الإطار القانوني للجريمة السيبرانية

الباحث : م. عمار مراد العيساوي

كلية القانون – جامعة الكفيل – العراق

The legal framework for cyber crime

Lect. Ammar Murad Al-Issawi / Faculty of Law / Al-Kafeel University

amar.morad1985@gmail.com

ملخص:

الجريمة السيبرانية تعد من أهم جرائم العصر التي تحدث أضراراً فادحة في اقتصاد الدول تفوق الأضرار تلك التي تحدثها الجرائم التقليدية، الأمر الذي لحق بسلطات الدول خسائر مادية ومعنوية باهضة مما دفعها إلى الإسراع في إيجاد حلول تشريعية للحَد من هذه الظاهرة التي تفاقمت وبدأت الدول الواحدة تلو الأخرى بسنُ تشريعات تكافح بها هذه الجرائم، كون المجرمون يستخدمون تقنيات جديدة لغرض ارتكاب هجمات سيبرية ضد الحكومات والشركات والأفراد. ولا تقف هذه الجرائم عند الحدود، سواء أكانت مادية أم افتراضية، وتسبب أضرارا خطيرة وتشكل تهديدات ملموسة للضحايا في جميع أنحاء العالم، نظراً للتطور الهائل في مجال تكنولوجيا المعلومات ودخول وسائلها إلى شتى مجالات الحياة مما أدى إلى تعاظم دورها بشكل غير محدود، إذ باتت الحواسيب الآلية والتقنيات الالكترونية وشبكة الانترنت لغة العصر التي لا يمكن الاستغناء عنها، وأصبح الاعتماد عليها متعلقاً بتسيير المرافق الاقتصادية والاجتماعية والعسكرية والطبية وغيرها، الأمر الذي يحتاج إلى توفير أقصى درجات الحماية لما يحيط بها وذلك تجنباً لتعطيل سير تلك المرافق والمصالح الحيوية أو الاعتداء عليها بما يؤثر على المصالح الجوهرية في المجتمعات.

الكلمات المفتاحية: السيبرانية، سماتها، موقف المجتمع الدولي، المجرم الالكتروني، أنواع السيبرانية

Abstract:

Cybercrime is one of the most important crimes of the era that causes great damage to the economy of countries that exceed the damage caused by traditional crimes, which inflicted huge material and moral losses on the authorities of the countries, which prompted them to speed up finding legislative

solutions to curb this phenomenon, which has exacerbated and started one country after another. By enacting legislation to combat these crimes, criminals are using new technologies for the purpose of committing cyber attacks against governments, companies and individuals. These crimes do not stop at the borders, whether physical or virtual, and cause serious damage and pose tangible threats to victims all over the world, due to the tremendous development in the field of information technology and the entry of its means to various areas of life, which led to an unlimited role in the growth of computers. Mechanism, electronic technologies and the Internet are the language of the era that cannot be dispensed with, and relying on them has become related to the management of economic, social, military, medical and other facilities. core interests in societies.

Key words : Cyber, its features, the position of the international community, cybercriminal, types of cyber

مقدمة

أولاً: موضوع البحث

أن انتشار الوسائل الحديثة للتكنولوجيا بين المجتمعات وشيوع استخدامها والتوسع في التعامل من خلالها، جعل لكل فرد القدرة على التفاعل والتواصل عبر الحدود، ونظراً لتوافر القدرة على نقل وتلقي المعلومات والتقنيات والاضطلاع على البيانات والبرامج بكل سهولة ويُسر، وبالرغم من الآثار الايجابية التي رافقت ظهور هذه الحقول الجديدة والمتطورة من العلوم والمعرفة، إلا أن ذلك قد ترافق مع بروز العديد من المشكلات والسلبيات التي ظهرت على شكل جرائم يقترفها بعض مستخدمي التكنولوجيا والتي تتصف بخطورتها وسهولة ارتكابها ومعضلة عبورها للحدود الوطنية، والتي يمكن أن يطلق عليها الجرائم السيبرانية التي تتوافق بوتيرة سريعة للغاية مع ظهور اتجاهات جديدة باستمرار، ويصبح مرتكبو الجرائم السيبرية أكثر مرونة، فيستغلون أدوات التكنولوجيا الحديثة بسرعة فائقة، ويخططون لاعتداءاتهم بدقة باستخدام أساليب جديدة، ويتعاونون فيما بينهم بطرائق لم نعهدها من قبل، وتنشط الشبكات الإجرامية المتشعبة في أنحاء العالم وتنسق اعتداءاتها المعقدة خلال فترات قصيرة.

ثانياً: أهمية البحث

إن التطور الهائل في استغلال الإرهابيين لوسائل التقنية الحديثة ومنها بالطبع شبكات المعلومات العالمية، يشكل عائق لجهات وهيئات الدولية، مما يجعل تفعيل الآليات القضائية المتعلقة بالتعاون الدولي في شأن ملاحقة الجرائم السيبرانية من شأنها أن تُخرج التحقيقات عن مسارها، أو يُعيقها في حالات أخرى، الأمر الذي يتوجب على الدول أن تتفاوض فيما بينها من أجل إبرام اتفاقيات دولية على المستوي الثنائي أو المتعدد الأطراف لغرض إرساء إطاراً قانونية من أجل مكافحة الجرائم المستحدثة، وخصوصاً منها الجرائم السيبرانية، ثم تستهدي وتستقي منها التشريعات الوطنية الجديدة أو تعدل تشريعاتها الموجودة بالفعل على أساس هذه الاتفاقيات الدولية التي تم إبرامها، ذلك بسبب الطبيعة الدولية لجرائم الإرهاب السيبراني العابر للحدود تجعل من مسائل التنازع حول اختصاص القضاء الوطني لأكثر من دولة بملاحقة الجريمة السيبرانية العابرة للحدود خاصة في الحالات، التي يعمد مرتكبيها إلى إخفاء هويتهم، حيث تحتاج المحاكم الوطنية إلى مزيد من الوقت والتدبر للتيقن من مدى اختصاصها بملاحقة الجريمة المرتكبة من خارج إقليم دولة المحكمة التي تلاحق الجريمة ولا تكمن الصعوبة في تحديد القضاء الوطني المختص بالملاحقة لهذه الجريمة العابرة للحدود فقط، ولكن أيضا عندما لا تكون الجريمة مشمولة في أحد تشريعات إحدى الدول التي يرتكب فيها جزء من الفعل السيبراني الإرهابي.

