International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (11)
November 2026
الإصدار (5)، العدد (11)

الحماية الجزائية لمستخدمي الوسائط الإلكترونية

راسم مسير جاسم
أستاذ مشارك دكتور، تخصص القانون الجنائي، قسم القانون، كلية المنصور الجامعة، العراق

معن زكي كاظم الكرعاوي
محامي، دكتور، المدير المفوض لشركة القسطاس الذهبي للخدمات والاستشارات القانونية، بغداد، العراق
maan_advocate99@yahoo.com

الملخص

يتناول البحث موضوع الحماية الجزائية لمستخدمي الوسائط الإلكترونية، بهدف بيان مدى كفاية المنظومة القانونية القائمة في حماية المستخدمين، واستجلاء الثغرات التشريعية والإجرائية التي تسمح بوقوع الاعتداءات الرقمية، والبحث في سبل تطوير الإطار القانوني بما يحقق التوازن بين حرية الاستخدام وأمن الفضاء الإلكتروني. وقد اعتمد البحث منهجاً تحليلياً مقارناً، تناول من خلاله النصوص القانونية العراقية وبعض التشريعات المقارنة.

خلص البحث إلى أن التشريعات العقابية التقليدية، بما فيها القانون العراقي، لا تزال غير قادرة على استيعاب الطبيعة الخاصة للجرائم الإلكترونية، وأن العديد من صور الاعتداءات تحتاج إلى تجريم خاص وعقوبات تتناسب مع خطورتها. كما تبين وجود صعوبات كبيرة في الإثبات الرقمي لسهولة محو الأدلة وسرعة انتقالها عبر الحدود الدولية، إضافة إلى محدودية الخبرات الفنية لدى جهات التحقيق، وغياب تشريع شامل لحماية البيانات الشخصية.

انتهى البحث إلى ضرورة تطوير الإطار التشريعي العراقي عبر إصدار قانون خاص للجرائم الإلكترونية يتضمن تعريفات دقيقة وصوراً واضحة للتجريم، وتشديد العقوبات على الاعتداءات الخطيرة، وتوفير آليات فعّالة للإثبات والتحقيق الرقمي، وتعزيز التعاون الدولي. كما أوصى البحث باعتماد نظام وطني لحماية البيانات الشخصية، وتأسيس هيئة وطنية للجرائم الإلكترونية.

وبذلك يؤكد البحث أن الحماية الجزائية لمستخدمي الوسائط الإلكترونية لم تعد رفاهية تشريعية، بل أصبحت ضرورة تفرضها طبيعة العصر الرقمي، وتتطلب منظومة قانونية متطورة قادرة على تأمين الفضاء الإلكتروني وضمان ثقة مستخدميه واستقرار المعاملات الرقمية.

حيث اتخذت العديد من الدول قوانين خاصة بالجرائم المعلوماتية والإلكترونية وخاصة دول الجوار وعلى سبيل المثال الأردن وسوريا وكذلك مصر واليمن وتونس وأخذت حيز التنفيذ لما لهُ من أهمية خاصة في المرحلة الحالية والذكاء الاصطناعي وخاصة عند إنشاء حساب أو صفحة أو مجموعة أو قناة أو ما يماثلها على منصات التواصل الاجتماعي وتنسيبها الى أشخاص أخرين طبيعي أو معنوي ويعاقب بالحبس إضافة الى بعض الجرائم التي تحدث عبر الاتصال الهاتفي عن سب وشتم وتهديد والتهجم وتشهير عبر التواصل الاجتماعي والذم والقدح الإلكتروني وأكيد على أن لا يدخل في حرية التعبير لأجل ذلك اصبح من المهم جداً إصدار تشريعاً ثابتاً يبين هذهِ التصرفات تماشياً مع الفعل والعقوبة وكذلك بالنسبة للعراق فلا يوجد أي قانون مستقل ومعتمد للجرائم الإلكترونية أو المعلوماتية وإنما موجود في أروقة مجلس النواب العراقي ولم يتم إقراره وفيه حماية البيانات الشخصية وكذلك الايصاء بإيقاع اقوى العقوبات بالمنتهك.

الكلمات المفتاحية: الجريمة الإلكترونية، الحماية الجنائية، الإعلام الإلكتروني، البيانات الشخصية، الاختراق الرقمي.

International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (11)
IJLRS
November 2026
الإصدار (5)، العدد (11)

Criminal Protection for Users of Electronic Media

Rasem Mseer Jasim
Assistant Professor, Department of Law, Al-Mansour University College, Iraq

Maan Zaki Kadhim Al Karraawi
Attorney-at-Law, PhD, Managing Director of Al-Qistas Al-Dhahabi Legal Services and Consultations Company, Baghdad, Iraq
maan_advocate99@yahoo.com

Abstract

This research addresses the criminal protection of electronic media users, aiming to evaluate the adequacy of the existing legal framework, identify legislative and procedural loopholes that facilitate digital attacks, and explore ways to enhance the legal system to balance usage freedom with cybersecurity. Adopting a comparative analytical approach, the study examines Iraqi legal provisions alongside select comparative legislations.

The study concludes that traditional penal laws, including the Iraqi Legal Code, remain incapable of accommodating the unique nature of cybercrimes, with many forms of digital abuse requiring specific criminalization and penalties proportional to their severity. Furthermore, significant challenges persist in digital forensics due to the ease of evidence deletion, cross-border data transfer, limited technical expertise within investigative authorities, and the absence of comprehensive personal data protection legislation.

The research emphasizes the urgent need to update the Iraqi legislative framework by enacting a dedicated Cybercrime Law featuring precise definitions, clear offense characterizations, stricter penalties for severe violations, effective digital investigation mechanisms, and enhanced international cooperation. Additionally, it recommends establishing a national personal data protection framework and a specialized national agency for cybercrime.

Ultimately, the study underscores that criminal protection for electronic media users is no longer a legislative luxury but an essential requirement of the digital era—vital for securing cyberspace, building user trust, and safeguarding digital transactions.

Numerous countries, particularly neighboring states such as Jordan, Syria, Egypt, Yemen, and Tunisia, have enacted and enforced specialized information and cybercrime laws. These legislations are crucial today, particularly regarding artificial intelligence and acts such as creating unauthorized accounts, pages, groups, or channels on social media platforms impersonating natural or legal persons, which carry prison sentences. They also cover offenses committed via telephone or social media, including libel, slander, threats, defamation, and digital insult, ensuring these acts are distinct from constitutionally protected freedom of expression. Consequently, enacting clear legislation aligning offenses with appropriate sanctions is imperative. In Iraq, no standalone or ratified cybercrime law currently exists; relevant draft legislation incorporating personal data protection and stringent penalties remains pending in the Iraqi Council of Representatives.

Keywords: Cybercrime, Criminal Protection, Electronic Media, Personal Data, Digital Intrusion.

المقدمة

شهد العالم خلال العقود الأخيرة تحولاً جذرياً في بنية التواصل الإنساني، بعد أن أصبحت الوسائط الإلكترونية – بمختلف صورها – جزءاً لا يتجزأ من الحياة اليومية للأفراد والمؤسسات والدول. فقد انتقلت العلاقات الاجتماعية، والعمليات التجارية، والممارسات الثقافية، وحتى المعاملات الرسمية إلى الفضاء الإلكتروني، مما أفرز واقعاً جديداً يوازي في أهميته الواقع المادي التقليدي، بل ويتفوق عليه في بعض الأحيان من حيث السرعة والانتشار وسهولة الوصول. غير أن هذا الانتقال الواسع إلى الفضاء الرقمي لم يكن خالياً من التحديات، إذ رافقته أنماط مستحدثة من الاعتداءات، وظهرت سلوكيات غير مشروعة اتخذت من البيئة الإلكترونية مجالاً خصباً لها، مستغلة الطبيعة اللامادية للوسائط الرقمية وصعوبة تعقب مرتكبي الجرائم فيها.

