M.S.A.R
مجلة دراسات وبحوث إعلامية
Journal of Media Studies and Research
مجلة علمية محكمة تصدر عن كلية الاعلام بالجامعة العراقية
ISSN: 2308 - 0728

Dr. Riad Muhammed Kazem

E-Mail :
riyadhmk1964@gmail.com

Phone Number :

07702755198

Studies and Research Center/Ministry of Culture, Tourism and Antiquities

Keywords:

- **Criminal liability.**
- **Civil responsibility.**
- **Cyber crimes.**
- **electronic platforms.**
- **globalization of crime.**

ARTICLE INFO

Article history:

Received : 1 / 11 /2021
Accepted : 15 / 12 /2021
Available Online : 3 / 1 /2021

RESPONSIBILITY ARISING FROM CYBERCRIMES IN LIGHT OF THE SPREAD OF ELECTRONIC PLATFORMS (COMPARATIVE STUDY)

ABSTRACT

This research sheds light on one of the new media crimes that appeared as a negative impact of the information revolution due to the expansion of the media field to include social media and the Internet in addition to its traditional field called (cybercrime), which emerged with new patterns and new crimes that were not committed by society and the legislator did not expect them, especially with the spread of the pandemic Corona, as the world witnessed a wide demand for using these means and relying on them in an unprecedented way as an educational, knowledge and commercial method and making it an alternative during periods of social distancing, so we discussed this topic in terms of defining cybercrime and the responsibility for it at the internal or international level, reaching the development of roads Ensure that it is controlled through effective legal cods.

Journal of Media Studies and Research (M.S.A.R) - Journal of Media Studies and Research (M.S.A.R) - Journal of Media Studies and Research (M.S.A.R)

© 2021 M.S.A.R, College of Media | The Iraqia University

المسؤولية الناشئة عن الجرائم السيبرانية في ظل انتشار المنصات الإلكترونية (دراسة وصفية)

م.د. رياض محمد كاظم

الإيميل :

riyadhmk1964@gmail.com

رقم الهاتف :

٠٧٧٠٢٧٥٥١٩٨

عنوان عمل الباحث:

مركز الدراسات والبحوث/ وزارة الثقافة والسياحة والآثار

المستخلص

يسلط هذا البحث الضوء على جريمة من جرائم الإعلام الجديد، ظهرت كأثر سلبي للثورة المعلوماتية لاتساع مجال الإعلام ليشمل وسائل التواصل الاجتماعي والانترنت اضافة إلى مجاله التقليدي، وتسمَّى بـ(الجريمة السيبرانية) التي برزت بأنماط جديدة وجرائم مستحدثة لم يعهدها المجتمع، ولم يتوقعها المشرع خصوصاً مع انتشار جائحة كورونا حيث شهد العالم اقبالاً واسعاً على استخدام هذه الوسائل والاعتماد عليها بشكل لم يسبق له مثيل كوسيلة تعليمية ومعرفية وتجارية وجعلها البديل أثناء فترات التباعد الاجتماعي؛ لذلك بحثنا هذا الموضوع من ناحية التعريف بالجريمة السيبرانية والمسؤولية التي تقوم عنها على المستوى الداخلي أو الدولي وصولاً إلى وضع الطرق الكفيلة للسيطرة عليها من خلال النصوص القانونية الفاعلة.

© 2021 مسار، الجامعة العراقية | كلية الاعلام ،

الكلمات المفتاحية:

- المسؤولية الجزائية.
- المسؤولية المدنية.
- الجرائم السيبرانية.
- المنصات الإلكترونية.
- عولمة الجريمة.

معلومات البحث

تاريخ البحث :

الاستلام : ١ / ١١ / ٢٠٢١

القبول : ١٥ /١٢/ ٢٠٢١

التوفر على الانترنت : ٣/ ١/ ٢٠٢٢

Journal of Media Studies and Research (M.S.A.R) - Journal of Media Studies and Research (M.S.A.R) - Journal of Media Studies and Research (M.S.A.R)

المقدمة : لقد كان من نتائج التطور التكنولوجي في الوقت الراهن و انتشار المنصات والاعتماد عليها بسبب جائحة كورونا كبديل عن التقارب الاجتماعي أن أصبحت تلك البرامج والمنصات والحاسب الآلي عموماً وسيلة لارتكاب بعض الجرائم المستحدثة، فأصبحت التكنلوجيا أداة لارتكاب الأفعال غير المشروعة أو محلاً لها، وان انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات التي تنشر بسرعة هائلة وغزوها مختلف مجلات الحياة أصبح يزيد من فرص انتشار هذا النوع من الجرائم المستحدثة.

وبالتالي فعندما يتم الاعتداء على الأموال المعلوماتية، أي مجموعة الأدوات المكونة للحاسوب الآلي والبيانات والبرامج، فإنَّ هذا الاعتداء يؤدي إلى نشوء مشاكل قانونية جديدة ترتبط بطبيعة الحال بتلك الآليات الجديدة، الأمر الذي يضعنا أمام مجموعة من الجرائم المستحدثة ذات التكنيك المتميز الذي يتسم بحداثة ممارساته.

فقد أفرزت الاختلافات الجوهرية بين التفسير المعمول به للقانون في ظل الاوضاع التقليدية والتفسير الذي نحتاجه لمعالجة الحالات التي فرضتها طبيعة التطور التقني أهم تلك الاختلافات فيما يتعلق بطبيعة هذه الظاهرة المستحدثة، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي، والبعض الآخر يسمّيها بالجريمة المعلوماتية أو السيبرانية أو جريمة الفضاء الالكتروني إلا أنَّ التسمية الأكثر انتشاراً في العالم لهذه الجريمة هي تسمية (الجريمة السيبرانية)، اما الاختلاف الآخر فيتعلق بصعوبة وضع تعريف محدد لهذه الظاهرة المستحدثة؛ وبالتالي تحديد ما يشمله القانون منها خصوصاً ان القانون الجنائي محكوم بمبدأ أن لا جريمة ولا عقوبة بغير نص، فالجريمة المعلوماتية أو الحادث السيبراني وإن كانت جريمة لكن مادام النص لا ينطبق عليها فلا يمكن تجريم فعل مرتكبها ولا معاقبته، كلّ هذا حدا بالباحثين إلى اختيار هذا الموضوع الذي أصبح موضوعاً مهماً على جميع الأصعدة وطنياً وعالمياً، فهنالك تهديدات سيبرانية رئيسة في جميع أنحاء العالم وهي بذات الوقت تضر بالمصلحة الوطنية أهمها الجريمة الالكترونية، والصراع السيبراني والإرهاب الإلكتروني والتجسس السيبراني واستغلال الأطفال والقصر وإساءة معاملتهم عبر الانترنت، ويلاحظ أن المتتبع لظاهرة القرصنة الإلكترونية يدرك التناقض الذي يميز هذه الظاهرة، فالجرائم السيبرانية ترتفع في الدول التي تصنفها التقارير في أقل درجات التطور التقني، وهذا ما تشير إليه التقارير والمعطيات المنشورة من قبل الهيئات والجهات المختصة.

وعليه فإننا من خلال هذا البحث سنقسم الدراسة فيها إلى مبحثين نتناول في المبحث الأول ماهية الحادث السيبراني من حيث تعريفه وصوره، بينما نسلط الضوء في المبحث الثاني منه على المسؤولية المدنية والجزائية والدولية الناشئة عن هذا الفعل على وفق القواعد القانونية الموجودة وبيان المأمول منها.

المبحث الأول : منهجية البحث

مشكلة الدراسة

بحكم التطور العلمي والتكنولوجي، أضحت السيبرانية جريمة من جرائم الإعلام الجديد اليوم ومشكلة من المشاكل الكبرى التي تواجه الأمم والشعوب والدول على حدّ سواء وعملية مكافحتها أو مواجهتها يقتضي وجود وعي ثقافي مجتمعي أولاً فضلاً عن وجود تشريعات وقوانين من شأنها الحدّ من هذه الجريمة ومعاقبة ومتابعة مرتكبيها إذا اقتض الأمر؛ وعليه فإنَّ مشكلة الدراسة تنحصر في تساؤل رئيسي (ما الجريمة السيبرانية وما المسؤولية المدنية والجزائية والدولية الناتجة عن فعلها وما التشريعات والقوانين التي تحدّ منها؟).

أهداف الدراسة : وتتمثل في:

١- التعريف بالجريمة السيبرانية كأثر سلبي من سلبيات الإعلام الجديد.

٢- التركيز على خصائصها من حيث نشاطها ونطاقها والمسؤولية المدنية والجزائية الناتجة عن فعلها.

٣- تحديد القوانين والتشريعات التي تسهم في الحدّ منها.

أهمية الدراسة

تأتي أهمية هذه الدراسة من أهمية الموضوع نفسه؛ لأنها، أي (الجريمة السيبرانية) أصبحت تشكل خطراً يهدد الأفراد والمؤسسات و المجتمعات والدول على حدّ سواء فضلاً عن الجدل الذي أثارته والآثار السلبية التي تركتها الأمر الذي استدعى وجود الحاجة للاهتمام بها ووضع القوانين والتشريعات التي تنظم عملها وتحدّ منها.

منهج الدراسة

اعتمد الباحث في دراسته هذه منهج التأصيل والتحليل والمقارنة من خلال الرجوع إلى أصول الجريمة السيبرانية ومن ثم تحليل وجهات النظر والقوانين والتشريعات الناتجة عنها فضلاً عن استعانة الباحث بالمنهج المقارن في الإشارة إلى قوانين وتشريعات دول عدَّة عانت من تنامي هذه الجريمة.

