مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

تطوير السياسات العامة لمكافحة جرائم المعلومات: رؤية مستقبلية لأمن رقمي مستدام

م.م شهد عماد حميد

قسم القانون، كلية مدينة العلم الجامعة، بغداد، العراق

s9788762@gmail.com

المستخلص:

يستعرض هذا البحث آليات تطوير السياسات العامة لمكافحة جرائم المعلومات في إطار تعزيز الأمن الرقمي، ويهدف إلى تقديم رؤية مستقبلية لتحقيق بيئة رقمية آمنة ومستدامة للأفراد والمؤسسات. يتضمن البحث تحليلًا للوضع الراهن لجرائم المعلومات، بما في ذلك أنماطها وأسبابها وتأثيراتها على الأمن المجتمعي والاقتصادي.

ويؤكد البحث على أهمية اتخاذ خطوات عملية واستشرافية لتحسين السياسات العامة في هذا المجال، مع مراعاة التقدم التقني السريع وما ينطوي عليه من تحديات. ويوصي بتطوير أنظمة مرنة وقابلة للتكيف مع التهديدات المتجددة، بما يضمن استدامة الأمن الرقمي للأجيال الحالية والمستقبلية.

الكلمات المفتاحية:

سياسات عامة، جرائم معلوماتية، أمن رقمي، الاستدامة الرقمية

A Future Vision for Developing Public Policies to Combat Cybercrime: Sustainable Digital Security

Abstract

This research reviews the mechanisms for developing public policies to combat information crimes within the framework of enhancing digital security, and aims to provide a future vision for achieving a safe and sustainable digital environment for individuals and institutions. The research includes an analysis of the current status of information crimes, including their patterns, causes, and effects on societal and economic security .The research emphasizes the importance of taking practical and forward-looking steps to improve public policies in this field, taking into account rapid technological progress and the challenges it entails. It recommends developing flexible and adaptable systems to emerging threats, ensuring the sustainability of digital security for current and future generations .

Keywords:

Public policies, information crimes, digital security, digital sustainability

المقدمة

يشهد العالم اليوم ثورة علمية وتقنية كبيرة، بدأت منذ انطلاق الثورة الصناعية في النصف الثاني من القرن العشرين، وقد امتدت هذه الثورة لتشمل جميع جوانب الحياة، بما في ذلك مجال الحاسب الآلي، الذي أحدث نقلة علمية هائلة عند ظهوره. بات تقدم الدول وتطورها يعتمد بشكل كبير على تطور هذا

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

المجال، حيث أصبح الحاسب الآلي من أهم ابتكارات العصر الحديث، وساهم عبر مراحل تطوره في حل الكثير من المشكلات التي كان يصعب على الإنسان حلها بجهوده ووقته، مع ضمان أكبر لدقة النتائج. ومع تطور استخدام الحاسب، أصبح عنصراً أساسياً وفعّالاً في تقدم الأمم ومؤشراً على مستوى تحضرها. صاحب هذا التقدم تزايد الاعتماد على نظم المعلومات الآلية والتقنيات الحاسوبية في حفظ ومعالجة البيانات داخل المؤسسات الحكومية والخاصة، وحتى في حياة الأفراد اليومية.

من جهة أخرى، تأثرت الجريمة بشكل واضح بمراحل تطور المجتمع وتفاعلت مع معطياته، مما أدى إلى ظهور أنماط جديدة من الجرائم المرتبطة باستخدامات الحاسب. فالتغير الحضاري والتقدم التقني الذي اجتاح العالم في العصر الحديث أحدث تحولاً في طبيعة الجرائم ونوعية المجرمين؛ حيث كانت الجرائم سابقاً تعتمد على العنف والقوة، أما الآن فقد أصبحت قائمة على المهارات الذهنية والذكاء. وتعد شبكة الإنترنت من أبرز نتائج هذا التحول، فهي تمثل عالماً واسعاً بلا حدود جغرافية أو عوائق مادية، وساهمت في ظهور وتطور العديد من السلوكيات الإجرامية التي تؤثر بشكل كبير على حياة الأفراد والمجتمع.

