معارف
ISSN 1112-7007
EISSN 6804 -2600
المجلد 17 / العدد 2 (ديسمبر 2022): ص.ص:210-230

جرائم الإنترنت، جرائم حقيقية في عالم افتراضي

Internet crimes, real crimes in a virtual world

أ. يوسف صغير*

جامعة البويرة، مخبر الدولة والإجرام المنظم، الجزائر، y.sghir@univ-bouira.dz

تاريخ الاستلام: 2021/12/07؛ تاريخ القبول: 2022/08/14؛ تاريخ النشر: 2022/12/31

ملخص:

قدمت الثورة التكنولوجية في مجال الاتصالات خدمات جليلة للأفراد والدول على حد سواء، حيث سهلت هذه الأخيرة الحياة اليومية الخاصة بهم، وخير دليل على ذلك الاعتماد الكبير على شبكة الإنترنت في مختلف التعاملات التي يقومون بها، غير أن هذا التوسع في استعمال هذه الوسيلة الاتصالية لم يمر بسلام، فالمجرمين قاموا بنقل أعمالهم الإجرامية إلى هذا العالم الافتراضي، لتفرض هذه الجرائم منطقها عبر الساحة القانونية الوطنية والدولية، الأمر الذي أدى بمختلف التشريعات إلى إعادة النظر في ترسانتها القانونية الموضوعية والإجرائية من أجل التعامل مع هذه الظاهرة الإجرامية المستحدثة.

كلمات مفتاحية: الإنترنت؛ الجريمة؛ جرائم الإنترنت؛ المجرم المعلوماتي؛ أركان الجريمة.

Abstract:

The technological revolution in the field of communications provided great services to individuals and countries alike, as the latter facilitated their daily lives, and the best evidence of this is the great reliance on the internet in the various transactions that they carry out, but this expansion in the use of this means of communication did not pass peacefully, criminals have transferred their criminal acts to this virtual world, so that these crimes impose their logic through the natoinal an international legal arena, which led various legislations to reconsider their substantive and procedural legal arsenal in order to

* المؤلف المرسل.

deal with this emerging criminal phenomenon.

Keywords: internet; crime; cybercrime; information criminal; elements of crime.

المقدمة:

تعتبر شبكة الإنترنت من الانتاجات الاجتماعية المذهلة التي عرفها العالم مؤخرا، فهذه الوسيلة الاتصالية وسعت مفهوم الحياة الاجتماعية للإنسان وفتحت له آفاق جديدة لم يكن يعرفها من قبل، حيث أصبح هذا الأخير يمكن أن يقوم بمختلف أعماله وهو قابع في مكانه وكل ما يحتاج إليه هو جهاز حاسوب ومودم لكي يفتح له العالم بمصراعيه.

كانت بداية استخدام هذه الوسيلة الاتصالية في مجالات بحثية وعسكرية بحتة، ثم تطورت إلى مجالات عديدة منها التجارية، والثقافية، والتواصلية وحتى الترفيهية، ولم يكن يعلم أحد من واضعي هذه الشبكة أنها سوف تستخدم في يوم من الأيام في ارتكاب العديد من الجرائم، حيث أن المجرمين والجماعات الإجرامية قاموا بنقل أعمالهم الإجرامية إلى هذا الفضاء الافتراضي، نظرا لما يقدمه من تسهيلات كعدم خضوعه إلى أي سلطة وتعديه للحدود الجغرافية للدول، وتميزه باللامادية وسهولة إخفاء الهوية والأفعال.

أدى هذا الوضع بالمجتمع الدولي والدول على حد سواء إلى محاولة مواجهة هذا النوع المستحدث من الجرائم، وذلك في بادئ الأمر عن طريق وضعها في نطاق النصوص القانونية القائمة، غير أن هذه الوضعية لم تدم طويلا نظرا للسرعة في التطور الذي تعرفه هذه الجريمة، الأمر الذي أدى إلى ضرورة استحداث نصوص قانونية خاصة بها، في إطار هذا التباين بين الرؤى بين القانونيين ارتأينا طرح الإشكالية التالية: ما هي طبيعة الجرائم المرتكبة عبر الإنترنت؟

المبحث الأول: مفهوم جرائم الإنترنت

اختلفت التسميات التي أطلقت على هذه الظاهرة الإجرامية، منها جرائم الحاسوب، الجرائم المعلوماتية، الجرائم الإلكترونية، جرائم الإنترنت، ويعد هذا الاختلاف في المصطلحات نتيجة للحداثة التي تتميز بها هذه الجريمة، والتي لم يكن يعرفها القانون من قبل، الأمر الذي أدى بالفقهاء والقانونيين إلى عدم الاستقرار على مقصود موحد لهذه الجرائم (مطلب أول).

واكب التطور الذي عرفته الجريمة في هذا المجال، ظهور تطورات كبيرة في العلوم الجنائية وخاصة المتعلقة بعلم الإجرام، ولعل أهمها المتعلقة بطبيعة المجرم في هذا المجال، حيث أن هذه الأخيرة أظهرت فئات جديدة من المجرمين يختلفون كل الاختلاف عن المجرمين التقليديين (مطلب ثانٍ).