المبحث الثاني: ماهية الجرائم السيبرانية

يناقش هذا البحث واحدة من أهم القضايا التي تقلق الحقوقيين والإعلاميين في الوقت الحاضر تلك هي جريمة الإعلام الجديد (الجريمة السيبرانية) أو (الجريمة المعلوماتية)؛ لأنها

جريمة لم يعالج المشرع خصوصيتها، وهي في الوقت نفسه تمثل تعدياً على حقّ يملكه الإعلاميون، وهو النشر ونقل المعلومة، إذ ان اتساع استخدام الحاسب الآلي وما تبعه من استخدام الانترنت (الشبكة الدولية للمعلومات)، الأمر الذي مكن أفراداً لا يملكون المِلكة والتدريب الإعلامي الكافي من أن يلعبوا دور الإعلامي مستغلين هذا الدور للوصول إلى أهداف إجرامية، الأمر الذي انتج أنماطاً جديدةً للسلوك الإجرامي لم يكن بإمكان مشرعي معظم البلدان توقعه مسبقا ممَّا حدا بالدول إلى اتخاذ مواقف سريعة وجدية في العمل على وضع حل لهذه المشكلة التي طرأت على النظام القانوني وبدأت تقوض أمنه، وللوقوف على أهمية هذه المشكلة وأبعادها القانونية والاجتماعية والاقتصادية لابد من تسليط الضوء أولاً على ماهيتها من خلال هذ المبحث، إذ اننا في هذا المبحث سنحاول أن نضع تعريفاً للجرائم السيبرانية، ومن ثم نبين خصائص هذا النوع من الجرائم.

- **تعريف بالجرائم السيبرانية**

إنَّ التقدم العلمي والتقني في استخدام أجهزة وشبكات الحاسب الآلي الذي نجم عنه ابتعاد المجرمين عن الأساليب التقليدية في ارتكاب الجرائم ممَّا أدى إلى ظهور نماذج تنطوي على أساليب إجرامية اطلق عليها بالجرائم السيبرانية؛ وعليه فإننا في هذا الفرع سنتعرف على المقصود بالجريمة السيبرانية.

فقد تعددت الآراء بشأن تعريف الجريمة الإلكترونية، كلّ رأي تبنى مفهوماً بالنظر إلى الزاوية التي رآها، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استناداً لمعايير أخرى حسب القائلين بها[١]، وهذا ما حدا بالأمم المتحدة (في مدونتها بشأن الجريمة المعلوماتية) إلى عدم التوصل لتعريف متفق عليه دولياً.

فقد جاءت لفظة السيبرانية من (سيبر) (Cyber space) وتعني النطاق المصطنع أو فضاء الانترنت كما تعني ترابط حواسيب مع أنظمة تقنية، والفضاء السيبراني (هو المجال المجازي لأنظمة الحاسوب والشبكات الالكترونية حيث تخزن المعلومات الكترونياً وتتم الاتصالات المباشرة

(١) عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دار ، مدبولي، القاهرة، ٢٠٠٩ ، ص ١.

على الشبكة)[١]، ويعدّ المجال السيبراني هو المجال الرابع الذي ينبغي السيطرة عليه من الناحية القانونية بعد المجالات الثلاثة التقليدية وهي الأرض والبحر والجو، إذ يعتمد الوجود الاقتصادي الرقمي للبلد على الأداء الفعال للبنية التحتية في الفضاء السيبراني؛ لأن البلد ليس معزولاً بل مترابط مع بلدان وجهات أخرى وجهات فاعلة في الفضاء السيبراني؛ لذلك كان لزاماً على البلد أن يحمي فضائه السيبراني من المخاطر بمختلف الوسائل المتاحة.

اما الجريمة فتعرف على أنها سلوك غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرًا احترازيًا .[٢]

وبذلك تعرف الجرائم السيبرانية على انها: احتمال وجود تهديد وهشاشة في داخل المجال الالكتروني للبلد بما يضر بأمن وسلامة نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية كما يمكن ان تُستغل الثغرات الحالية الموجودة وبشكل يؤثر على سلامة وأمن نظام المعلومات أو شبكات المعلومات أو البنى التحتية للشبكات [٣]، ويلاحظ على هذا التعريف أنه يسلط الضوء على النتيجة منها وهي الاضرار بالجانب الأمني.

بينما ذهب اتجاه آخر إلى تعريفها على أساس الفعل الجرمي أو موضوع الجريمة، فقد عرفها رأي على أنها: قيام مرتكب الفعل الضار بنشاط ذي نتائج غير مقبولة قانوناً، وفي الاتجاه نفسه عُرفت على أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[٤]، وعرفها آخر على أنها: كلّ سلوك غير مشروع أو غير مسموح به يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[٥]، كما عرفت على أنها أي نمط من أنماط الجرائم المدونة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات [٦]، وهي

(١) فلاح حسن منور التميمي، الجريمة السيبرانية، مقالة منشورة على موقع مجلس القضاء الاعلى ، رفعت بتاريخ ١٨-٩-٢٠٢٠.

(٢) حسني، د. محمود نجيب ،" شرح قانون العقوبات ، القسم العام "، ط ٦ ، دار النهضة العربية ، القاهرة، ص ٤٠ . ١٩٨٩

(٣) مستشارية الأمن الوطني أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الأمن السيبراني العراقي، دراسة منشورة .

(٤) يونس عرب، "موسوعة القانون وتقنية المعلومات، دليل امن المعلومات والخصوصية، جرائم الكومبيوتر" ، ج ١ . ، منشورات اتحاد المصارف العربية ، ط ١ ، ص ٢١٣.

(٥) د. هدى حامد قشقوش ،" جرائم الحاسب الالكتروني في التشريع المقارن "، ط ١ ، دار النهضة العربية ، القاهرة ، ١٩٩٢ . ، ص ٢.

(٦) د. هشام محمد فريد رستم، "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط، ص ٣١ و ما بعدها ١٩٩٤.

الجريمة الناتجة عن ادخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم اكثر تعقيدًا من الناحية التقنية مثل تعديل الكومبيوتر. [١]

كل هذه التعاريف السابقة للجريمة السيبرانية ركزت على موضوع الجريمة الا انها لم تكن كافية لوضع معنى متكامل لها لذلك جاء اتجاه اخر انطلق في تعريفه لها من خلال الوسيلة التي تتم من خلالها لاعطائها صفتها المميزة عن باقي الجرائم ، بما ان الفعل الجرمي يتم باستخدام جهاز الحاسب الآلي كوسيلة، فيصنف الفقيه (تدمان) جرائم السيبرانية على أساس استخدام الحاسب الآلي من عدمه في اسباغ صفة السيبرانية عليها، ويستند في رأيه إلى تقييم مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA فيقول بأنها: الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً [٢]، وبالرغم من أن أصحاب هذا الاتجاه وضعوا تعريفاً للجريمة السيبرانية يجعل بالإمكان تمييزها بسهولة عن الجرائم الأخرى إلا أنه يؤخذ على هذا الاتجاه أنه لا يفرق بين الاستخدام المشروع وغير المشروع للحاسب الآلي والانترنت وبالتالي يمكن أن يكون مربكاً من الناحية التطبيقية.

الأمر الذي دعا إلى ظهور اتجاه يعرف الجريمة السيبرانية على أساس سمات شخصية لدى مرتكب الفعل، وهي صفة درايةٍ ومعرفه الفنية كما في التعريف الذي وضعته وزارة العدل الأمريكية في دراسة أعدها (معهد ستانفورد للأبحاث) واعتمدتها هذه الوزارة في دليلها لعام ١٩٧٩ الذي يعرفها على أنها، أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها[٣]، ويذهب تعريف آخر إلى أنها: كلّ فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[٤]، وكما في الاتجاهات السابقة لم يوفق أصحاب هذا الاتجاه في أن يسلموا من الانتقاد، فيؤخذ على هذا الاتجاه أنه يركز على شخصية الجاني ولكن في الواقع الكثير من المجرمين السيبرانيين غير معروفين ويخفون هوياتهم الحقيقية ولا يمكن الاعتماد على سمات شخصياتهم لتبين الجريمة السيبرانية لمجهوليتهم عموماً.

---

(١) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوسيع، عمان، الأردن، الطبعة الأولى، ٢٠٠٤ ،ص، ٨٠.

(2) om Forester , Essential proplems to hig _Techsaciety first MIT edition ،Cambridge , Massachusetts , p104 , 1989.

(3) Last source, p103.

(4) MERWE (vander) computer crimes and other crimes against information technology in sauth africa, R.I.D, 1993,p554.

وبعد ذلك جاء تعريف (منظمة التعاون الاقتصادي والتنمية) للجريمة السيبرانية المادية أو المعنوية على أنها نتيجة التدخل بطريقة مباشرة أو غير مباشرة بالتقنية المعلوماتية[١]، ويبدو أن هذا التعريف على الرغم من ايجازه الشمولية أكثر من التعاريف الأخرى، إذ يصنف الجريمة السيبرانية على أساس كلّ الاحتمالات المتعلقة بالجريمة المعلوماتية من حيث الطابع التقني لهذه الجرائم وامكانية التعامل مع المستجدات العلمية التقنية، ومثله يوجد تعريف آخر أورده الفقيه الانكليزي (توماس جي) الذي يذكر أنَّ الجريمة السيبرانية ما هي إلا ضرب من النشاط المنطوي على استخدام الحاسب الآلي أو أحد الأجهزة الشبيهة بنشاط موجه ضدّ الضحية ينطوي على اغراء أو احتيال أو اعتداء بقصد تحقيق ربح عن طريق أحد البرامج التقنية، أو أنها تلك الاعتداءات التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح [٢]، وان هذه الجرائم يمكن أن ترد في مواضع عدَّة نذكر منها ما تعاني من مخاطره الدول اليوم من عمليات تخريبية تصيب بعض المواقع الحكومية، والممارسات الاحتيالية، والابتزاز الالكتروني واساءة استخدام وسائل الإعلام ومواقع التواصل الاجتماعية لشن حملات خبيثة ضدّ الدولة، والتشجيع على الصراع والعنف المستمر من خلال الإنترنت والتجسس الإلكتروني المنسق و التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى والقرصنة الالكترونية والإرهاب الالكتروني وسرقة الأصول الفكرية وغسيل الأموال وتبييضها إضافة إلى العديد من الجرائم المالية عبر الانترنت. [٣]

اما تعريف مسودة "الجرائم المعلوماتية" العراقي الذي لا يزال على طاولة مجلس النواب العراقي على أنه "نشاط إجرامي إيجابي أو سلبي تستخدم فيه تقنية متطورة تكنولوجياً بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ الفعل الإجرامي العمدي في البيئة المعلوماتية".