ومن بين أكثر الفئات حاجة إلى الحماية القانونية في هذا السياق هم مستخدمو الوسائط الإلكترونية، الذين يتعرضون لأشكال متعددة من الاعتداءات، بدءاً من انتهاك الخصوصية، مروراً بالاحتيال الإلكتروني، ووصولاً إلى التهديد والابتزاز، إضافة إلى الاعتداءات على البيانات الشخصية والمحتوى الرقمي. وقد كشفت التجربة المعاصرة أن الأدوات القانونية التقليدية، التي وُضعت لحماية الأفراد في البيئة المادية، لم تعد كافية لمواجهة الجرائم الإلكترونية، مما استدعى تدخل المشرع لإعادة صياغة مفاهيم الحماية الجزائية بما يتلاءم مع طبيعة الوسائط الإلكترونية وحدودها التقنية والقانونية.

وانطلاقاً من ذلك، يتناول هذا البحث موضوع الحماية الجزائية لمستخدمي الوسائط الإلكترونية، بوصفه موضوعاً متجدداً ومتعدد الأبعاد، يجمع بين القانون الجنائي وتكنولوجيا المعلومات، ويعكس حاجة ملحة لإيجاد منظومة قانونية فعّالة تضمن أمن الأفراد وحقوقهم في البيئة الرقمية. ويهدف البحث إلى بيان الإطار القانوني لحماية مستخدمي الوسائط الإلكترونية، وتحديد صور الاعتداءات التي تستلزم حماية جزائية، وتحليل النصوص القانونية الوطنية والمقارنة التي عالجت هذا الموضوع، مع الوقوف على مدى كفايتها، والثغرات التي تحتاج إلى معالجة، والضوابط التي ينبغي أن تُراعى في التجريم والعقاب الإلكتروني.

أولا: أهمية البحث:

تنبع أهمية هذا البحث من مجموعة من الاعتبارات العلمية والعملية التي تجعل موضوع الحماية الجزائية لمستخدمي الوسائط الإلكترونية من الموضوعات الجوهرية في الوقت الراهن، ويمكن إجمال أهميتها في النقاط الآتية:

1. تزايد الاعتماد على الوسائط الإلكترونية في مختلف جوانب الحياة اليومية، مما يجعل أي اعتداء يقع عبر هذه الوسائط ذا أثر مباشر على الأفراد والمجتمع والاقتصاد الوطني.
2. ظهور أنماط جديدة من الجرائم الإلكترونية لم تكن معروفة في البيئة التقليدية، كالاختراق، والاستيلاء على البيانات، وانتحال الشخصية، والابتزاز الإلكتروني، وهي جرائم تستلزم أدوات قانونية ملائمة لطبيعتها التقنية.
3. قصور التشريعات التقليدية عن استيعاب خصوصيات الجرائم الإلكترونية، مما فرض على المشرّع ضرورة تطوير منظومة حماية جزائية تتماشى مع التطور التقني الهائل، وتحقق الفعالية في التجريم والعقاب.

وبذلك، لا تقتصر أهمية البحث على الجانب النظري أو التشريعي، بل تمتد لتلامس البعد الاجتماعي والاقتصادي والتقني، وتُسهم في تعزيز الأمن القانوني في فضاء أصبح جزءاً لا يتجزأ من الواقع المعاصر.

ثانياً: إشكالية البحث:

رغم الجهود التشريعية المبذولة في تنظيم استخدام الوسائط الإلكترونية، لا تزال الحماية الجزائية لمستخدميها تواجه إشكاليات متعددة، تنبع من طبيعة الفضاء الإلكتروني ذاته، ومن محدودية القواعد القانونية التقليدية في مواجهة الاعتداءات الرقمية. وعليه، تتمثل الإشكالية الرئيسة لهذا البحث في السؤال الآتي:

إلى أي مدى استطاعت المنظومة الجزائية الحالية أن توفر حماية فعّالة لمستخدمي الوسائط الإلكترونية، في ضوء تعدد صور الاعتداءات الإلكترونية وتعقيدها، وما هي حدود القصور التشريعي والإجرائي التي تستلزم إعادة نظر أو تطوير لضمان حماية واقعية للضحايا؟

ثالثاً: منهج البحث:

للإلمام بموضوع البحث اتبعنا أكثر من منهج بحثي، إذ اتبعنا المنهج التحليلي وذلك من خلال تحليل نصوص قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل لبيان مدى كفايتها لتجريم الاعتداءات الواقعة على مستخدمي الوسائط الإلكترونية، مع بيان بعض الأحكام الواردة في مشروع قانون جرائم المعلوماتية العراقي، كما اعتمدنا المنهج المقارن لمقارنة ما توصلنا له من أحكام مع ما يقابلها في قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008، مع التطرق لبعض الأحكام الواردة في التشريعات المقارنة كلما دعت الحاجة لذلك.

رابعاً: خطة البحث:

اتبعنا في هذا البحث التقسيم الثنائي، حيث قسمنا هذا البحث كالآتي:

المبحث الأول: النظام العقابي على مستخدمي الوسائط الإلكترونية:

- المطلب الأول: العقوبات الأصلية.
- المطلب الثاني: العقوبات التبعية.

المبحث الثاني: كفاية النصوص العقابية في حماية مستخدمي الوسائط الإلكترونية:

- المطلب الأول: الصعوبات التشريعية والإجرائية في مكافحة الجرائم المعلوماتية.
- المطلب الثاني: تبني آليات ملاحقة أكثر فعالية.

المبحث الأول: النظام العقابي على مستخدمي الوسائط الإلكترونية

الجزاء العقابي هو الأثر الذي يقرّره النص الجزائي الخاص على مخالفة النهي أو الأمر بالقيام بفعل مقرر فيه، وله صورتان: العقوبات والتدابير الاحترازية وهما تمثلان الوسيلتين اللتين استقرت عليهما التشريعات لإسباغ الحماية الجزائية على المصالح والحقوق التي يرغب المشرع بحمايتها وعملاً بمبدأ الشرعية الجزائية القائل إنه لا جريمة ولا جزاء إلا بمقتضى النص، فمن المفروض أن تتضمّن النصوص الجزائية الخاصة بتشريعات الجرائم الإلكترونية صورتي الجزاء العقابي وهما العقوبات والتدابير إلى جانب التجريم أو عطفاً أو إحالة إلى جزاء وارد في القسم الخاص من قانون العقوبات العام وسائر القوانين الجزائية[1] كما هو حاصل في جرائم النشر الإلكتروني والتزوير الإلكتروني إذ خلو قانون المعاملات الإلكترونية من تحديد صور هذه الجرائم وجزاءاتها، إنما يعني بالضرورة الإحالة على نصوص القسم الخاص من قانون العقوبات العام وسائر النصوص الجزائية النافذة.

ولبيان ذلك سنقسم هذا المبحث على مطلبين، سنتطرق في المطلب الأول لدراسة العقوبات الأصلية، أما المطلب الثاني فسنتطرق فيه لدراسة العقوبات التبعية.

المطلب الأول: العقوبات الأصلية:

بداية لابد من القول، أن الأنظمة القانونية نصت صراحةً على أفعال الجرم المعلوماتي كما في تشريعات "مكافحة الجرائم المعلوماتية" لبعض البلدان العربية، ولكن النقطة الأساسية هنا، في ظل هذه التشريعات المتخصصة بجرائم المعلوماتية، تبقى الحاجة الملحة إلى الرجوع إلى تلك التشريعات التقليدية التي حددت مفهوم الأفعال الجرمية لتطبيق أحكامها[2]، وبناء عليه سنقوم بتقسيم هذا المطلب إلى فرعين سنتناول في الفرع الأول تطبيق التشريعات التقليدية في ظل غياب التشريعات المتخصصة أما في الفرع الثاني سنتناول مشروع قانون جرائم المعلوماتية وآثاره على الضمانات القانونية.

الفرع الأول: تطبيق التشريعات التقليدية في ظل غياب التشريعات المتخصصة:

وهو ما سيتم الرجوع فيه إلى التشريعات التقليدية التي تملأ هذا الفراغ في تشريعات مكافحة جرائم المعلوماتية. غير أن

---

[1] حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها، مكتبة بدران الحقوقية، بيروت، لبنان، 2017، ص9.
[2] محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2019، ص16.

