HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير للعام 2022 = 4.91

عنوان البحث

الصعوبات القانونية في مكافحة الجريمة الإلكترونية

شيماء علوان حسن[1]

[1] الجامعة الإسلامية في لبنان– كلية الحقوق

إشراف الأستاذ الدكتور/ محمد عبده

HNSJ, 2024, 5(10); https://doi.org/10.53796/hnsj510/21

تاريخ النشر: 2024/10/01م تاريخ القبول: 2024/09/15م

المستخلص

نظراً لما تميزت به الجرائم الإلكترونية من صفة العالمية، باعتبارها جرائم عابرة للقارات، فكان لابد من صدور قوانين دولية وتكاتف جهود دولية لاتخاذ تدابير فعالة للحد والقضاء عليها ومعاقبة مرتكبيها، فرغم وجود بعض الاتفاقيات المقررة لمكافحة الجريمة بصورة عامة، خاصة بالجريمة المنظمة والعابرة للحدود، والتي تنطبق تماماً وسمات الجرائم الإلكترونية، فقد وجدت معاهدات سنت خصيصا لمكافحة الجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية – الحياة الشخصية- السرقة الإلكترونية- التشريعات الوطنية.

RESEARCH TITLE

Legal Difficulties in Combating Cybercrime

Shimaa Alwan Hassan[1]

[1] Islamic University of Lebanon - Faculty of Law

Supervision by Professor Dr. Mohammed Abdu

HNSJ, 2024, 5(10); https://doi.org/10.53796/hnsj510/21

Published at 01/10/2024 **Accepted at 15/09/2024**

Abstract

Given the global nature of cybercrimes, as they are crimes that cross continents, it was necessary to issue international laws and combine international efforts to take effective measures to limit and eliminate them and punish their perpetrators. Despite the existence of some agreements established to combat crime in general, especially organized and cross-border crime, which fully apply the characteristics of cybercrimes, there were treaties enacted specifically to combat cybercrimes.

Key Words: Cybercrime – Personal life – Cybertheft – National legislation

المقدمة

مع إتيان الثورة الإلكترونية وهيمنتها على الحياة الاجتماعية العملية والمهنية لمعظم فئات المجتمع، فقد نشأت معها نتائج سلبية متمثلة بظاهرة الاجرام المعلوماتي في العصر الحديث، حيث تطورت تطوراً ملحوظا ومذهلا سواء في اشخاص مرتكبيها او في اسلوب ارتكابها والذي يتمثل في استخدام آخر ما توصلت اليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة، وقد تميز القرن العشرين باختراعات هائلة على المستوى التقني لعل من أهمها ظهور الحاسبات الالكترونية، والذي تطور بالشكل الذي افضى الى استحداث شبكات المعلومات ونظم المعلومات حتى بات يطلق على هذه التقنية بالنظام المعلوماتي.

ولما كانت الجرائم الإلكترونية لارتباطها بنظم المعالجة الآلية للمعلومات، هي ظاهرة اجرامية حديثة النشأة لتعلقها بتكنولوجيا الحاسبات الآلية، فقد اكتنفها الغموض بالشكل الذي دعى الكثيرين الى القول بأن الجريمة الإلكترونية هي اشبه بالخرافة، وانه لا يوجد اي تهديد حقيقي منبعه الحاسبات الالكترونية، وان كانت هناك أشكال غير المشروع التي ترتبط بالحاسبات الالكترونية هي جرائم عادية يمكن تطبيق النصوص التقليدية بشأنها [1]، غير أن تطبيق النصوص التقليدية على هذه الانماط المستحدثة من الجرائم قد أسفر عن الكثير من المشكلات القانونية، حيث اختلفت اراء الفقهاء بشأن تطبق النصوص التقليدية عليها وتضاربت احكام القضاء في البلد الواحد فصدرت أحكام لتطبيق النصوص التقليدية على اي سلوك يتعلق بالحاسبات او نظم معالجة المعلومات، في حين اعتبرته أحكام أخرى سلوكاً مباحاً لم يرد بشأنه نصاً يجرمه احتراماً بمبدأ ولا جريمة ولا عقوبة إلا بنص[2].

وإذا كانت الجرائم الإلكترونية لم تقنن بعد في بعض البلدان العربية سواء من حيث الكم، أو تنوع صور ارتكابها مثال الدول المتقدمة كفرنسا والولايات المتحدة الأمريكية وبريطانيا، إلا أن هذا لا ينفي ضرورة التصدي لها مبكراً، لاسيما وأن العالم العربي، سواء اكان أفراداً أو دولاً او مؤسسات، أصبحوا يشهدوا إقبالاً كبيراً على استعمال وسائل التقنية الإلكترونية، والاستفادة من ايجابياتها، ومحاولة الحد من سلبياتها [3].

ومع ذلك، مع ندرة النصوص القانونية المتعلقة بهذه الجرائم الحديثة والتي تحدث فيما أصبح يطلق عليه جرائم المعلومات، فهل من الممكن دائمًا استخدام القواعد العامة للتجريم كمبدأ عام، وهل هي كافية للتصدي لأخطار التعدي على برامج الحاسب الآلي، أم لابد من تدعيمها بقواعد عقابية جديدة تتناسب والطبيعة الخاصة لبرامج الحاسب الآلي.

إشكالية البحث:

تشكل الجريمة خطراً يهدد وجود البشرية منذ نشأتها وقد تطور مفهوم الجريمة بتطور العصور والأزمنة واختلفت مسمياتها وتعددت صورها وأشكالها وتعتبر المصارف الأساس العملي في الاقتصاد المعاصر حيث تساهم المصارف من خلال الآليات المتبعة لديها في تسهيل التعاملات الاقتصادية بين الدول والأفراد على حدٍ سواء وبسبب التطور الكبير في التكنولوجيا ظهر نوع جديد من الجرائم يتماشى مع التطور التكنولوجي وأصبحت الجرائم الإلكترونية تشكل خطراً كبيراً على أمن الدول واستقرار المجتمعات بسبب وجود عوامل عديدة أهمها ارتكاب الجرائم عن بعد وصعوبة التعرف على الفاعل كل هذا حذا بالدول إلى خلق صيغة من التفاهم والتعاون لمحاربة هذا النوع من الجرائم والقضاء عليه .

---

[1] **محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر، 2019، ص 45.**

[2] **يونس عرب، جرائم الكومبيوتر والانترنت، ورقة عمل مقدمة الي مؤتمر الامن القومي المنظم من قبل المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002، ص13.**

[3] **محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، المرجع السابق، ص48.**

ومن هنا تظهر إشكالية هذا البحث في تساؤل رئيسي:

ما هي الصعوبات التي تعترض مكافحة الجرائم الإلكترونية الماسة بالحياة الشخصية؟

منهجية البحث: نظراً لتشعب المسائل التي يتطرق لها موضوع البحث، فقد اعتمدت على عدة مناهج علمية تتكامل فيما بينها بقصد إغناء موضوع البحث **المنهج التحليلي:** اعتمدت على هذا المنهج من أجل استعراض القواعد القانونية ذات الصلة بموضوع البحث والآراء المتعلقة به وتحليلها ووصفها لبيان ماهيتها وتفاصيلها، **المنهج المقارن:** من أجل المقارنة بين القواعد القانونية في التشريع المقارن والتي ناقشت موضوع مكافحة الجرائم المصرفية الإلكترونية اتبعت في هذا البحث المنهج المقارن.

المطلب الأول

أنواع الجرائم الالكترونية

إن المعيار الأساسي في التصنيف ينبغي أن يقوم على التمييز ما بين الجرائم المعلوماتية الصرفة باعتبارها جرائم مستجدة، وبين الجرائم التقليدية التي ترتكب بواسطة نظم تكنولوجيا المعلوماتية[4].

وهذا ما دفعنا إلى تقسيم هذا المطلب إلى فرعين، تخصص الأول لعرض الجرائم المعلوماتية البحتة، أما الثاني فنخصصه لعرض الجرائم التقليدية التي ترتكب بوسائل وتقنيات معلوماتية.