ويهدف القانون وفقاً لما جاء في نص الفقرة رقم "٢" منه إلى "توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات ومعاقبة مرتكبي الأفعال التي تشكل اعتداء على حقوق مستخدميها من الأشخاص الطبيعية أو المعنوية ومنع إساءة استخدامه في ارتكاب جرائم

(١) د. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣، ص ٣٢. د . محمد حسام محمود ،" الحماية القانونية لجرائم الحاسب الآلي" ، دار الثقافة للطباعة و النشر ، القاهرة ، ١٩٨٧ ، ص ٣.

(٢) يونس عرب، جرائم الكومبيوتر والانترنت، ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة الى مؤتمر الامن العربي ٢٠٠٢ ، تنظيم المركز العربي. ١٠-١٢/٢/٢٠٠٢ ، للدراسات والبحوث الجنائية ، ابو ظبي ، ص ١١.

(٣) استراتيجية الأمن السيبراني العراقي، المصدر السابق. يونس عرب، جرائم الكومبيوتر والانترنت، المصدر السابق، ص ١٣.

الحاسوب"، وهو اتجاه محمود من المشرع في جعله الجريمة السيبرانية تشمل كلّ نشاط ايجابي أو سلبي في البيئة المعلوماتية السيبرانية إلا أنه يؤخذ عليه مأخذاً مهماً وهو توسيع نطاق الجريمة وامكان استغلال ذلك من قبل الجهات التنفيذية، إذ انه من الممكن أن تصبح هذه المادة منطلقاً للقمع؛ لأنَّ اطلاق لفظ نشاط بهذا الشكل سيجعل الفرد معرضاً للاتهام بعد أي استخدام للحاسب أو الانترنت؛ لأنه لا يعرف مقدماً بدقة ما هو السلوك المحظور والخاضع للعقوبة لكي يتجنبه، هذا من جانب.

ومن جانب آخر فإنَّ هذا الاطلاق من جانب المشرع ينتهك المادتين ٩ و١٤ من العهد الدولي الخاص بالحقوق المدنية والسياسية والمادة ١٤ من الميثاق الدولي العربي لحقوق الإنسان، وهذه المواد الثلاث المذكورة تحمي الحقّ في الحرية والحقّ في التقاضي على وفق الأسس السليمة، وكذلك يخالف هذا التعريف المادة ١٩ من العهد الدولي الذي ينص في الفقرة ١ منه على: (حقّ الفرد في اعتناق أي راي يختار دون مضايقة)، فيما تنص الفقرة ٢ من المادة نفسها على: (حقّ الإنسان في حرية التعبير، ويشمل هذا الحقّ حريته في التماس مختلف ضروب المعلومات...)، كما نجد أنَّ هذا التعريف يخالف نص المادة ٣٨ من الدستور العراقي في جزء وثيق الصلة التي تنص على أن: (تكفل الدولة وبما لا يخل بالنظام العام والآداب: أولاً – حرية التعبير عن الرأي بكلّ الوسائل. ثانياً – حرية الصحافة والطباعة والإعلان والإعلام والنشر)، وتنص المادة ٤٦ من الدستور العراقي على: (لا يكون تقييد ممارسة أي من الحقوق أو الحريات الواردة في هذا الدستور أو تحديدها إلا بقانون أو بناء عليه، على ألا يمس هذا التحديد والتقييد جوهر الحقّ أو الحرية).

وممَّا تقدم نستنتج أنَّ الجريمة السيبرانية جريمة تؤثر بالدرجة الأولى على أمن وسلامة البلد بالنظر إلى أثرها، وهي جريمة يُساء فيها استخدام التقنية بالنظر موضوعها، وتقع باستخدام الحاسب الآلي أو الاجهزة الذكية والانترنت بالنظر إلى وسيلة استخدامها، كما تصدر من فاعل يمكن تمييزه عن غيره فهو على دراية فنية إلى حدّ ما بالنظر إلى السمات الشخصية لمرتكبها، وهي جريمة تتعلق بنظم المعلومات بالنظر إلى الحق الذي تنتهكه، ومن هذه الآراء نستطيع أن نستنتج تعريفاً جامعاً مانعاً للجريمة السيبرانية على أنَّها: (أنَّها كلّ فعل أو امتناع عن فعل يشكل اعتداءً على حقّ يحميه القانون ترتكب بواسطة التقنية الحديثة ويوجه الفعل الجرمي للوصول إلى معلومات

الكترونية محمية بحقّ الخصوصية أو تعطيلها يصاحبه ربح للجاني أو خسارة للمجنى عليه أو كلاهما معاً).

إذ اننا في تعريفنا هذا للجريمة السيبرانية أكدنا الجانب القانوني والمبرر الشرعي الذي يمكن معه تجريم الفعل بسبب نشاطه الايجابي أو السلبي الذي يعتدي فيه على حقّ المعلومة[١] المحمي بالقانون، ويكون الهدف من هذا النشاط الحصول على منفعة أياً كان نوع هذه المنفعة، وكما يمكن أن يؤسس التعويض عن هذه الجريمة على أساس الخطأ والضرر سواء كان الضرر مادياً أو معنوياً في الجرائم الماسة بالأشخاص أو سمعتهم، فإنَّه يمكن أن تلحق به مسؤولية مدنية نتيجتها التعويض تؤسس على أساس الاثراء بلا سبب، وسنتطرق إلى كلّ هذا في المبحث الثاني من هذا البحث عند بحث المسؤولية المترتبة عن هذه الجريمة أو الحادثة بالنسبة للدول التي لم تجرم فيها هذه الأفعال.

- **خصائص الجرائم السيبرانية**

من المعروف أن المشرع وهو بصدد تجريمه لسلوك معين يضع في حساباته مصالح المجتمع الذي يحاول حمايته من خلال وضع عقوبة مناسبة، والجريمة السيبرانية أحد الصور التي يمكن أن يأتيها الجاني ويعتدي بها على مصالح قدر المشرع أنها مصالح جديرة بالحماية، ويلاحظ وجود خصيصة محددة في الجرائم السيبرانية وهي أن المشرع في العادة يكون واجبه الأول أبعاد كلّ ما يمكن أن يكون وسيلة تسهل ارتكاب الجريمة، مثلاً بعد أن تم تشخيص كون الأسلحة النارية وسيلة يمكن استخدامها للقتل أو التهديد منع المشرع حيازتها إلا لفئات محددة وجعل كلّ جريمة قتل أو سرقة أو تهديد تتم مع استخدام السلاح جريمة بعقوبة مشددة، وكذلك الحال بالنسبة لاستخدام المسكر عمداً وارتكاب الجريمة، أو التسور أو استعمال مفاتيح مصطنعة عند سرقة دار أو مخزن وغيرها من الحالات التي وضعت فيها قيود إدارية وقانونية من لدن المشرع أو الجهات التنفيذية على الوسائل التي تسهل ارتكاب الجريمة أو التي تستخدم فيها [٢]، إلا أنَّ هذا الأمر لا

(١) (وتعرف أنَّها رسالة معبر عنها في شكل قابلة للتنقل أو الابلاغ برموز أو مجموعة من رموز تنطوي على إمكانية الافضاء إلى معنى).

(٢) انظر في ذلك قانون العقوبات العراقي ومنها المادة ٤٤١ منه التي تنص على: (يعاقب بالسجن المؤبد أو المؤقت على السرقة التي تقع على شخص في الطريق العام خارج المدن والقصبات أو قطارات السكك الحديدية أو غيرها من وسائل النقل البرية أو المائية حال وجودها بعيداً عن العمران؛ وذلك في إحدى الحالات التالية: ١ – إذا حصلت السرقة من شخصين فأكثر وكان أحدهم حامل سلاحاً ظاهراً أو مخبأ. ٢ – إذا حصلت السرقة من شخصين فأكثر بطريق الاكراه. ٣ – إذا حصلت السرقة من شخص يحمل سلاحاً ظاهراً أو مخبأ بين غروب الشمس ....).

يمكن القول بأنه ما تم فعلاً مع الجريمة السيبرانية، فهذا النوع من الجرائم يرتكب باستخدام الحاسب الآلي والتقنية الحديثة وهذا أمر لا تستطيع الجهات التشريعية أو التنفيذية تقييده إلا في أحوال استثنائية ويعود ذلك إلى عدَّة أسباب تمثل هذه الأسباب خصائص تختص بها الجريمة السيبرانية وهي:

أولاً- من حيث النشاط (أنها جريمة متعددة النشاط):

إذ ان النشاط المستخدم في ارتكاب الجريمة السيبرانية هو نشاط يشتبه مع غيره من النشاطات المباحة قانوناً فمجرد استخدام الحاسب الآلي أو الانترنت لا يعدّ جريمة بل لابد من حصول اختراق أو احتيال أو نسخ لمعلومات محمية قانوناً وغيرها أي لابد أن تحصل النتيجة الضارة من وراء النشاط[١]، فالتكنلوجيا أخذت حيزاً واسعاً من حياتنا اليوم خصوصاً مع انتشار جائحة كورونا، إذ شهد العالم اقبالاً واسعاً على استخدام الحاسب الآلي أو الهاتف الذكي مع استخدام الانترنت بشكل لم يسبق له مثيل كوسيلة للتعليم والتبادل التجاري والثقافي والمعرفي اضافة إلى ارتفاع استخدامه كوسيلة للتواصل بعد أن حل التباعد الاجتماعي بدل التواصل وتزامن بدايات هذا الاستخدام مع فترات الأعياد والمناسبات التي اعتاد الأفراد فيها اللقاء؛ وبالتالي فإنَّ المشرع لا يستطيع أن يجرم كلّ فعل يبدأ بنشاط مماثل بل لابد أن يتحقق جزء من النتيجة الجرمية للقول بالشروع بالجريمة إن لم نقل بتمامها.