المشكلة ستبدو بشكل أوضح في بعض البلدان، كما في العراق[3]، التي ليس لديها تشريعات لجرائم المعلوماتية، ولذلك سيكون السؤال حول مدى إمكان تطبيق هذه النصوص التقليدية على أفعال التعدي على مستخدمي الوسائط الإلكترونية.

الحقيقة ليس هنالك ما يمنع من تطبيق أحكام القوانين التقليدية على الجرائم المعلوماتية، لأنها في حقيقتها جرائم تستحق العقاب، وأن ذلك سيبدو أنجع مما لو أفلت مرتكبوها من العقاب؛ إذ إن مثل هذا التجريم سيؤدي إلى تطويق هذه الجرائم والحيلولة بين فاعليها وبين الإفلات من جرائمهم، كما أن هذه الجرائم المعلوماتية لا تختلف عن نظيرتها التقليدية إلا في وسيلة ارتكابها، وهو أمر ليس مؤثراً في التجريم في التقدير، فضلاً عن أن الإجرام المعلوماتي يبدو أشد خطورة من الإجرام التقليدي بآلاف المرات نظراً إلى اتساع الهائل في استخدام شبكة الإنترنت.[4]

وإذا كانت بعض التشريعات العربية، تناولت في نصوصها جريمة المعلوماتية في نصوصها التقليدية، مع ما قد يثار في ظلها من مشكلات قانونية، فإن عدداً من التشريعات العربية المتخصصة بجرائم المعلوماتية، قد نصت على تجريم أفعال الجرم المعلوماتي والعقاب عليها، ومنها القانون الإماراتي بالقول "كل من أنشأ موقعاً على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات تحت مسميات تمويهية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالسجن مدة لا تزيد على خمس سنوات".[5]

يتضح أن غياب التشريعات المتخصصة بالجرائم المعلوماتية في بعض الدول، ومنها العراق، لا يمنع من تطبيق القواعد الجنائية التقليدية لمواجهة هذه الأفعال، باعتبار أن جوهر الجريمة يبقى واحداً وإن اختلفت وسيلة ارتكابها. كما أن الرجوع إلى هذه النصوص يسهم في سد الفراغ التشريعي ومنع إفلات الجناة من العقاب، إلى حين صدور قوانين خاصة تنظم الجرائم المعلوماتية بصورة أكثر دقة، كما فعلت بعض التشريعات العربية التي جرّمت هذه الأفعال بنصوص صريحة وحددت العقوبات المقررة لها.

الفرع الثاني: مشروع قانون جرائم المعلوماتية وآثاره على الضمانات القانونية:

قامت الحكومة العراقية في سبيل ذلك بسنّ ما تشير إليه بـ "قانون جرائم المعلوماتية" لتنظيم استخدام شبكات المعلومات وأجهزة الحاسوب والأجهزة والأنظمة الإلكترونية. وكانت القراءة الأولى للقانون المقترح قد تمت أمام مجلس النواب العراقي يوم 27 يوليو/تموز 2011، وكانت القراءة الثانية للقانون المقترح قد تمت يوليو/تموز 2012. وبينما تتم كتابة مسوّدته الأولى حاليا، وقد ينتهك التشريع المقترح المعايير الدولية الحامية لإجراءات التقاضي السليمة، وحرية التعبير، وحرية تكوين الجمعيات.

يقول القانون المقترح في المادة (2) إنه يهدف إلى "توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات، ومعاقبة مرتكبي الأفعال التي تشكل اعتداءً على حقوق مستخدميها." على وجه التحديد يوفر القانون عقوبات على استخدام أجهزة الحاسوب فيما له علاقة بالعديد من الأنشطة الممنوعة، مثل الاحتيال المالي والاختلاس المادة 7 وغسيل الأموال المادة 10 وتعطيل الشبكات المادة 14 والمراقبة غير المشروعة المادة 15 أولاً ب والمادة 16 والاعتداءات على الملكية الفكرية المادة 21 ومع ذلك، فإن هذا القانون لا يقتصر في استهدافه على نطاق محدود، و بالأحرى ستجرّم أحكامه استخدام الحاسوب فيما يتصل بنطاق واسع من الأنشطة التي يتم تعريفها بشكل فضفاض – الكثير منها غير خاضع للقواعد حالياً – دون الرجوع إلى أية معايير محددة، وبالسماح للسلطات العراقية بمعاقبة الأفراد بهذه الطريقة، تبدو أحكام القانون متعارضة مع القانون الدولي والدستور العراقي، وإذا تم تطبيقها فسوف تشكل تقليصاً خطيراً لحق العراقيين في حرية التعبير وتكوين الجمعيات.[6] ويتبين مما سبق أن الحكومة في العراق سعت إلى تنظيم الجرائم المعلوماتية من خلال إعداد مشروع قانون خاص بذلك، يهدف إلى حماية الاستخدام المشروع للحاسوب وشبكات المعلومات وتجريم الأفعال التي تمس حقوق المستخدمين، كجرائم الاحتيال المالي وتعطيل الشبكات والمراقبة غير المشروعة. ومع ذلك، فقد وُجهت إلى هذا المشروع انتقادات تتعلق باتساع نطاق

[3] لم يصدر الى الآن قانون عقابي يعالج الجرائم المعلوماتية في العراق وإنما فقط مشروع قانون وقد تم تعديله لعام 2020.
[4] عدلي محمد عبد الكرخي، جريمة الإرهاب عبر الوسائل الإلكترونية في القانونين اللبناني والعراقي، رسالة ماجستير، الجامعة الإسلامية، بيروت، 2018، ص 102 وما بعدها.
[5] المادة 21 من القانون الاتحادي الخاص بمكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006.
[6] عدلي محمد عبد الكرخي، جريمة الإرهاب عبر الوسائل الإلكترونية في القانونين اللبناني والعراقي، مرجع سابق، ص 103 وما بعدها.

التجريم وغموض بعض مفاهيمه، الأمر الذي قد يثير تعارضاً مع بعض الضمانات الدستورية والمعايير الدولية المتعلقة بحرية التعبير وتكوين الجمعيات.

المطلب الثاني: العقوبات التبعية:

يرتبط إجرام المعاملات الإلكترونية غالباً بإجرام المشروعات العاملة في هذا المجال حيث يحصل من خلال الهيئات المعنوية الاعتبارية وبأدواتها ولمصلحتها، وقد فرض القانون العراقي على إجرام هذه الهيئات تدابير احترازية عينية تتلاءم مع طبيعتها إلى جانب العقوبات المقررة للفاعلين الطبيعيين.[7]

ويقتضي التأكيد على أن القسم العام من قانون العقوبات يعتبر القانون المشترك لسائر التشريعات الجزائية التكميلية والخاصة حال خلو النص الخاص من قاعدة تحكم الموضوع، ولدراسة العقوبات التبعية سنقوم بتقسيم هذا المطلب إلى فرعين سنتناول في الفرع الأول أنواع التدابير الاحترازية أما في الفرع الثاني سنتناول خصائصها.

الفرع الأول: أنواع التدابير الاحترازية:

هذا ويلاحظ على التشريع الجزائي للمعاملات الإلكترونية خلوه أو سهوه عن فرض هذه التدابير الجزائية المتلائمة مع طبيعة هذه الجرائم، ورغم أهميتها الكبيرة في تحقيق فعالية هذا التشريع وتفادي الأخطار أو الأضرار الناجمة عن هذه الجرائم، كون التدابير المذكورة تصيب المجرم في نطاق مشروعه الذي بمناسبته ارتكبت الجريمة، وهذا أقسى ما يمكن أن يتعرض له إذ يحرم من الأرباح غير المشروعة التي كان يطمح في تحقيقها. كما أن في هذه التدابير الاحترازية تتحقق الوقاية من خطورة التمادي في مثل هذه الجرائم وتكرار وقوعها في المستقبل.