المطلب الأول: المقصود بجرائم الإنترنت

يقصد بالجريمة في العالم التقليدي بصفة عامة أنها: "فعل غير مشروع صادر عن إرادة جنائية ويقرر له القانون جزاء"، غير أن السؤال المطروح في هذا النطاق هل يمكن وصف الجريمة المرتكبة عبر الإنترنت عن طريق هذا التعريف، ومن أجل الإجابة على هذا التساؤل ارتأينا التطرق إلى نقطتين هما: التعريف بجرائم الإنترنت (فرع أول)، ثم خصائصها (فرع ثان).

الفرع الأول: تعريف جرائم الإنترنت

تباينت الآراء التي حاول القانونيين من خلالها إلى وضع تعريف جامع ومانع لظاهرة جرائم الإنترنت، وذلك راجع إلى اختلاف المعايير التي اعتمد عليها في ذلك والتي سوف نجيزها على النحو التالي:

يعتمد أصحاب الاتجاه الأول في تعريفهم لجرائم الإنترنت على الوسيلة التي من خلالها يتم ارتكاب هذه الجريمة، حيث عرفها الفقيه "توم فوريستر" في مؤلفه عن قصة ثورة المعلومات على أنها: "فعل إجرامي تم باستخدام الحاسوب كأداة رئيسية".

كما عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج دورا رئيسيا"[1].

وقد ذهب جانب آخر في تعريف جرائم الإنترنت على اعتماده على صفة الجاني فيها وذلك باعتباره: "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني"[2].

(1) - **معاشي سميرة**، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 17، جوان 2018، ص402.

(2) - **محمد السعيد زناتي**، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إليزي، العدد الثاني، ديسمبر 2017، ص31.

ركز أصحاب الاتجاه الثالث اهتمامهم على موضوع الجريمة، ولم يركزوا على الوسيلة المستخدمة في ارتكابها، أي عندما يكون الكمبيوتر هو محل الجريمة، ولا تعني بذلك سرقة الحاسب الآلي، وإنما تشمل كل شيء غير ملموس مرتبطا بالكمبيوتر أي الكيان المنطقي كالمعلومات المخزنة في الذاكرة[1].

نظرا لعدم نجاح أصحاب الاتجاهات السابقة في وضع تعريف جامع لظاهرة جرائم الإنترنت، ظهر جانب آخر عمد في تعريفه لهذه الظاهرة الإجرامية على دمج أكثر من معيار، حيث اعتبروها: "الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها"[2].

وقد حاول المشرع الجزائري في هذا الصدد أن يقدم تعريفا لها حيث سماها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وذلك بمقتضى المادة 02 فقرة 1 من القانون رقم 09-04 المتضمن الوقاية من جرائم الإعلام والاتصال ومكافحتها حيث نصت على: "يقصد في مفهوم هذا القانون بما يأتي: أ-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[3].

الفرع الثاني: خصائص جرائم الإنترنت

تتميز جرائم الإنترنت بخصائص عديدة تميزها عن الجرائم التقليدية وذلك من خلال ما يأتي:

- جرائم تتميز بالخطورة: حيث إن ما يتميز به عمل الكمبيوتر والوظائف التي يقوم بها من سرعة في العمل، وطاقة كبيرة لاستيعاب المعلومات، جعلت منه يشكل خطورة على حياة الأفراد وأسرار حياته الشخصية، وكذلك اقتصاديات المؤسسات، وأمن

(1) - **حبيباتي بثينة**، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، جامعة الجلفة، مجلد 12، عدد 03، جويلية 2020، ص608.

(2) - **غازي عبد الرحمن هيان الرشيد**، الحماية القانونية من الجرائم المعلوماتية (الحاسب والإنترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص108-109.

(3) - أنظر المادة 02 من القانون رقم 09-04 المؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47، صادر 16 غشت سنة 2009.

البلاد واقتصادها[1].

- جرائم متعدية للحدود: من أهم الخصائص التي تتميز بها جرائم الإنترنت هي تخطيها للحدود الجغرافية، ذلك أن الشبكات المعلوماتية جعلت العالم قرية صغيرة ومحت كل الحدود الوهمية بين الدول[2].
- صعبة الاكتشاف: توصف الجرائم المرتكبة عبر الإنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة واتلافها، والتجسس واعتراض المراسلات وغيرها من الجرائم، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها[3].
- صعبة الإثبات: حيث يصعب في الكثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية، ولعل السبب في ذلك يعود إلى استخدام الجاني وسائل فنية وتقنية معقدة في الكثير من الأحيان، كما يتمثل السلوك المكون للركن المادي فيها بعمل سريع قد لا يستغرق أكثر من بضع ثوان علاوة على سهولة محو الدليل والتلاعب به في الوقت الذي تفتقر فيه هذه الجرائم إلى الدليل المادي التقليدي[4].
- قصور النصوص التقليدية على مواكبتها: يعد التطور السريع في الميدان المعلوماتي من أهم العوائق التي تحول دون مكافحة الجريمة المرتكبة عبر الإنترنت بطريقة ناجعة، ففي كل يوم تظهر تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مجاراته من طرف السلطة التشريعية[5].