الفرع الأول

الجرائم المعلوماتية البحتة

تمتاز الجرائم المندرجة ضمن هذه الفئة بكونها من الجرائم المستجدة، والتي لها علاقة مباشرة بنظم المعلوماتية، ولا يمكن تصور ارتكابها من دونها، وبالتالي إن هذه الجرائم لم تكن معروفة قبل اختراع الحاسوب أو شبكة الإنترنت، ويندرج ضمنها الجرائم التالية:

1- **النّفاذ غير القانوني أو القرصنة:** تعتبر جريمة النفاذ غير القانوني إلى أنظمة الحاسوب من أقدم جرائم المعلوماتية وأخطرها، وقد عرفت حتى قبل انتشار استعمال شبكة الإنترنت، ولكن هذه الشبكة ساهمت بشكل أو بآخر في إضعاف الحماية الفردية والاقتصادية والأمنية وغيرها، الأمر الذي أدى إلى إفساح المجال أمام المجرمين للتوسع في نطاق انتهاكاتهم، حيث أضحى بمستطاعهم ارتكابها عن بعد.

وكما أن انتشار البرمجيات المستعملة لهذه الغاية قد مكنهم من النفاذ بسهولة إلى الكثير من الحواسيب والمواقع على الرغم من تحصنها بوسائل حماية متنوعة ومعقدة، ورغم ذلك استطاع العديد من الهاكرز اختراق حواسيب مواقع وبرامج العديد من الوكالات والمنظمات والمؤسسات الهامة، ولم تسلم منهم حواسيب المصارف والمؤسسات والشركات التجارية، كما لم يتورعوا عن اختراق العديد من المواقع العسكرية والأمنية على الرغم من حرص الأجهزة المعنية وتشددها في توفير وسائل الحماية والإنذار[5]. وعالمنا العربي، ولبنان جزء منه، ليس بمنأى عن تلك الانتهاكات الخطيرة التي تعاني منها المواقع الرسمية وغير الرسمية، من وزارات ومؤسسات وشركات وأفراد.

---

[4] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الطبعة الأولى، دار النهضة العربية، ، مصر، 2002، ص 23.

[5] ومن الوسائل المعتمدة: الهجمات الوقتية، وهي كناية عن عمليات تقنية معقدة تهدف الى الدخول الى مواقع غير الوصول اليها إلا لأشخاص معينين.

إذ إن أي ولوج أو اختراق لهذه الحواسيب من قبل أشخاص غير مجاز لهم بذلك، والإطلاع على معطيات مخزنة داخل تلك الحواسيب يعتبر عملاً غير مشروع. وسيان حصل الجرم بغفلة من مستعمل الحاسوب أو باستعمال كلمة السر الخاصة به، أو من خلال الاستعانة ببرمجيات تمكنه من اختراق حاسوب من دون مسوغ قانوني، وكذلك الأمر إن حصل الفعل باستعمال الحاسب الآلي الخاص بالضحية أم عبر جهاز آخر مربوط به بواسطة شبكة محدودة أو عبر شبكة الإنترنت. بمعنى آخر تكون العملية بمثابة اختراق وتجسس بغض النظر عن الوسيلة التي اعتمدها الجناة في الوصول إلى المعطيات، وذلك بمجرد اختراقهم لبرامج الحماية وأنظمة المراقبة وتشفير المعلومات[6].

2 –جريمة الاعتراض غير القانوني: وتتم عبر متابعة حركة الاتصالات داخل النظام وتحليلها من أجل تحديد سلوك المستخدمين، وتحديد نقاط الضعف في النظام بغية اختيار التوقيت المناسب والأسلوب الأفضل للهجوم أو التعرض للنظام، من خلال متابعة ما يجري عبره من عمليات، وما يتم تبادله من معطيات، وسيان حصل ذلك سلكياً أو لا سلكياً، طالما كانت المعلومات المنقولة محمية أو غير مباحة، طالما أن الإطلاع عليها لم يكن أمراً عارضا، ومع انتشار استعمال شبكة الإنترنت أضحى بإمكان المجرمين أو أي جهة ترغب في اعتراض المعلومات التي يتم تبادلها عبر الشبكة بأساليب ووسائل مختلفة، من خلال الربط المادي بالشبكة، وإنشاء متفرع لها، يصار من خلاله إلى نقل المعطيات في ذات الوقت للجهة الموجهة أصلاً إليها، وفي الوقت عينه للجهة التي يحددها الجناة، أو من خلال اعتماد برمجيات تقنية تتيح اعتراض المعلومات على نحو غير مشروع والاطلاع على المعطيات والاطلاع على المعطيات المتبادلة (صوت، صوت وصورة، بيانات نصوص مكتوبة، صور أو مقاطع فيديو)، وهذا النوع من الإجرام يتسم بالخطورة نظرا لطابع الخصوصية في الاتصالات التي تُجرى ومضامينها، والتي تكون في الكثير من الأحيان على درجة كبيرة من السرية، وخاصة إذا كانت متبادلة ما بين مؤسسات حكومية أو فروع لمؤسسات وشركات هامة تتعلق بطبيعة أنشطتها.

3– جريمة العبث أو التلاعب في البيانات: يسعى بعض المجرمون المعلوماتيون إلى النفاذ إلى بعض المواقع أو الحواسيب الخاصة بمؤسسات أو شركات أو أفراد للوصول إلى الأنظمة المشغلة لبعض المواقع أو للبيانات التي تحتويه، والعبث بها حذفاً أو إضافة أو تحويراً أو تقييد النفاذ إليها، إما مباشرة وإما بواسطة فيروسات إلكترونية، وذلك بهدف شل الموقع أو عدم تمكين المستفيدين من استخدام الموقع أو منعهم من الاستفادة من البيانات الموجودة، وذلك من خلال إجراء عمليات من شأنها الإخلال بتكاملية البرامج والبيانات، الأمر الذي يؤدي إلى الحؤول دون الاستخدام العادي لها أو للبيانات التي تحتويها.

الجدير ذكره، أن التلاعب بالبيانات والبرمجيات في ظل التطور التقني والتحول المضطرد نحو الاعتماد بشكل أساسي في معظم النشاطات بما في ذلك التجارية منها، بحيث أن معظم المؤسسات والشركات تعمد إلى تخزين كميات هائلة من البيانات والمعطيات، كما إلى تنفيذ معظم المهمات والنشاطات وتلبية حاجات وطلبات الزبائن عبر شبكة الإنترنت، كل ذلك يجعل العبث في البرمجيات والبيانات ينطوي على مخاطر كبيرة، كما قد يتسبب بخسائر مالية ضخمة غير معهودة من قبل[7].

من هنا تأتي أهمية تجريم الانتهاكات المتمثلة في العبث أو التلاعب في البيانات، واتخاذ ما يلزم من تدابير للحؤول دون ارتكابها.

---

[6] عادل مشموشي، مكافحة الارهاب، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2011، ص 309.

[7] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الاول، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص 35.

4-جريمة الولوج (الدخول) غير المصرح به: تعتبر جريمة الدخول غير المصرح به الأكثر انتشاراً بين الأنشطة الجرمية ذات العلاقة بنظم المعلوماتية[8]، ويتم من خلال استخدام وسيلة اتصال عن بعد كالمودم، أو من خلال نقاط الإتصال والموجهات المتصلة بشبكة الإنترنت للوصول إلى جهاز حاسوب، والولوج إليه والاطلاع على المعطيات والبرامج المخزونة بداخله، وغالباً ما يتطلب ذلك تخطي بعض وسائل الحماية التقنية، ككلمات المرور وإجراءات التعريف، أو من خلال استغلال نقطة ضعف أو فجوة في برنامج الحماية المعتمد.

وفي هذا الإطار ينبغي الإشارة إلى أن المشرع اللبناني قد تنبه لهذا الخطر، فعمد إلى تجريم الولوج غير المصرح به إلى نظام معلوماتي بكامله أو في جزء منه، كما المكوث فيه، وعاقب على ذلك بالحبس من ثلاث أشهر إلى سنتين، وبالغرامة من مليون إلى عشرين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين، وتشدد العقوبة إلى الحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مليونين إلى اربعين مليون ليرة، إذا نتج عن العمل الغاء البيانات الرقمية أو البرامج المعلوماتية أو نسخها أو تعديلها أو المساس بعمل النظام المعلوماتي.