وبافتراض خلو التشريع الجزائي الخاص بالمعاملات الإلكترونية من نص على فرض التدابير الاحترازية يقتضي الرجوع إلى القاعدة لعامة في قانون العقوبات العام، والتي تفرض تدابير احترازية عينية وجوبية.

وللتدابير أهداف متعددة تتناسب مع كل حالة إجرامية على حدة، وعلى ذلك تتنوع التدابير وفقاً لطبيعة الهدف الذي تسعى إلى تحقيقه، وهي كما يأتي:[8]

1- تدابير تستهدف التهذيب والإصلاح، وتطبق على الأحداث والصم والبكم.

2- تدابير تستهدف العلاج والرعاية ، وتطبق على مرضى العقل والمجرمين الشواذ.

3- تدابير تستهدف مباشرة الدفاع والرقابة، وتطبق على المجرمين العائدين والمعتادين على الإجرام ولكن على الرغم من تنوع أهداف التدابير حسب أنواعها، إلا أنها تهدف جميعاً إلى إزالة الخطورة الإجرامية، أي القضاء على العوامل الدافعة إلى الإجرام والحيلولة بين من تتوافر لديه وبين ارتكاب جريمة في المستقبل لكي يعود بعدها عضواً صالحاً في المجتمع ويسلك السلوك المطابق للقانون.

يتضح مما سبق أن التشريع الجزائي المتعلق بالمعاملات الإلكترونية يفتقر إلى النص على التدابير الاحترازية الملائمة لطبيعة الجرائم المعلوماتية، رغم أهميتها في تعزيز فعالية المواجهة الجنائية والحد من المخاطر الناجمة عنها. وفي حال غياب هذه النصوص، يمكن الرجوع إلى القواعد العامة في قانون العقوبات التي تجيز فرض تدابير احترازية مختلفة، تهدف إلى الإصلاح أو العلاج أو الرقابة، بحسب حالة الجاني.

الفرع الثاني: خصائص التدابير الاحترازية:

تتميز التدابير الاحترازية بجملة خصائص تتمثل بما يأتي:

1. تخضع التدابير لمبدأ الشرعية، وهذا ما أكدت عليه المادة (1) من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل[9]، كما نصت المادة (5) من ذات القانون على أنه: "لا يفرض تدبير احترازي إلا في الأحوال بالشروط المنصوص عليها في القانون...".

[7] سمير عالية، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020، ص 110.
[8] علي عبد القادر قهوجي، علم الإجرام والعقاب، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص 211.

ويعني ذلك وجوب أن يحدد المشرع الجريمة أو الوضع المشبه بها الذي يجيز إنزال التدبير ووجوب أن يحدد كذلك التدابير التي يجوز للقاضي أن يختار من بينها ما يوقعه على المدان وبهذا تنحصر سلطة المحكمة في توقيع التدبير ضمن الحدود وبالشروط التي رسمها المشرع في ضوء ظروف الجاني والجريمة.

ويعد من النتائج الضرورية لإخضاع التدابير الاحترازية لمبدأ الشرعية الجزائية، عدم رجعية النصوص التي تقرر تدابير احترازية ما لم تكن في مصلحة المتهم، الأمر الذي تقضي به المادة (5) من قانون العقوبات العراقي والتي جاء فيها: ...وتسري على التدابير الاحترازية الأحكام المتعلقة بالعقوبات من حيث عدم رجعيتها وسريان القانون الأصلح للمتهم".

فإذا صدر قانون جديد بعد أن يكون الفاعل قد ارتكب الجريمة، وكان هذا القانون يلغي تدبيراً مقرراً بمقتضى القانون السابق أو يستبدله بتدبير آخر أخف، فإن هذا التدبير يسري بأثر رجعي بحيث يطبق على المحكوم عليه وإن كان القانون الذي يقرره قد صدر بعد ارتكاب الجاني جريمته[10]، ولا يسري القانون الجديد إذا كان يفرض تدبيراً لم يكن مقرراً في القانون السابق أو كان مقرراً لكنه أخف.

2. كما تنطوي التدابير على إيلام ولكن غير مقصود، كما تتجه هذه التدابير إلى المستقبل، بمعنى منع الجاني من ارتكاب الجريمة مستقبلاً[11]، وهذه التدابير لا تصدر التدابير إلا بحكم قضائي لحماية حقوق وحريات الإنسان.
3. يجب إنزال كل التدبير الذي تقتضيه الخطورة الإجرامية، وعليه لا يجوز التذرع بظروف مخففة لعدم النطق بالتدبير، كما لا وجه لإيقاف تنفيذه.[12]
4. إن وظيفة التدابير هي الوقاية المنع الخاص وتتمثل في القضاء على العوامل المسببة للحالة الخطرة الفردية.[13]
5. يستند تطبيق التدابير على أساس موضوعي الجريمة وآخر شخصي الحالة الخطرة، كما تخضع التدابير الاحترازية لمبدأ المساواة، أي المساواة أمام القانون.[14]
6. إن التدبير الاحترازي لا يرتبط بالمسؤولية الجزائية، فيمكن توقيعه على شخص غير مسؤول جزائياً، كما هو الشأن بالنسبة للمجانين والصغار، وذلك أن مناط التدبير الاحترازي هو الخطورة الإجرامية .[15]
7. أنها محددة في قانون العقوبات من حيث النوع، ومن ثم فأن دور محكمة الموضوع يقتصر على إنزال التدبير ضمن الحدود المبينة في القانون.[16]

نلاحظ مما سبق أنه لم يرد في مجال التدابير الاحترازية ما يشير إلى حالات التكرار، وهذا ما يتناسب مع طبيعتها الإصلاحية المجردة عن عنصر الإيلام المقصود، كما أن الأسباب المخففة لا تطبق على التدابير الاحترازية، لأن هذه الأسباب واردة فقط بشأن العقوبات دون التدابير الاحترازية، وهذا مما يوضح الفوارق بين العقوبات والتدابير.

المبحث الثاني: كفاية النصوص العقابية في حماية مستخدمي الوسائط الإلكترونية

إن الجهود الوطنية في تطوير سبل مواجهة الجرائم الالكترونية كثرت في الآونة الأخيرة وذلك لأهمية هذه الوسائل في مكافحة الجرائم الخطيرة التي تحدث في عالمنا وتطور باستمرار، ويجب على ذلك ان تتطور الوسائل التي تؤدي الى مكافحة هذه الجرائم.

---

[9] نصت المادة (1) من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل على أنه: "لا عقاب على فعل أو امتناع إلا بناءً على قانون ينص على تجريمه وقت اقترافه ولا يجوز توقيع عقوبات أو تدابير احترازية لم ينص عليها القانون".
[10] فخري عبد الرزاق الحديثي، قانون العقوبات، القسم العام، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 511.
[11] علي عبد القادر قهوجي، علم الإجرام والعقاب، مرجع سابق، ص 214.
[12] سامر سلمان الجبوري، جريمة الاحتيال الإلكتروني، منشورات زين الحقوقية، بيروت، لبنان، 2018، ص94.
[13] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتبة الجامعي الحديث، مصر، 2012، ص281.
[14] فخري عبد الرزاق الحديثي، قانون العقوبات، القسم العام، مرجع سابق، ص317.
[15] علي عبد القادر قهوجي، علم الإجرام والعقاب، مرجع سابق، ص 209.
[16] جمال إبراهيم الحيدري، الوافي في القسم العام من قانون العقوبات، مكتبة السنهوري، بغداد، العراق، 2017، ص793.

وبناء على ذلك سنوضح التحديات التي تواجه المشرع العراقي في مكافحة الجرائم الإلكترونية عامةً، ومواجهة التعديات على مستخدمي الوسائط الإلكترونية بشكل خاص.

ولبيان ذلك سنقسم هذا المبحث على مطلبين، سنتطرق في المطلب الأول لدراسة الصعوبات التشريعية والإجرائية في مكافحة الجرائم المعلوماتية، أما المطلب الثاني فسنتطرق فيه لدراسة تبني آليات ملاحقة أكثر فعالية.