---

(1) - **معاشي سميرة**، مرجع سابق، ص410.

(2) - **محمد السعيد زناتي**، مرجع سابق، ص32.

(3) - **رحموني محمد**، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أدرار، مجلد 16، عدد 3، سبتمبر 2017، ص441.

(4) - **محمد علي سالم، حسون عبيد عجيج**، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 02، 2008، ص92.

(5) - **أنيس العذار**، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، المجلد 17، العدد 01، 2018، ص730.

المطلب الثاني: مجرمي الإنترنت

برزت حقيقة الجريمة المرتكبة عبر الشبكة العالمية للإنترنت ببروز أصناف من المجرمين يتميزون عن نظرائهم في العالم التقليدي، والذين غالبا ما يسعون إلى استغلال هذه الوسيلة الاتصالية لكي يرتكبوا العديد من الجرائم التي تكون نتائجها وخيمة على الأفراد والدول على حد سواء.

سوف نتطرق في هذا المجال إلى أصناف مجرمي الإنترنت فرع أول، ثم سنبين الصفات التي يتميز بها مجرم الإنترنت عن المجرم التقليدي فرع ثاني.

الفرع الأول: أصناف مجرمي الإنترنت

أظهرت الجريمة المرتكبة عبر الإنترنت العديد من أصناف المجرمين الذين يرتكبون جرائمهم عبرها، حيث كان هذا التصنيف تبعا للمجال الذي يقوم فيه كل مجرم بالسلوك الإجرامي فيه، والتي سوف نبينها على النحو التالي:

- **فئة القراصنة:** هم عادة من أصحاب الخبرة الذين يدخلون إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها، وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، وهم نوعين: القراصنة الهواة الهاكرز، وهم المتطفلون والمتسللون الذين يتحدون إجراءات أمن الشبكات لكن لا تتوفر لديهم في الغالب دوافع التحدي وإثبات الذات، وهذه الفئة أغلبها من التلاميذ وطلبة الثانويات والشباب العاطل عن العمل، أما القراصنة المحترفون الكراكرز أو كما يطلق عليه بالمقتحم، هو الشخص الذي يقوم بالتسلل إلى نظام الحاسوب للاطلاع على المعلومات المخزنة فيه أو لإلحاق الضرر أو العبث بها أو سرقتها[1].
- فئة المتطرفون: يعرف التطرف في هذا المجال بأنه عبارة عن أنشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري وخاصة المحرض على العنف أيا كان التيار

(1) - **عبد السلام محمد المايل، عادل محمد الشربجي، علي قابوسة**، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم –الأسباب- سبل المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات، المركز الجامعي إليزي، العدد 04، جوان 2019، ص248.

أو الشخص أو الجماعة التي تتبنى أو تشجع أو تمول كل ما من شأنه توسيع دائرة ترويج مثل هذه الأنشطة[1].

- **فئة الحاقدون:** تقوم هذه الفئة بجرائمها في هذا النطاق بدافع الانتقام، حيث يعد هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية، ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية أو الطرد من الوظيفة فيتولد لدى المجرم المعلوماتي الرغبة في الانتقام من رب العمل[2].
- فئة الجريمة المنظمة: ترتكب في هذا المجال أغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب وتحويل المكاسب إليه، كما أن من عادة من يمارسون التلصص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطتهم عقد المؤتمرات[3].

الفرع الثاني: صفات مجرمي الإنترنت

يتميز المجرم المعلوماتي عن غيره من المجرمين في العالم التقليدي بعدة صفات منها:

- مجرم يتسم بالمهارة والذكاء: يتميز المجرم المعلوماتي غالبا بالذكاء، حيث يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف بل يحقق هدفه الإجرامي بهدوء، فالإجرام

(1) - **فايز بن عبد الله الشهري**، ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25-2010/10/27، ص05.

(2) - **صابر بحري، منى خرموش**، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الانحراف، جامعة باتنة 1، المجلد 06، العدد 01، سنة 2021، ص52.

(3) - **هشام محمد فريد رستم**، أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 01-03 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص436-437.

المعلوماتي هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يميل إلى العنف[1].

