جريمة غسيل الأموال بواسطة الهاتف النقال.	71
الفرع الأول: مفهوم جريمة غسيل الأموال.	71
الفرع الثاني: طرق غسيل الأموال بواسطة الهاتف النقال.	77
الفرع الثالث: موقف التشريعات المقارنة من جرائم غسيل الأموال.	81
الفصل الثاني: **جرائم الاختراق الإلكترونـــــي بواسطة الهاتف النقال.**	83
المبحث الأول: **مفهوم الاختراق الإلكترونـــــي**	84
المطلب الأول: تعريف وأسباب الاختراق الإلكتروني.	84
الفرع الأول: تعريف جريمة اختراق الهاتف النقال.	84
الفرع الثاني: أسباب الاختراق الإلكتروني.	85
المطلب الثاني: طرق اختراق الهاتف النقال .	87

الفرع الأول: اختراق الهاتف النقال عن طريق فيروسات.	87
الفرع الثاني: اختراق الهاتف النقال عن طريق وسائط تبادل المعلومات.	91
الفرع الثالث: اختراق الهاتف النقال عن طريق الإنترنت.	93
الفرع الرابع: اختراق الهاتف النقال عن طريق برامج التجسس الإلكتروني.	97
المبحث الثانـــي: **نـماذج من جرائم اختراق الهاتــف النقال.**	98
المطلب الأول: جرائم الإتلاف وتضخم البريد الإلكتروني	98
الفرع الأول: جرائم الإتلاف.	98
الفرع الثاني: جريمة تضخم البريد الإلكتروني.	105
المطلب الثاني: جريمة الإرهاب الإلكتروني.	108
الفرع الأول مفهوم الإرهاب الإلكتروني.	109
الفرع الثاني: موقف التشريعات من جريمة الإرهاب الإلكتروني.	113
المطلب الثالث: جريمة التجسس الإلكتروني.	118
الفرع الأول: مفهوم جريمة التجسس الإلكتروني.	119
الفرع الثاني: موقف التشريعات من جريمة التجسس.	121
الباب الثاني: **الحماية الإجرائية من الجرائم المرتكبة بواسطة الهاتف النقال.**	126
الفصل الأول: **آليات البحث والتحري عن الجرائم المرتبة بواسطة الهاتف النقال**	127
المبحث الأول: **السلطات المختصة بالتحري والتحقيق عن الجرائم المرتكبة بواسطة الهاتف النقال**	128
المطلب الأول: تحريك الدعوى العمومية في جرائم الهاتف النقال.	128

المطلب الثاني: السلطات المختصة في التحري وجمع الاستدلالات	129
الفرع الأول: الضبطية القضائية ذات الاختصاص العام.	130
الفرع الثاني: الضبط القضائي المختص في الجرائم الإلكترونية.	133
المطلب الثالث: السلطات المختصة في التحقيق.	140
الفرع الأول: التحقيق الابتدائي.	140
الفرع الثاني: التحقيق النهائي.	145
المبحث الثانـــي: **طرق البحث عن الجرائم المرتكبة بواسطة الهاتف النقال.**	150
المطلب الأول: أدوات التحري والتحقيق التقليدية.	150
الفرع الأول: التفتيش.	150
الفرع الثاني: المعاينة.	159
الفرع الثالث: الضبط في الـجرائم المرتكبة بواسطـة الهاتف النقال.	161
المطلب الثاني: أدوات التحري والتحقيق المستحدثة	163
الفرع الأول: مراقبة الاتصالات عبر الهاتف النقال.	164
الفرع الثاني: إجراء التسرب.	169
الفرع الثالث: الإستعانة بمزود الخدمات.	171
الفصل الثانـــي: **أدلة الإثبات في الجرائم المرتكبة بواسطة الهاتف النقال**	174
المبحث الأول: **الشـــــهادة والـخبرة.**	175
المطلب الأول: الشهادة	175
الفرع الأول: مفهوم الشهادة.	175

الفرع الثاني: الشاهد المعلوماتي.	177
المطلب الثاني: الخبرة في الجرائم المرتكبة بواسطة الهاتف النقال.	183
الفرع الأول: مفهوم الخبرة.	183
الفرع الثاني: الخبرة التقنية في الجرائم المرتكبة بواسطة الهاتف النقال.	185
المبحث الثاني: **الدليل الإلكتروني.**	190
المطلب الأول: مفهوم الدليل الإلكتروني.	190
الفرع الأول: تعريف الدليل الإلكتروني.	190
الفرع الثاني: خصائص الدليل الإلكتروني.	192
الفرع الثالث: عوائق اكتشاف الدليل الإلكتروني.	195
المطلب الثاني: أنواع الأدلة الإلكترونية المستمدة من الهاتف النقال.	196
الفرع الأول: الدليل الناتج عن فحص مسار وبروتوكول الهاتف النقال.	197
الفرع الثاني: الدليل الناتج عن النظام المادي والمعلوماتي للهاتف النقال.	199
المطلب الثالث: حجية الدليل الإلكتروني.	199
الفرع الأول: شروط قبول الدليل الإلكتروني.	200
الفرع الثاني: سلطة القاضي في تقدير الدليل الإلكتروني.	203
الخاتـمة	208
قائمة المصادر والمراجع	213
فـهرس المحتويـــات	229

الملخـــص:

شكل الهاتف النقال ثورة في مجال الاتصالات الحديثة من خلال التقنيات والخدمات التي يوفرها للمستخدمين، وصاحب هذا التطور العديد من الأضرار سواء على مستوى الفردي كالصحة، أو على المستوى الاجتماعي كتدهور الأخلاق العامة، فضلاً عن مساهمته في تفشي العديد من الجرائم التي ظهرت في البداية كسلوكيات عادية يسعى البعض من خلالها للمتعة والتسلية متناسي الأضرار التي قد تنتج عنها.