ثالثاً: إشكالية البحث

عادةً ما يستخدم الفضاء الالكتروني لغرض شن هجمات إلكترونية من شأنها إلحاق خسائر بالخصم، فقد تكون مالية؛ من خلال استهداف المصارف أو المواقع الحكومية التي تحتوي على بيانات هامة، أو حتى استهداف منشآت صناعية، الأمر الذي يتطلب وضع حلولاً أو معايير غير تقليدية لغرض الحد من هذه الجرائم ممثلة في الرقابة الصارمة وغلق المواقع وحسابات التواصل الاجتماعي التابعة لتنظيمات وفصائل مسلحة. لذا تبرز إشكاليات عدة منها ما هي الجريمة السيبرانية؟ وما هي أنواعها؟ وما السمات التي تميزها عن بقية الجرائم؟ وما هو موقف المجتمع الدولي منها؟ وما هو موقف القانون والقضاء العراقي من هذه الجريمة؟

رابعاً: خطة البحث

لغرض الإحاطة بهذا الموضوع سنقسم البحث على مبحثين لبيان مفهوم الجريمة وأنواعها، موقف السياسة الجنائية منها، على أن تبقهما مقدمة وتليهما خاتمة متضمنة عدة نتائج وتوصيات.

المبحث الأول

ماهية الجريمة السيبرانية

الجريمة لغة هو التعدي أو الذنب، والجريمة هي ظاهرة إنسانية أزلية تختلف في أشكالها وأنماطها عبر الزمن لكنها تتوحد في كونها تمثل عملاً غير مشروع يمثل عدواناً على مصلحة إنسانية جديرة بالحماية والاعتبار القانوني[1].

وتعد ظاهرة الجرائم في البيئة الالكترونية بشقيها (الحاسب الآلي والتشبيك الاتصالي (الانترنيت) ظاهرة إجرامية مستجدة رافقت نشوء ونماء وتطور نظم الحاسب الآلي والشبكات وثورة تكنولوجيا الاتصالات والمعلوماتية، ورغم الفوائد الجمة في مجال التقدم التكنولوجي أصبح استخدامها منطوياً على مخاطر كبيرة وكان تقاناتها حافزا لتطور العقلية الإجرامية البشرية والتي أفرزت نوع جديد من الإجرام يطلق عليه الإجرام السيبراني[2]. وعليه سنقسم هذا الموضوع على مطلبين كالآتي:

المطلب الأول

مفهوم الجريمة السيبرانية

لغرض الإحاطة بماهية الجريمة السيبرانية، سنقسم هذا المطلب على فروع، سنبين في الفرع الأول نشأة الجريمة السيبرانية، في حين سنتناول الفرع الثاني تعريفها، وآخرهما لبيان عناصرها وكما يلي:

الفرع الأول

النشأة التاريخية للجريمة السيبرانية

مرت الجرائم السيبرانية بتطوُّر تاريخي بدأ من اختراع الحاسوب عام 1946 وإنشاء الشبكة العنكبوتية وصولاً إلى الثورة العالمية في الاتصالات والتكنولوجيا، وبحكم هذا التطور تطورت الجريمة بشكل عام والجريمة السيبرانية بشكل خاص ويمكن ملاحظة ثلاث مراحل لتطورها:المرحلة الأولى وتمتد من مرحلة ظهور الإنترنت ولغاية بداية السبعينيات حيث اقتصرت الجرائم على العبث بالبيانات المخزَّنة أو تدميرها، أو تدمير أنظمة الحاسوب للأفراد والمؤسسات الخاصة والعامة.وتمتد الثانية حتّى التسعينيّات مع بروز مفهوم جديد لجرائم المعلوماتية، وهو اقتحام نظام الحاسوب عن بعد ونشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج أو سرقتها. وظهر المقتَحمون أو ما يسمى ''الهاكرز ''وأصبحوا أداة إجرام، وظهرَ أيضًا أشخاص متفوّقون ولكن أصحاب نوايا إجرامية خطيرة وقدرة على الاستيلاء على المال، والتجسس، والاستيلاء على البيانات السرية الاقتصادية، الاجتماعية، السياسية والعسكرة. ومن التسعينات وحتى يومنا، وعرفتْ هذه المرحلة تناميًا هائلاً في حقلِ الجرائم الإلكترونية وتَغييرًا في نطاقِها ومفهومِها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيلٍ لعمليَّات دخول الأنظمة واقتحام شبكة المعلومات[3].

وظهرت أنماط جديدة توقيف الخدمة الَّتي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وجرائم نشر الفيروسات عبر المواقع الالكترونية لسهولة انتقالها إلى ملايين المستخدمين في الوقت نفسه، كما ظهرت الرَّسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على إثارة الكراهية، والتمييز العنصري والديني، الأحقاد، والمساس بكرامة الأشخاص، بالإضافة إلى ترويج لمواد غير قانونيَّة أو غير مشروعة. وأخيراً الترويج للإرهاب بكافة أشكاله: نشر الأفكار الإرهابية، الترهيب، التطويع، الدعاية، التدريب على صنع المتفجرات واستعمال الأسلحة المختلفة وغيره من الأعمال المشبوهة[4].

الفرع الثاني

التعريف الجريمة السيبرانية

جريمة معلوماتية أو جريمة سيبرانية أو جريمة الفضاء الإلكتروني (بالإنجليزية: Cybercrime تشير إلى أي جريمة تتضمن الحاسوب أو الشبكات الحاسوبية، إذ يستخدم الحاسوب في ارتكاب الجريمة، وهي جريمة حديثة ،نظراً لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة هذه الجريمة فقد تباينت التعاريف التي تناولتها في مضامينها وفي صياغاتها، ومصطلح الجرائم السيبرانيةcrime cyber هو مصطلح غير عربي، لكنه

هو المتداول والمستخدم حديثاً في وقتنا الحالي في هيئة الاتصالات وتقنية المعلومات وكذلك في المؤتمرات والندوات[5].