- مجرم اجتماعي: يختلف الإجرام المعلوماتي عن الإجرام التقليدي من حيث أن المجرم في هذا الشأن يحيا ويعيش وسط المجتمع ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى، فهو شخصية اجتماعية[2].
- مجرم حذر: يتصف المجرمون عبر الإنترنت بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي الإنترنت بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان[3].
- مجرم يتمتع بالسلطة تجاه النظام المعلوماتي: يقصد بالسلطة جملة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي، والتي تسمح له وتمكنه من ارتكاب جريمته، فكثير من المجرمين في هذا المجال لديهم سلطة مباشرة أو غير مباشرة في مواجهة محل الجريمة كشفرة الدخول إلى النظام المعلوماتي، وشفرة الدخول للملفات وقراءتها وتعديل مضمونها أو محوه[4].
- مجرم يعود للإجرام: يتميز المجرم المعلوماتي بأنه يعود للجريمة دائما، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به عدة مرات، فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء، وإنما نتيجة شعوره بقدراته ومهاراته في الاختراق[5].

المبحث الثاني: الطبيعة القانونية لجرائم الإنترنت

إن النمو السريع لشبكة ا إنترنت وتوسع استعمالها وتنوع أشكال وصور الجريمة المرتكبة عبرها، جعل أمر تحديد الطبيعة القانونية لهذه الأخيرة يتميز بصعوبة كبيرة،

(1) - **حبيباتي بثينة**، مرجع سابق، ص610.

(2) - **ربيعي حسين**، المجرم المعلوماتي- شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 40، جوان 2015، ص289.

(3) - **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2008، ص79.

(4) - **ربيعي حسين**، مرجع سابق، ص290.

(5) - **علاء الرواشدة، أسماء ربحي**، الجريمة في ظل العولمة: دراسة تحليلية للبنية وسياسات المواجهة، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، جامعة أدرار، مجلد 18، عدد 02، جوان 2019، ص223.

خاصة في ظل التباين والاختلاف في الرؤى بين الفقهاء بسبب عدم تبنيهم لمعايير واحدة وثابتة ولضوابط مشتركة من أجل تصنيف هذه الجرائم المستحدثة (مطلب أول).

يعتبر كذلك تحديد أركان هذه الجريمة جزءًا لا يتجزأ من تحديد طبيعتها القانونية، وتخلف أحد هذه الأركان يؤدي بالضرورة إلى انتفاء الجريمة، حيث يتطلب قانونا كأصل عام وجود ركن مادي وركن معنوي، وركن شرعي بمقتضاه يتم التجريم والعقاب (مطلب ثان).

المطلب الأول: تصنيف جرائم الإنترنت

تعتبر الجرائم المرتكبة عبر الإنترنت من الجرائم الحديثة، الأمر الذي جعل الفقهاء والقانونيين لا يستقرون على معيار واحد لتصنيفها، وذلك راجع إلى تشعبها وسرعة تطورها، فمنهم من صنفها على أساس الوسيلة التي ترتكب بها ومنهم من صنفها على أساس محل الجريمة.

وفي نطاق هذا التباين ارتأينا تقسيم وتصنيف هذه الجريمة من حيث اعتبارها جرائم واقعة على الأموال (فرع أول)، ثم جرائم واقعة على الأشخاص (فرع ثان)، وأخيرا جرائم واقعة على أمن الدول (فرع ثالث).

الفرع الأول: جرائم واقعة على الأموال عبر الإنترنت

تتمثل الجرائم الواقعة على الأموال عبر الإنترنت في:

- جرائم السطو على أرقام بطاقات الاتمان: واكب استخدام البطاقات الائتمانية من خلال شبكة الإنترنت ظهور الكثير من المتسللين للسطو عليها، باعتبارها نقودا إلكترونية، خاصة من جهة أن الاستيلاء على بطاقات الائتمان أمرا ليس بالصعوبة بما كان، فلصوص بطاقات الائتمان مثلا يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت ومن ثم بيع هذه المعلومات للآخرين[1].
- تبييض الأموال عبر الإنترنت: ساعدت شبكة الإنترنت القائمون بعمليات غسيل

(1) - **حسن طاهر داود**، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص73.

الأموال بتوفير عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها الدول من أجل إعاقة هذا النشاط، وكذا تشفير عملياتهم مما يعطيها قدر كبير من السرية، وخاصة في تسهيل على مرتكبي جرائم غسيل الأموال نقلها إلى أي مكان في العالم[1]، من أجل استثمارها في إقليم أي دولة من العالم، وإعطاء هذه الأموال الصبغة المشروعة[2].

- جرائم السرقة: تتم سرقة المال المعلوماتي –إن أمكن الوصف- عن طريق اختلاس البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية –مثل الاسم، العنوان، الأرقام السرية- الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الإنترنت بحيث تؤدي بالغير إلى تقديم الأموال –الإلكترونية أو المادية- إلى الجاني عن طريق التحويل البنكي[3].
- تجارة المخدرات: ظهرت في عصر الإنترنت مخاوف من مواقع السوء –إن صح التعبير- وهو تعبير مقارب لصدق السوء، ومن تلك الواقع طبعا المواقع المنتشرة عبر الإنترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشء لاستخدامها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة[4].