5-جريمة التدخل غير المشروع في النظم المعلوماتية: يعنى بالتدخل في النّظم المعلوماتية العبث في أحد أو بعض البرمجيات المعتمدة في تسيير أعمالها، من قبل شركة أو مؤسسة أو قطاع معين، من ذلك التدخل في البرمجيات التي تسير محطات إنتاج أو توزيع الطاقة، أو تسير أعمال إطلاق وهبوط الطائرات أو إطلاق وتسيير القطارات، أو عمليات شراء وبيع السلع عبر الإنترنت لشركة ما، وغيرها من البرامج. وقد يتسبب العبث بهذه البرامج بحوادث بالغة الخطورة، تسفر عن خسائر كبيرة في الأرواح والممتلكات، يلجأ إليها الإرهابيون كأسلوب لارتكاب أعمال إرهابية بوسائل معلوماتية تفوق من حيث مخاطرها وحجم أضرارها الاعتداءات بوسائل حربية غير تقليدية[9].

ووفق القانون اللبناني يمكن تطبيق أحكام المادة 111 من القانون 81/ 2018، كونها تنص على تجريم التعدي على سلامة النظام، من خلال الإقدام، بنية الغش وبأي وسيلة على إعاقة عمل نظام معلوماتي أو على إفساده، وعاقب على ذلك بالحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين[10].

6 -جريمة تدمير المعطيات: يُعنى بالإتلاف في نطاق جرائم الحاسوب، وفقا لمحددات هذه الجرائم، ذاك الإتلاف الذي تتعرض له نظم المعلومات من تدمير لمعطيات الحاسوب، (بيانات ومعلومات وبرامج)، ومن المفيد التأكيد على أن الاتلاف المنصب على الكيانات المادية للحاسوب، ينبغي التعامل معه كما يتم التعامل مع سائر الجرائم الواقعة على هذه الأشياء المادية الملموسة، تماماً كما هو الحال في جريمة السرقة، والاختلاس وإساءة الامانة والتخريب والتدمير[11].

أما جريمة الاتلاف التي تستهدف المساس بالجوانب غير المادية، ومنها المعطيات والبيانات والمعلومات المخزنة في نظم الحواسيب المختلفة والبرامج وكذلك المعطيات المتبادلة بين الحواسيب عبر شبكات الاتصال، فهي مواد ذات طبيعة خاصة غير مادية، ونظراً لكونها كيانات غير مادية فإن تدميرها يكون مجازياً، أي من خلال محوها كليا أو جزئياً، كما يتم من خلال تعطيلها أو تشويه مضمونها، أو بمنع المعنيين من الوصول إليها أو استخدامها وفق ما أعدت له وبما يحقق الغاية

---

[8] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، الطبعة الأولى، الدار الجامعية للطباعة والنشر، بيروت، 2000، ص131.

[9] توماس ميلهورن، جرائم الانترنت، مؤسسة الناشر الدولي، فلوريدا، 2007، ص 127.

[10] المادة 111 من القانون 81/ 2018 اللبناني.

[11] عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2007، ص 136.

من استعمالها، أما الوسائل المعتمدة في جريمة الإتلاف فكثيرة منها: الفيروسات والديدان والقنابل المنطقية والموقوتة[12].

7-جريمة إنكار الخدمة: عادة ما ترتكب من خلال هجمات إلكترونية تستهدف تعطيل واحد أو أكثر من مواقع الانترنت، أو تعطيل العمل بنظام إلكتروني معين يستعمل في تسيير بعض الأمور، وتتم عادة من خلال ضخ كميات هائلة من الطلبات والرسائل في وقت واحد، لا لشيء سوى لشل النظام أو البرنامج أو الموقع أو إسقاطه، والسعي إلى جعله عاجزاً كلياً أو جزئياً عن العمل أو تلبية المطلوب، أو العمل على المساس بتكاملية وروحية المعطيات والمعلومات والخدمات التي يوفرها.

8- جريمة خرق الحماية المادية لنظم المعلوماتية : وتحصل من خلال التفتيش في المخلفات التقنية، بحيث يعمد المجرم إلى البحث بمخلفات بعض الهيئات والمنظمات أو الشركات بحثاً عن أية أوراق أو تجهيزات أو أقراص يمكن من خلالها الحصول على كلمات مرور، تمكنه من الدخول إلى برنامج ما، أو من خلال العثور على قرص صلب أو مدمج أو أية وسيلة مستعملة لتخزين المعلومات والاطلاع على المعلومات التي تحتويها واستغلالها على نحو غير مشروع[13].

بعد أن انتهينا من عرضنا لجرائم المعلوماتية الصرفة، وتحديد موقف المشرع اللبناني منها، وفق ما نص عليه القانون رقم 81/ 2018، يبقى أن نتطرق إلى بعض صور الجرائم التقليدية التي ترتكب بوسائل تكنولوجيا المعلومات، وهذا ما سنتطرق له في الفرع الثاني.

الفرع الثاني

جرائم تقليدية ترتكب بوسائل تكنولوجيا المعلومات

إن الجرائم التي يمكن أن ترتكب بواسطة أدوات ووسائل إلكترونية متنوعة ومتعددة ويصعب حصرها ببعض الجرائم، ومن غير المجدي التطرق إلى كل منها على حدة، لذا سنكتفي بالتطرق إلى بعض تلك الجرائم، ولكن ضمن تصنيفات تأخذ بعين الاعتبار إلى حد كبير التصنيف الذي اعتمدته غالبية التشريعات الوطنية ومنها المشرع اللبناني.

أولاً: الانتهاكات الجرمية الواقعة على الأشخاص:

نذكر من بين تلك الجرائم:

أ- جريمة إساءة استعمال البيانات ذات الطابع الشخصي : يسعى بعض المجرمون إلى الحصول على بعض المعلومات الشخصية الخاصة بشخص أو أكثر من دون موافقة أصحاب العلاقة، كالاسم والشهرة وتاريخ الميلاد والجنس والجنسية، واستغلال تلك المعلومات بطريقة غير مشروعة بانتحال صفة أو شخصية الفرد وفتح حسابات مشبوهة باسمه لمزاولة أعمال غير مشروعة، أو للحصول على بطاقات ائتمان مزورة، أو بغية تسهيل عمليات الاحتيال التي يقع ضحيتها عدد من المستخدمين[14].

وليس ما يمنع من تطبيق نصوص قانون العقوبات المطبقة على الجرائم التقليدية، وخاصة فيما لو أجري بعض التعديل على نص المادتين 391 و392، وكذلك المادتين 469 و470 من قانون العقوبات اللبناني، بحيث تشمل انتحال شخصية

---

[12] لقد حظر المشرع اللبناني كل فعل ينطوي على ادخال بيانات رقمية، بنية الغش، في نظام معلوماتي وكل من ألغى أو عدل، بنية الغش، البيانات الرقمية التي يتضمنها نظام معلوماتي، وعاقب على ذلك بالحبس من ستة أشهر الى لاث سنوات وبالغرامة من ثلاثة ملايين الى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين.

[13] عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 118.

[14] عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، مرجع سابق، ص 160.

فرد آخر عبر وسائل تكنولوجيا المعلومات، وبالتحديد عبر شبكة الإنترنت ووسائط التواصل الاجتماعي.

ب-الجرائم الماسة بخصوصية المعلومات الخاصة بشخص الفرد: تتمحور خصوصية المعلومات الشخصية حول حق الفرد في الحفاظ على سرية المعلومات الخاصة به، وعدم الاطلاع عليها إلا لمن يأذن لهم، أو الأشخاص المخولين بحكم القانون أو الواقع الاطلاع عليها، ومن ذلك المعلومات ذات العلاقة ببيانات الهوية والوضع المالي ومختلف السجلات الحكومية الخاصة به، لذا يحرم على الغير الاطلاع عليها أو استنساخها أو نشرها من دون موافقة صاحبها[15].