ثانياً- من حيث نطاق الجريمة (أنَّها جريمة من جرائم الإعلام الحديث)

إنَّ الجريمة السيبرانية لا يمكن أن تقع في غير نطاق الحاسب الآلي والانترنت، أي أن جزء منها جريمة تقع في نطاق الإعلام، فيمكن أن تستخدم وسائل التواصل الالكترونية كوسيلة لمباشرة النشاط الجرمي المكون لهذه الجريمة، وقد ظهر الانترنت كشبكة إعلام اجتماعي منذ العام ١٩٦٠ م ليصبح نقل الخبر أسرع وأقل تكلفة ممَّا كان عليه في السابق، وفيما بعد صارت وسائل التواصل ضحية من ضحايا هذه الجريمة وقد أصبحت وسائل التواصل جزءاً لا يتجزأ من الإعلام، نظراً لاعتماده مصدراً للمعلومة من قبل شريحة لا يستهان بها من الأشخاص وهي في تزايد مستمر نظراً لما يطرأ من ظروف، إذ انَّ ظهور جائحة كورونا كان من الأسباب التي رفعت من

(١) د. محمد حماد مرهج ،" التكنولوجيا الحديثة و القانون الجنائي"، دار الثقافة ، عمان ،٢٠٠٤/ ص ١٥٦.

تلك النسبة؛ لذلك فإنَّ من الخصائص المميزة للجريمة السيبرانية أنَّها من جرائم الإعلام الجديد التي ظهرت وتطورت وتزايدت بشكل طردي بتزايد عدد المستخدمين .[١]

ثالثاً– من حيث محل الحماية الجنائية (انَّها جريمة مزدوجة المحل):

بما ان وسيلة الاعتداء المباشر هي الحاسب الآلي، والحاسب الآلي ينقسم بدوره إلى كيان مادي وكيان معنوي؛ فالاعتداء على الكيان المادي أو التقني للحاسب الآلي هو اعتداء مباشر ينطبق عليه من القواعد القانونية الجنائية التي تحكم الجرائم التقليدية وتخضع للقواعد العامة في الاثبات.[٢]

اما الشق الثاني من مكونات الحاسب الآلي وهو الكيان المعنوي المتمثل بالمعلومات والبرامج والشيفرات والحسابات وما تحمله هذه من معنوية أو مادية للمستخدم صاحب الحقّ بها[٣]، وهنا تقف نصوص قانون العقوبات موقف القصور مع الأسف؛ لأنَّ هذا الكيان لا يمكن وصفه أنَّه مال على وفق أغلب القواعد المعمول بها لعدم توفر شروط معينة بها – وليست محل بحثنا هنا– فبالرغم من أنَّ البعض من الفقهاء ينظر إلى الكيان المعنوي على أنها عبارة عن مال كما في الكيان المادي إلا أنَّه يختلف عن غيره من الأموال بأنَّه غير قابل للنفاد بكثرة الاستعمال، ثمَّ إنَّه مال تتلاشى قيمته بظهور الجديد من المعارف والتقنيات، وان استعمال هذا المال يكون على متسع فمن الممكن أن يستعمله العديد في آن واحد، اخذين بعين الاعتبار أنَّ نفقات نقل هذا المال تكاد تكون ضئيلة جداً. [٤]

رابعاً– من حيث اكتشافها واثباتها:

يصعب اكتشاف الجريمة السيبرانية واثباتها وكشف شخصية الجاني عند الاكتشاف ويعود سبب ذلك إلى أنَّ الدليل الجنائي لإثبات الجريمة المعلوماتية يختلف تماماً عن الدليل الجنائي في الجريمة التقليدية، إذ انَّ أجهزة العدالة الجنائية خصوصاً في بلداننا غير مؤهلة لهذا الدور وهذه الثغرة يعتمد عليها المجرم السيبراني بشكل كبير فهو مجرم ذكي نسبياً يعكس أعلى درجات المهارة في فنون التعامل مع الحاسب الآلي، ويكفى للتدليل على خطورة هذا الأمر أنَّ بعضهم يتعامل مع

(١) حسنين شفيق، الإعلام الجديد والجرائم الالكترونية، دار فكر وفن للطباعة والنشر والتوزيع، ٢٠١٥، ص٣٢.
(٢) الصغير د. جميل عبد الباقي ،" القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي "، ط ١ ، دار النهضة العربية ، القاهرة ، ١٩٩٢، ص٨.
(٣) المصدر نفسه ، ص ١٢.
(٤) د. نواف كنعان، "النماذج المعاصرة لحقّ المؤلف ووسائل حمايته"، ط ٣، الجامعة الأردنية، كلية الحقوق ، ٢٠٠٠ ، ص ٧٣.

هذا النوع من الجرائم بوصفه يمارس هواية لا حرفة، فهو شخص اما انه يعمل لدى مؤسسة حكومية أو في مصرف أو في مكتب طباعة ما أو غيرها ممَّا يصعب اكتشافه لاختفائه خلف لوحة المفاتيح عند ارتكابه لجريمته عن بعد، كما ان من الجدير بالذكر أن الدراسات والأبحاث العلمية تؤكد أيضاً على أنَّ فئات الجناة في هذا المجال تشمل فئات متباينة تشمل: (مستخدمو الحاسب بالمنازل، الموظفون الساخطون على منظماتهم، المتسللون ومنهم الهواة أو العابثون بقصد التسلية، و العاملون في الجريمة المنظمة). [١]

اما الصعوبات التي تعترض تحصيل الدليل الجنائي في هذه الجرائم كثيرة ومتنوعة منها ما يتعلق بالدليل الجنائي ذاته، ومنها ما يتعلق بموضوع الجريمة، والآخر يتعلق بجهات الضبط القضائي أو التحقيق الجنائي في هذه الجرائم، على أنَّه يمكن القول أنَّ استحصال الدليل الجنائي في هذه الجرائم محكوم بمبدأين مهمين هما:

١- وجود نص قانوني يقرر الاجراء الواجب اتباعه من قبل سلطة الضبط القضائي مع مراعاة طبيعة الجريمة.

٢- الحاجة إلى توفر المعرفة الفنية والتقنية لدى رجل الضبط القضائي أو المحقق الجنائي فلابد من أن يكون مؤهلا فنياً إضافة إلى مؤهلاته الحقوقية [٢]، وهذا أمر صعب نسبياً، إذ يحتاج إلى ملاكات تدريبية ووقت، وهو الأمر الذي يعزف المجرم السيبراني على وتره، فهو يسبق المحقق خطوة دائماً بسبب السياقات الإدارية.

خامساً- من حيث استخدام العنف (أنها جريمة سريعة وهادئة):

فهي جريمة يندر فيها استخدام العنف، الأمر الذي يجعل مرتكبها يباشر النشاط الجنائي وينتهي منه دون أثر ظاهر ولا يتجاوز ركنها مجرد لمسات بسيطة لمفاتيح التشغيل لجهاز الحاسب الآلي أو ملحقاته .[٣]

---

(١) د . محمد حسام محمود، "الحماية القانونية لجرائم الحاسب الآلي"، دار الثقافة للطباعة والنشر، القاهرة، ١٩٨٧ ، ص٣.

(٢) د. محمد حماد مرهج ، المصدر السابق، ص ١٥٧.

(3) - FRAYSSINET (J) ; Laprotectiondes donnes personnelles face aux nouvelles technologies de I in formation et de la Communi Cation dans le monde; Constantes es et nouveautes , une recherche persente auperemiere de I informatique legal et Juridique au Koweit Le , p 10, 15_17 , Janv , 1999

وانَّ عدد الحالات التي تم اكتشافها عن هذه الجريمة قليل جداً قياساً بالجرائم غير المكتشفة، ويعود السبب الأكبر في عدم الكشف عن هذه الجرائم إلى عدم وجود آثار مادية ملموسة؛ لأنَّها جريمة ترتكب الخفاء ودون أي أثر يشير إلى مرتكبها، خلافاً للجرائم التقليدية التي يترك فيها الجاني آثاراً كالجثة أو البصمات أو الشعر أو الدماء وغيرها، كما أنَّ سرعتها وارتكابها في الخفاء يجعلها في أغلب صورها صعبة الاكتشاف من قبل المجنى عليه فلا يشعر بها ولا يعلم بوقوعها إلا بعد أن يقوم الجاني بسلوك معين يبين من خلاله للمجنى عليه أنَّه ارتكب جريمته؛ وذلك بحكم توافر المعرفة والخبرة الفنية في مجال الحاسب الآلي غالباً لدى مرتكبها التي يفتقر لها أغلب المجنى عليهم المتضررين منها كما أن الإبلاغ عنها قليل ويكاد يكون منعدماً في بعض المجتمعات .[١]

سادساً – من حيث انتشارها (أنها جريمة عالمية):

إنَّ عولمة هذا النمط من الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مرتكبيها، فهذه الجرائم بحقّ صورة من صور العولمة، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة، ومن حيث الزمان تختلف المواقيت بين الدول، فما القانون الواجب التطبيق على هذه الجرائم، وحتى ان قواعد الاسناد في القانون الدولي الخاص تقف عاجزة أمام معالجة هذا التنازع القانوني.[٢]

وترتكب الجريمة السيبرانية بعدَّة صور – كما ذكرنا مسبقاً– فالجرائم السيبرانية ليست من نوع واحد بل تتعدد وتشترك جميعها أنها ذات نشاط ينطوي على استخدام التقنية الحديثة من خلال الحاسب الآلي فقط أو من خلال استخدام الحاسب الآلي مع الانترنت في التعدي على حقوق حماها القانون وهي أجدر بالحماية، وان تحقق هذه الجريمة بأي صور من صورها توجب قيام المسؤولية القانونية عنها، وتختلف المسؤولية القانونية التي يتحملها الجاني حسب الجريمة التي يرتكبها؛ لذلك فإننا سنناقش كلّ صورة من تلك الصور حسب المسؤولية التي تقوم بسببها، وذلك في المطلب الثاني من هذا البحث.

---

(١) د. محمد السيد رشدي،" الانترنت والجوانب القانونية لنظم المعلومات"، مجلة الفتوى والتشريع ، العدد ٩، مايو ٢٠٠٠ . مجلس الوزراء ، ص ١٠٧ .

(٢) د. احمد عبد الكريم سلامة،" الانترنت والقانون الدولي الخاص، فراق أم تلاق"، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت تنظمه كلية الشريعة والقانون بالتعاون مع مركز الامارات للدراسات والبحوث مايو - الاستراتيجية، مركز تقنية المعلومات دولة الامارات العربية المتحدة، ص ٨ و ما بعدها للفترة من ١-٣ ٢٠٠٠.