واصطلاحا عرف الفقه القانوني بتعريفات عدة ؛ فمنهم من نظر إليها من خلال وسيلة ارتكابها ومنهم من خلال موضوعها، ومنهم من خلال توافر المعرفة بتقنية المعلومات ووجهات نظر مختلفة"، إذ عرفت بأنها "تلك التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما" أو أنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[6].

كما عرفت بأنها "كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالباً ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات" أو أنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جريمة محلة معطيات الكمبيوتر"[7]. خبراء منظمة التعاون الاقتصادي والتنمية حيث عرفتها بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها حيث اعتمد على معيار السلوك إضافة إلى وسيلة ارتكاب الجريمة"[8].

ويتبين من هذه التعريفات المذكورة أن الجريمة السيبرانية تشمل جميع الأنشطة غير القانونية التي تنفذ باستخدام التكنولوجيا. ويستخدمها مجرمو الإنترنت، والذين يتفاوتون بين أفراد مارقين أو جماعات الجريمة المنظمة والفصائل التي ترعاها الدول، ويستخدمون تقنيات مثل الخداع والهندسة الاجتماعية وجميع أنواع البرمجيات لتنفيذ مخططاتهم الضارة إذ تشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، الأمر الذي يؤدي نحو تطور أدوات الجريمة الإلكترونية وارتكبها بطرق أكثر تعقيداً أو أشد ضرراً من قبل، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم واستحداث خطوط دفاع وسن قوانين لغرض توعية الناس بأنواع هذه الجرائم وحثهم على الإبلاغ عنها، فمجرمو الإنترنت يتنوعون بين الأفراد إلى المنظمات الإجرامية إلى الجهات الفاعلة التي ترعاها الدولة تماماً كما يختلف نوع المجرم ، كذلك تختلف جرائمهم والأساليب التي يستخدمونها لخرق القانون، فمثلاً المتطفلين الذين تمكنوا من اختراق سوق الأسهم الأمريكية إلى المجموعات التي ترعاها دولة كوريا الشمالية التي نشرتها وتطالب الضحايا بدفع الفدية على نطاق واسع ، وهناك عدد هائل من مجرمي الإنترنت الذين ينشطون يوميًا. علاوة على ذلك، لم يعد من المهم أن يكون المجرم الالكتروني خبيراً حتى يبقى متصلاً بالإنترنت[9]

وصفوة القول أن الجريمة السيبرانية مصطلح شامل لجرائم الحاسوب، ويشمل مختلف أشكال الجريمة، منها العنف الجنسي (الابتزاز الإلكتروني) أو الجرائم بحق الممتلكات (كالمتاجر الزائفة) أو جرائم العنف (مثل التنمر الإلكتروني،

والمطاردة الإلكترونية)، ويمكن تعريفها بأنها " كل فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا

الفرع الثالث

سمات الجريمة السيبرانية

الأصل أن التطور في مجال المعلوماتية أدى إلى ظهور أنواع جديدة من الجرائم وتمارس بمظاهر مختلفة منطوية على إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني عامة، وعلى الاستثمارات الكبيرة في قطاع المعلوماتية خاصة، الأمر الذي يحد من جدواها بسبب القرصنة التي تهدم ما تشيده، لذا هنالك ثمة سمات تتوافر بالجريمة السيبرانية أبرزها ما يأتي:-

أ- جرائم صعبة الإثبات: كون الجاني يستخدم وسائل فنية معقدة وسريعة في العديد من الأحيان قد لا تستغرق أكثر من بضع ثواني، فضلاً عن سهولة محو الدليل والتلاعب فيه والأهم عدم تقبل القضاء في الكثير من الدول للأدلة التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس الطبيعية للإنسان، أي بمعنى سهولة ارتكاب الجريمة بعيداً عن الرقابة الأمنية، كونها ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون أن يراه أحد أو يكتشفه، فهي جرائم ناعمةSOFT CRIME وأطلق عليها البعض اسم جرائم الياقات البيضاء، وعند توفر التقنية اللازمة للجاني يصبح ارتكاب الجريمة من السهولة بمكان ولا تحتاج إلى وقت ولا جهد[10].

ب-صعوبة التحكم في تحديد حجم الضرر الناجم عنه قياساً بالجرائم الإلكترونية فالجرائم الالكترونية تتنوع بتنوع مرتكبيها وأهدافهم، ومن ثم لا يمكن تحديد حجم الأضرار الناجمة عنها، بالإضافة إلى سهولة إتلاف الأدلة من قبل الجناة، فالمعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهي عبارة عن نبضات إلكترونية غير مرئية مما يجعل أمر طمس ومحو الدليل أمر سهل[11].

ج-تعد أقل عنفاً في التنفيذ فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، لأن المجرم عند تنفيذه لمثل هذه الجرائم لا يبذل جهداً فهي تطبق على الأجهزة الإلكترونية وبعيداً عن أي رقابة مما يسهل القيام بها، لذا فأن مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعباً أعمارهم تتراوح غالباً ما بين 18 إلى 48 سنة)[12]، وعادةً ما يكون المجرم متمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات وكسر الشفرات وكلمات المرور، وتخزين البيانات والمعلومات والتحكم في أنظمة الشبكات،كما أنه يتميز بأنه فرد ذو مكانة في المجتمع من أصحاب الوظائف الحيوية[13]، سواء في القطاع الخاص أوفي القطاع العام، وقد أطلق عليهم

مصطلح ذوي الياقات البيضاء، لذا فأنها تنطوي على سلوكيات غير مألوفة عن المجتمع. وبسبب استخدام هذه الوسائل المتطورة في ارتكاب الجرائم وامتداد آثارها الضارة على مستوى العالم، فقد أدى ذلك إلى قلق المجتمع الدولي ، لما لهذه الظاهرة من انعكاسات خطيرة على المجتمعات بالإضافة إلى تهديدها لاستخدامات هذه التقنيات في الأغراض المشروعة[14].