الفرع الثاني جرائم واقع على الأشخاص عبر الإنترنت

أفرزت الشبكة العالمية للإنترنت العديد من الممارسات التي تمس بالأفراد سواء في سمعتهم أو شرفهم أو حتى في حقهم في الحياة الخاصة، نذكر منها ما يلي:

---

(1) - **خالد بن عبد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009، ص50.

(2) - **صالحة العمري**، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الإجتهاد القضائي على حركة التشريع، جامعة بسكرة، ديسمبر 2009، ص179.

(3) - **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004، ص138.

(4) - **محمد محمد صالح الألفي**، أنماط جرائم الإنترنت، ص11، مقال متوفر على الموقع التالي:
http://www.eastlaws.com

- جرائم السب والقذف: تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، فتستعمل للمساس بشرف الغير أو كرامتهم واعتبارهم، ويتم السب والقذف وجاهيا عبر خطوط الاتصال المباشر أو يكون كتابيا، أو عن طريق المطبوعات، وذلك عبر المبادلات الإلكترونية بريد إلكتروني، صفحات الويب، غرف المحادثة[1].
- **الاعتداء على الحق في الحياة الخاصة:** تعتبر جرائم الاعتداء على حرمة الحياة الخاصة من الجرائم القديمة التي عرفتها المجتمعات الإنسانية القديمة ولكنها سرعان ما تطورت نظرا للتقدم التكنولوجي الذي لعب دور في سرعة وسهولة انتشار الأخبار والصور الذي من شأنه أن يمثل تهديدا لخصوصية الأشخاص وسهولة الاعتداء على حرمة حياتهم الخاصة[2].
- انتحال الشخصية: يقصد بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الإنترنت، وتتخذ جريمة انتحال الشخصية عبر الإنترنت أحد الوجهين التاليين: انتحال شخصية الفرد وانتحال شخصية المواقع[3].
- التهديد والمضايقة: يقصد بالتهديد الوعيد بشر، وهو زرع الخوف في النفس بالضغط على إرادة الإنسان، وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له بها صلة، ويعد تهديد الغير من خلال البريد الإلكتروني واحدا من أهم الاستخدامات غير المشروعة للإنترنت، حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها[4].
- نشر الإباحة: يتم ذلك من خلال المواقع الإلكترونية الموجودة على الشبكة، والتي

(1) - **عبد الرحمان بن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات (الإنترنت)، الطبعة الأولى، دار الوراقين للنشر والتوزيع، بيروت، 2004، ص312.

(2) - **حوالف حليمة، مهاجي فاطمة الزهراء**، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، مجلد 03، العدد16، جوان 2021، ص150.

(3) - **محمد بن عبد الله بن علي المنشاوي**، جرائم الإنترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص54-55.

(4) - **خالد بن عبد الله بن معيض العبيدي**، مرجع سابق، ص52.

تستخدم بغرض الإثارة الجنسية من خلال قيام المجرم الإلكتروني بنشر صور جنسية فاضحة وأفلام جنسية، التي كثيرا ما تستهدف الأطفال والشباب؛ لأن هذه الفئة أقل تحصينًا[1].

الفرع الثالث: جرائم واقعة على أمن الدولة عبر الإنترنت

يمكن حصر الجرائم التي تمس أمن الدول عبر الإنترنت فيما يلي:

- الإرهاب: تعد الشبكات المعلوماتية وفي مقدمتها شبكة الإنترنت الملاذ الآمن للإرهابيين وتشكل شبكة الإنترنت أيضا الملتقى الحر لهم، فأخذ الإرهابيون ينشرون مبادئهم وأفكارهم الضالة والهدامة عبر هذه الشبكة وبواسطة غرف المحادثة لكسب أكبر عدد ممكن من الناس المتعاطفين معهم ولتجنيدهم في جماعتهم ومنظماتهم الإرهابية لكي يتسنى لهم دعمهم ماليا ومعنويا وبالطرق والوسائل المتاحة كافة، ومما ينشره الإرهابيون على مواقعهم ا إرهابية الأفكار التي تفسد العقول وتحرف الأفكار والعقائد، وكذلك تعليم المتعاطفين معهم تصنيع الأسلحة والقنابل للمواقع المعادية والعبث بها وكذلك شن هجمات ضد المواقع الإلكترونية التي تحارب أفكارهم ومبادئهم والقيام بعمليات إرهابية على أرض الواقع وفي أماكن محددة[2].
- الجريمة المنظمة: يعد الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس طبيعيا فقط، ولكنه ترابط من المرجح ان يتطور إلى حد أبعد في المستقبل، فشبكة الإنترنت تؤمن الأقنية والأهداف في نفس الوقت للجريمة، وتمكن من استغلال هذه الأقنية والأهداف لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر، وجماعات الجريمة المنظمة لا تريد أكثر من ذلك، ولهذا السبب من الأهمية بمكان تحديد بعض الطرق التي تتداخل فيها الجريمة المنظمة حاليا مع الجريمة التي ترتكب من خلال الشبكات الإلكترونية[3].

---

(1) - **رحموني محمد**، مرجع سابق، ص445-446.