أهمية البحث

تأتي أهمية البحث من زيادة استخدام نظم المعلومات في المجلات العلمية والاقتصادية والاجتماعية الى جانب استخدام الانترنت في زيادة جرائم نظم المعلومات فأصبحت جرائم نظم المعلومات متسعة النطاق باهظت التكاليف وصعبت الرصد والمعالجة وتشكل خطراً كبير على المجتمع الابد من دراستها ومعرفة الآثار والأسباب والجهود الدولية للحد من هذه الجريمة.

هدف البحث

يهدف البحث الى تسليط الضوء على جريمة بالغة الخطورة ظهرت مع ظهور التطور في تقنيات المعلومات والاتصالات تتميز بمجموعة من الخصائص اذ تعد جريمة عابرة للحدود صعبة الكشف والاثبات يتميز من يقوم بها بالذكاء والمهارة.

إشكالية البحث

تأتي إشكالية البحث من خلال مجموعة من التساؤلات:

١_ما هو مفهوم جرائم نظم المعلومات؟

٢_ ما هو مفهوم السياسات العامة؟

٣_ وهل توجد لهذا النوع من الجرائم اثار في ابرز مجالات الحياة؟

٤_وماهي الأسباب التي تدفع الارتكاب هذا النوع من الجرائم

٥_ وماهي الجهود الدولية للحد من هذا الجرائم؟

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

فرضية البحث

تكمن فرضية البحث بنتيجة مفادها ان تطوير السياسات العامة لمكافحة جرائم المعلومات سيسهم في تعزيز الأمن الرقمي المستدام، من خلال اعتماد استراتيجيات مرنة ومتجددة قادرة على مواجهة التحديات التقنية المستمرة والتكيف مع التهديدات المعلوماتية المتغيرة، مما يؤدي إلى حماية فعالة للأفراد والمؤسسات وتحقيق بيئة رقمية آمنة.

منهجية البحث

ان المنهج الذي تم اعتماده في اعداد هذا البحث هو المنهج الاستقرائي والمقربات التي تم اعتماده هو التحليل الوصفي

هيكلية البحث

تم تقسيم البحث الى ثلاث مباحث تضمن المبحث الأول : الاطار المفاهيمي للبحث

في حين تضمن المبحث الثاني : أسباب جرائم نظم المعلومات واثارها والمبحث الثالث : الجهود الدولية المكافحة لجرائم نظم المعلومات

المبحث الأول :الاطار المفاهيمي للبحث

تعد من ضروري الإحاطة بالأطر المفاهيمية للبحث العلمي، لأجل بيان أبرز المفاهيم والمصطلحات التي تخص موضوع البحث ، لذلك سيتم التطرق في هذا المبحث لمفهوم السياسات العامة ،وكذلك مفهوم جرائم نظم المعلومات وتطورها .

المطلب الأول : مفهوم السياسات العامة

السياسة في اللغة

نجد أنها لا تخرج عن المعاني التالية : الولاية، والرياسة والقيادة، والأمر والنهي، والرعاية وتدبير أمور الناس وإصلاحها، والقيام على الشيء بما يصلحه . بهذه المعاني كلها وردت كلمة السياسة ، كما هو مبين في القواميس والمعاجم اللغوية الرئيسة ويظهر ذلك في قول صاحب اللسان وغيره : (السوس : الرياسة، يقال ساسوهم سوساً، وساس الأمر؛ سياسة : قام به وسست الرعية سياسة وسوس الرجل امور الناس إذا مللك أمرهم وفي الحديث : « كان بنوا اسرائيل يسوسهم أنبياؤهم » أي تتولى أمورهم كما يفعل الأمراء والولاة بالرعية والسياسة القيام على الشيء بما يصلحه [١].

[١] ابن منظور لسان العرب ، ج٦ ، دار صادر بيروت ، ص ١٠٨.