د–جرائم عابرة للدول: وهي الجرائم التي تقع بين أكثر من دولة ولا تعترف بالحدود الجغرافية مثلها مثل جرائم غسيل الأموال والمخدرات وغيرها. ففي عصر الحاسوب والانترنت أمكن ربط أعداد هائلة من الحواسيب عبر العالم، وعند وقوع جريمة الكترونية عادةً ما يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر في بلد ثالث، وبذلك تعد جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[15].

المطلب الثاني

أنواع الجرائم السيبرانية

تتنوع صور هذه الجرائم نظراً لاختلاف محل ارتكابها والهدف منه بالإضافة إلى اختلاف شخصية المجني عليه، ومن هذه الأنواع الآتي:

1– **الاعتداء على حرمة الحياة الخاصة:** ويتمثل إما بالإفشاء العلني للمعلومات الخاصة المتعلقة بحياة الشخص كإفشاء واقعة إصابته بمرض، أو يتعلق بالوضع المالي له كالإفلاس والعجز عن سداد ديونه أو نشر صور لغرض تشويه سمعة الشخص والتشهير به، أو تتمثل بالاستيلاء على البيانات الشخصية كالاسم والصورة، فمن القضايا الأكثر شهرة في مجال الجرائم الإلكترونية على مستوى العالم هو طلب دفع الفدية والابتزاز الإلكتروني، التي تنطوي على تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية. وعادة ما يتم تصيد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعي المختلفة كالفيس بوك، تويتر، وإنستغرام وغيرها من وسائل التواصل الاجتماعي نظرًا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع. وتتزايد عمليات الابتزاز الإلكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الاجتماعي والتسارع المشهود في أعداد برامج المحادثات المختلفة[16].

باختراق أجهزة أشخاص وحصلوا من خلال تلك " أي في هذا النوع من الجرائم يقوم المجرمين الإلكترونيين"الهكرز الأجهزة على معلومات حساسة أو وثائق سرية أو وسائط متعددة ثم قاموا بنسخ تلك البيانات إلى أجهزتهم وابتزاز أصحابها بمبالغ مادية حتى يقوموا بإعادة تلك المعلومات لهم، أو حتى يقوموا بعدم نشرها على الانترنت.

2- الاعتداء على حقوق الملكية الفكرية

وتتمثل بالجرائم المتعلقة بحقوق الملكية الفكرية في مجال الحاسب الآلي التي تمس ما يعرف بالمصنفات الالكترونية ومنها، أفعال النسخ وتقليد البرامج والمعلومات وإعادة إنتاجها وضعها دون ترخيص.

3-الجرائم التي تستهدف مراكز معالجة وخزن المعطيات،لغرض استغلالها بطريقة غير مشروعة، كجرائم الاستيلاء على أرقام بطاقات الوفاء الممغنطة، أو بطاقات الائتمان الالكترونية أو بطاقات الصرف الآلي، وتشمل الجرائم الماسة بالمصارف والمؤسسات المالية وذلك من خلال الحصول على المعلومات المالية للمصرف أو المعلومات المتعلقة بالمركز التجاري لها، كالبيانات المالية والوظيفية التي تحتوي على معلومات عن دخل الفرد الشهري[17]، والاتفاقات المالية المبرمة من قبلهن الديون في ذمتهن الوضع المالي، السمعة المالية لدى المصارف والمؤسسات أو اختراق المعلومات الشخصية المخزنة في ذاكرة الحاسبات الآلية للمصارف والمؤسسات المالية، وقد تهدد هذه الاعتداءات سرية الحياة الخاصة،كبيانات السيرة الاجتماعية والصحية والسياسية المتعلقة بمكانة الفرد وارتباطاته ومكانته الاجتماعية والعاطفية وحياته السياسية ووضعه الصحي والجسدي والعقلي[18].

المبحث الثاني

السياسة الجنائية للدول في الجرائم السيبرانية

إن من أهم التطورات التي شهدتها المجتمعات هو ظهور عالماً افتراضياً لا سيطرة مطلقة عليه لأحد، إذ أن أطرافه جيوش إلكترونية تحشد وتستنفر، ولجان إلكترونية أمنية تراقب وتتعقب، ومخبرون ومتسللون ومجرمون وجواسيس، وسباق تسلح محموم بأحدث ما توصلت إليه التقنيات الرقمية والتكنولوجية، ووحدات اقتحام، وأهداف تُضرب، وجبهات تشتعل، ومنصات رقمية تؤثر على الرأي العام وتوجهه، ومعلومات سرية تتسرب، وحقوق تنتهك، وأموال تغنم، وقراصنة يتقاسمونها، وخسائر في العدة والعتاد وربما الأرواح، وأدت هذه الهجمات السيبرانية إلى إلحاق أضراراً مادية ومعنوية، كما خلفت أزمات سياسية[19].

والسياسة الجنائية تتمثل بمجموعة القواعد والمبادئ التي تتحدد على ضوئها صياغة نصوص القانون الجنائي سواء فيما يتعلق بالتجريم أو الملاحقة أو الوقاية والمعالجة[20]، إذ إن تحقيق مبادئ السياسة الجنائية لظاهرة معينة إنما تقتضي في بداية الأمر رصد هذه الظاهرة ودراستها بصورة مستفيضة بحيث تتوافر جميع المعلومات المحيطة بها . ومن ثم تحديد ملامح الحماية القانونية لهذه الظاهرة، بحيث يتم استظهار المصالح التي تدور في فلك تقنينها، وذلك

كله وصولا إلى تحديد النقص في نصوص التجريم التي يمكن من خلالها إسدال ستار الحماية الجنائية على تلك المصالح المعتبرة والجديرة بالحماية، وذلك كله مع الأخذ بعين الاعتبار أسباب الوقاية والمنع [21]. وعليه سنقسم هذا المبحث على مطلبين.