ج- جريمة المساس بحرمة مكاني الإقامة أو العمل: حرصت معظم التشريعات على احترام خصوصيات الأفراد في الأماكن التي يقيمون فيها، وذلك لأن الفرد بحاجة لمكان يختلي به إلى نفسه بعيداً عن أية رقابة، وهذا هو العامل الأساس وراء تحريم انتهاك حرمة المنزل، ومع التطور التقني الذي شهدته البشرية في مختلف المجالات أضحى من السهل على الغير المساس بالحقوق، اللصيقة بشخصية الفرد، إن كان من خلال الإطلاع على المعلومات الخاصة به أو بمراقبته أو باستراق النظر إليه أو التنصت عليه في منزله أو في مكان عمله أو حتى عبر الاتصالات التي يجريها، من هنا تشدّدت التشريعات في حماية هذه الخصوصيات والعقاب على المساس بها[16].

ثانياً: الانتهاكات الجرمية الواقعة على الأموال: غالباً ما يكون الدافع إلى ارتكاب هذه الجرائم الإثراء غير المشروع، من خلال المساس بحق عيني يحميه القانون، بنية الاستئثار بسلطات ومزايا ينطوي عليها هذا الحق، وغالباً ما تطال حق الملكية، ومن هذه الجرائم: السرقة، الاحتيال وإساءة الائتمان، ومع ثورة تكنولوجيا المعلومات التي شهدها العالم لوحظ نمو في معدل هذه الجرائم عبر شبكات الإنترنت، وبأنماط وأساليب لم تكن معهودة من قبل، وخاصة في ظل تنامي النشاطات التجارية وما يعرف بالتجارة الإلكترونية، حيث أصبح يتم تبادل المنتجات والإتجار بها عبر شبكة الإنترنت، كما أدى شيوع التعامل واتمام الصفقات بواسطة المعاملات الإلكترونية بما في ذلك التفاوض وإبرام العقود والاتفاقات الكترونياً، واعتماد البطاقات الائتمانية، والنقود الإلكترونية إلى ظهور نوع آخر من الجرائم المرتكبة عبر الإنترنت منها: السرقة بواسطة البطاقات الائتمانية، الاحتيال، الغش التجاري، تبييض الأموال، المقامرة وألعاب الميسر الإلكترونية، الإتجار بالبشر عبر الإنترنت[17].

ومن أهم تلك الجرائم:

أ جريمة السرقة (الإلكترونية): السرقة هي اعتداء على ملكية منقول وحيازته بنية تملكه، وتمثل اعتداء على الملكية والحيازة معاً، وينبغي أن يكون محل الجريمة مال منقول مملوك من الغير، وأن يكون القصد من الفعل هو تملك المال الذي نقلت حيازته من مالكه الحقيقي إلى حيازة المجرم السارق، وفي جرائم المعلوماتية تثار إشكالية تتمحور حول طبيعة الشيء موضوع الحيازة، وما إذا كان ينبغي أن يكون شيئاً مادياً ينتمي إلى عالم المحسوسات، أي يمكن لمسه وتحسسه، أم أن الشيء قد ينضوي ضمنه أمور معنوية كما هو الحال بالنسبة للمعطيات والبيانات والمعلومات، والتي أضحى لها قيمة مالية في يومنا الحاضر.

ولا تقوم الجريمة إلا بتوفر القصد الجنائي المتمثل بعنصري العلم والارادة، بالإضافة إلى توفر قصد خاص، يستدل منه على نية السارق بتملك المال موضوع السرقة، وتقوم هذه النية على عنصرين: سلبي، يتمثل بإرادة حرمان المالك من

---

(15) المادة 581 من قانون العقوبات اللبناني.

(16) منصور محمد حسين، المسؤولية الالكترونية، الاسكندرية، دار الجامعة الجديدة، 2003، ص359.

(17) منير وممدوح محمد الجبهيني، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2004، ص68.

سلطاته الاستئثارية على الشيء، ومظهره العزم على عدم رد الشيء، وعنصر ايجابي، قوامه، إرادة المتهم أن يحل محل المالك في سلطاته على الشيء. وهذا ما يحصل في عمليات الاستحصال على الأموال من خلال التلاعب في الحسابات المصرفية، أو باستخدام البطاقات الائتمانية.

ب الإحتيال: الاحتيال هو الاستيلاء على مال مملوك للغير عن طريق مناورات احتيالية، بخداعه وحمله على تسليم ذلك المال، ولكن ماذا بالنسبة لعمليات (جرائم) الاحتيال التي تحصل بواسطة تكنولوجيا المعلومات وعبر شبكة الإنترنت؟

فهل يصح تطبيق تلك النُصوص عينها المعتمدة حيال عمليات الاحتيال التقليدية، أم أنه ينبغي إجراء بعض التعديلات عليها، أو اعتماد نصوص جديدة، بحيث تخصص للاحتيال المعلوماتي إن صح التعبير؟ والتي يرتكبها أشخاص يستعملون أسماء وهمية عادة، من خلال مناورات احتيالية تتم عبر الإنترنت للإيقاع ببعض المستخدمين، جراء التأثير عليهم ودفعهم إلى تحويل مبلغ مالي لقاء تنفيذ خدمة مزعومة، أو شراء سلعة ما أو من خلال إنشاء موقع مزيف يزعم منشئه أنه يوفر خدمة ما إلى الزبائن لقاء دفع مبلغ معين، ومن صوره: إنشاء موقع وهمي للتوظيف، بحيث يصطادون من خلاله طالبي العمل بإيهامهم أنهم وجدوا لهم عملاً يتناسب مع كفاءاتهم ومهاراتهم، وكل ما عليهم دفع مبلغ من المال لكي يتم توظيفهم أو من خلال الإتصال ببعض مستخدمي شبكة الإنترنت، وإيهامهم أنه بمقدورهم ربح جائزة أو مبلغ من المال في حال شاركوا بدفع مبلغ يخولهم ربح الجائزة، أو بإيهامهم بوجود جائزة قد رست عليهم وأنه يتوجب عليهم دفع مبلغ يعادل تكاليف تسليم الجائزة لهم، وما شابه ذلك من المناورات[18].

باعتقادنا أن النصوص الجزائية المعتمدة حيال جرائم الاحتيال التقليدية يمكن اعتمادها حيال المرتكب منها عبر تكنولوجيا المعلومات. خاصة وأن المشرع لم يحدد الوسيلة التي تعتمد فيها المناورات الاحتيالية، ولا نرى ضيراً في إجراء بعض التعديلات على النصوص التي ترعاها بحيث تشير إلى إمكانية الأخذ بالمناورات المنفذة عبر شبكة الإنترنت أو بأي أسلوب كان[19].

ثالثاً: الإنتهاكات الجرمية الماسة بأمن الدولة: وفرت شبكة الإنترنت مجالاً للتواصل المباشر بين الأفراد بغض النظر عن المسافات الجغرافية والضوابط السياسية التي كانت تحد من تلك الإمكانيات عندما كانت الدول قادرة على مراقبة الاتصالات الهاتفية والرسائل البريدية بسهولة، كونها كانت تمر عبر سنترالات مركزية في الدولة تربطها بالعالم الخارجي، ولكن في ظل شبكة الإنترنت، وما أتاحته من إمكانية للاتصال والتواصل شبه المجاني بين الأفراد، وبسرعات ويسر غير متوفرين من دون المرور عبر سنترالات الهاتف والشبكات العائدة لها، وخاصة بعد انتشار البرمجيات التي تُعنى بتوفير سبل التواصل بين الأفراد مثل الواتس أب والفايس بوك والتانغو والفايبر وغيرها من مئات المواقع التي تُعنى بذلك، الأمر الذي شجع جهات مختلفة من حيث التطلعات والتوجهات على استغلال خصائص الأنترنت والخدمات التي توفرها هذه الشبكة من أجل التجسس على الدول الأخرى، وتجيش العملاء الذين يعملون لصالحها، هذا بالإضافة إلى إمكانية القيام بأعمال التجسس عن بعد عبر شبكة الإنترنت، والتي أضحت متصلة بمختلف المؤسسات والمرافق الحساسة بما في ذلك القوى العسكرية، ومواقع الصواريخ ومحطات الطاقة النووية والهيدروجينية والمطارات العسكرية، وغيرها من المواقع العسكرية والأمنية والاقتصادية الحساسة، وتقسم الجرائم الماسة بأمن الدولة ما بين:

---

[18] يعمد بعض المحتالين الى طلب مبالغ صغيرة بحيث يرى الضحايا انه لا جدوى مادية من إقامة دعوى ضدهم لبخس المبلغ موضوع المناورة الاحتيالية مقابل تكاليف ومصاريف الدعوى وصعوبة الملاحقة.