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

السياسة في الاصطلاح

يختلف المعنى الاصطلاحي للسياسة تبعاً لاختلاف وجهات النظر فمن المفكرين من يرى أن السياسة : هي احتراف الحكم والسلطان، أي ممارسة السلطة. ومن المفكرين من يعرف السياسة : "بأنها فن الممكنات، أو فن الممكن، أو هم الممكن وإرادة الوصول، أو هي أفكار تتعلق برعاية الشؤون" ومنهم من يرى أنها التنفيذ العملي أو الإشراف على التنفيذ العملي لفلسفة معينة، أو هي العملي لمنظومة من المفاهيم والمعايير السلوكية المتعلقة بالإنسان في حياته . أو أنها : إجراءات لتحقيق القيم الدينية والاقتصادية والثقافية في سلوك الناس وعلاقاتهم ونظام حياتهم. ومنهم من يرى أنها : نظريات لتنظيم المجتمع وعلاقات البشر ، وفي الصدد يقول جورج بوردو : السياسة هي : (تقنية تحقيق القيم الدينية والاقتصادية والثقافية وفي موضع آخر ، يقول : السياسة : نظريات التنظيم الاجتماعي هي : النضال للسيطرة على السلطة هي : هم الممكن وإرادة الوصول هي إدارة المجتمع بالتوافق مع جوهره [٢]. ويقول محمد البهي إن السياسة في أصلها هي : إشراف على تنفيذ فلسفة معينة، وقد تكون احترافا بالحكم لذاته [٣].

يمكن تعريف السياسة العامة :

ان السياسة العامة التي تقررها وتنفذها الحكومة تتميز بالتنوع والشمول والتغلغل الذي يمس كافة جوانب الحياة في المجتمع وان من أهدافها تنظيم حياة الافراد وحل مشاكلهم و إجابة مطالبهم وان لهم مغزى ومعنى موضوعي يتعلق مباشرة بنوع ومستوى حياة الأفراد في المجتمع[٤].

عرفت السياسة العامة بأنها مجموعة أو سلسلة من القرارات تتعلق بمجال معين كالتعليم والصحة وغيرها وكأن السياسة هي بمثابة مرشد للقرارات الخاصة بمشكلة أو ميدان معين .

ويعرفها جيمس اندرسون "بأنها برنامج عمل مقترح لشخص أو جماعة أو حكومة في نطاق بيئة محددة لتوضيح الغرض المستهدف والمحددات المراد تجاوزها سعياً للوصول إلى هدف أو لتحقيق غرض مقصود"[٥]. لذلك فالسياسة العامة نتاج تفاعل ديناميكي معقد يتم في إطار نظام فكري بيئي سياسي محدد تشترك فيه عناصر رسمية وغير رسمية يحددها النظام السياسي وأهم هذه العناصر : دستور الحكم في الدولة أو فلسفة الحكم السلطة التشريعية، السلطة التنفيذية، السلطة القضائية، الأحزاب السياسية ، جماعات الضغط والمصالح، الصحافة والرأي العام والإمكانات والموارد المتاحة الطبيعية منها والبشرية أخذة في نظر الاعتبار طبيعة الظروف السائدة في هذا البلد .

---

[٢] بوردو (١٩٨٥). المعلم (سليم حداد) ، ، بيروت ، المؤسسة الجامعية للدراسات والنشر .ص ١٦٣.

[٣] محمد البهي(١٩٧٥)، ، بيروت . الفكر الاسلامي والمجتمع المعاصر. ص ٣٩٠.

[٤] القوي.(١٩٨٩) . دراسة السياسة العامة ذات السلاسل للطباعة والنشر ، الكويت ، ،ص ٣٥.

[٥] اندرسون(١٩٩٩) ، المعلم (عامر الكبيسي)، صنع السياسات العامة، عمان. دار الميسرة للنشر والتوزيع والطباعة ، ص ١٥

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

هناك مجموعة من **خصائص للسياسة العامة** يمكن أن نذكر منها

١_انها قرار تتخذه الحكومة بمعنى انها تختار اسلوبا معينا لتحقيق الاهداف المنشودة .

٢_أن السياسة العامة عملية ديناميكية حركية مستمرة دائمة التطور والتغير. والقرار يتميز بالثبات اي الدوام او عدم التغير نسبياً – مادامت السياسة العامة لم تتغير.

٣_ان تطبيق السياسة العامة عام شامل وبنفس الاسلوب على كل افراد المجتمع الذين تخدمهم هذه السياسة.