المطلب الأول

دور التعاون الدولي في مكافحة الجرائم السيبرانية

تؤدي التدابير القانونية دوراً رئيسياً في منع الجريمة السيبرانية ومكافحتها، وهذه التدابير ضرورية في جميع المجالات بما في ذلك التجريم، والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي لتحديد المسؤولية ، ويُعد التعاون الدولي في مجال مكافحة الجرائم السيبرانية ضرورة ملِحة تفرضها التحديات والتطورات العالمية الراهنة خصوصاً بعد تنامي حجم الإرهاب السيبراني العابر للحدود، حتى لا يفلت مرتكبو هذه الجرائم من العقاب، وتتعدد أوجه التحديات والعوائق التي تُصعب من إمكانيات التعاون الفعال بين الدول بغرض مجابهة ذلك الخطر الداهم الحديث، الذي يهدد الدول والهيئات والشركات وغيرها تهديداً خطيراً ومباشراً[22].

والجدير بالذكر أن اختلاف النظم القانونية وقواعد الاختصاص للدول التي تطمح إلى تحقيق التعاون فيما بينها في مجال مكافحة الجرائم الإرهابية السيبرانية، عقبةً كبيرةً تحول في معظم الحالات دون تحقيق غايات وأهداف الدول خاصة عندما لا تواكب بعض الدول التطورات الهائلة الحاصلة في أنواع الجرائم المعقدة، نظراً لعدم إصدارها التشريعات المتطورة التي تلاحق الثورة الكبيرة في مجال استخدام الحاسوب وشبكات المعلومات العالمية في ارتكاب جرائم الإرهاب السيبراني على وجه الخصوص، مما يؤدي إلى البطيء في التعاون القضائي الدولي في مجال مواكبة التطورات السريعة الحاصلة في الجريمة السيبرانية من ناحية، ومن ناحية أخرى اختلاف العادات والتقاليد والديانات والثقافات في المجتمعات، ومن ثم اختلاف الدول في تحديد المصطلحات وتكييفها للجريمة السيبرانية، مما يشكل عائق أمام إجراءات التعاون الدولي، ويُعيق من تأطير آليات التعاون القضائي المختلفة لمكافحة هذه الجريمة الخطيرة، وهنا يفلت الجناة بجرائمهم من العقاب، وتُهدر حقوق ضحايا الجرائم المعلوماتية في أن يحصلوا على حقوقهم ورد اعتبارهم[23].

ويتمثل التعاون الدولي من خلال إبرام الاتفاقيات الدولية لغرض الوقاية والحد من جرائم الانترنت والتعاون القضائي من خلال المساعدة القضائية وتسليم المجرمين وعدم إفلاتهم من العقاب، ومنها اتفاقية بودابست 2001 لمكافحة الجرائم المعلوماتية التي أكدت على توحيد التدابير التشريعية بين الدول للوقاية من هذه الجرائم، فضلاً عن ضرورة تفعيل خطة العمل على الجانب الموضوعي والإجرائي للحد من هذه الظاهرة لغرض تأكيد أهمية التعاون

الإقليمي والدولي للوقاية من هذه الجرائم، كما نصت على ضرورة ملائمة التدابير الإجرائية التقليدية من قبل البحث والضبط والبيئة التكنولوجية الجديدة ولذلك تم وضع مجموعة من التدابير الإجرائية الجديدة من أجل الحفاظ على فعالية التدابير التقليدية لجمعها كالبحث والضبط في البيئة التكنولوجية المتقلبة[24] لذلك نجد أن اتفاقية بودابست اهتمت بالجانب الإجرائي حيث وضعت القواعد تتعلق بالبحث و التحري والتعاون الدولي[25] ، لذا جاءت المادة (22) من اتفاقية بودابست بمجموعة من المعاير التي تحدد صلاحيات الدول المنخرطة فيما يتعلق بالاختصاص القضائي عند ارتكاب أحد الجرائم الواردة في الاتفاقية وأكدت أنه في حال مطالبة أكثر من دولة طرف بالولاية القضائية على جريمة تقرها هذه الاتفاقية على دول الأطراف المعنية، الأخذ بمبدأ التشاور بغرض تحديد الولاية القضائية الأنسب ، فضلاً عن تأكيدها نظام تسليم المجرمين فيما بين الدول الأطراف بالاتفاقية من خلال تحديد القواعد الواجب إتباعها في تسليم المجرمين، وسبل تعزيز الحماية من الجرائم التقليدية المعلوماتية وأيضاً بينت طرق ربط الاتصال بين الدول الأعضاء من خلال النص على أن لكل دولة نقطة اتصال تعمل باستمرار على مدار 24 ساعة وطيلة أيام الأسبوع، وذلك بهدف ضمان وتقديم المساعدة الفورية والفعالة أثناء التحقيق في الجرائم المرتبطة بنظم وبيانات إلكترونية، أو جمع الأدلة ذات الطابع الإلكتروني عن هذه الجرائم[26].

كما أكدت اتفاقية بودابست على ضرورة التوفيق بين مكافحة الجرائم الإلكترونية واحترام حقوق الإنسان، من خلال إلزام الدول الأطراف في الاتفاقية بتقديم المساعدات المتبادلة فيما بينها إلى أقصى حد ممكن وذلك لأغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التي لها علاقة بنظم وبيانات الكمبيوتر أو بالنسبة بتجميع الأدلة الخاصة بالجريمة في شكل إلكتروني. فاتفاقية بودابست جاءت بمجموعة من الإجراءات فيما يخص التعاون الدولي بحيث يمكن لدولة أن تطلب من دولة أخرى أن تأمر أو تفرض حماية سريعة للبيانات المخزنة في نظم معلوماتية داخل حدود الدولة التي طلب منها ذلك، وذلك لتسهيل عمليات البحث والحفاظ على تلك البيانات المخزنة[27].

كما نجد أن القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية لعام 2003 ألزمت الدولة بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات إلا أنه لم يعين أي جهة تتولى عملية الضبط القضائي في جرائم السيبرانية مما يعني ترك المجال مفتوحا للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادرة على اكتشاف ومتابعة تلك الجرائم لذلك فعلى كافة الدول أن تأخذ بعين الاعتبار التداعيات السلبية التي تنشأ عن القصور التشريعي في مجال مجابهة هذا النوع من الجرائم الخطيرة، وتُبادر من فَورها بتجريم الأفعال الإرهابية السيبرانية عن طريق إصدار التشريعات الوطنية الملائمة، والتشريعات الجنائية التي تمنع محاولات مرتكبي هذه الجرائم من الإفلات من العقاب، بالإضافة إلى مراجعة وإعادة النظر في التشريعات المختلفة

السارية في ذلك الصدد وتعديل ما تفرضه مستجدات التطور المتلاحقة والمستمرة للجرائم الإرهابية السيبرانية، والنص عليها في الاتفاقيات الدولية سواء الثنائية أم المتعددة الأطراف.