(2) - **عبد الرحمان عوض رجا الملالحة، فتيحة عمارة**، جريمة الإرهاب المعلوماتي أسبابه وأساليبه، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 34، العدد 01، 2020، ص1324.

(3) - **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص42-43.

- التجسس: يقوم قراصنة الحاسوب باختراق المواقع أو الحواسيب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء[1].
- الجرائم الماسة بالأمن الفكري: بناءً على خصائص الشبكة العالمية للإنترنت، التي منحت المستخدم الكثير من الخيارات، من خلال عدم خضوعها لأي رقابة، وعبورها للحدود الجغرافية بين الدول، ونموها السريع والمتواصل، وإمكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي وعدم المواجهة نتيجة للافتراضية التي تعد من أهم خصائص هذه الشبكة، إضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى الانحراف الفكري، من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية للإنترنت، وتهدد الأمن بأبعاده كافة[2].

المطلب الثاني: أركان جرائم الإنترنت

تتشابه الجريمة المرتكبة عبر الإنترنت مع الجريمة التقليدية بضرورة توفر أركان يتم من خلالها وصف هذه الأفعال بالجريمة رغم اتخاذها للعالم الافتراضي مسرحا لها، فهي تشترك معها بوجود فعل غير مشروع، ووجود مجرم يقوم بهذا الفعل ووجود نص قانوني يحدد التجريم والعقوبة اللازمة له، وعلى هذا الأساس سنتطرق إلى تبيان الركن الشرعي لهذه الجريمة (فرع أول)، ثم الركن المادي (فرع ثان)، وأخيرا الركن المعنوي (فرع ثالث).

الفرع الأول: الركن الشرعي

حاولت قوانين العقوبات مواجهة تحديات الجرائم المرتكبة عبر الإنترنت بطرق تقليدية كتلك المقررة في جرائم الأموال، إلا أنه تبين قصور هذه الوسائل التقليدية عن مواجهة

(1) - **شرقي صبرينة**، الإرهاب الإلكتروني والتحول في مفهوم القوة، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، المجلد 07، العدد 02، 2020، ص564.

(2) - **ناصر بن محمد البقمي**، أثر التحول إلى مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة السعودية، 22-25 جمادى الأول 1430هـ، ص18.

العديد من الأفعال التي تهدد مصالح اجتماعية والتي ارتبطت بظهور وانتشار أجهزة الكمبيوتر.

تبين في بعض الأحوال أن ثمة أفعالا جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، من ذلك الاعتداء على حرمة الحياة الخاصة، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر، فإنه لا يخضع للتجريم وفقا للقواعد العامة، كما أن التداخل في نظام الحاسب الآلي وتغيير البيانات، فهي صورة جديدة لا يعرفها قانون العقوبات قبل ظهور الكمبيوتر وشبكة الإنترنت، كل ذلك يؤكد قصور القواعد التقليدية في القانون الجنائي على مكافحة هذا النوع الجديد من الجرائم[1].

أصدر المشرع الجزائري - سدًّا لهذا الفراغ التشريعي- العديد من النصوص التي تجرم هذا الفعل، كإضافة القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المادة 394 مكرر إلى المادة 394 مكرر 7[2]، حيث شدد في العقوبة بمجرد المحاولة بالمساس بالمنظومة الآلية للمعطيات، كما أنه ومن أجل الحد من هذه الجريمة، أصدر قانون خاص يعمل على وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها طبقا للقانون رقم 09-04[3]، كما تبنى المشرع حماية حرمة الحياة الخاصة للمواطنين، من خلال منع التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة وسرية بغير إذن صاحبها، أي منع استخدام الوسائل التكنولوجية وإساءة استعمالها تطبيقا للمادة 303 مكرر من قانون العقوبات، وكذلك من خلال القانون رقم 18-07[4] المتعلق بمعالجة المعطيات ذات

(1) - **غنام محمد غنام**، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 01-03 ماي 2003، المجلد الثاني، ص625-626.

(2) - قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن تعديل قانون العقوبات، ج.ر عدد 71، صادر في 2004/11/10.

(3) - القانون رقم 09-04 المؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

(4) - قانون رقم 18/07 المؤرخ في 10 يوليو 2018، يتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34، صادر في 10 يوليو 2018.

الطابع الشخصي، وهذا كله يصب في موضوع مبدأ شرعية التجريم والعقاب[1].

الفرع الثاني: الركن المادي

جرم المشرع الجزائري - كما أسلفنا ذكره- هذه الجرائم في المادة 394 مكرر من قانون العقوبات في فقرتها الأولى، ولعل جريمة الدخول والبقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات من أهم الجرائم المعلوماتية عموما، وذلك أن أغلب جرائم المعلومات لا يمكن ارتكابها إلا بعد الدخول للنظام، لهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف الجرائم المعلوماتية الأخرى، لذا حرص المشرع على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات، فجرم الدخول غير المصرح به وكذا البقاء بغير تصريح سواء تم ذلك في كل النظام أو جزء منه، كما تتحقق الجريمة سواء أدى هذا التواجد أو لم يؤدِّ إلى نتائج معينة.