المطلب الأول: الصعوبات التشريعية والإجرائية في مكافحة الجرائم المعلوماتية:

يمثل تطور الجرائم المعلوماتية تحدياً متزايداً أمام الأنظمة القانونية المعاصرة، إذ أفرزت البيئة الرقمية أنماطاً جديدة من السلوك الإجرامي تختلف في طبيعتها ووسائل ارتكابها عن الجرائم التقليدية. وقد أوجد ذلك صعوبات تشريعية وإجرائية تتعلق بمدى كفاية النصوص القانونية القائمة، وإمكانية تكييفها لمواجهة هذا النوع من الجرائم، فضلاً عن الإشكالات المرتبطة بإجراءات التحقيق وجمع الأدلة الرقمية وإثباتها. وتبدو هذه التحديات أكثر وضوحاً في الدول التي ما زالت تفتقر إلى تشريعات متخصصة في مجال الجرائم المعلوماتية، ومنها العراق، الأمر الذي يفرض الاعتماد على القواعد الجنائية التقليدية وما قد يثيره ذلك من إشكالات قانونية وعملية، يمكن توضيح موقف القانون العراقي في مواجهة الجرائم المعلوماتية بشكل عام وجريمة التعدي على مستخدمي الوسائط الإلكترونية ضمن فرعين، حيث سنتناول في الفرع الأول تنظيم المعاملات الإلكترونية في العراق أما في الفرع الثاني سنتناول التنظيم القانوني للجرائم المعلوماتية في إقليم كوردستان.

الفرع الأول: تنظيم المعاملات الإلكترونية في العراق:

يمكن توضيح موقف القانون العراقي في مواجهة الجرائم المعلوماتية بشكل عام وجريمة التعدي على مستخدمي الوسائط الإلكترونية بصدور قانون التوقيع الالكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012، الذي يتكون من 29 مادة موزعة على 8 فصول، حيث وفر هذا القانون الإطار القانوني لاستعمال الوسائل الإلكترونية في إجراء المعاملات الإلكترونية ومنح الحجية القانونية للمعاملات الإلكترونية والتوقيع الإلكتروني وذلك لتعزيز الثقة في صحة هذه المعاملات، وكذلك أعطى هذا القانون الحجية القانونية للمستندات الإلكترونية والعقود الإلكترونية والأوراق التجارية والمالية الإلكترونية وفقاً لشروط معينة، وأجاز التحويل الإلكتروني للأموال مع الزام المؤسسات المالية التي تقوم بأعمال التحويل المالي باتخاذ الإجراءات اللازمة لتوفير هذه الخدمات بطريقة مأمونة والحفاظ على سرية المعاملات المصرفية.[17]

وعلى صعيد الجرائم المعلوماتية، فلا يوجد في العراق باستثناء إقليم كوردستان حتى تاريخ إعداد هذا البحث قانون متخصص يكافح هذه الجرائم، إلا أن هناك مشروع قانون عراقي تم إعداده ووصل إلى مجلس النواب العراقي وتمت قراءته قراءة أولى فيه، ولكنه لم يصدر بسبب الاعتراضات التي وجهت لهذا المشروع ومنها المبالغة في بعض العقوبات وكذلك عدم تحديد بعض المفاهيم في مواده والتي اعتبرتها منظمات المجتمع المدني اعتداء على الحريات العامة والحرية في إبداء الرأي التي كفلها الدستور العراقي لسنة 2005 في المواد 38 و40، وقد تناولت مسودة قانون الجرائم الإلكترونية العراقي جريمة الاحتيال الإلكتروني في المادة 10 تحت تسمية جريمة الاحتيال حيث عرف المشرع الاحتيال بانه التسبب بالحاق الضرر عن قصد وبغير وجه حق بنية الاحتيال للوصول الى المصالح والمنافع بطريقة غير شرعية للفاعل والغير عن طريق:

- تعمد استخدام نظام الكمبيوتر أو شبكة المعلومات التابعة لأشخاص أو شركات أو هيئات أو بنوك أو أسواق مالية، واستطاع الاستيلاء على أموال أو حقوق مالية للغير، أو حقق منفعة مالية لنفسه أو لغيره، أو حرم الآخرين من حقوقه المالية عن طريق بأي وسيلة من الوسائل الإلكترونية.
- توصل بواسطة أحد أجهزة الحاسوب أو شبكة المعلومات إلى الاستيلاء لنفسه أو لغيره على برامج أو معلومات أو بيانات أو شفرات في أية معاملة أو تعاقد الإلكتروني أو بطاقات الإلكترونية أو مال منقول أو سند أو توقيع على سند باستخدام طرق احتيالية أو اتخاذ اسم كاذب أو صفة غير صحيحة من شانها خداع المجني عليه.[18]

---

[17] سمير عالية، القانون الجزائي للأعمال، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2018، ص 78.

[18] فضل سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، مصر، 2016، ص 216.

أما الفقرات ج ، د، هـ، فتتناول التلاعب بالأسهم وأسعار العملة واستخدام العلامة التجارية وكذلك استخدام البطاقة الإلكترونية بعد نفاذ الرصيد أو بعد الغائها أو انتهاء صلاحيتها مع العلم بذلك، والملاحظ أن المشرع العراقي حاول شمول معظم جوانب الاحتيال الإلكتروني في هذه المادة وعلى الرغم من ذلك فكان الأفضل عدم حصر الوسائل الاحتيالية كونها مرتبطة بالتقدم التقني الذي لا يعرف الحدود بالإضافة إلى تجاهل المشرع لتزوير البطاقة الإلكترونية واكتفى بتجريم استخدام هذه البطاقة دون علم صاحبها[19]، ولكون قانون الجرائم المعلوماتية العراقية لم يصدر لحد الآن فلا نريد استباق الأمور ونترك التعليق عليه لحين صدوره بالشكل النهائي واستيفائه مراحل تشريعه.

يتضح لنا أن القانون العراقي قد خطا خطوة مهمة نحو تنظيم البيئة الإلكترونية من خلال قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012، الذي وفر الإطار القانوني لاستخدام الوسائل الإلكترونية ومنح الحجيّة القانونية للمعاملات والتوقيع الإلكتروني والمستندات والعقود والأوراق المالية الإلكترونية، مع ضمان حماية التحويلات المالية وسرية المعاملات المصرفية، أما على صعيد الجرائم المعلوماتية، فلا يوجد في العراق حتى تاريخه سوى تشريعات إقليمية مثل إقليم كوردستان، فيما لم يصدر قانون وطني متخصص لمكافحة الجرائم المعلوماتية بسبب اعتراضات على مشروع القانون، أبرزها غموض بعض المفاهيم والمبالغة في العقوبات، وهو ما يثير مخاوف بشأن انتهاك الحريات العامة المكفولة دستورياً.

الفرع الثاني: التنظيم القانوني للجرائم المعلوماتية في إقليم كوردستان:

للمواجهة التشريعية للجرائم المعلوماتية في العراق، هو صدور قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008 وهو يتألف من أربعة أبواب وأسباب موجبة، وتتجسد الجرائم التي تناولها القانون في:

1. جرائم ضد الاعتبار الشخصي للإنسان.
2. جرائم ضد الأخلاق والآداب العامة.
3. جرائم ضد حرمة الحياة الخاصة والعائلية.
4. وجريمة الإزعاج.

وقد أضاف المشرع الكردستاني جريمة خامسة حيث أشار، إلى أنه في حال أدت الأفعال المجرمة في هذا القانون، إلى ارتكاب جريمة فيعد المتسبب فيها، شريكا ويعاقب بالعقوبة ذاتها المقررة للجاني فيها.[20]

في حين أن جرائم ضد الاعتبار الشخصي فتشمل جريمتين رئيسيتين هما القذف أو السب وجريمة التهديد، وهذه المواد هي مكملة للمواد 430-436 من قانون العقوبات العراقي التي نظمت جرائم التهديد والقذف والسب ولكن تختلف في الوسيلة المستخدمة في ارتكاب هذه الجرائم.