- **المسؤولية الناشئة عن الجريمة السيبرانية**

بعد أن تعرفنا على تعريف الجرائم السيبرانية والخصائص التي تميزها عن غيرها من الجرائم سنتطرق إلى المسؤولية الناشئة عنها، حيث تتنوع الجرائم المعلوماتية، فهناك جرائم اعتداء على أشخاص وهناك جرائم تقع على المال وأخرى ضدّ الحكومة، والمسؤولية الناشئة عنها تختلف تبعاً للحقّ الذي تم الاعداء عليه، وهذه المسؤولية المترتبة على عاتق الجاني قد تفرضها التشريعات الوطنية الداخلية، وقد تكون مفروضة من جانب دولي كالاتفاقيات الدولية التي تشرعها المنظمات الدولية وتصادق عليها الدول، ولأجل التعرف أكثر على الجرائم السيبرانية، فإننا سنبحث في هذه المسؤولية من جانب التشريعات الداخلية في فرع أول ومن جانب التشريعات الدولية في فرع ثانٍ.

- **المسؤولية الناشئة عن الجرائم السيبرانية في التشريع الداخلي**

بعد أن فتحت ثورة المعلوماتية الباب على مصراعيه أمام الجرائم السيبرانية ظهر لنا نوع جديد من الجرائم لا يستوعبه النص الجنائي أو المدني، لكن يمكن أن يشمله النص العام والمبدأ القانوني المستوحى من روح القانون حتى تصدر السلطة التشريعية تشريعاً يستوعب الجريمة الحديثة النشأة؛ وعليه فإننا في هذا الفرع سنبحث في اثر قيام الجريمة السيبرانية على وفق التشريعات الداخلية ونقصد بها كلّ من المسؤوليتين الجزائية والمدنية، تقوم المسؤولية الجزائية عن الأفعال التي يرتكبها الجناة وتشكل اعتداءً على حقّ يحميه القانون سواء كان هذا الاعتداء على النفس أو المال أو الحقوق المعنوية الأخرى؛ وذلك عند توفر الأركان العامة في الجريمة والخاصة، اما المسؤولية المدنية فتقوم بتوفر أركانها –كما سنبين لاحقاً– المتمثلة بالخطأ والضرر والعلاقة السببية.

أولا: المسؤولية الجزائية

يهدف القانون الجنائي إلى وضع حدّ للجرائم؛ وذلك من خلال التعرف على الجرائم وبيان أركانها والمصالح المحمية من كلّ جريمة؛ لذا نرى أن مبدأ شرعية الجرائم والعقوبات (لا جريمة ولا عقوبة

الا بنص) من المبادئ المستقرة في القانون الجنائي، إذ لا يمكن للقاضي استحداث جرائم أو عقوبات غير منصوص عليها من قبل المشرع، ولا يعني ذلك لزاماً أن تكون منصوصة في قانون العقوبات بل يمكن أن ترد في قوانين اخرى أو تعليمات تشرعها الجهات المختصة عند طروء الحاجة إليها.

وهنالك عدَّة صور من الجرائم السيبرانية التي يمكن معها الحصول على المعلومات بو اسطة الحاسب الآلي يمكن أن تخضع لنصوص قانون العقوبات كالتهديد والفعل الفاضح والسرقة والقذف والسب وغيرها.

فقد نصت المادة(٤٣٠)[١] من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ العراقي التي ذكرت جريمة التهديد، ومن ثم بينت المادة (٤٣٢)[٢] عدم اشتراط وسيلة معينة في السلوك الجرمي الذي يمكن أن يرتكب بأي وسيلة، إذ لم يحدد المشرع وسيلة لارتكابها بل ركز على الفعل الجرمي الصادر من الجاني واستخدم مصطلحات مرنة وقابلة للتفسير بعدَّة أشكال، فقد يكون التهديد شفوياً، وقد يكون مكتوباً وقد يكون بواسطة شخص آخر وهذا لا يمنع من استخدام وسائل التقنية الحديثة كالحاسب الآلي والأنترنت لإرسال التهديد، فالتويتر أو الفيسبوك أو البريد الالكتروني يمكن أن يكون وسيلة للتهديد حسب القانون، وعليه لا يوجد مانع من الأخذ بالنص الذي ينطبق على الجرائم التقليدية في هذه الجريمة السيبرانية.

(١) التي تنص على: (١-يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كلّ من هدد آخر بارتكاب جناية ضدّ نفسه أو ماله أو ضدّ نفس أو مال غيره أو بإسناد أمور مخدشة بالشرف أو افشائها وكان ذلك مصحوباً بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصوداً به ذلك. ٢ – ويعاقب بالعقوبة ذاتها التهديد إذا كان التهديد في خطاب خالٍ من اسم مرسله أو كان منسوباً صدوره إلى جماعة سرية موجودة أو مزعومة.)

(٢) التي تنص على: (كلّ من هدد آخر بالقول أو الفعل أو الإشارة كتابة أو شفاها أو بواسطة شخص آخر في غير الحالات المبينة في المادتين ٤٣١ و٤٣١ يعاقب بالحبس مدة لا تزيد على سنة واحدة أو بغرامة لا تزيد على مائة دينار)

.

وذات الأمر ينطبق على المادة (٢٨٦)[١] من قانون العقوبات التي عالجت التزوير، فالتزوير يمكن أن يكون بأي طريقة مادية أو معنوية ومن الطرق التي يمكن أن يستخدمها المجرم السيبراني هي المادية بتغيير الكتابة الموجودة وطباعتها أو التلاعب بها قبل طباعتها من قبل الجهات المعنية أو حتى بحفظها على السيرفر المخصص للحفظ، اما الطريق الآخر فيكون بإعطاء معلومات للموظف المختص مخالفة للحقيقة وجعل الحاسب الآلي أو الانترنت وسيلة القيام بالتحايل، والمادة (٤٣٣)[٢]، والمادة (٤٣٧) [٣] اللتان تناولتا السب والقذف وبينتا أنَّ اسناد الصفة التي توجب احتقار الشخص يمكن أن تكون جريمة عندما ترتكب بأي وسيلة من وسائل العلنية دون تحديد للوسيلة وذلك من خلال مصطلح مرن يقبل التطور ، والمادة (٤٦٧) [٤]من القانون نفسه التي تناولت الغش في المعاملات التجارية حيث لم تحدد بالضبط الوسيلة التي يتم من خلالها التحايل والتدليس ممَّا يعني ترك الباب مفتوح للقياس وامكان اعتبار الجريمة الحاصلة عبر الانترنت أو الحاسب الآلي غشاً في المعاملات التجارية على وفق قانون العقوبات، وأخيراً المادة (٤٥٢)[٥] المتعلقة بالابتزاز التي يمكن أعمالها في جرائم الابتزاز الالكتروني.

وبالرغم من إمكان انطباق النص عليها تبقى قواعد الإجراءات في قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ قاصرة لا تستطيع أن تجاري التطور التقني الذي تنطوي عليه

(١) التي تنص: (التزوير هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر بإحدى الطرق العادية والمعنوية التي يبينها القانون، تغييراً من شأنه أحداث ضرر بالمصلحة العامة أو بشخص من الأشخاص).

(٢) التي تنص: (القذف هو اسناد واقعة معينة إلى الغير بإحدى طرق العلانية من شأنها لو صحت أن توجب عقاب من أسندت إليه أو احتقاره عند أهل وطنه. ويعاقب من قذف غيره بالحبس وبالغرامة او بإحدى هاتين العقوبتين. وإذا وقع القذف بطريق النشر في الصحف أو المطبوعات أو بإحدى طرق الإعلام الأخرى عد ذلك ظرفا مشدداً).

(٣) التي تنص: (القذف هو اسناد واقعة معينة إلى الغير بإحدى طرق العلانية من شأنها لو صحت أن توجب عقاب من اسندت إليه أو احتقاره عند أهل وطنه. ويعاقب من قذف غيره بالحبس وبالغرامة او بإحدى هاتين العقوبتين. وإذا وقع القذف بطريق النشر في الصحف أو المطبوعات أو بإحدى طرق الإعلام الأخرى عد ذلك ظرفاً مشدداً).

(٤) التي تنص: (يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على مائتي دينار أو بإحدى هاتين العقوبتين من غش متعاقداً معه في: حقيقة بضاعة أو طبيعتها أو صفاتها الجوهرية أو العناصر الداخلة في تركيبها أو نوع البضاعة أو مصدرها في الأحوال التي يعتبر فيها ذلك سبباً أساسياً في التعاقد أو كان الغش في عدد البضاعة أو مقدارها أو مقياسها أو كيلها أو وزنها أو طاقتها أو كان في ذاتية البضاعة إذا كان ما سلم منها غير ما تم التعاقد عليه).

(٥) التي تنص: (١– يعاقب بالسجن مدة لا تزيد على سبع سنين أو بالحبس من حمل آخر بطريق التهديد على تسليم نقود أو أشياء أخرى غير ما ذكر في المادة السابقة. ٢– وتكون العقوبة مدة لا تزيد على عشر سنين إذا ارتكبت الجريمة بالقوة أو الاكراه).

الجريمة السيبرانية في جميع إجراءاته ونذكر منها المادة (١) فيما خص الجريمة المشهودة، والفقرة ب من المادة (٣) التي تنص: (لا يجوز تحريك الدعوى الجزائية في الجرائم الواقعة خارج الجمهورية العراقية إلا بإذن من وزير العدل)، وهذه المادة التي تعدّ من المبادئ في القانون المذكور إلا أنها لا تتماشى مع سرعة العصر وتطوره حيث قد لا يمكن تحديد الاختصاص المكاني لمعظم الجرائم السيبرانية المتعولمة الشمولية، وهذه عقبة كبيرة في طريق من يود تقديم الشكوى في الدعوى عن الجريمة السيبرانية، وكذلك الحال بالنسبة للتفتيش في جرائم المعلوماتية الذي يحتاج أن يقطع شوطاً لكي يواكب التطور الملموس في الجريمة السيبرانية.[١]

على الرغم من أنَّ المشرع العراقي يأخذ بالاختصاص الجنائي الشامل على وفق المادة ١٣ من قانون العقوبات التي تنص على (... تسري أحكام هذا القانون على كلّ من وجد في العراق بعد أن ارتكب في الخارج بوصفه فاعلاً أو شريكاً جريمة من الجرائم التالية التي تخرب أو تعطل وسائل المخابرات والمواصلات الدولية والاتجار بالنساء أو بالصغار أو بالرقيق أو بالمخدرات (وعلى الرغم من وجود هذا النص إلا أنَّه يعدّ قاصر أمام جرائم المعلومات العابرة للحدود كما أنَّ هناك من جرائم السيبرانية ما يخرج عن نطاق هذه قواعد قانون العقوبات، وهذا يحتم التدخل التشريعي لمعالجة بعض السلوكيات الخاطئة من قبل البعض، أو على الأقل تشديد العقوبة ممَّا يجعلها منسجمة مع الضرر الجسيم الذي قد يلحق بالمؤسسات الاجتماعية التي تعنى بقطاعات ضخمة جداً من أفراد المجتمع وتكون مخصصة لخدمتهم؛ فالأضرار التي تسببها هذه الجرائم قد تكون على نطاق واسع خصوصاً إذا كانت موجهة ضدّ المصارف وقطاعات الدولة الأخرى كالنقل والقطاع العسكري وغيرها.