[19] ورد في الفقرة الأولى من المادة 655 والتي جرمت الاحتيال (كل من حمل الغير بالمناورات الاحتيالية على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء أو منفعة واستولى عليها).

أ_ جرائم ماسة بأمن الدولة الخارجي، ومنها:

_ جريمة الخيانة: ويندرج ضمنها الأفعال التالية، حمل السلاح في صفوف العدو أو الإقدام في زمن الحرب على أعمال عدوان ضد دولته، التجنيد في جيش معاد خلال الحرب أو عمل عدوان ضد الدولة التي ينتمي إليها، دش الدسائس لدى دولة أجنبية أو الإتصال بها لدفعها لمباشرة العنوان ضد الدولة أو معاونتها أو توفير الوسائل لها للقيام بذلك، أو الإضرار بالمنشآت والمصانع والبواخر والمركبات الهوائية والأدوات والذخائر وسبل المواصلات، وأية أشياء ذات طابع عسكري أو معدة لاستعمال القوى العسكرية الوطنية، ويتبين جيا أن بعضاً من هذه الأفعال يمكن ارتكابها عبر نظم تكنولوجيا المعلومات، ولا نرى من مانع لتطبيق نصوص قانون العقوبات المعتمدة حيال ك الأفعال المرتكبة بوسائل تقليدية على ما يرتكب منها بوسائل تقنية المعلومات، إلا أنه يفضل العمل على تعديلها وتحديثها بما يكفل تطبيقها على الجريمة فيما لو ارتكبت بوسائل تكنولوجيا المعلومات.

ب الجرائم الماسة بأمن الدولة الداخلي: ومنها:

_الاعتداءات التي تستهدف تغيير دستور الدولة بطرق غير مشروعة، والأفعال التي تعترف بقصد اثارة عصيان مسلح ضد السلطات القائمة بموجب الدستور، والتي قد ترتكب بوسائل معلوماتية، وعبر شبكة الإنترنت.

_جريمة الإرهاب: يعني بالأعمال الارهابية وفق نصوص قانون العقوبات اللبناني: جميع الأفعال التي ترمي إلى إيجاد حالة ذعر، وتُرتكب بوسائل كالأدوات المتفجرة والمواد الملتهبة، والمنتجات السامة أو المحرقة، والعوامل الوبائية أو الميكروبية التي من شأنها أن تحدث خطراً عاماً.

ويضاف إليها المؤامرة التي يقصد منها ارتكاب عمل أو أعمال إرهاب يعاقب عليها بالأشغال الشاقة المؤقتة، وتشدد العقوبات فيما لو نتج عن العمل الإرهابي تخريب أو هدم ولو جزئي في بناية عامة أو مؤسسة صناعية أو سفينة أو منشآت أخرى أو تعطيل في سبل المخابرات والمواصلات والنقل، كذلك لم يغفل المشرع اللبناني تجريم تمويل الإرهاب أو الأعمال الإرهابية، أو تمويل شخص إرهابي أو منظمات إرهابية، أو الأعمال المرتبطة بها[20].

رابعاً: الانتهاكات الجرمية ماسة بالأخلاق والآداب العامة: لقد ساهمت الإنترنت إلى حد كبير في تفشي ظاهرة الإباحية الجنسية، لما وفرته من امكانيات لنشر الصور ومقاطع الفيديو بالصوت والصورة، ما أتاح للمجرمين إمكانية للتسويق لهذه التجارة ونشر ما يحلو لهم من صور وأفلام إباحية، كما إنشاء مواقع تتيح التواصل مع بنات الهوى بقصد الدردشة الفاضحة أو التواعد أو بغية ممارسات جنسية عن بعد، وحيث أن معظم التشريعات في مجتمعنا العربي قد تشدّدت في ملاحقة الجرائم الماسة بالأخلاق العامة. ومنها: جرائم الأخلاق والآداب العامة أو اللاأخلاقية التي تستهدف الأطفال إذ إن الأطفال والمراهقين هم أكثر الأفراد عرضة لمخاطر إساءة استعمال النظم الإلكترونية وبخاصة الإنترنت، وقد يكونون الأكثر استهدافاً من بعض المجرمين المعلوماتيين، الذين يستغلون براءتهم وثقتهم بالآخرين، في ظل غياب القدر الكافي من التوجيه والرقابة في كثير من الأحيان[21]. من حيث الواقع يلاحظ أن حجم مشكلة المواد الإباحية بوجه عام، والمواد والانشطة الجنسية المتصلة بالأطفال والقصر بوجه خاص، يتزايد بشكل غير عادي، لذا تتشدد معظم التشريعات في العقاب على تلك الجرائم طالما كانت تستهدف الأطفال والقصر عامة، وباعتقادنا ليس ما يمنع من تطبيق نصوص قانون العقوبات على مثل هذه الجرائم فيما لو ارتكبت عبر وسائل تكنولوجيا المعلومات، تجدر الإشارة إلى أن المشرع اللبناني حرص على إجراء التعديلات اللازمة فيما خص استغلال القاصرين في مواد إباحية.

---

[20] عادل مشموشي، مكافحة الارهاب، المرجع السابق، ص 134.

[21] احمد خالد محي الدين، الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المغرب، 2010، ص37.

خامساً: الإنتهاكات الجرمية الماسة بالملكية الفكرية والعلامات التجارية : اهتمت معظم الدول مؤخراً في حماية الملكية الفكرية والأدبية، ومنها لبنان، حيث أقر القانون رقم 75 تاريخ 3/ 4/ 1999، والذي هدف إلى حماية إنتاج العقل البشري سواء كانت كتابية أو خطية أو شفهية، وبغض النظر عن مقدار قيمتها وكيفية التعبير عنها ، وقد حددها حصراً في المادة الثانية منه، ومن بينها الكتب والمحفوظات والمنشورات والمطبوعات ، والأعمال السمعية والبصرية والصور الفوتوغرافية والأعمال الموسيقية، كما أعمال الرسم والنّحت والزخرفة والأعمال المسرحية والموسيقية، وبرامج الحاسب الآلي، والخرائط والتصاميم والمخططات والمجسمات الجغرافية والطبوغرافية والهندسية والعلمية، وغيرها.

مع نشأة شبكة الإنترنت وما عرفته من تطور، واعتمادها كوسيلة لنشر المعرفة، والتي يندرج ضمنها نشر المقالات والكتب والدراسات وغيرها من الأمور ذات القيمة المادية والمعنوية انتشرت ظاهرة الانتهاكات الماسة بالملكية الفكرية التي تُرتكب عبر وسائل تكنولوجيا المعلومات.

المطلب الثاني

دور التشريعات الجزائية العراقية واللبنانية في مكافحة الجريمة الإلكترونية

تعد الجرائم الإلكترونية إحدى أهم صور الجرائم ذات البعد الدولي العابر للحدود، حيث لم تعد تلك الحدود بعد تشكل حاجزاً أمام مرتكبي هذه الجرائم، كما أن نشاط هؤلاء الجناة لم يعد قاصراً على إقليم معين بل امتد إلى أكثر من إقليم، ومن هنا جاءت الصعوبة في مكافحة هذه الجرائم من قبل التشريعات الوطنية، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين، ويقبل على التنفيذ في بلد آخر، ويهرب إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالجريمة أصبح لها طابع دولي، والمجرم أصبح مجرماً دولياً [22] .