أما الجرائم المخلة بالآداب العامة والآداب العامة فقد تعامل معها المشرع الكوردستاني، وهي تسريب أحاديث، أو صور ثابتة أو متحركة، أو رسائل قصيرة، أو رسائل مخالفة للأخلاق والآداب العامة، أو التقاط صور بدون ترخيص أو إذن، والتنازل عنها. الفاحشة أو التحريض على ارتكاب الجرائم أو أعمال الفسق والفجور، والصورة الرابعة التي جرمها القانون هي جريمة الإزعاج حيث عاقبت المادة رقم 3 من القانون بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن سبعمائة وخمسين ألف دينار ولا تزيد على ثلاثة ملايين دينار أو بإحدى هاتين العقوبتين كل من تسبب عمداً في الاستخدام والاستغلال. الهاتف الخلوي أو أي من أجهزة الاتصال السلكية أو اللاسلكية أو الإنترنت أو البريد الإلكتروني في إزعاج الآخرين في غير الحالات المذكورة في المادة 2 من هذا القانون.[21]

وأخيراً ونحن بصدد اتجاه المشرع العراقي من جريمة الاحتيال الإلكتروني بشكل خاص والجرائم الإلكترونية بشكل عام لابد أن نشير بأن برامج الحاسوب قد تم بسط الحماية عليها من خلال التعديل الذي تم على قانون حق المؤلف رقم 3

[19] مازن ليلو راضي وعدي سليمان علي، المواجهة التشريعية للجريمة الإلكترونية في إقليم كوردستان العراق، بحث منشور في مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الأول لكلية القانون، العراق، 2009، ص 30.
[20] المادة 4 قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008.
[21] المادة 2 قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008.

لسنة 1971 بالأمر رقم 83 لسنة 2004 الصادر عن سلطة الائتلاف المؤقتة المنحلة.[22]

وفي مجمل القول نلاحظ أن الموقف التشريعي في العراق يتجسد إقليمياً من خلال قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان رقم 6 لسنة 2008، الذي جرم مجموعة من الأفعال الإلكترونية الضارة، تشمل الجرائم ضد الاعتبار الشخصي، الأخلاق والآداب العامة، حرمة الحياة الخاصة، وجريمة الإزعاج، مع اعتبار المتسبب شريكاً إذا نتج عن الفعل ارتكاب جريمة أخرى. كما تم تعزيز حماية برامج الحاسوب عبر تعديل قانون حق المؤلف رقم 3 لسنة 1971.

المطلب الثاني: تبني آليات ملاحقة أكثر فعالية:

يشكّل الإنترنت في العصر الحديث جزءاً أساسياً لا يتجزأ من الحياة اليومية للأفراد، إذ أضحى وسيلة رئيسية للتواصل وتبادل المعلومات وبناء العلاقات الاجتماعية وتطوير مختلف مجالات الحياة. ومع ذلك، فإن هذا الفضاء الرقمي لا يخلو من مخاطر متعددة قد يتعرض لها المستخدمون أثناء استعماله، ولا تقتصر هذه المخاطر على الفيروسات الإلكترونية أو عمليات التصيّد الاحتيالي وبرامج التجسس الحاسوبي فحسب، بل تمتد لتشمل ممارسات ضارة يقوم بها بعض الأفراد من مختلف الفئات العمرية بقصد الإضرار بالغير عبر الوسائط الإلكترونية، ومن هنا سنقوم بتقسيم هذا المطلب الى فرعين سنتناول في الفرع الأول صعوبات التحقيق والإثبات في الجرائم المعلوماتية أما في الفرع الثاني الصعوبات القانونية والفنية في تفتيش الأنظمة المعلوماتية.

الفرع الأول: صعوبات التحقيق والإثبات في الجرائم المعلوماتية:

على الرغم من أن الإنترنت يوفر بيئة واسعة لإقامة علاقات جديدة وتبادل الاهتمامات والخبرات، فإن الاستخدام الآمن له يقتضي قدراً من الحذر والوعي، ولا سيما فيما يتعلق بعدم الإفصاح عن المعلومات الشخصية أو البيانات الحساسة، لما قد يترتب على كشفها من مخاطر تمس خصوصية الأفراد وأمنهم المعلوماتي.

وذلك لأن بعض الأشخاص يخفون هويتهم الحقيقية ويحاولون التقرب من الغير لأغراض جنسية وينجحون في مسعاهم هذا، ربما عن طريق إحالة رسائل جنسية في إطار إحدى غرف الدردشة أو عبر برمجيات مخصصة للمراسلات الفورية أو عن طريق السعي إقناع الشخص المعني بلقائهم في العالم الواقعي.[23]

إن أنشطة مجابهة جرائم الكمبيوتر والإنترنت أبرزت صعوبات ومشكلات جمة تختلف في جوانب كثيرة التحديات والمشكلات التي تتعلق بالجرائم التقليدية الأخرى وتستدعي تبني آليات أكثر تطوراً من حيث الملاحقة:[24]

1. لا تترك هذه الجرائم أثرًا ماديًا في مسرح الجريمة، مثل الجرائم الأخرى ذات الطبيعة المادية، ولمرتكبيها القدرة على إتلاف الأدلة أو تشويهها أو إهدارها في فترة وجيزة.
2. أن التفتيش في هذا النمط من الجرائم يتم عادة على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة، وهذا هو الوضع الغالب في ظل شيوع التشابك بين عادة ما يتم التفتيش في هذا النوع من الجرائم على أنظمة الكمبيوتر وقواعد البيانات وشبكات المعلومات ، وقد يتجاوز النظام المشتبه به الأنظمة المرتبطة الأخرى، وهذا هو الوضع السائد في ظل انتشار التشابك بين أجهزة الكمبيوتر وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدولة إن امتداد التفتيش إلى أنظمة أخرى غير النظام محل الاشتباه يخلق تحديات كبيرة ، أولها شرعية هذا الإجراء ومدى انتشاره. أنه يؤثر على حقوق خصوصية المعلومات لمالكي الأنظمة التي يمتد إليها الفحص. الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه يخلق تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

---

[22] عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، مطبعة الوئام للحاسبات والطباعة والنشر، بابل، 2009، ص190.

[23] حسين توفيق فيض الله، الإباحية بالأطفال على شبكة الإنترنت، مجلة القانون المقارن، تصدر عن جمعية القانون المقارن العراقية، العدد 37، العراق، 2005، ص53.

[24] محمد السيد رشدي، «الإنترنت والجوانب القانونية لنظم المعلومات»، مجلة الفتوى والتشريع، العدد 9، مجلس الوزراء، ص 107، مايو، 2000، ص45.

3. أن الضبوط لا تعتمد النوبة على الاستيلاء على الكمبيوتر، حيث قد تمتد من حيث التحكم في المكونات المادية إلى أجزاء النظام المختلفة التي تتزايد يومًا بعد يوم، والأهم أن الضبط يركز على البيانات، البيانات والبرامج المخزنة في النظام أو الأنظمة المرتبطة بالنظام محل الاشتباه، أي بشأن الأشياء ذات الطبيعة غير الملموسة التي تخضع للريبة عرضة للتغيير والتدمير بسهولة، وهذه الحقائق تثير مشاكل متعددة، بما في ذلك المعايير المقبولة لرقابة المعلومات ومعايير الحفظ، بالإضافة إلى مدى تأثير إجراءات التحكم في محتويات النظام على خصوصية صاحبه - حتى لو إنه مشتبه به- عندما تتجاوز أنشطة الرقابة جميع محتويات النظام، والتي عادة ما تتضمن المعلومات والبيانات. السرية أو الخضوع للحماية (25) بحكم القانون أو لطبيعتها أو لارتباطها بجهات أخرى.