(١) سلسبيل بن اسماعيل، الحامية الجنائية للحقّ في الخصوصية، بحث منشور في مجلة الاجتهاد القضائي- مجلد ١٢، عد ٢٢، افريل ٢٠٢٠، ص ٧٤١.

ومن تلك الجرائم جرائم السرقة فبالرغم من أن جريمة السرقة من الجرائم التي تمت معالجتها ضمن قانون العقوبات العراقي إلا أنَّ النص التقليدي يكاد لا ينفع في شيء فيما خص الجريمة السيبرانية، فالسرقة حسب نص المادة (٤٣١)[١] من قانون العقوبات تشترط إخراج الشيء المسروق من الحرز المغلق الموجود فيه، بينما سرقة المعلومات تكون بنسخها أو الوصول إليها دون إخراجها من حرزها المغلق، والأمر ذاته بالنسبة للتحريض على القتل، يضاف إلى ذلك جريمة اختراق الشيكات التي هي من الجرائم المستحدثة، وتعطيل الشبكات، والإرهاب الالكتروني، إضافة إلى جرائم مستحدثة أخرى سنبينها بعد قليل.

وقد تنبه المشرع إلى بعض الحالات وأسرع بوضع تشريعات كفيلة بحلّ هذه المشكلة القانونية ومنها تشريع قانون التوقيع الالكتروني والمعاملات الالكترونية رقم ٧٨ لسنة ٢٠١٢.

وكذلك تصديق جمهورية العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١، إلا أنَّ الاتفاقية لم تطبق كاملة لحدّ الآن، إذ نصت المادة (٥) منها على ضرورة أن: (تلتزم كلّ دولة طرف بتجريم الأفعال المبينة في الاتفاقية؛ وذلك وفقاً لتشريعاتها وأنظمتها الداخلية) وكذلك المادة (٢٢) التي تنص: (تلتزم كلّ دولة طرف أن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة هذه الاتفاقية)، والأفعال حسب نص المواد (٦-٢٠) من الاتفاقية هي: جريمة الدخول غير المشروع جريمة الاعتراض غير المشروع، وجريمة الاحتيال، وجريمة الإباحية، والجرائم الأخرى المرتبطة بالإباحية كالمقامرة والاستغلال الجنسي وجريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات و الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بانتهاك حقّ المؤلف

(١) التي تنص على: (السرقة اختلاس مال منقول مملوك لغير الجاني عمدا....).

والحقوق المجاورة، والاستخدام غير المشروع لأدوات الدفع الالكترونية، والشروع والاشتراك في ارتكاب الجرائم، والمسؤولية الجنائية للأشخاص الطبيعية والمعنوية.

وبعد أن بينا الأساس القانوني للجريمة السيبرانية نستطيع أن نقول أنَّه متى ما توافر الأساس القانوني للجريمة كان بالإمكان فرض العقوبة على الجاني بعد التأكد من توافر أركان الجريمة، وأركان الجريمة مادية ومعنوية، تشمل الأركان المادية كلّ سلوك يباشره الجاني ايجابياً كان أم سلبياً يعدّ القوام المادي للجريمة، اما الركن المعنوي فيتمثل بالإدراك والإرادة فإذا توافرت هذه الأركان قامت الجريمة وكان مرتكب الفعل مسؤولاً جزائياً عما قام به من نشاط إجرامي.

وهنا يثور تساؤل حول مدى امكانية ان تكون الجرائم السيبرانية جرائم غير عمدية؟

فمن الغالب أن يكون المجرم السيبراني شخصاً فطناً ذكياً ذا خبرة ومهارة فنية ودراية وهو ما يطلق عليه قانون بالرجل الحريص الذي يمتاز عن الرجل المعتاد أن يملك من الحيطة والعناية ما يفوق الرجل العادي؛ فالجرائم التي قوامها سرقة الأعضاء البشرية تتطلب دراية ومهارة في علم الطب، وكذلك غسيل الأموال التي تستدعي معرفة اقتصادية عالية بالبيع والشراء وفطنة في اخفاء الطابع غير الشرعي لهذه الأموال وإظهارها بمظهر المشروعية، كلّها تجعل أصابع الاتهام تشير إلى اشخاص تلقوا مستوى غير عادي في التعليم، لكن ذلك لا يمكن أن ينفي إمكانية أن يرتكب الجريمة السيبرانية شخص أقل من هذا المستوى، فقد يرتكب الجريمة السيبرانية شخص مهمل أو كان خطأه نتيجة لرعونته أو عدم انتباهه أو لعدم احتياطه أو مراعاته للقوانين والأنظمة، فبموجب نص المادة(٣٥)[١] من قانون العقوبات العراقي تكون الجريمة غير عمدية إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواء كان هذا، ومن الممكن تصور حصول الجريمة المعلوماتية

(١) وتنص على: (تكون الجريمة غير عمدية إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواء كان هذا أو رعونة أو عدم انتباه أو عدم احتياط أو عدم مراعاة القوانين والأنظمة الخطأ إهمال والأوامر.).

على وفق هذه الصورة، فقد يستخدم موظفا (الفلاش) في نقل المعلومات إلى الحاسب الآلي لدائرته دون أن ينتبه إلى أنَّه يحمل الفايروسات الالكترونية ممَّا يسبب عطلاً في الأجهزة لإهماله، أو يستخدم الحاسب الآلي لأغراضه الشخصية بإفراط فيتسبب بتعطيله بسبب عدم مراعاته للقوانين والانظمة، كلّ هذه الأمثلة تدخل في نطاق الجرائم السيبرانية غير العمدية.

ثانياً: المسؤولية المدنية

تتحقق المسؤولية المدنية تقصيرية كانت أو عقدية بقيام أركانها الثلاثة المتمثلة بالخطأ الذي يصدر من مرتكب الفعل الضار (أي من يقوم بالنشاط السيبراني الذي يسبب الضرر قاصداً كان متعمداً أو غير قاصد)، والركن الثاني هو الضرر (أي أن يلحق المضرور خسارة مالية أو كسب فائت يصيبه في ذمته المالية فينقصها ويؤثر عليها سلباً)، والركن الثالث هو العلاقة السببية بين الخطأ و الضرر (أي أن يكون الضرر نتيجة طبيعية للخطأ الحاصل فيكون مباشراً متوقعاً بالنسبة للمسؤولية العقدية ومباشراً متوقعاً أو غير متوقع بالنسبة للمسؤولية التقصيرية)، وانَّ المسؤولية المدنية يمكن أن تكون مسؤولية عقدية أو أن تكون مسؤولية تقصيرية ولا يمكن أن تجتمع المسؤولية عن كلا المسؤوليتين لغرض التخيير في التعويض.

فإذا حدثت الجريمة السيبرانية بين طرفين متعاقدين قامت المسؤولية العقدية ووجب على مرتكب الفعل الضار دفع تعويض أو أي ترضية من جنس الضرر للمضرور ويدفع له الأضرار المباشرة المتوقعة من العقد إلا إذا كان هنالك اتفاق بين الطرفين على التخفيف من المسؤولية بوضع حدّ أعلى لا يمكن أن يتجاوزه التعويض، أو كان هناك إعفاء من المسؤولية، وفي كلّ الأحوال لا يمكن

تخفيض التعويض أو الإعفاء منه إذا ثبت أنَّ هنالك غشاً أو خطأ جسيماً قد صدر من المدين مرتكب الفعل الضار.[١]

اما إذا لم يكن بين المضرور ومرتكب الخطأ السيبراني من عقد قامت مسؤولية مرتكب الفعل الضار على أساس المسؤولية التقصيرية التي يقوم فيها التعويض عن الأضرار المباشرة المتوقعة وغير المتوقعة التي لحقت المضرور، ويقدر الضرر على أساس الخسارة التي لحقت الدائن المضرور والكسب الذي فاته بشرط أن يكون نتيجة طبيعية للخطأ الذي ارتكبه المدين مرتكب الفعل الضار.[٢]

- **المسؤولية الناشئة عن الجرائم السيبرانية في التشريع الدولي**

تعدّ المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم السيبرانية، وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة هذه الجرائم ومن تلك المعاهدات معاهدة بودابيست والمعاهدة الأوروبية، معاهدة برن، ومعاهدة تربس.

أوّلاً : معاهدة بودابيست لمكافحة جرائم الإنترنيت ٢٠٠١

تعدّ معاهدة بودابيست أوّل معاهدة دولية تكافح جرائم الإنترنيت والجرائم الأخرى السيبرانية، حيث وقعت هذه المعاهدة في بودابيست في المجر عام ٢٠٠١ ، بعد أن وصلت الجرائم إلى حدّ خطير أصبح يهدد الأشخاص والممتلكات ممَّا دفع بالدول إلى توقيع هذه الاتفاقية من أجل الحدّ منها وتوحيد الجهود الدولية من أجل الحدّ منها عالمياً، وقد شهدت تلك الفترة انتقال جرائم السيبرانية من

(١) صدقي عيسى، التعويض عن الضرر ومدى انتقاله للورقة دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة،ط١ ، ٢٠١٤ ، ٤٨.

(٢) د. عصمت عبد المجيد بكر، نظرية العقد في القوانين المدنية العربية، دار الكتب الوطنية، بيروت، ١٩٧١، ص ٣٦٧.