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.

وبناء على ذلك سنوضح التحديات التي تواجه المشرعين اللبناني والعراقي في مكافحة الجرائم الإلكترونية من خلال فرعين، نتناول في الأول منهما الصعوبات التشريعية والاجرائية التي تواجه المشرعين وكيفية تفاديها، أما في الفرع الثاني فسنتوجه للحديث عن تبني اليات ملاحقة أكثر فعالية.

الفرع الأول

الصعوبات التشريعية والاجرائية التي تواجه المشرعين وكيفية تفاديها

تعرض كل من التشريعين العراقي واللبناني لمسألة الاختصاص في جرائم الاحتيال الإلكتروني وسنتعرض لهما تباعاً:

أولاً: موقف القانون اللبناني:

1_ مرحلة ما قبل صدور قانون المعاملات الإلكترونية رقم 2018/81:

تختلف استجابة المشرعين في الدول المختلفة لمواجهة الجرائم الإلكترونية الحديثة باختلاف درجة التقدم العلمي في هذه الدولة أو تلك، فقد واجه المشرعون في الدول المتقدمة هذه الجرائم المستحدثة بقوانين خاصة، تتضمن جزاءات تتناسب مع درجة خطورتها، بالإضافة إلى تعديل قوانين الإثبات والإجراءات الجزائية لتتكيف مع المستجدات، أصدرت الولايات المتحدة

[22] **فتوح عبد الله الشاذلي، المواجهة التشريعية للجرائم المستحدثة، بحث مقدم لمؤتمر الامن والسلامة الذي عقدته وزارة الداخلية بدولة الامارات العربية المتحدة، الامارات، 2003، ص1.**

الأميركية في عام 1994 مجموعة من التشريعات على المستوى المحلي للولايات والاتحادي، ولحقت بها فرنسا بتضمين قانونها للعقوبات الصادر 1994 [23] .

وأما في لبنان، ورغم دخول شبكة الإنترنت إليه وانتشار استخدامها وما نشأ عن ذلك من جرائم إلكترونية، وقيام التشريعات العربية التي سبقته في مكافحة هذا النوع من الجرائم المستحدثة، لم تشرع الحكومة بالتفكير في هذه المواجهة إلا عام 2012، حيث عمدت إلى تقديم مشروع قانون إلى مجلس النواب، وذلك بموجب المرسوم رقم 9341 تاريخ 17_11_2012 تحت عنوان «قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي» [24] .

لكن يصدر هذا القانون إلا بتاريخ 10_10_2018 على أن يعمل به بعد ثلاثة أشهر من تاريخ نشره في لجريدة الرسمية، والحاصل في العدد 45 تاريخ 2018/10/18، رغم تزايد عدد الجرائم الناجم عن استخدام شبكة الإنترنت وفي حال غياب النص في الفترة السابقة على القانون رقم 2018/81، كان يتم اللجوء إلى القواعد التقليدية لقانون العقوبات ومحاولة تكييف الجرائم الإلكترونية على ضوء نصوص القسم الخاص منه [25] .

أيضاً الصعوبات التي رافقت تطبيقه، ومدى تعارضه مع مبدأ الشرعية العقابية والإجرائية بالنسبة لبعض الجرائم الإلكترونية كجرائم الإعلام الإلكتروني مثلا، لأن طرق العلانية المحددة حصرة في المادة209عقوبات لم تكن تشمل هذه الجرائم، الأمر الذي حدا بالمشرع إلى تضمين مشروع قانون المعاملات الإلكترونية إضافة على البند الثالث من هذه المادة بتشميله الوسائل الإلكترونية المعتمدة في النشر، وهذه الإضافة للوسائل الإلكترونية إلى طرق العلانية تكشف أن ما اعتبر من الجرائم علانية قبل نفاذ القانون الحالي رقم2018/81 إنما هو تطبيق خاطئ يتعارض مع مبدأ الشرعية، لغياب النص على الوسيلة الإلكترونية من ضمن طرق النشر بالعلانية المحددة حصرة في البند الثالث من المادة209عقوبات، الأمر الذي لم يتطرق إليه أحد رغم عدم مشروعية التطبيقات القضائية التكييف النصوص التقليدية قبل هذا التعديل الحاصل بالقانون رقم2008/81.

2_ مرحلة التقنين للنشر الإلكتروني والجرائم الإلكترونية:

بعد انتظار طويل ومرور فترة زمنية غير قصيرة على ظهور الجرائم الإلكترونية واستخدام شبكة الإنترنت في لبنان وما نشأ عنها من جرائم الإعلام الإلكتروني، ظهر أخيراً في وقت متأخر قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم 2008/81، والذي لا يعتبر قانون عقوبات خاص، بقدر ما هو تشريع لكافة المعاملات الإلكترونية من مدنية وتجارية وجزائية وغيرها[26] .

أ–معالم قانون المعاملات الإلكترونية رقم 2018/81:

هذا القانون صدر بتاريخ 2018/10/10، وعلى أن يعمل به بعد مرور ثلاثة أشهر على نشره في الجريدة الرسمية الحاصل في العدد 45 تاريخ 2018/10/18، أي بمعنى آخر سوف لن يكون نافذة إلا اعتبارا من 2019/1/18، مع ملاحظة هذا البطء وعدم الانتباه إلى خطورة الفراغ التشريعي للفترة السابقة على نفاده، رغم إحالة عدد كبير من الجرائم الإلكترونية، وحتى أنه صدرت أحكام مبرمة بشأنها مع وجود إشكالية انتفاء النص على علانية الإعلام الإلكتروني، قبل

---

[23] **عباس ناجي حسن، الوسائط المتعددة في الإعلام الالكتروني، دراسة مقارنة، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، 2016، ص 49.**

[24] **سمير عالية، القانون الجزائي للأعمال، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2018، ص 32.**

[25] **جورج لبكي، المعاهدات الدولية للإنترنت حقائق وتحديات، مقال منشور في مجلة الدفاع الوطني اللبناني، العدد 83، تاريخ 23 كانون الثاني، بيروت، 2013، ص 9.**

[26] **محمد عبد الكريم حسين الداودي، المسؤولية الجنائية لمرود خدمة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2017، ص 123.**

صدور ونفاذ القانون، وعدم التأكد من صحة التكييف الجرائم تقليدية أخرى.

ب- تحديد موقع الشق الجزائي من القانون رقم 2018/81 من القسم الثاني: إن مدلول القسم الخاص من قانون العقوبات لا يقتصر على مجموعة مواده المعدة في الكتاب الثاني منه الوارد بعنوان جرائم المواد 270 حتى 770، وإنما يمتد هذا القسم الخاص ليشمل جميع التشريعات الجزائية المكملة لتعداد مواده أو الملحقة بها [27] .

فقد يرى المشرع أن يعالج بعض فئات الجرائم في تشريعات منفردة خارج الإطار التقليدي لتعداد جرائم القسم الخاص من قانون العقوبات، كون هذه الجرائم المستحدثة تمثل اعتداء على مصالح جديرة بالحماية لم تكن معروفة بتاريخ وضع قانون العقوبات، أو لكونها تنطوي على مصالح غير ثابتة أو متغيرة، فيكون من الأجدى عدم إدراجها في صلب نصوص القسم الخاص من قانون العقوبات، حتى لا يتعرض للتعديل والتغيير كلما استوجب الأمر تعديلاً.

حيث إن مفهوم قانون العقوبات التكميلي لمواد القسم الخاص من قانون العقوبات العادي، ينطبق على الشق الجزائي من قانون المعاملات الإلكترونية اللبناني رقم 2018/81 لكونه ينطوي على تعداد للجرائم الإلكترونية دون أن يخصها بقواعد مغايرة أو متعارضة مع نصوص القسم العام القانون العقوبات.

هذا وإن وصف هذا الشق الجزائي من قانون المعاملات الإلكترونية والبيانات الشخصية بأنه قانون مكمل أو ملحق بالقسم الخاص من قانون العقوبات العادي، إنما يعني بالضرورة أنه يشكل جزء منه وملحقة به، مما يجعله خاضعة لقواعد القسم العام [28] .