4. تتميز أدلة التجريم بجودة مختلفة، لأنها غير ملموسة بطبيعتها، مثل سجلات الكمبيوتر، ومعلومات الإدخال، والاشتراك، والوصول، والبرامج، وقد أثارت ولا تزال تثير العديد من المشاكل أمام القضاء من حيث مدى قبولها وسلطتها، والمعايير المطلوبة لذلك، لا سيما في ظل قواعد الإثبات التقليدية.(26)

5. كما أن اختصاص القضاء في النظر في جرائم الكمبيوتر والقانون الواجب تطبيقه على الفعل ليس دائمًا واضحًا أو مقبولًا في مواجهة حقيقة أن غالبية هذه الأفعال يرتكبها أشخاص من خارج الحدود أو يمرون بها. من خلال شبكات المعلومات وأنظمة المعلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، مما يبرز أهمية فحص قواعد الاختصاص والقانون المطبق وما إذا كانت النظريات والقواعد القائمة تمتد في هذا المجال إلى هذه الجرائم، أو ما إذا كانت القواعد الخاصة بها مطلوبة في ضوء خصوصيتها والمشكلات التي تثيرها في مجال الاختصاص القضائي. (27)

وتتصل مشكلات الاختصاص القضائي وإنفاذ القانون بمشاكل توسيع نطاق أنشطة الملاحقة والتحقيق والرقابة والتفتيش خارج الحدود، وما يتطلبه ذلك هو تعاون دولي شامل للموازنة بين مقتضيات الرقابة وضرورة حماية السيادة الوطنية.

لذا فإن البعد الإجرائي لجرائم الكمبيوتر والإنترنت يتضمن على العديد من التحديات والمشكلات، أهمها ضرورة الكشف السريع خوفاً من ضياع الأدلة، وخصوصية قواعد التفتيش والرقابة المناسبة لهذه الجرائم، وشرعيتها وقوانينها. مصداقية الأدلة على جرائم الكمبيوتر والإنترنت، ومشكلات الاختصاص والقانون المعمول به، والحاجة إلى تعاون دولي شامل في مجال توسيع إجراءات التحقيق والادعاء خارج الحدود، وهذه المشاكل كانت ولا تزال موضع اهتمام على المستوى الوطني والمستويات الدولية.

توجيهات عملية في ضبط وتفتيش أنظمة الكمبيوتر والشبكات ثمة في هذا المقام بعض التوجيهات، لكنها ليست ذات قيمة دون التدخل التشريعي لإفراد قواعد تفتيش وضبط خاصة على نحو ما قررته التشريعات الوطنية المقارنة والوثائق الدولية.[28]

فالقاعدة الأساسية أن التفتيش يتطلب إذن قضائي يجيز تفتيش أنظمة الكمبيوتر وأما إجراء التفتيش دون إذن قضائي أو الحصول على بيانات من جهات ليست محلا للاشتباه لتعلقها بالمشتبه به، فإنها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد وتوجب مشروعية الدليل وسلامة مرجعه ، أو تبطل كل إجراء يتم خلافا للقواعد الأصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون، وهي مسائل – طبعا تختلف أحكامها باختلاف النظم القانونية - ينفد من خلالها الجناة عند عدم إجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعلنا متمسكين بضرورة عدم اللجوء إلى هذا السلوك – حتى لو أتاح النظام القانوني المعني ذلك تحفظنا على مثل هذا الحكم لأن المشروعية الإجرائية توجب تحقيق أقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة – ونرى الإصرار على وجوب استصدار إذن قضائي للتفتيش، و مما سبق نلاحظ أن مكافحة هذه الجرائم تواجه صعوبات إجرائية تتعلق بطبيعة الدليل الإلكتروني، وإمكانية إتلافه بسرعة، واتساع نطاق التفتيش ليشمل أنظمة معلوماتية متعددة، مما يثير تحديات قانونية مرتبطة بحماية الخصوصية وضمان مشروعية إجراءات التحقيق.

---

(25) ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، 2009، ص47.
(26) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص117.
(27) جمال سيف فارس، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية - دراسة مقارنة بين القوانين الوضعية الأجنبية والقانون الدولي الجنائي، دار النهضة العربية، القاهرة، 2007، ص25.
(28) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، 2002، ص78.

الفرع الثاني: الصعوبات القانونية والفنية في تفتيش الأنظمة المعلوماتية:

يواجه تفتيش الأنظمة المعلوماتية مشكلات عديدة وان أمر حلها وتجاوزها أمر منوط بالقواعد القانونية المتعين سنها إضافة إلى التزام جهات التفتيش الحيطة في توفير متطلبات القانون والحيطة في مراعاة بعض المسائل الفنية في هذا الشأن - نورد بعضها تاليا:[29]

1. أهمية مباشرته ممن تتوفر لديهم الخبرات الفنية الكفيلة بتحقيق التفتيش غرضه.
2. فاذا كان المحقق يعلم ابتداءً عن وجود الأدلة المتصلة بجريمة ما ضمن أحد أنظمة الكمبيوتر أو الشبكات، وكان الجرم إبتداءً من طبيعة الجرائم الإلكترونية، فإن إذن التفتيش يتعين أن يكون واضحا في تحديد النظام محل التفتيش وإيراد أوسع وصف يغطي ما يعرفه المحقق سلفا وما يفترض أنه يتصل بالمسائل التي يعرفها.[30]
3. أما إن كان النظام أو مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش فيتعين أن تجيء عبارات مذكرة التفتيش عامة ما امكن حتى لا يكون نصها قيدا على نطاق التفتيش والضبط ، فعلى سبيل المثال يمكن أن تتضمن مذكرة التفتيش والضبط إجراء التفتيش والضبط لأي من أو لكل سجل أو معلومات توجد بصورة إلكترونية أو مادية أو خطية موجودة في أي جهاز لتخزين المعطيات سوآءا كان نظام كمبيوتر أيا كان وصفه أو شبكة معلومات أو وسائط تخزين أو أجهزة اتصال أو أية نظم معالجة وتخزين يمكن أن يوجد فيها الدليل لكن عمومية مذكرة التفتيش لا تعني عدم وجوب بيان السبب ومبرر التفتيش، ولا تعني تجاوز الإجراء بذاته للقواعد القانونية المقررة لحماية الأفراد، خاصة أولئك الذين لا صلة مباشرة لهم بالمشتبه به أو بفعله.
4. ومن حيث الأصل فان التحري والتفتيش في بيئة جرائم الكمبيوتر والإنترنت يتوقف على مدى دقة إذن التفتيش ونطاقها المكاني، ويتعين أن يحرص المحققون أو جهات الضبط المكلفة بالتفتيش من قبل النيابة على أن يغطي محضر التحريات اللازم لاستخراج الإذن أي مكان توجد فيه هذه البيانات الإلكترونية في نطاق الاختصاص المكاني وبالنظر إلى الشخص أو الجهة التي يدور التفتيش بشأنها.[31]

وهنا تظهر أهم مشكلة في مسائل التفتيش بالنسبة إلى اختراقات الإنترنت أو الاختراقات الخارجية، إذ قد يتطلب التحري تفتيش أنظمة كمبيوتر عائدة لجهات لا صلة لها بالفعل أو نتيجته ، كتفتيش نظم مزودي خدمات الإنترنت، أو تفتيش أنظمة الخوادم خارج الحدود أو الطلب من مالكيها ومديريها تزويد جهة التحقيق ببيانات معينة ، ولا يمكن أن يقبل قانونا أن يغطى إذن التفتيش مواطن ومواقع وأماكن خارج صلاحية نظام العدالة المكانية، ومن هنا نشأت الحاجة إلى تعاون دولي حقيقي في ميدان أنشطة التحري والتحقيق والضبط والتفتيش خارج الحدود.[32]