يتمثل السلوك الإجرامي في جريمة الدخول والبقاء غير المصرح بهما في نشاط إجرامي إما في فعل الدخول إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، وإما فعل البقاء في هذا النظام أو جزء منه[2].

يتطلب النشاط أو السلوك المادي في جرائم ا إنترنت وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضا معرفة بداية هذا النشاط فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها أشياء أو صور مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها[3].

تثير مسألة النتيجة الإجرامية والعلاقة السببية في جرائم الإنترنت العديد من الإشكالات القانونية، فبالنسبة لتحديد النتيجة الإجرامية طرحت عدة أسئلة فهل

(1) - **حوالف عبد الصمد**، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة الأغواط، العدد 4، نوفمبر 2018، ص89.

(2) - **قسمية محمد، خضري حمزة**، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، جامعة خميس مليانة، المجلد السابع، العدد 02، نوفمبر 2020، ص131.

(3) - **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د..س.ن، 2005، ص58.

تقتصر على العالم الافتراضي، أم أن لها جزءا في العالم المادي، وهل تقتصر النتيجة على مكان واحد أو تمتد لتشمل دولا وأقاليم عدة، كذلك الأمر بالنسبة لتحديد الرابطة السببية اعتبرت من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والإنترنت، وتطور إمكانياتها وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب الحقيقية للإساءات المرتكبة في هذه المسؤولية[1].

الفرع الثالث: الركن المعنوي

يقوم الركن المعنوي للجريمة المرتكبة عبر الإنترنت على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون، كانتحال شخصية المزود عبر الإنترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجرمية المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية من العمل غير المشروع الذي بيت النية على ارتكابه، وهو عالم بالآثار الضارة الناشئة عنه[2].

تعتبر جريمة الدخول أو البقاء في النظم المعلوماتية من الجرائم العمدية، بحيث يكفي فيها القصد العام، فيكفي لتوافر هذه الجريمة أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه أو تعمد البقاء فيه رغم انتهاء مدة حقه في البقاء ولو كان الدخول مشروعا، أما إذا انتفى علمه فإنها لا تتوافر الجريمة، كأن يجهل وجود حظر الدخول، أو أنه مسموح له الدخول فيه، ولا يتأثر القصد الإجرامي بالباعث على الدخول أو البقاء، فيظل القصد الإجرامي قائما حتى ولو كان الباعث من الدخول أو

(1) - **منصور بن صالح السلمي**، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2010، ص75-76.

(2) - **عبد الله ذيب عبد الله محمود**، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009، ص96.

البقاء للفضول أو التنزه أو إثبات القدرة على الانتصار على النظام[1].

لذلك يشترط توفر القصد الجنائي في هذا النوع من الجرائم الحديثة، أي أن الشخص يتعامل في تصرف ممنوع قانونا، لأن الجريمة المعلوماتية تتطلب نوع من الملكات الذهنية وقدرة في تحكم في البرمجيات، فالدخول والولوج للموقع خاص دون وجه حق، من خلال فك شيفرة وغيرها من هذه التصرفات، تتطلب القصد الجنائي وأنه يعلم بأن هذا التصرف يشكل جريمة معلوماتية يعاقب عليها القانون، وبذلك إذا تحققت الأركان السالف ذكرها، نكون أمام جريمة معلوماتية سخر لها المشرع كل التدابير القانونية والوقائية من أجل الحد منها[2].

خاتمة:

يتجلى لنا من خلال هذه الدراسة أن الجريمة المرتكبة عبر الإنترنت من بين أخطر الجرائم التي عرفها العالم في الآونة الأخيرة، حيث برزت حقيقة هذه الجرائم من خلال تحرك الدول والمجتمع الدولي على حد سواء من اجل معالجة هذه الظاهرة الإجرامية المستحدثة، وذلك عن طريق وضعها في إطارها القانوني من خلال تحديد مفهومها وتصنيفها وتبيان أركانها بالإضافة إلى تبيين المجرم الذي يقوم بها، وذلك إدراكا منهم بأن شبكة الإنترنت كوسيلة اتصالية غيرت وجه العالم، فالجرائم التي ترتكب عبرها تكون لها نفس الصفة، ومن هذا المنطلق يمكن لنا أن نتقدم ببعض الاقتراحات التي يمكن أن تساهم في معالجة هذه الظاهرة الإجرامية المستحدثة حيث نوجزها على النحو التالي:

- ضرورة وضع آليات تكرس التعاون الدولي الفعلي والحد من الإجراءات الدولية التقليدية تمشيا مع خصوصية الجريمة التي تتميز بالسرعة وتعديها للحدود الوطنية.
- ضرورة تكوين الضبطية القضائية والقضاة بمختلف مناصبهم في مجال المعلوماتية وشبكات الاتصال.
- ضرورة وضع أقطاب جزائية خاصة بهذا النوع من الجرائم.