المطلب الثاني

موقف المشرع العراقي من الجرائم السيبرانية

إن واقع الجرائم الالكترونية في العصر الحديث فرض ذاته في مجال التشريعات والمجال القضائي بغالبية دول العالم ،إذ لا يوجد تشريع خاص بالجرائم الالكترونية في العراق إلا أن هذا الموضوع ونتيجة ضغط الواقع أصبح حائزاً على اهتمامات كل القطاعات الناظمة للشأن التشريعي والإداري والاقتصادي في العراق[28] .

إلا أن هذا الاهتمام مازال يبارح مرحلة المحاولات التي تهدف للوصول إلى صياغة أطر قانونية حديثة تقوم بتحقيق المواجهة الفاعلة للجرائم الالكترونية. فبالنسبة للتجريم المطبق في العراق فإن المواجهة تقتصر على قواعد قانون العقوبات رقم 111 لسنة 1969 بحيث يتم تطويع هذه النصوص والمفاضلة فيما بينها لتنطبق على السلوك المخالف لتخدم قطاع العدالة في معاقبة مرتكبي هذه الجرائم، التي قد لا تؤدي الغرض منها في مواجهة هذا السلوك سواء كان ذلك بسبب عدم التكييف القانوني السليم لهذا السلوك، ومن ثم إفلات المجرم من العقاب أو بسبب عدم كفاية العقوبة المقررة وعدم تناسبها مع حجم الفعل والضرر اللذَينِ تحققاً[29].

إذ يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكمبيوتر والانترنت عن طريق إسقاط نصوص قوانين العقوبات السارية في العراق، مثل نصوص الابتزاز والنصب ونصوص السرقة والإتلاف والتزييف وتقليد الأختام والتزوير وخيانة الأمانة والسب والقذف والتشهير وإفشاء الأسرار والحض على الفجور، بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكمبيوتر أو شبكة الانترنت، وهذه النصوص تعد قاصرة عن الوفاء بالغرض، الأمر الذي يدعو إلى استحداث نصوص قانونية تجرم هذه الجرائم، ذلك أن نصوص هذه الجرائم تنطبق عندما يكون الكمبيوتر وسيلة لارتكاب السلوك وفي بعض الأحيان عندما تقع على الكمبيوتر ذاته إلا أن المجرم في كثير من الأحيان يفلت من العقاب بسبب عدم وجود النص التشريعي المناسب للتجريم .

وباعتبار أن العراق لم يقر قانون مكافحة الجرائم الالكترونية لسنة 2019 لحد الآن على الرغم من كثرة تكرار حالات مخالفات الأمن السيبراني وخاصة جرائم الابتزاز الالكتروني، إذ حدد في الفصل الثالث من مشروع القانون المذكور والمخصص لإجراءات جمع الأدلة والتحقيق والمحاكمة، بأنه لمجلس القضاء الأعلى تأسيس محاكم مختصة للنظر في الدعاوى الجزائية المتعلقة بالجرائم الالكترونية، بحيث يختص بالنظر في الجرائم المنصوص عليها في هذا القانون قاضٍ أو أكثر من ذوي الخبرة والاختصاص وممن تلقوا تدريباً متخصصاً في مجال الجريمة الالكترونية،

ونص في المادة (12) منه بأن ((تتولى جهات التحقيق إجراء التحقيق وجمع الأدلة وطلبها من مصادرها في الجرائم المنصوص عليها في هذا القانون))، لذا أكد بأنه لا يجوز لجهات التحقيق المباشرة بإجراءات التحقيق والتفتيش دون أمر قضائي يصدره القاضي المختص، على أن يتولى قاضي التحقيق أو المحقق المباشرة في إجراءات الضبط وجمع الأدلة أو أي إجراء تحقيقي نص عليه قانون أصول المحاكمات الجزائية النافذ.

كما أن قانون العقوبات العراقي النافذ لم يعالج هذه الجريمة كونها من الجرائم المستحدثة و لم يبق القضاء العراقي مكتوف الأيدي أمام جريمة الابتزاز الالكتروني بسبب عدم وجود قانون يعالج الجرائم المعلوماتية والالكترونية كما فوت الفرصة على المبتزين من استغلوا الفراغ التشريعي أو أن يتمسكوا بقاعدة لا جريمة ولا عقوبة إلا بنص[30].

لذا كان للقضاء العراقي الدور الحازم في معالجة هذا الخلل وفقاً لأحكام المواد 430 و 433 و 437 و 452 من قانون العقوبات العراقي التي تشمل جرائم التهديد والتشهير وانتهاك حرمة الحياة الخاصة وإفشاء الأسرار والسب والشتم من ابتزاز النساء والأطفال والرجال، ويكون الدوافع وراء ارتكاب جريمة الابتزاز الالكتروني قد تكون جنسية أو الابتزاز المالي أو الانتقام، لذا نرى من الضروري تشريع قانون لمكافحة جريمة السيبرانية وعدم الاكتفاء بما ورد في قانون العقوبات العراقي واعتبارها من جرائم الحق العام وذلك لكونها من الجرائم الخطيرة على الأسرة والمجتمع، ذلك أن المجتمع العراقي كغيره من المجتمعات من المتضررين من شيوع الجرائم السيبرانية، فلا بد من التصدي لهذه الجرائم من خلال وسائل الدفاع الاجتماعي المتعددة والتي من ضمنها الحماية القانونية الجزائية التي تعد من أهم وسائل المجتمع في الحفاظ على ذاته ومصالحه، الأمر الذي يتطلب الإسراع في وضع الأطر القانونية السليمة والمرجعيات الإجرائية الواضحة لمكافحة هذا النوع الخطير من الجرائم.