ثانياً: موقف القانون العراقي.

يمكن توضيح موقف القانون العراقي في مواجهة الجرائم الإلكترونية بشكل عام وجريمة الاحتيال الالكتروني بشكل خاص في ثلاث نقاط:

النقطة الأولى: صدور قانون التوقيع الالكتروني والمعاملات الالكترونية رقم78لسنة2012، الذي يتكون من 29 مادة موزعة على 8فصول، حيث وفر هذا القانون الإطار القانوني لاستعمال الوسائل الالكترونية في إجراء المعاملات الالكترونية ومنح الحجية القانونية للمعاملات الالكترونية والتوقيع الالكتروني وذلك لتعزيز الثقة في صحة هذه المعاملات، وكذلك أعطى هذا القانون الحجية القانونية للمستندات الالكترونية والعقود الالكترونية والأوراق التجارية والمالية الالكترونية وفقاً لشروط معينة، واجاز التحويل الإلكتروني للأموال مع الزام المؤسسات المالية التي تقوم بأعمال التحويل المالي باتخاذ الاجراءات اللازمة لتوفير هذه الخدمات بطريقة مأمونة والحفاظ على سرية المعاملات المصرفية[29].

النقطة الثانية: وعلى صعيد الجرائم الإلكترونية، فلا يوجد في العراق باستثناء اقليم كوردستان حتى تاريخ إعداد هذه الرسالة قانون متخصص يكافح هذه الجرائم، إلا أن هناك مشروع قانون عراقي تم اعداده 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 ابداء الرأي التي كفلها الدستور العراقي لسنة 2005 في المواد 38 و40، وقد تناولت مسودة قانون

---

[27] **حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الناشئة عنها، منشورات الحلبي الحقوقية، بيروت، 2017، ص 65.**

[4] **المادة 13 والمادة 23 قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم 78 لسنة 2012.**

[29] **سمير عالية، القانون الجزائي للأعمال، المرجع السابق، ص 78.**

الجرائم الإلكترونية العراقي جريمة الاحتيال الالكتروني في المادة 10 تحت تسمية جريمة الاحتيال حيث عرف المشرع الاحتيال بانه التسبب بالحاق الضرر عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل والغير عن طريق:

أ_ استخدم عمدا نظام الحاسوب أو شبكة المعلومات العائدة للأشخاص أو الشركات أو الهيئات أو المصارف أو الاسواق المالية وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الالكترونية.

ب- 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 الكتروني أو بطاقات الكترونية أو مال منقول أو سند أو توقيع على سند باستخدام طرق احتيالية أو اتخاذ اسم كاذب او صفة غير صحيحة من شانها خداع المجني عليه [30] .

أما الفقرات ج ، د، هـ فتتناول التلاعب بالأسهم واسعار العملة واستخدام العلامة التجارية وكذلك استخدام البطاقة الالكترونية بعد نفاذ الرصيد أو بعد الغائها أو انتهاء صلاحيتها مع العلم بذلك، والملاحظ أن المشرع العراقي حاول شمول معظم جوانب الاحتيال الالكتروني في هذه المادة وعلى الرغم من ذلك فكان الافضل عدم حصر الوسائل الاحتيالية كونها مرتبطة بالتقدم التقني الذي لا يعرف الحدود بالإضافة إلى تجاهل المشرع لتزوير البطاقة الالكترونية واكتفى بتجريم استخدام هذه البطاقة دون علم صاحبها، ولكون قانون الجرائم الإلكترونية العراقية لم يصدر لحد الان فلا نريد استباق الامور ونترك التعليق عليه لحين صدوره بالشكل النهائي واستيفائه مراحل تشريعه[31].

النقطة الثالثة: للمواجهة التشريعية للجرائم الإلكترونية في العراق، هو صدور قانون منع اساءة استعمال اجهزة الاتصالات في اقليم كوردستان العراق رقم 6 لسنة 2008 وهو يتألف من ثمانية ابواب واسباب موجبة، وتتجسد الجرائم التي تناولها القانون في:

1) جرائم ضد الاعتبار الشخصي للإنسان.
2) جرائم ضد الاخلاق والآداب العامة.
3) جرائم ضد حرمة الحياة الخاصة والعائلية.
4) وجريمة الازعاج.

وقد أضاف المشرع في إقليم كوردستان جريمة خامسة حيث أشار، إلى أنه في حال أدت الافعال المجرمة في هذا القانون، إلى ارتكاب جريمة فيعد المتسبب فيها، شريكا ويعاقب بالعقوبة ذاتها المقررة للجاني فيها[32].

في حين أن جرائم ضد الاعتبار الشخصي فتشمل جريمتين رئيسيتين هما القذف او 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.

---

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

[31] **مازن ليلو راضي وعدي سليمان علي، المواجهة التشريعية للجريمة الالكترونية في اقليم كوردستان العراق، بحث منشور في مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الاول لكلية القانون، العراق، 2009، ص 30.**

[32] **المادة 4 قانون منع اساءة استعمال اجهزة الاتصالات في اقليم كوردستان العراق رقم 6 لسنة 2008**

اما الجرائم ضد الاخلاق والآداب العامة فتناولها المشرع في إقليم كردستان وهي، تسريب محادثات أو صور ثابتة أو متحركة أو الرسائل القصيرة المسج المنافية للأخلاق والآداب العامة أو التقاط صور بلا رخصة أو اذن وإسناد امور خادشه للشرف أو التحريض على ارتكاب الجرائم أو افعال الفسوق والفجور، والصورة الرابعة التي جرمها القانون هي جريمة الازعاج حيث عاقبت المادة الثالثة من القانون بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على السنة وبغرامة لا تقل عن سبعمائة وخمسون الف دينار ولا تزيد على ثلاثة ملايين دينار أو بإحدى هاتين العقوبتين كل من تسبب عمداً باستخدام واستغلال الهاتف الخلوي أو أية اجهزة اتصال سلكية أو لاسلكية أو انترنت أو البريد الالكتروني في ازعاج غيره في غير الحالات الواردة في المادة الثانية من هذا القانون[33].

وأخيراً ونحن بصدد موقف المشرع العراقي من جريمة الاحتيال الالكتروني بشكل خاص والجرائم الإلكترونية بشكل عام لابد ان نشير بأن برامج الحاسوب قد تم بسط الحماية عليها من خلال التعديل الذي تم على قانون حق المؤلف رقم 3 لسنة 1971 بالأمر رقم 83 لسنة 2004 الصادر عن سلطة الائتلاف المؤقتة المنحلة [34].

الفرع الثاني

تبني اليات ملاحقة أكثر فعالية

يشكل الإنترنت جزءا لا يتجزأ من حياتنا اليومية، ولكنه ينطوي أيضاً على بعض المخاطر التي نتعرض لها كلما استخدمناه، ولا نقصد بذلك الفيروسات والتصيّد الاحتيالي وبرامج التجسس الحاسوبي فقط، فهناك أشخاص من مختلف الأعمار يستخدمون الإنترنت بهدف إلحاق الأذى بالغير.

لئن كان الإنترنت أداة عظيمة إقامة علاقات صداقة جديدة وتبادل الاهتمامات، من الأهمية بمكان عدم الكشف في إطاره عن الكثير من المعلومات المتصلة بكم.

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.

إن أنشطة مكافحة جرائم الكمبيوتر والإنترنت أبرزت تحديات ومشكلات جمة تغاير في جوانب كثيرة التحديات والمشكلات التي ترتبط بالجرائم التقليدية الأخرى وتستدعي تبني آليات أكثر تطوراً من حيث الملاحقة [35] :

1. هذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

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 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 الإلكترونية

---

[33] **المادة 2 قانون منع اساءة استعمال اجهزة الاتصالات في اقليم كوردستان العراق رقم 6 لسنة 2008.**

[34] **عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، مطبعة الوئام للحاسبات والطباعة والنشر، بابل، العراق، 2009، ص 190.**

[35] **محمد السيد رشدي، «الإنترنت والجوانب القانونية لنظم المعلومات»، مجلة الفتوى والتشريع، العدد 9، مجلس الوزراء، آيار، 2000، ص 45**

لأصحاب النظم التي يمتد إليها التفتيش.