ومع النقلة الكبيرة التي شهدها الهاتف النقال في السنوات الأخيرة أصبح الهاتف النقال أحد الأدوات الإلكترونية الأكثر استخدماً، وذلك من خلال الميزات العديدة التي استطاعت شركات الاتصالات استحدثها من حلال دمج الهاتف النقال بتقنية المعلوماتية وتوفير خدمات الإنترنت، ما جعل الهاتف صورة مصغرة عن الحاسوب في مجال المعلوماتية، مما أسهم في استخدام الهاتف النقال في ارتكاب العديد من الجرائم ذات الطبيعة الإلكترونية.

وفي الوقت الذي تزداد فيه خطورة استخدام الهاتف النقال في الجريمة بمختلف أنواعها، مازالت التشريعات العربية لم تتخذ موقف جاد حيال تجريم استخدام هذه الوسيلة في الإجرام، أو استحداث آليات عقابية وإجرائية تكون على القدر الكافي لزجر وردع هذا النوع من الجرائم.

ومن خلال الإشكالية الواردة في هذه الدراسة، حاولنا الوقوف على العديد من الأنماط والصور الإجرامية التي ترتكب بواسطة الهاتف النقال؛ والتي تتنوع بين جرائم أشخاص، وجرائم أموال، أو جرائم ضد أمن الدول، كما قد تتخذ صوراً إجرامية ذات طبيعة إلكترونية أو تقليدية، كما وقفنا على الإجراءات المتبعة في الكشف والتحقيق في مثل هذا النوع من الجرائم والجهات القضائية المختصة في ذلك، فضلاً عن وسائل الإثبات الإلكترونية التي تستعين بها المحكمة في إصدار حكمها في هذا النوع من الجرائم.

الكلمات المفتاحية: الهاتف النقال، الإيذاء المبهج، التجسس، الإرهاب الالكتروني، الفيروسات، الدليل الالكتروني.

Abstract:

The mobile phone revolution in the field of modern communications has constituted through the technologies and services provided to users and the developers of this means a lot of damage, both at the level of individual health or at the level of social deterioration of public morals. It has also contributed in the outbreak of many crimes that initially emerged as normal behaviors for fun and entertainment but they have serious consequence in the long terms.

With mobile phone penetration in recent years, mobile phones have become one of the most widely used electronic devices through the many features that telecom operators have been able to use to integrate mobile phones with it and Internet services. The use of these technologies has contributed in the spread of many crimes of electronic nature.

At a time when the use of mobile phones in various forms of crime is increasing, Arab legislation has not taken a serious stance on the criminalization of the use of this means of criminality or the development of punitive and procedural mechanisms that are sufficient to deter such crimes.

Through the problematic of this study, we tried to identify the many patterns and criminal images that are caused by inappropriate use of the mobile phone. The study shows that the State has not created sufficient legislations against mobile phone crimes, which range from crimes of persons, money crimes, or crimes against the security of States. We have also observed the procedures taken for the detection and investigation of such crimes as well as the means of evidence used by the Court in issuing its verdicts.

Keywords: Mobile Phone, Delicious Abuse, Spyware, Electronic Terrorism, Viruses, Electronic Directory.

Résumé :

Le mobile représente une révolution dans le domaine de la télécommunication moderne, à travers les techniques et les services fournis aux utilisateurs et, le développement de cette évolution a provoqué (causé) de nombreux dommages, tant au niveau individuel comme sur la santé et, ou sur le niveau social comme la détérioration de la moralité, ainsi que sa contribution à la propagation de nombreux crimes qui sont apparus au début comme des comportements normaux dont lesquels certains gens cherchent à se distraire et se divertir, en oubliant, les dommages (les effets négatifs) qui pourraient en résulter.

Avec le grand changement (la transition ou le bond) qu'a connu le téléphone mobile ces dernières années, il est devenu l'un des outils électroniques les plus utilisés grâce aux nombreuses fonctionnalités que les opérateurs de télécommunication ont pu innover pour l'intégrer aux services informatiques et Internet. Ce qui a fait du téléphone une vignette de l'ordinateur dans le domaine de l'informatique, ce qui a contribué à l'utilisation du téléphone mobile dans la perpétration de nombreux crimes de nature électronique.

Alors que au moment où le téléphone mobile est de plus en plus utilisé dans diverses formes de criminalité, les législations arabes n'ont pas adopté des positions sérieuses en vue de criminaliser l'utilisation de cet outil ou de mettre en place des mécanismes punitifs et des procédures suffisantes pour dissuader des tels crimes.

À travers la problématique de cette étude, nous avons essayé d'identifier des nombreux schémas et images criminelles que le téléphone mobile peut contribuer à leur perpétration, ou des crimes contre le téléphone mobile, allant des crimes contre les individus, les crimes pécuniaires (financiers) ou les crimes contre la sécurité d' États, qui peuvent avoir un Caractère électronique ou traditionnel: nous avons également commenté les procédures suivies pour la détection et l'investigation de tels crimes et les autorités judiciaires compétents en la matière, ainsi que les moyens de preuve utilisés par la Cour en rendant son jugement.

Mots-clés: Téléphone Mobile, Abus Délicieux, Logiciels Espions, Terrorisme Electronique, Virus, Répertoire Electronique.