الخاتمة

أولاً : النتائج

1- أن الجريمة السيبرانية مصطلح شامل لجرائم الحاسوب، ويشمل مختلف أشكال الجريمة، منها العنف الجنسي (الابتزاز الإلكتروني) أو الجرائم بحق الممتلكات (كالمتاجر الزائفة) أو جرائم العنف (مثل التنمر الإلكتروني، والمطاردة الإلكترونية)، ويمكن تعريفها بأنها " كل فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا

2- الأصل أن التطور في مجال المعلوماتية أدى إلى ظهور أنواع جديدة من الجرائم وتمارس بمظاهر مختلفة منطوية على إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني عامة، وعلى الاستثمارات الكبيرة في قطاع المعلوماتية خاصة، الأمر الذي يحد من جدواها بسبب القرصنة التي تهدم ما تشيده،

3- للقضاء العراقي الدور الحازم في معالجة هذا الخلل وفقاً لأحكام المواد 430 و 433 و 437 و 452 من قانون العقوبات العراقي التي تشمل جرائم التهديد والتشهير وانتهاك حرمة الحياة الخاصة وإفشاء الأسرار والسب والشتم من ابتزاز النساء والأطفال والرجال، ويكون الدوافع وراء ارتكاب جريمة الابتزاز الالكتروني قد تكون جنسية أو الابتزاز المالي أو الانتقام، لذا نرى من الضروري تشريع قانون لمكافحة جريمة السيبرانية وعدم الاكتفاء بما ورد في قانون العقوبات العراقي واعتبارها من جرائم الحق العام وذلك لكونها من الجرائم الخطيرة على الأسرة والمجتمع، ذلك أن المجتمع العراقي كغيره من المجتمعات من المتضررين من شيوع الجرائم السيبرانية، فلا بد من التصدي لهذه الجرائم من خلال وسائل الدفاع الاجتماعي المتعددة والتي من ضمنها الحماية القانونية الجزائية التي تعد من أهم وسائل المجتمع في الحفاظ على ذاته ومصالحه

4- تسعى الدّول والحكومات بشكلٍ واضح لغرض الحدّ من الجَرائم السيبرانية وآثارها عبر طُرقٍ كثيرة منها كفرضُ سياساتٍ دوليّة وعقوباتٍ كبيرة على مُرتكبي هذه الجَرائم، وتفعيل أحدث التقنيات والوسائل للكشفِ عن هويّة مُرتكبي الجرائم، فضلاً نشر التّوعية في المجتمعات حول الجرائم الإلكترونية ومَخاطرها، وتَعريف الأفراد بكيفيّة الحِفاظ على معلوماتهم وخصوصيّاتهم؛ كحساباتهم البنكية وبطاقاتهم الائتمانية، بالإضافة إلى إنشاء خطوط هاتفيّة ومؤسسات مُعيّنة تابعة للدّولة لغرض الإبلاغ عن الحالات التي تتعرّض لمثل هذا النّوع من الجرائم.

ثانياً: المقترحات

1- يتوجب على المشرع تعديل نصوص التّشريعات والقوانين بما يَتلاءم مع التّطورات التكنولوجية، لفرض قَوانين جديدة فيما يستجدّ من هذه الجرائم ، فضلاً عن تشريع قانون إجرائي يتضمن القواعد الخاصة بكيفية إجراء التحري والتفتيش والاستدلال والضبط في المجال الالكتروني وكذلك النص من خلاله على الأدلة الالكترونية وحجيتها في الإثبات، وتشكيل وحدة خاصة بالتحقيق في هذه الجرائم في مراكز الشرطة، مع إيجاد قضاء متخصص يمتلك التدريب اللازم للنظر في هذه الجرائم.

2- ضرورة إعداد كوادر بشرية من أفراد الضبط القضائي لديهم إمكانية التعامل مع الجريمة الالكترونية لما تتضمنه من بيانات دقيقة على الأجهزة الالكترونية وعدم التعامل معها بشكل فني دقيق سيؤدي إلى فقدانها، لاسيما وأن نوعية المجرم الالكتروني تختلف في أسلوبه الإجرامي عن المجرم التقليدي الذي يرتكب جريمته باستعمال أدوات مادية يسهل التعامل معها وضبطها والتحفظ عليها .

المصادر

أولاً : الكتب القانونية

1. د.أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة 1972.

2. بولين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت 2009.
3. تميم عبد الله سيف التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الرياض، 2016.
4. خالد الغثبر ومحمد القحطاني، أمن المعلومات بلغة ميسرة، ط1، جامعة الملك سعود، الرياض 2009.
5. عبد الفتاح بيومي حجازي، الجرائم المستحدثة، ط1، منشأة المعارف، الإسكندرية 2009.
6. علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، 2011 .
7. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، ط1، 2003.
8. د .محمود عمر محمود، الجرائم المعلوماتية والإلكترونية، خوارزم العلمية، 2015.
9. د.محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار النهضة العربية، القاهرة، ط1، 2003 .
10. محمد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر، عمان، 2002.
11. د. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة وللنشر والتوزيع، عمان، ط2، 2001.
12. د. نائلة معوض، جرائم الحاسب الآلي الاقتصادية، لبنان منشورات الحلبي الحقوقية، 2005.
13. هدى حامد قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992 .

ثانياً: الاطاريح الجامعية

1- د. تميم طاهر احمد، تنفيذ العقوبة وأثره في الردع الخاص، أطروحة دكتوراه، جامعة بغداد، 1994.

ثالثاً: البحوث والمقالات المنشورة

1. حليمة بن حفو، محاربة الجرائم الإلكترونية على الصعيد الدولي " الواقع و الآفاق، مجلة العلوم الجنائية، الإمارات، العدد الأول 2014 .
2. فهد وزاني الشاهدي، الحق في الحياة الخاصة أية حماية، مجلة المعيار، الأردن، العدد52، 2014.
3. د. هاشم محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب المتخصص، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، 2004.

4. يوسف قباج، خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية، منشور بمجلة المنارة مكتبة دار السلام الرباط، العدد 14، 2016.
5. يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، من 10 – 12 / 2 / 2003 .