(1) - **أمحمدي بوزينة آمنة**، خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، جامعة تبسة، العدد 05، د.س.ن، ص78.

(2) - **حوالف عبد الصمد**، مرجع سابق، ص90-91.

- ضرورة وضع أجهزة أمنية متخصصة بمراقبة شبكات الاتصال خاصة شبكة الإنترنت.
- ضرورة تحسيس المواطنين بخطورة هذه الجرائم وحثهم على التبليغ عنها.

المراجع:

1- الكتب

1. **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د.ن، د.س.ن، 2005
2. **حسن طاهر داود**، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000
3. **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004
4. **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2008
5. **عبد الرحمان بن عبد الله السند**، الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات الإنترنت، الطبعة الأولى، دار الوراقين للنشر والتوزيع، بيروت، 2004
6. **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والإنترنت الجرائم الإلكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007

2- المقالات:

1. **أمحمدي بوزينة آمنة**، خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، جامعة تبسة، العدد 05، د.س.ن.
2. **أنيس العذار**، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة بجاية، المجلد 17، العدد 01، 2018.
3. **حبيباتي بثينة**، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، جامعة الجلفة، مجلد 12، عدد 03، جويلية 2020.

4. **حوالف حليمة، مهاجي فاطمة الزهراء**، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة سعيدة، مجلد 03، العدد 16، جوان 2021.

5. **حوالف عبد الصمد**، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة الأغواط، العدد الرابع، نوفمبر 2018.

6. **ربيعي حسين**، المجرم المعلوماتي- شخصيته وأصنافه، مجلة العلوم الإنسانية، جامعة بسكرة، العدد 40، جوان 2015.

7. **رحموني محمد**، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أدرار، مجلد 16، عدد 3، سبتمبر 2017.

8. **شرقي صبرينة**، الإرهاب الإلكتروني والتحول في مفهوم القوة، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة، المجلد 07، العدد 02، 2020.

9. **صابر بحري، منى خرموش**، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية، مجلة دراسات في سيكولوجية الانحراف، جامعة باتنة 1، المجلد 06، العدد 01، 2021.

10. **صالحة العمري**، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة بسكرة، ديسمبر 2009.

11. **عبد الرحمان عوض رجا الملالحة، فتيحة عمارة**، جريمة الإرهاب المعلوماتي أسبابه وأساليبه، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 34، العدد 01، 2020.

12. **عبد السلام محمد المايل، عادل محمد الشربجي، علي قابوسة**، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم –الأسباب- سبل المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات، المركز الجامعي إليزي، العدد 04، جوان 2019.

13. **علاء الرواشدة، أسماء ربحي**، الجريمة في ظل العولمة: دراسة تحليلية للبنية وسياسات المواجهة، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، جامعة أدرار، مجلد 18، عدد 02، جوان 2019.

14. **غنام محمد غنام**، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون المجلد الثاني، 01-03 ماي 2003.

15. **فايز بن عبد الله الشهري**، ثقافة التطرف على شبكة الإنترنت الملامح والاتجاهات، الندوة العلمية استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 25-2010/10/27.

16. **قسمية محمد، خضري حمزة**، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، جامعة خميس مليانة، المجلد السابع، العدد 02، نوفمبر 2020.

17. **محمد السعيد زناتي**، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إليزي، العدد الثاني، ديسمبر 2017.

18. **محمد علي سالم، حسون عبيد عجيج**، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 02، 2008.

19. محمد محمد صالح الألفي، أنماط جرائم الإنترنت، مقال متوفر على الموقع التالي: http://www.eastlaws.com

20. **معاشي سميرة**، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 17، جوان 2018.

21. **ناصر بن محمد البقمي**، أثر التحول إلى مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة السعودية، 22-25 جمادى الأول 1430هـ.

22. **هشام محمد فريد رستم**، أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد من 01-03 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004.

3- الرسائل والمذكرات الجامعية:

1. **عبد الله ذيب عبد الله محمود**، حماية المستهلك في التعاقد الإلكتروني دراسة مقارنة، رسالة قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009.

2. **محمد بن عبد الله بن علي المنشاوي**، جرائم الإنترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.

3. **منصور بن صالح السلمي**، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2010.

4. **خالد بن عبد الله بن معيض العبيدي**، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية دراسة تحليلية مقارنة، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية، الرياض، 2009.

5. **غازي عبد الرحمن هيان الرشيد**، الحماية القانونية من الجرائم المعلوماتية الحاسب والإنترنت، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.

4- النصوص القانونية:

1. قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن تعديل قانون العقوبات، ج.ر عدد 71، صادر في 2004/11/10.

2. قانون رقم 09-04، المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ر عدد 47، صادر في 16 غشت 2009.

3. قانون رقم 07/18 المؤرخ في 10 يوليو 2018، يتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34، صادر في 10 يوليو 2018.