المطلب الثاني: مفهوم جرائم نظم المعلومات وتطورها التاريخي

اولا: مراحل تطور جرائم نظم المعلومات: مرت جرائم نظم المعلومات بتطور تاريخي حالها حال اي جرائم أخرى تبعاً لتطور هذه التقنية واستخداماتها . وقد مرت بثلاث مراحل

–**المرحلة الأولى:** بدات هذا المرحلة في الستينات والسبعينات استخدام الحواسيب واقتصرت على المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة، وتدمير أنظمة الكمبيوتر. وترافقت هذه المرحلة عده تساؤلات حول ما إذا كانت هذه الجرائم مجرد شيء عابر ام هي ظاهرة إجرامية مستحدثة؟ وما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية ؟ ومع تزايد استخدام الحواسيب الشخصية في السبعينات، ظهر عدد من الدراسات القانونية التي اهتمت بجرائم الكمبيوتر، وعالجت عدداً من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

–**المرحلة الثانية:** بدأت في الثمانينيات عندما ظهر مفهوم جديد لجرائم الكمبيوتر والإنترنت مرتبطا بالتطفل على نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تدمر الملفات أو البرامج. انتشر مصطلح (الهاكرز) ، معبراً عن متسللين على النظام ، لكن الحديث عن دوافع ارتكاب هذه الأفعال ظل محصوراً في رغبة المحترفين في تجاوز أمن المعلومات ، وإظهار تفوقهم التقني. لكن هؤلاء المغامرين أصبحوا أداة إجرامية ، وظهر مجرم المعلومات المتفوق بدوافع إجرامية خطيرة ، قادراً على ارتكاب أعمال تهدف إلى الاستيلاء على الأموال أو التجسس أو الاستيلاء على البيانات السرية (الاقتصادية والاجتماعية والسياسية والعسكرية).

–**المرحلة الثالثة** :شهدت التسعينات تنامياً هائلاً في حقل الجرائم الإلكترونية، وتغيراً في نطاقها و مفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل العمليات دخول الأنظمة، واقتحام شبكة المعلومات. وظهرت أنماط جديدة، تقوم على فكرة تعطيل نظام تقني، ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة، التي يتسبب انقطاعها عن الخدمة الساعات، في خسائر مالية بالملايين.. ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

إلى ملايين المستخدمين في ذات الوقت. وظهرت الرسائل المنشورة على الانترنت، أو المراسلة بالبريد الإلكتروني، المنطوية على إثارة الأحقاد أو المروجة للمواد غير القانونية، أو غير المشروعة[٦].وقد زادت معدلات هذه الجرائم في العقدين الأخيرين على وجه الخصوص بشكل أدى إلى ظهور ظاهرة إجرامية جديدة تعرف بجريمة المعلومات أو الجريمة الإلكترونية. استخدام الكمبيوتر على أساس البعد الأخلاقي وحتى الستينيات توسعت دائرة التعامل مع أنشطة إساءة استخدام الكمبيوتر من خلال وسائل الإعلام. منذ أول حالة موثقة عام ١٩٥٨ م الجريمة ارتكبت في الولايات المتحدة الأمريكية عن طريق الكمبيوتر وحتى الآن ازداد حجم هذه الجرائم وتنوعت أساليبها وتضاعفت اتجاهاتها وتضاعفت خسائرها وخسائرها. وزادت الأخطار حتى أصبحت مصادر لتهديدات خطيرة للأمن القومي للدول ، خاصة تلك التي ترتكز مصالحها الحيوية على تكنولوجيا المعلومات. وتعتمد عليها في تصريف شؤونها. لأن جريمة المعلومات من الظواهر الحديثة. ويرجع ذلك إلى ارتباطها بالتكنولوجيا الحديثة وتكنولوجيا المعلومات والاتصالات.

ثانيا: مفهوم جرائم نظم المعلومات :

قبل التطرق لمفهوم جرائم نظم المعلومات ان نميز ونتطرق لمفاهيم التالية: ان نعرف تقنية المعلومات تم استخدام المعلومات في السنوات الاخيرة على نطاق واسع بسبب التطورات التي حدثت في مجال تكنولوجيا المعلومات ويقصد بها علم المعلومات العلمية أو علم التعامل المنطقي مع المعلومات وفقا للقواعد و النصوص المنظمة وتنظيم استخدامها وعرفت تقنية المعلومات هي أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم التخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكي أو لاسلكي.

تعريف جريمة المعلومات كان محاطا بالكثير من الغموض حيث كانت هناك جهود كثيرة تهدف إلى وضع تعريف شامل لكن لم يتفق على وضع تعريف محدد لها. بل ذهب البعض إلى اقتراح عدم وضع هذا التعريف بحجة أن هذا النوع من الجرائم ليس جريمة تقليدية ترتكب بطريقة إلكترونية [٧].