رابعاً: الاتفاقيات الدولية

1. اتفاقية بودابست 2001 لمكافحة الجرائم المعلوماتية
2. القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية لعام 2003

[1]د. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة وللنشر والتوزيع، عمان، ط2، 2001، ص79.

[2] يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، من 10 – 12 / 2 / 2003 ، ص 5.

[3] عبد الفتاح بيومي حجازي ، الجرائم المستحدثة ، ط1، منشأة المعارف ، الإسكندرية 2009 ،ص1.

[4] د.محمد أمين الرومي ، مصدر سابق ،ص23.

[5] د. احمد فتحي سرور ، أصول السياسة الجنائية ، دار النهضة العربية ، القاهرة ، 1973 ، ص177.

[6]د. نائلة معوض ، جرائم الحاسب الآلي الاقتصادية ، لبنان منشورات الحلبي الحقوقية ، 2005 ، ص 98 وما بعدها .

[7]د. هاشم محمد فريد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب المتخصص ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ، ص 45 وما بعدها .

[8] د. تميم طاهر احمد ، تنفيذ العقوبة وأثره في الردع الخاص ، أطروحة دكتوراه ، جامعة بغداد ، 1994 ، ص152

[9]د. نائلة معوض ، مصدر سابق ، ص99.

[10]المجرم السيبراني هو مجرم يتمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات وكسر الشفرات كلمات المرور ، موظفا مهاراته تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات ، وهو على أنواع منهم الهواة : وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه . والقراصنة ، الهاكر ، المهووسون ، الجريمة المنظمة كون جهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا ، و الحكومات الأجنبية ، المتطرفون : من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية. ينظر: ميم عبد الله سيف التميمي ، الجرائم المعلوماتية في الاعتداء على الأشخاص ، مكتبة القانون والاقتصاد ، الرياض ، 2016، ص3.

[11]علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة ، المكتب الجامعي الحديث ، 2011 ، ص 3،

[12]ومن الجرائم التي ارتكبها صغار المجرمين مثلاً في ألمانيا تمكن طالب عمره تسعة عشر عاماً من نسخ وإفشاء بيانات حاسب آلي على نحو غير مصرح به ، مما أدى إلى خسارة هذه الصناعة في ألمانيا بمبلغ (23) ألف مارك ألماني واستفاد الجاني بمبلغ (26) ألف مارك . ينظر في ذلك عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، منشورات الحلبي الحقوقية ، ط1 ، 2003، ص 308

[13] وأنواع المجرم السيبراني هم :

1 الهواة : وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه .

2 القراصنة : هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أو اثبات الذات.

3 المهووسون : ويكون المجرم في حالة الجنون الذي يهدف إلى تحطيم كل الأنظمة .

4 الجريمة المنظمة : فجهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا .

5- الحكومات الأجنبية : وذلك باستعمال أجهزة الحاسب في مجال الجاسوسية .

6 المتطرفون : وهم من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة . ينظر: د .محمود عمرم حمود، الجرائم المعلوماتية والإلكترونية، خوارزم العلمية، 2015، ص24.

[14] د. نهلا عبد القادر المؤمني ، الجرائم المعلوماتية ، مصدر سابق ، ص79.

[15] د.محمد أمين الرومي ، جرائم الكمبيوتر والانترنت ، دار النهضة العربية ، القاهرة ، ط1 ، 2003 ،ص23.

[16] محمد الزعبي وآخرون ، الحاسوب والبرمجيات الجاهزة ، ط1 ، دار وائل للنشر ، عمان، 2002، ص5.

[17] هدى حامد قشوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة،1992 ، ص6.

[18] خالد الغثبر ومحمد القحطاني ، أمن المعلومات بلغة ميسرة، ط1، جامعة الملك سعود، الرياض 2009، ص7.

[19]محمد الزعبي وآخرون ، مصدر سابق ، ص32.

[20]د.أحمد فتحي سرور، مصدر سابق ، ص10.

[21] بولين أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت 2009،ص450.

[22]حليمة بن حفو، محاربة الجرائم الإلكترونية على الصعيد الدولي " الواقع و الآفاق ، مجلة العلوم الجنائية ، العدد الأول 2014 ص 203

[23] من أبرز القضايا المثيرة في تضارب المصالح بين الدول وغياب التعاون القضائي في ملاحقة أحد المواطنين البريطانيين بارتكاب الجرائم الإرهابية السيبرانية، حيث كان المتهم اخترق أنظمة الحاسوب للجيش الأميركي فضلا عن وكالة الفضاء الأميركية، وبعد مرافعات ومحاولات مضنية من جانب الإدارة الأميركية لتسليمه إليها لمحاكمته أمام القضاء الأميركي، رفضت تسليمه للولايات المتحدة ورفضت محاكمته أمام محاكمها.ينظر: فهد وزاني الشاهدي، الحق في الحياة الخاصة أية حماية ، مجلة المعيار العدد52، 2014، ص160.

[24]يوسف قباج، خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية، منشور بمجلة المنارة مكتبة دار السلام الرباط، العدد 14،2016، ص33.

[25]القواعد الخاصة بالبحث والتحري : إذ أن اتفاقية بودابست تحمل في طيتها العديد من المواد التي تخص الجانب الإجرائي وخصوصا فيما يتعلق بالبحث و التحري بحيث أنه يمكن عرض هذه القواعد في النقط التالية :

تفتيش وحجز بيانات الكمبيوتر المخزنة (المادة 19 من اتفاقية بودابست)

إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة (المادة 18 من اتفاقية بودابست)

سرعة التحفظ على البيانات المخزنة (المادة 17 من اتفاقية بودابست)

التجميع الفوري لبيانات الكمبيوتر وإمكانية اعتراض هذه البيانات (المادة 20 من اتفاقية بودابست)

[26] المادة (24) من اتفاقية بودابست.

[27]فهد وزاني الشاهدي، مصدر سابق، ص160.

[28] علي نعمة جواد الزرفي ، مصدر سابق، ص 3.

[29] د. تميم طاهر احمد ، مصدر سابق ، ص154.

[30] د. تميم طاهر احمد ، مصدر سابق ، ص155.