مرحلة ابتدائية متمثلة في محاولات من هواة للتسلل إلى الشبكة العنكبوتية والقيام بأعمال احتيالية إلى مرحلة جديدة أبطالها أشخاص محترفين في عالم الحاسب الآلي والانترنت يشنون هجمات منظمة في الاختلاس والاحتيال والابتزاز الالكتروني، وكان أوائل ضحاياها هم رواد الانترنت من مؤلفي الكتب وحقوق النشر الأخرى، فقد وقعت الاتفاقية بعد مخاض دام أربعة أعوام انضمت فيها دول أوروبا اضافة إلى امريكا وكندا واليابان وجنوب إفريقيا .[١]

ثانياً : المعاهدة الأوروبية لمكافحة جرائم الانترنت

وتهدف هذه الاتفاقية لمساعدة البلدان في مكافحة الجرائم السيبرانية، وقد الزمت هذه الاتفاقية الدول التي انضمت لها عليها بسنّ الحدّ الأدنى من القوانين الضرورية أو تعديل تشريعاتها للتعامل مع جرائم التقنية العالية كالدخول غير المصرح به إلى الشبكات المحمية والتلاعب ببيانات الأشخاص والمؤسسات ذات الصلة بالحاسب الآلي والصور التي يعرضها أصحابها وانتهاك حقوق الملكية الفكرية ونسخ البينات الرقمية، وقد لاقت هذه الاتفاقية معارضة كبيرة من المدافعين عن الحقوق الخاصة حيث عدّوها انتهاكاً لحقوق التعبير والخصوصية، ممَّا جعل الدول الموقعة على الاتفاقية بشكل يجعلها اتفاقية تقف لجانب الأفراد وتحميهم أكثر ممَّا تحمي سيادة الدول وتحافظ على أمنها فقد أوردت هذه الاتفاقية نصوصاً توجب على الدول مراقبة الأفراد في المجال السيبراني وتقديم المساعدة من الدول التي تملك معرفة تقنية أعلى من دول أخرى لكن تم الاتفاق على أنَّ هذه الخدمات متاحة للأفراد دون الحكومات. [٢]

ثالثاً: معاهدة برن لحماية المصنفات الأدبية والفنية1971

(١) رمضان مدحت، "جرائم الاعتداء على الاشخاص والانترنيت"، دار النهضة العربية، بدون طبعة، القاهرة،٢٠٠٠ ، ص ٢٤ .

(٢) الشاعر نضال، "الإجرام المعلوماتي في وسائل الاتصال الالكتروني"، دراسة منشورة في نشرة المعلومات القانونية الصادرة عن جمعية اماء المعلوماتية في لبنان، العدد ٣ ايار ٢٠٠٥ ، دار ناشرون، بيروت ٢٠٠٥، ص٤.

تعدّ معاهدة برن حجر الأساس في مجال الحماية الدولية لحقّ المؤلف، وقد وقعت هذه الاتفاقية من قبل ١٢٠ دولة، وتعدّ المادة (٩) منها أهم مادة في الاتفاقية حيث تنص على منح أصحاب حقّ المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة أو شكل، اضافة إلى منحه حقاً في ترخيص أو منع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه وقد نصت هذه الاتفاقية لأول مرة بإيقاع جزاءات وعقوبات على كلّ من يخالف أحكامها سواء كان وطنياً ذلك المخالف أم أجنبياً.

وقد تم التركيز على حقّ المؤلف كونه يمثل وسيلة قانونية مهمة تحمى من خلالها حقوق المؤلفين على مختلف الأصعدة من السرقة أو الاختلاس أو الاحتيال أو حتى النسخ المخالف للنصوص، فحقّ المؤلف يمثل حقاً ذا طيف واسع من الحقوق الثانوية التي يمكن أن تنشأ بظله وتحت عنوان واحد، خصوصاً أنَّ دول العالم تبحث عن اتفاقية سلسة وغير متشعبة تبدأ بها محاربة نوع معقد من أنواع الجرائم، وهو الجرائم المرتكبة في المجال السيبراني الذي منذ نشأ والدول لم تسيطر عليه؛ لأنَّه يمثل مجالاً سائباً لا يمكن ضبطه بسهولة دون امتلاك تقنيات تماثل أو تفوق تلك التي بثتها الشركات التكنلوجية التي احترفها الجناة في الظل لأعوام قبل أن تظهر الجريمة السيبرانية بشكلها المضر، فقد تكفلت النظم القانونية حقّ المؤلف على اختلافها للمبدعين والمؤلفين لحماية إبداعاتهم الفكرية في مختلف العلوم والفنون والاتجاهات وقد اعطت هذه الاتفاقية بعداً جديداً لحقوق الملكية الفكرية وأبرزتها كحقوق مهمة وإن لم تكن حقوقاً ملموسة، إلا أنَّها تفوق في كثير من الأحيان حقوق أخرى تقليدية كحقّ ملكية العقار.[١]

(1) ٣٩ Chassaing (J-F) L Intent etle droit penal Recueil Dalloz Sirey , p38 ,1996.

وقد صاغت هذه الاتفاقية المقام الأوَّل للحقوق الفكرية وأبرزتها كحقوق يمكن أن تشكل مورداً مهماً من موارد القطاع الخاص أو العام ممَّا أثر على اقتصاد الكثير من الدول المنضمة ايجاباً موضوع الحماية القانونية لبرامج الحاسب الآلي، كما أن النتائج المشجعة للدول التي التزمت بالاتفاقية حدت بالدول الأخرى إلى تعديل قوانينها أو تشريع قواعد قانونية لمسايرة اتجاه هذه الاتفاقية.

رابعاً: معاهدة تربس ١٩٩٤

وهي المعاهدة الأهم في حقوق الملكية الفكرية التي دعت إليها الحاجة بعد أن بدأت أنواع جديدة من الجرائم السيبرانية بالظهور وهي جرائم السطو السيبراني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية.

وقد تضمنت هذه الاتفاقية التعريف بالتجارة الخاصة بالملكية الفكرية فوسعت من حقوق الملكية الفكرية وتوسعت في معالجة أحكامها وتضمنت تلك الاتفاقية العديد من الإجراءات المهمة والفعالة لردع الاعتداءات على حقوق الملكية الفكرية، كما أنَّها فرضت على الدول الموقعة والمصادقة عليها اتخاذ مجموعة من التدابير المهمة لمعالجة اشكالات داخلية تتعلق بجرائم سيبرانية خارجة عن سيطرة القانون في بعض البلدان الوضع، مثلاً إعطاء الحقّ للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة خصوصا أنَّ تلك الأدلة من الأدوات التي يسهل التخلص منها ولا يترك التخلص منها اثراً فحذف البرنامج من قائمة البرامج ومن ثمَّ حذفه من سلة المحذوفات لا يترك أي أثر، وهو ليس كالتخلص من آثار جريمة أخرى توافرت على الأدلة التقليدية، كما أنَّها ضمت لأوَّل مرَّة عقوبات جنائية رادعة تفرضها تلك الدول على الأفراد المنتهكين لقواعدها، إلا أنَّها اعطت الحقّ للدول التي يحصل فيها ضبط الجريمة اتباع

الإجراءات والشروط الواجب توفرها حسب تشريعاتها في قيام المسؤولية ووجوب فرض العقوبة والتعويض وتقديره، فهذه التفاصيل تختلف بين الدول وان اتفقت من حيث المبدأ العام.

اما عن موقف المنظمات الدولية فقد عقدت الكثير من المؤتمرات التي دعت لمواجهة النتائج السيئة والأضرار التي تلحق بالنظام الاجتماعي والاخلاقي للمجتمع الدولي من مخاطر الجرائم السيبرانية؛ ذلك أنَ مخاطر هذه الوسائل أخذ منحى في منتهى الخطورة، إذ أصبحت هذه الجرائم تستطيع أن تصيب بأضرارها كلّ شخص لكثرة استخدام الأفراد للتقنية إضافة إلى أنَّها أصبحت ذات طابع عال من التقنية، فقد حصلت حوادث كأرسال الفايروسات بمواعيد معينة من السنة أدت إلى تدمير عدد هائل من أجهزة الحاسوب التابعة للدولة أو المؤسسات ممَّا سبب أضرار فادحة في عملية التنمية للدول، وبما أنَّ جميع الدول ملزمة بتأمين جانبين رئيسيين لأفرادها وهما حماية حياة الأفراد وحرياتهم الشخصية من جانب وتأمين انتقال المعلومة من جانب آخر، والدول عاجزة غير قادرة على اتخاذ خطوات فردية لعالمية وشمولية الجريمة؛ لذلك فقد أصبحت النشاطات التي تقوم بها المنظمات الدولية على درجة من الأهمية بسبب الطبيعة التي تفرضها الجريمة، فقد أكدت منظمة التعاون والتنمية (O C D E) في توصياتها في ٢٣ سبتمبر ، ١٩٨٠ على هذا المبدأ، وقد صدر عن الجمعية العامة للأمم المتحدة القرار رقم ٩٥،٤٥ نص على أنَّ كلّ معلومة تؤدي إلى التفرقة العنصرية أو التمييز بشكل عام بين البشر مثل المعلومات عن العرق، اللون، المذهب، الجنس، الحياة الجنسية، الآراء السياسية، الآراء الفلسفية، هي معلومة تنتهك الحقوق المحمية قانوناً وتمثل جريمة سيبرانية.

كما أنَّ منظمة التجارة الدولية قد كللت جهودها باتفاقية تنظيم وانتقال المعلومة، وأكدت في المادة (١٤) منها على: (حرية انتقال المعلومة بشرط أن لا تستخدم كأسلوب تعسفي أو غير مبرر

للتمييز فيما بين الدول أو لاتخاذه كذريعة خفية للحظر التجاري، ولا يمكن تفسير أي تدبير وارد في هذا الاتفاق كسبب لامتناع أي عضو عن تطبيق ما ورد فيه...).