اما **تعريف المجرم المعلوماتي** تحتاج الجرائم المعلوماتية كغيرها من الجرائم الى طرفين) جاني ومجني عليه (الا ان اطراف الجريمة المعلوماتية يختلفون نوعا ما عن اطراف باقي الجرائم. في جرائم المعلومات ، نحن لا نتعامل مع مجرم عادي ، بل مع مجرم يمتلك المهارات وعلى دراية بالتكتيكات المستخدمة في نظام الكمبيوتر. إن شخصية مجرم المعلومات ، سواء كانت طبيعية أو معنوية ، وآلية ارتكاب الجريمة ، تجعله شخصا يتسم بسمات خاصة تضيف إلى الخصائص الأخرى التي يجب أن

[٦] مريم عبد الرحمن، مفهوم الجريمة الالكترونية ومراحلها التاريخية(٢٠٢٠)
http://alhiwarmagazine.blogspot.com/2020/07/blog-post_10.html?m=1

[٧] سكيكر(٢٠١٠)، الجريمة المعلوماتية وكيفية التصدي لها،القاهرة. مطالع دار الجمهورية للصحافة .ص ١٢.

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

تتوفر في المجرم العادي. أهم ما يميز الشخص المذكور أن لديه خبرة في الأمور الإعلامية ومعرفة كافية بالية عمل الحاسب وتشغيله ، حيث أن جريمة المعلومات تنشأ من تقنيات التدمير الهادئ التي تتمثل في التلاعب بالمعلومات أو البيانات. هذا لا يعني أن العنف ضد نظام المعلومات يمكن تخيله. قد يكون موضوع الجريمة تدمير الكمبيوتر نفسه أو وحدة المعالجة المركزية. أي أن ما يمكن مهاجمته قد يكون هيكل أجهزة الكمبيوتر والمعلومات المنقولة عبر شبكة المعلومات.[٨]

سنتعرض فقط إلى ما تقدمه تكنولوجيات الإعلام الحديثة للمجرمين من مجالات سهلة وسريعة للقيام بارتكاب جرائم خاصة في الميدان الاقتصادي والمالي مثل : تخريب المعلومات، الابتزاز، تزوير العلامات التجارية – النصب والاحتيال – انتهاك الأسرار الاقتصادية – الرشوة

أولا : تخريب المعلومات وإساءة استخدامها : و هي من جرائم نظم المعلومات الهامة ، وهذا بالنظر للآثار التي تتركها على الجهات.

ثانيا : تزوير البيانات : وهذا إما بإدخال بيانات خاطئة إلى قواعد البيانات أو تعديل البيانات الموجودة.

ثالثا: التزييف : . وخاصة تزييف الوثائق وتقليدها، مثل تزييف الشيكات والبطاقات البنكية وهذه العمليات شائعة الاستعمال في الولايات المتحدة الأميركية مثلا.

رابعا : تزوير العلامات التجارية : تشكو بعض الشركات المنتجة لشرائح المعالجة المركزية ، من ظاهرة خطيرة تضر بمصالحها ، كما تضر بمصلحة المستهلك وهي تزوير العلامات التجارية على الشرائح ذات الأداء المنخفض ، وبيعها على أنها شرائح ذات أداء أعلى، بأسعار مرتفعة ترتكب هذه الجريمة سعيا وراء جني الأرباح ، وبحثا عن التفوق في المنافسة (غير الشرعية) يعتبر الكشف عن الجرائم المعلوماتية وتقييمها عملية صعبة في ضوء عدة عوامل منها عدم رد فعل المجتمع تجاه هذا النوع من الجرائم الخفية ، فضلاً عن عدم وجود إلزامية للضحايا لتقديم دعاوى للحصول على تعويضات عن الأضرار التي يتعرضون لها من قبل شركات التأمين على عكس الجرائم الأخرى مثل سرقة السيارات على سبيل المثال. تقوم شركات ترتد بإبلاغ السلطات أمنيًا أو قضائيا ، من خلال الإجراءات التي ترتكب ضدهم ، خوفا من كشف بعض نقاط الضعف في نظم المعلومات لديهم ، والإجرام ، الذي يرتكب في كثير من الأحيان دون أن يلاحظه ضحاياه . ويتضح من ذلك ان هناك علاقة الوثيقة والمترابطة بين جرائم الرشوة والاحتيال وغسيل المعلومات والجرائم الاقتصادية والمالية الدولية تكمل بعضها البعض وتستفيد من بعضها البعض.