3. أن الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوما بعد يوم ، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه ، أي على أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والاتلاف ، وهذه الحقائق تثير مشكلات متعددة ، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه – وإن كان المشتبه به – عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية [36] بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى .

4. أن أدلة الإدانة ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، وقد أثارت وتثير أمام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية.

5. كما أن اختصاص القضاء بنظر جرائم الكمبيوتر والقانون المتعين تطبيقه على الفعل لا يحظى دائما بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها ، وهو ما يبرز أهمية امتحان قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين أفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي [37] .

ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية.

إذن فان البعد الإجرائي لجرائم الكمبيوتر والإنترنت ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسة، الحاجة إلى سرعة الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم، وقانونية وحجية أدلة جرائم الكمبيوتر والإنترنت، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني أم الدولي.

توجيهات عملية في ضبط وتفتيش انظمة 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 [38] .

1- أن القاعدة الأولى 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

---

[36] **ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، الطبعة الثالثة، دار النهضة العربية القاهرة 2010، ص 47**

[37] **جمال سيف فارس، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية – دراسة مقارنة بين القوانين الوضعية الأجنبية والقانون الدولي الجنائي، دار النهضة العربية، القاهرة، 2007، ص 25**

[38] **جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، 2002، ص78.**

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 ، أما مشكلات التفتيش فان 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 تالياً:

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 ابتداءً 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 [39] .

3– أما إن كان النظام أو مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش فيتعين ان تجيء عبارات مذكرة التفتيش عامة ما امكن حتى لا يكون نصها قيدا على نطاق التفتيش والضبط ، فعلى سبيل المثال يمكن ان 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 سواءً 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 [40] .

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 .

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

---

[39] **محمد عبد الله سلامة، جرائم الكومبيوتر والانترنت، الطبعة الأولى، منشأة المعارف، الاسكندرية، 2006، ص69.**

[40] **جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص 98.**

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 [41].

فمثل 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

تعد الثورة التكنولوجية وخصوصاً ثورة الاتصالات، أهم التطورات التي يعيشها العالم، كما تعدّ ثورة الاتصالات هي المحرك الأساسي في التطورات الحاصلة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات، إذ إن التطور الكبير في تكنولوجيا الحاسبات، قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصال والمعلومات.

وفي نهاية هذا البحث توصلنا إلى جملة من النتائج والتوصيات سنوردها كما يلي:

أولاً: النتائج:

1- إن محل الجريمة الإلكترونية وموضوعها هو المعطيات والمعلومات الموجودة على الحاسب والذي تستهدفه اعتداءات الجناة بشكل عام، إذ إن الجرائم إما أن تقع على الكمبيوتر ذاته أو بواسطته، وذلك باعتباره محل الجريمة تارةً ووسيلة لارتكابها تارةً أخرى على محل آخر وهو المعلومات والمعطيات الإلكترونية.
2- توصلنا إلى أن المصالح الواجب حمايتها جنائياً في إطار التجريم الإلكتروني هي حماية حق السرية وحرمة الحياة الخاصة وحماية حق الملكية الإلكترونية والفكرية والذي يمكن أن نطلق عليه الذمة الإلكترونية أو التكنولوجية وحماية حقوق الملكية المادية، وحماية النظام العام الإلكتروني كجزء من النظام العام الإداري والاقتصادي في الدولة.

ثانياً: المقترحات:

1- ندعو المشرع العراقي لاستحداث نصوصاً قانونية في قانون العقوبات العراقي تحت ما يسمى الجريمة الإلكترونية تحدد بشكل واضح ودقيق صور هذه الجرائم مقتدياً بالمشرع اللبناني وإيجاد العقوبات الملائمة لها التي من شأنها تحقيق الردع العام والخاص، ولا بد من توسع المشرع الجزائي في مفهوم المال بحيث يشمل كل شيء ينطوي على قيمة.
2- ضرورة إحداث جهاز خاص للخبرة الجنائية للجريمة الإلكترونية يتكون أعضاؤه من فريق متخصص فنياً في تقنيات المعلومات، على أن يتم إعادة النظر في القواعد التقليدية للخبرة، على اعتبار أن إثبات الجريمة الإلكترونية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم.

[41] **محمود شريف بسيوني، «الوثائق الدولية المعنية بحقوق الإنسان»، المجلد الثاني، دار الشروق، القاهرة، 2003، ص 12**

قائمة المصادر والمراجع

الكتب:

1. احمد خالد محي الدين، الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المغرب، 2010.
2. توماس ميلهورن، جرائم الانترنت، مؤسسة الناشر الدولي، فلوريدا، 2007.
3. جمال سيف فارس، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية – دراسة مقارنة بين القوانين الوضعية الأجنبية والقانون الدولي الجنائي، دار النهضة العربية، القاهرة، 2007.
4. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الطبعة الأولى، دار النهضة العربية، مصر، 2002.
5. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، 2002.
6. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الاول، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.
7. حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الناشئة عنها، منشورات الحلبي الحقوقية، بيروت، 2017.
8. سمير عالية، القانون الجزائي للأعمال، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2018.
9. عادل مشموشي، مكافحة الارهاب، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2011.
10. عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، مطبعة الوئام للحاسبات والطباعة والنشر، بابل، العراق، 2009.
11. عباس ناجي حسن، الوسائط المتعددة في الإعلام الالكتروني، دراسة مقارنة، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، 2016.
12. عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2007.
13. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، الطبعة الأولى، الدار الجامعية للطباعة والنشر، بيروت، 2000.
14. فتوح عبد الله الشاذلي، المواجهة التشريعية للجرائم المستحدثة، بحث مقدم لمؤتمر الامن والسلامة الذي عقدته وزارة الداخلية بدولة الامارات العربية المتحدة، الامارات، 2003.
15. فضل سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، مصر، 2016.
16. محمد عبد الكريم حسين الداودي، المسؤولية الجنائية لمرود خدمة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2017.
17. محمد عبد الله سلامة، جرائم الكومبيوتر والانترنت، الطبعة الأولى، منشأة المعارف، الاسكندرية، 2006.

18. محمود رجب فتح الله، الوسيط في الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

19. محمود شريف بسيوني، «الوثائق الدولية المعنية بحقوق الإنسان»، المجلد الثاني، دار الشروق، القاهرة، 2003.

20. ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، الطبعة الثالثة، دار النهضة العربية القاهرة 2010.

21. منصور محمد حسين، المسؤولية الالكترونية، الاسكندرية، دار الجامعة الجديدة، 2003.

22. منير وممدوح محمد الجبهيني، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2004.

المجلات والدوريات:

1. جورج لبكي، المعاهدات الدولية للإنترنت حقائق وتحديات، مقال منشور في مجلة الدفاع الوطني اللبناني، العدد 83، تاريخ 23 كانون الثاني، بيروت، 2013.

2. مازن ليلو راضي وعدي سليمان علي، المواجهة التشريعية للجريمة الالكترونية في اقليم كوردستان العراق، بحث منشور في مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الاول لكلية القانون، العراق، 2009.

3. محمد السيد رشدي، «الإنترنت والجوانب القانونية لنظم المعلومات»، مجلة الفتوى والتشريع، العدد 9، مجلس الوزراء، آيار، 2000.

4. يونس عرب، جرائم الكومبيوتر والانترنت، ورقة عمل مقدمة الي مؤتمر الامن القومي المنظم من قبل المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 2002.

القوانين:

1. قانون العقوبات اللبناني رقم 340 لعام 1943 وتعديلاته
2. قانون العقوبات العراقي رقم 111 لعام 1969 وتعديلاته.
3. قانون منع اساءة استعمال اجهزة الاتصالات في اقليم كوردستان العراق رقم 6 لسنة 2008
4. مشروع قانون الجرائم الإلكترونية العراقي لعام 2010.
5. قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم 78 لسنة 2012.
6. قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم 81 لعام 2018.