5- أما مسالة حاجة أنشطة التفتيش للسرعة ومسألة قدرة الجناة على إخفاء الدليل ، ومعلوم أنه لا يمكن إلزام أية جهة بتقديم أية بيانات بشأن الخدمات المقدمة للزبائن أو علاقتهم به، لأن هذه البيانات في الأصل سرية ولا يجوز إفشاؤها إلا وفق القانون، فان الحاجة تعدو ماسة للتدخل التشريعي لإتاحة مكنة وأيضا آلية الضبط المستعجل للنظم المشتبه بها مع أمر كف يد المشتبه به عن استخدام النظام فورا بمجرد البدء بإجراءات التفتيش، إضافة إلى الحق في ضبط الأجهزة لإجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش ، خاصة إذا ما علمنا أن تفتيش جزء صغير جدا من الذاكرة قد يحتاج ساعات، فكيف هو الحال وقد أصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات، إضافة إلى أن التفتيش الأولي قد لا يحل مشكلة الملفات المخبأة أو المحمية أو المشفرة، لكن هذه الحلول في نطاق التفتيش تناقض القواعد المقررة قانونا في حقل ضمانات المتهم أي المتهم الإلكتروني في حالتنا وضمانات احترام حقوق الإنسان والحريات الفردية وفي مقدمتها الخصوصية.[33]

---

(29) محمود احمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2019، ص75.
(30) محمد عبد الله سلامة، موسوعة الجرائم المعلوماتية، منشأة المعارف، الإسكندرية، مصر، 2016، ص69.
(31) علي حمزة عسل، الظروف القضائية المخففة في التشريع العراقي، مرجع سابق، ص 98.
(32) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص183.
(33) محمود شريف بسيوني، «الوثائق الدولية المعنية بحقوق الإنسان»، المجلد الثاني، دار الشروق، القاهرة، 2003، ص12.

ومما سبق يتضح لنا أن مثل هذه الإجراءات قد تؤدي إلى كشف بيانات شخصية أو كشف أسرار العمل أو الوصول إلى ملفات يحرص أصحابها على سريتها أو تيح لهم القانون ذلك، وتعدو المسالة أكثر خطورة عندما يمتد التفتيش إلى نظم مرتبطة بالنظام موضوع الاشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية أو قواعد حماية سرية بيانات العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات أو نظم البنوك أو الجهات الصحية أو أعمال المحاماة أو غيرها.

الخاتمة

شكّل التحول الرقمي المتسارع تحدّياً مركّباً للمنظومات القانونية التقليدية، بعد أن أصبحت الوسائط الإلكترونية فضاءً موازياً للواقع المادي، يمارس فيه الأفراد أنشطتهم الاجتماعية والاقتصادية، ويتداولون معلوماتهم وبياناتهم الشخصية. وقد رافق هذا التحول ظهور أنماط غير مسبوقة من الأفعال الجرمية اتسمت بالخطورة وسرعة الانتشار وإمكان ارتكابها دون مغادرة موقع الجاني، الأمر الذي جعل مستخدمي الوسائط الإلكترونية عرضة لاعتداءات قد تمس أمنهم الشخصي وخصوصيتهم وسمعتهم وذممهم المالية.

وفي ضوء ذلك، تناول هذا البحث الحماية الجزائية لمستخدمي الوسائط الإلكترونية، محاولاً تحليل الواقع التشريعي، وتشخيص الثغرات، واقتراح بدائل ملائمة تضمن الحماية الفعّالة للضحايا، وتحقق التوازن بين التطور التكنولوجي والمبادئ الجنائية التقليدية، وبين الأمن الرقمي وحرية التعبير وكذلك استخدام الذكاء الاصطناعي في ارتكاب الجرائم الإلكترونية الجانب الهجومي.

أولاً: النتائج:

1. قصور النصوص العقابية العراقية التقليدية عن استيعاب صور الجرائم الإلكترونية الحديثة.
2. وجود اعتداءات رقمية تستلزم تجريماً خاصاً مثل الاختراق، التنصت الرقمي، انتحال الهوية الإلكترونية، والابتزاز عبر الوسائط الإلكترونية.
3. حاجة النظام الإجرائي إلى تطوير أدوات الإثبات الرقمي، واعتبار الدليل الإلكتروني دليلاً قائماً بذاته ضمن ضوابط محددة.
4. افتقار جهات التحقيق إلى الخبرة الفنية اللازمة للتعامل مع الأدلة الرقمية.
5. غياب نصوص واضحة تعاقب على التحريض والاشتراك الإلكتروني، واستعمال المنصات لأغراض إجرامية.
6. الذكاء الاصطناعي علامة سلاح ذو حدين فهو أداة تطوير وشن هجمات ومن جهة وسيلة أساسية للتنبؤ بها ومكافحتها.

ثانياً: التوصيات:

1. إصدار قانون خاص للجرائم الإلكترونية، بصياغة شاملة ومتكاملة، يُعرّف الجرائم ويحدد العقوبات والإجراءات اللازمة للتحقيق فيها، ووضع ضوابط رقابية توازن بين الأمن الرقمي وحريات التعبير.
2. إنشاء هيئة وطنية للجرائم الإلكترونية تتولى التحقيق الفني والتنسيق بين الجهات الأمنية والقضائية.
3. تطوير آليات الإثبات الرقمي واعتماد الدليل الإلكتروني وفق معايير قانونية واضحة.
4. إلزام الشركات والمواقع الإلكترونية باتخاذ تدابير لحماية بيانات المستخدمين.
5. يتم استخدام الذكاء الاصطناعي في ارتكاب الجرائم الإلكترونية من قبل القراصنة ومتابعتهم.

قائمة المصادر والمراجع

أولاً: الكتب القانونية:

1. جمال إبراهيم الحيدري، الوافي في القسم العام من قانون العقوبات، مكتبة السنهوري، بغداد، العراق، 2017.
2. جمال سيف فارس، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية - دراسة مقارنة بين القوانين الوضعية الأجنبية والقانون الدولي الجنائي، دار النهضة العربية، القاهرة، 2007.

3. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، 2002.
4. حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها، مكتبة بدران الحقوقية، بيروت، لبنان، 2017.
5. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط 1، دار الثقافة للنشر والتوزيع، عمان، 2011.
6. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010.
7. سامر سلمان الجبوري، جريمة الاحتيال الإلكتروني، منشورات زين الحقوقية، بيروت، لبنان، 2018.
8. سمير عالية، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020.
9. سمير عالية، القانون الجزائي للأعمال، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2018.
10. عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، مطبعة الوئام للحاسبات والطباعة والنشر، بابل، 2009.
11. علي عبد القادر قهوجي، علم الإجرام والعقاب، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.
12. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتبة الجامعي الحديث، مصر، 2012.
13. فخري عبد الرزاق الحديثي، قانون العقوبات، القسم العام، دار الثقافة للنشر والتوزيع، عمان، 2010.
14. فضل سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، مصر، 2016..
15. محمد عبد الله سلامة، موسوعة الجرائم المعلوماتية، منشأة المعارف، الإسكندرية، مصر، 2016.
16. محمود احمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2019.
17. محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2019.
18. محمود شريف بسيوني، «الوثائق الدولية المعنية بحقوق الإنسان»، المجلد الثاني، دار الشروق، القاهرة، 2003.
19. ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، 2009.

ثانياً: الأبحاث والمجلات والدوريات:

1. حسين توفيق فيض الله، الإباحية بالأطفال على شبكة الإنترنت، مجلة القانون المقارن، تصدر عن جمعية القانون المقارن العراقية، العدد 37، العراق، 2005.
2. مازن ليلو راضي وعدي سليمان علي، المواجهة التشريعية للجريمة الإلكترونية في إقليم كوردستان العراق، بحث منشور في مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الأول لكلية القانون، العراق، 2009.
3. محمد السيد رشدي، «الإنترنت والجوانب القانونية لنظم المعلومات»، مجلة الفتوى والتشريع، العدد 9، مجلس الوزراء، ص 107، مايو، 2000.

ثالثاً: الرسائل الجامعية:

1. عدلي محمد عبد الكرخي، جريمة الإرهاب عبر الوسائل الإلكترونية في القانونين اللبناني والعراقي، رسالة ماجستير، الجامعة الإسلامية، بيروت، 2018.

رابعاً: القوانين:

1. القانون الاتحادي الخاص بمكافحة جرائم تقنية المعلومات الإماراتي لسنة 2006.
2. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
3. قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008.
4. مشروع قانون الجرائم المعلوماتية العراقي.