[٨] شنيف، وتوحيدي، (٢٠٢٢).صور الجرائم المعلوماتية ومواجهتها بالتشريعات القانونية ،مجلة إكليل للدراسات الانسانية العدد١١ ،ص٢٦.

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

المبحث الثاني: أسباب جرائم نظم المعلومات واثارها

لكي نتعرف عن الاسباب التي تقف خلف ارتكاب جرائم نظم المعلومات واثارها سنقسم هذا المبحث الى مطلبين والذي ستخصص في المطلب الأول لأسباب جرائم نظم المعلومات اما المطلب الثاني فستناول الآثار الاقتصادية لجرائم نظم المعلومات

المطلب الأول: اسباب جرائم نظم المعلومات

مما لاشك فيه أن مرتكبي الجريمة المعلوماتية يختلفون عن مرتكبي الجريمة التقليدية ويعود ذلك الى اختلاف الاشخاص من حيث السن والجنس ، والمستوى التعليمي وغير ذلك من المؤثرات الخارجية كما ان الاسباب والدوافع هي ايضا تختلف في هذا المحور سنحاول بيان وتوضيح اهم الاسباب والدوافع التي تقف وراء ارتكاب هذه الجريمة والتي تشمل ما يلي :

١_**الرغبة في جمع المعلومات وتعلمها: والتي** تكون غاية المجرم الالكتروني فيها هو الحصول على الجديد من المعلومات والتي يقوم بها الأفراد القراصنة عندما يعلنون أن هدفهم من الوصول للمعلومات ودخولهم الشبكات والحواسيب الالكترونية هو التعلم فقط ويتم تقاسم المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في انشطة هادفة ولو بطرق غير مشروعة[٩].

٢_**الرغبة في اثبات الذات والتفوق على تطور وسائل التقنية :** في بعض الاحيان يكون وراء ارتكاب هذه الجرائم هو اثبات قدرة الجاني وتفوقه على تعقيدات وتطورات وسائل التقنية الحديثة اذ يمضي كل وقته امام شاشات اجهزة لكسر الحواجز الأمنية للأنظمة الالكترونية ليثبت براعته في القدرة على تحدي اي تطور جديد في عالم التقنية والتكنولوجيا[١٠] .

٣_**تحقيق الربح والمال :** يعد دافع الثراء والحصول على الأموال من اهم الدوافع والاسباب التي تقف وراء جرائم نظم المعلومات نظرا للربح الكبير الذي يحصل عليه المجرم من وراء جريمته والذي يقوده الى الاستمرار في تنفيذ جرائمه مستغلا الفرص المتاحة وتحقيق اعلى المكاسب باقل جهد ودون اثر يكشف جريمته.

٤_ **الحاق الأذى بأشخاص أو جهات** حيث تكون الغاية من هذه الجرائم الالحاق الضرر بأشخاص محددين او جهات معينة اذ غالبا ما تكون تلك الجرائم مباشرة متمثلة بصور ابتزاز، تهديد، تشهير، او تمارس بصورة غير مباشرة من خلال الحصول على البيانات والمعلومات الخاصة بتلك الجهات او الاشخاص لاستخدامها في ما بعد بصورة مباشرة.

---

[٩] حسين بن سعيد الغافري ، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت(٢٠٢٤). http://hussain-alghfri.blogspot

[١٠] المومني(٢٠٠٨)، الجرائم المعلوماتية ،ط١، الاردن .دار الثقافة للنشر والتوزيع، ص ٩٠

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

٥_تهديد الأمن القومي والعسكري

يمثل التهديد الأمني والعسكري احد الاسباب وراء جرائم نظم المعلومات والذي يتمثل باختراق الانظمة الالكترونية والحواسيب التابعة للمؤسسات الأمنية والعسكرية والتي تكون بالغة الخطورة خاصة اذا ما تم تعطيل او تخريب او تسريب للوثائق السرية أو البيانات التابعة لها [١١].