اما على صعيد الدول العربية فهي بشكل عام وبحكم تأخرها في مجالات التقنية فلقد اتسمت الاتفاقيات التي أبرمتها هذه الدول فيما بينها في هذه الدول بأنَّها غير كافية لمعالجة الجرائم السيبرانية ولم تمثل معالجة جدية لها وقد برزت دول الخليج العربي بشكل خاص بالتصدي لهذه الجريمة بسن التشريعات والقوانين؛ فأصدرت عمان أوَّل قانون عربي يتطرق لمواجهة هذه الجرائم، تبعتها دولة الإمارات العربية المتحدة ثمَّ المملكة العربية السعودية. جميع هذه القوانين مختصة في مكافحة الجرائم السيبرانية، وتعدّ هذه القوانين نموذجية حيث تطرقت إلى غالبية الجرائم المعلوماتية، وتعدّ أول ثلاثة قوانين عربية تصدر بشكل مستقل لمواجهة هذه الجرائم، اما العراق فقد توقفت جهوده في هذا المجال عند حدّ وضع مسودة لقانون (جرائم المعلوماتية) وقد تمت أمام مجلس النواب العراقي يوم ٢٧ يوليو /تموز ٢٠١١ القراءة الثانية له، إلا أنَّه لم ير النور حتى اليوم، وعلى الرغم من وجود الكثير من الملاحظات وكونه لا يسد رمق حاجة المجتمع إلا أنَّ تشريعه مع بعض التعديلات والإضافات للمسودة المطوحة سيكون إضافة مهمة إلى المنظومة التشريعية، علماً أنَّ هنالك حاجة إلى تعديل القوانين الجزائية والمدنية لتستوعب معالجة هذه الجريمة والحدّ منها، وهو أمر أيسر بكثير من سن تشريع جديد.

الخاتمة

بعد دراسة هذا الموضوع لاحظنا تشعبه وصعوبته؛ وذلك من خلال كثرة صور الجريمة السيبرانية وظهور أنواع جديدة من الجرائم قبل إحصاء جميع الأنواع الموجودة؛ وعليه فقد توصلنا إلى جملة من الاستنتاجات والتوصيات بخصوص هذه الجرائم وهي:

أولاً: الاستنتاجات

١-تختلف الجريمة السيبرانية عن الجريمة التقليدية من حيث عالميتها ومحلها ونشاطها إضافة إلى وجود عدد منها لا يستوعبها النص الجرمي بالردع والزجر، وهو أمر خطير ؛ لأنَّها أصبحت تمس حياة الأفراد وأموالهم دون وجود الحماية الكافية.

٢-إنَّ الجريمة السيبرانية من جرائم الإعلام الجديد التي ظهرت وتنامت طردياً مع انتشار وسائل التواصل الاجتماعي والاعتماد عليها كوسيلة إعلامية يتم من خلالها الوصول للمعلومة من قبل الأفراد مما يعرض عدداً أكبر من الأفراد؛ لأنَّ يكونوا ضحايا لهذه الجريمة.

٣-بما ان المجتمع لم يألف هذا النوع من الجرائم فإنَّ امكان الوقوع كضحية لها مرتفع وامكان التبليغ عنها أو اكتشافها أو كشف جناتها منخفض وهو مؤشر خطير في مجال حقوق الإنسان ودلالة على افتقاد المجتمع عنصراً مهماً من عناصره وهو الأمن والسكينة.

٤-تبين لنا من خلال البحث أنَّ العراق عضو في اتفاقيات توجب عليه تعديل قوانينه الموجودة لتتماشى مع الأوضاع المحيطة لحماية أفراد المجتمع، وفي هذا الأمر لم نلاحظ أي تحرك تجاهه من قبل الجهات التشريعية.

ثانياً: التوصيات

١-ضرورة تعديل النصوص القانونية في القوانين المدنية والجزائية المعمول بها في العراق وجعل النص يستوعب التطور الحديث للتقنية، والابتعاد عن الإكثار من القوانين التي اثقلت كاهل المنظومة القانونية دون حاجة ملحة، إذ يستطيع مجلس النواب الاستعانة بذوي الخبرة القانونية من المختصين في أخذ آرائهم في تعديل بعض النصوص في

القانون المدني وقانون الملكية الفكرية وقانون العقوبات بإضافة ما يجعلها تستوعب نواتج التطور التقني وذلك أمر أيسر من سن قانون جديد.

٢- تكاتف الجهود العربية بأنشاء منظمة عربية متخصصة مهمتها التنسيق بشأن مواجهة الجرائم المعلوماتية وتبادل الخبرات مع الدول التي لها باع طويل في أساليب التجريم والمكافحة لمثل هذه الجرائم تسمى (المنظمة العربية لمكافحة الجريمة المعلوماتية) وتضم لجان حقوقية وإعلامية وأمنية.

٣- إنشاء هيئة وطنية تسمَّى (الهيئة الوطنية لمراقبة المجال المعلوماتي) تتولى مراقبة المواقع الالكترونية عبر شبكة الانترنيت لحجب المواقع المشبوهة التي تهدد أمن واستقرار المجتمع خصوصاً الجرائم غير الأخلاقية التي تتعارض مع قيم ومبادئ المجتمع العراقي وتجعل الإعلام عبر الانترنت موثوقاً.

المصادر والمراجع

١. **أحمد عبد الكريم سلامة، "الانترنت والقانون الدولي الخاص، فراق ام تلاق"، بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت تنظمه كلية الشريعة والقانون بالتعاون مع مركز الامارات للدراسات والبحوث، ٢٠٠٥.**

٢. **جميل عبد الباقي الصغير، "القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول ، الجرائم الناشئة عن استخدام الحاسب الآلي "، ط ١ ، دار النهضة العربية ، القاهرة ، ١٩٩٢.**

٣. **حسني، د. محمود نجيب، "شرح قانون العقوبات، القسم العام "، ط ٦ ، دار النهضة العربية ، القاهرة ،١٩٨٩.**

٤. **حسنين شفيق، الإعلام الجديد والجرائم الالكترونية، دار فكر وفن للطباعة والنشر والتوزيع، ٢٠١٥، ص٣٢.**

٥. رمضان مدحت، "جرائم الاعتداء على الاشخاص والانترنيت"، دار النهضة العربية، بدون طبعة ، القاهرة، ٢٠٠٠.

٦. سلسبيل بن اسماعيل، الحامية الجنائية للحق في الخصوصية، بحث منشور في مجلة الاجتهاد القضائي- مجلد ١٢، عد ٢٢، افريل ٢٠٢٠.

٧. صدقي عيسى، التعويض عن الضرر ومدى انتقاله للورقة دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة،ط١ ، ٢٠١٤ .

٨. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دار، مدبولي، القاهرة، ٢٠٠٩ .

٩. عصمت عبد المجيد بكر، نظرية العقد في القوانين المدنية العربية، دار الكتب الوطنية، بيروت، ١٩٧١.

١٠. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣، ص ٣٢.

١١. فلاح حسن منور التميمي، الجريمة السيبرانية، مقالة منشورة على موقع مجلس القضاء الأعلى، رفعت بتاريخ ١٨-٩-٢٠٢٠ مايو - الاستراتيجية، مركز تقنية المعلومات دولة الأمارات العربية المتحدة للفترة من ١-٣، ٢٠٠٠.

١٢. محمد السيد رشدي،" الانترنت والجوانب القانونية لنظم المعلومات"، مجلة الفتوى والتشريع ، العدد ٩، مايو ٢٠٠٠ . مجلس الوزراء .

١٣. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوسيع، عمان، الأردن، الطبعة الأولى، ٢٠٠٤ .

١٤. محمد حسام محمود ، "الحماية القانونية لجرائم الحاسب الآلي"، دار الثقافة للطباعة والنشر ، القاهرة ، ١٩٨٧ .

١٥. محمد حسام محمود ، "الحماية القانونية لجرائم الحاسب الآلي"، دار الثقافة للطباعة والنشر ، القاهرة ، ١٩٨٧ .

١٦. محمد حماد مرهج ، "التكنولوجيا الحديثة و القانون الجنائي"، دار الثقافة، عمان، ٢٠٠٤.

١٧. مستشارية الأمن الوطني أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الأمن السيبراني العراقي، دراسة منشورة.

١٨. نضال الشاعر، "الاجرام المعلوماتي في وسائل الاتصال الالكتروني"، دراسة منشورة في نشرة المعلومات القانونية الصادرة عن جمعية اماء المعلوماتية في لبنان، العدد ٣ ايار ٢٠٠٥ ، دار ناشرون، بيروت.

١٩. نواف كنعان، "النماذج المعاصرة لحقّ المؤلف ووسائل حمايته"، ط ٣ ، الجامعة الأردنية، كلية الحقوق،.٢٠٠٠ .

٢٠. هدى حامد قشقوش، "جرائم الحاسب الالكتروني في التشريع المقارن"، ط ١، دار النهضة العربية، القاهرة، ١٩٩٣.

٢١. هشام محمد فريد رستم،" قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط ، ١٩٩٤.

٢٢. يونس عرب، "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكومبيوتر"، ج ١، منشورات اتحاد المصارف العربية ، ط ١ .

٢٣. يونس عرب، جرائم الكومبيوتر والانترنت، ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢ ، تنظيم المركز العربي للدراسات والبحوث الجنائية، ٢٠٠٢.

ثانياً: المصادر الأجنبية

1. **FRAYSSINET (J) ; Laprotectiondes donnes personnelles face aux nouvelles technologies de I in formation et de la Communi Cation dans le monde; Constantes es et nouveautes , une recherche persente auperemiere de I informatique legal et Juridique au Koweit Le , Janv , 1999**
2. **Chassaing (J-F) L Intent etle droit penal Recueil Dalloz Sirey , ,1996**
3. **MERWE (vander) computer crimes and other crimes against information technology in sauth africa, R.I.D, 1993.**
4. **om Forester , Essential proplems to hig _Techsaciety first MIT edition ،Cambridge , Massachusetts , 1989.**

ثالثاً: القوانين والاتفاقيات:

١- قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
٢- قانون أصول المحاكمات العراقي رقم٧٣ لسنة .
٣- معاهدة برن لحماية المصنفات الأدبية والفنية ١٩٧١.
٤- دليل وزارة العدل الأمريكية لعام ١٩٧٩.
٥- معاهدة تربس ١٩٩٤.
٦- معاهدة بودابيست لمكافحة جرائم الإنترنيت ٢٠٠١.
٧- المعاهدة الأوروبية لمكافحة جرائم الانترنت.
٨- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠.
٩- مسودة قانون الجرائم المعلوماتية العراقي.