٦_التحول للمجتمع الرقمي : اذ ساهم دخولنا لعصر المعلوماتية الجديدة أي الفضاء الالكتروني او العالم الافتراضي، والذي فسح المجال للبشر بتحويل انشطتهم الى هذا الفضاء من اعمال، وتواصل اجتماعي، وغيرها اضافة الى انكشاف البنى التحتية المعلوماتية سواء على مستوى الدولة نفسها أو على مستوى العالم، وبالتالي جعلها اهدافا سهلة من قبل المجرمين المتخصصين في هكذا نوع من الجرائم ومما زاد الأمر صعوبة هو عدم السيطرة التامة وتامين الحماية الكافية في الفضاء السيبراني بالرغم من كل الجهود التي بذلت والاجراءات التي طبقت في العديد من الدول الا انها لازلت تتعرض للعديد من الهجمات على المستوى الأفراد أو المجموعات او حتى الدول.

المطلب الثاني: الآثار الاقتصادية والاجتماعية والسياسية لجرائم نظم المعلومات

رغم الايجابيات والمميزات التي قدمها التطور الهائل لتكنولوجيا المعلومات والاتصالات للبشرية والذي انعكس على شتى المجالات الحياتية الا انها افرزت مجموعة من العيوب أو السلبيات من بينها جرائم نظم المعلومات او الجرائم الالكترونية والتي عرضت المستخدمين المجموعة من الانتهاكات كان لها اثارا اقتصادية واجتماعية وحتى سياسية وفي هذا المحور سنتاول اهم الآثار لتلك الجرائم وكالاتي :

اولا : الآثار الاقتصادية لجرائم نظم المعلومات

على مستوى الفرد

حيث اصبح الفرد ينجز تعاملاته ويدير اعماله وبحوثه ويتواصل مع العالم الخارجي بواسطة استخدام الانترنت أن الجرائم الالكترونية التي قد يتعرض لها الفرد والتي لها اثارا اقتصاديا سلبية تشمل[١٢] :

. جريمة سرقة الهوية الشخصية

. جريمة سرقة بطاقة الائتمان

.الابتزاز والتهديد

.عمليات الاحتيال

---

[١١] الطائر(٢٠١٢)، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة المعلوماتية)،ط١، عمان ، دار البداية ، عمان ، ،ص ١٤١.

[١٢] دقيش جمال صراع كريمة ، الابعاد الاقتصادية للجريمة الالكترونية ، مجلة الدراسات التسويقية وادارة الاعمال القاهرة، المجلد٢ ، العدد١، ٢٠١٨، ص٢١٤.

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

على مستوى الشركات:

ان تتعرض الشركات الى جرائم نظم المعلومات والتي تتسبب بخسائر مالية كبيرة وتشمل[١٣] :

- العبث بمخازن المعلومات الخاصة بالشركة بحذفها او تعديلها او تعطيل الوصول اليها الاطلاع على معلومات سرية لصفقة أو مناقصة او امور تسويقية والاستفادة منها
- سرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة
- عمليات الاحتيال
- التهديد والابتزاز
- اختراق الموقع الالكتروني الخاص بالشركة

على مستوى البنوك:

- السطو الالكتروني
- العبث بمخازن المعلومات الخاصة بالبنك بحذفها او تعديلها
- تعطيل النظام
- نقل ملكية الأسهم
- اختراق الموقع الخاص بالبنك

على مستوى الجهات والاجهزة الحكومية:[١٤]

- تعطيل الانترنت بالكامل
- سرقة الاموال
- تعطيل انظمة القطاعات الحكومية الحيوية
- تعطيل وتخريب الخوادم الموفرة للمعلومات

اخيرا يمكن القول ان الطبيعة العالمية لهذه الجريمة كونها لا تعترف بحدود معينة لبلد معين قد زاد من الآثار السلبية لها والتي انعكست على الاقتصاد العالمي ككل فهذه الجرائم اختلفت اثارها عن الجرائم التقليدية بسبب الترابط والتشابك بين القطاعات الاقتصادية عبر شبكة الانترنت ففي حال تعرض أي من هذه القطاعات الى جريمة عبر نظامها المعلوماتي فإن تأثيراتها قد تمتد خارج حدود الدولة مسببا حالة من الفوضى المالية وقد تتسبب في انهيار البورصات والاسواق المالية واحداث خسائر مالية باهضه.

---

[١٣] منى شاكر فراج العلي، تأثير الجريمة الالكترونية على النواحي الاقتصادية، www.kenanaonline.com.

[١٤] المصدر السابق

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

ثانيا :الآثار الاجتماعية

على مستوى الفرد: يمثل الأطفال أو المراهقين نسبة كبيرة من ضحايا عمليات الابتزاز الإلكتروني، حيث يتعامل الأطفال مع الأجهزة الرقمية واللوحية بشكل يفوق تعاملهم مع أسرهم وذويهم، وهو ما يجعلهم فريسة سهلة أمام الجناة من مستخدمي هذه الأجهزة بشكل إجرامي والذين يقومون بإرسال طلبات الصداقة إلى هؤلاء الأطفال مستخدمين أساليب الإطراء وتقديم الهدايا لاستدراجهم واستغلالهم في تصوير محتويات وبيعها على الإنترنت. وفي حالة كون الضحية من الأشخاص الناضجين فإن تأثير عمليات هذه الجرائم تحدث بهم أثارا نفسية هائلة، فغالبا ما يقوم المبتز بتركيب صور أو مقاطع الضحية بشكل مسيء وغير لائق يسبب له الحرج والخجل ويطلب الجاني مقابل مادي أو جنسي من أجل عدم نشر هذه الصور أو المقاطع ويعيش المجنى عليه ضغطا نفسيا وعصبيا غير محتمل خشية أن يقوم هذا الجاني بنشر هذه المادة في محيط عمله أو أسرته أو على وسائل التواصل الاجتماعي، مع خوفه من الاتصال بالأجهزة المعنية فيقوم الجاني بنشر المحتوى المسيء فورا ، وهو ما أدى للجوء بعض الضحايا إلى الانتحار.

على مستوى الأسرة: قد تنال الجرائم الإلكترونية من العلاقات الأسرية وتكون سببا في نشأة الخلافات بين أفراد الأسرة مما يؤدي إلى التفكك الأسري، وذلك بسبب الكثير من النتائج التي تسببها تلك الجرائم كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة وسرقة الملفات الخاصة بالأفراد ونشرها في الإنترنت ووسائل التواصل الاجتماعي المختلفة. ولقد أصبحت سمعة الأشخاص محل تهديد من قبل القراصنة الذين قد يستهدفون بزيف صورهم و مقاطعهم الزوج أو الزوجة أو الأبناء ، وحتى بعد التيقن من خداع هؤلاء وزيف المحتوى الذي يبتزون به الضحية تحدث لا محالة فجوة في العلاقة بين الزوجين أو بين الآباء والأبناء ، خاصة مع غياب ثقافة التعامل مع هذا النوع من الجرائم والنقص الشديد في المعلومات حول طبيعتها وطرق التعامل مع مرتكبيها، ولقد شهد المجتمع انهيار عدد كبير من الأسر بسبب هذا النوع من الانتهاكات الإلكترونية.

على مستوى المجتمع: أصبحت الجرائم الإلكترونية تشكل خطرا على النسق القيمي والاخلاقي للمجتمع ولعل أبرز اثارها السلبية هو زيادة معدلات الجريمة خاصة أن هذه الجريمة تتسم بعدد من الصفات تجعلها أمرا سهلا للأشخاص العاديين الذين يتمتعون بقدرة مميزة للتعامل مع تكنولوجيا الانترنت المستحدثة ، خاصة وأن الضحية عادة ما يفتقر إلى آليات التعامل مع هذه التكنولوجيا ويخشى إبلاغ الجهات المختصة فيستجيب لطلبات الجاني والذي في أغلب الأحيان يطلب مبلغا ماديا كبيرا ، فيقوم المجني عليه بسرقة هذا المبلغ – إذا لم يتوافر لديه – أو ارتكاب جريمة أخرى تمكنه من الحصول على المبلغ المطلوب ، فيصبح الأمر كسلسلة من الجرائم ترتكب بداية من عملية دنيئة للابتزاز الإلكتروني.

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

ثالثاً: الآثار السياسية

جرائم نظم المعلومات قد يكون لها تأثير سياسي مما تتيح الى امكانية تسريب اسرار و معلومات حساسة للدول، فقد يقوم مواطن عادي في القيام باختراق المعلومات والاطلاع على البيانات والوصول إليها، ويكون محرك أساسي في اللعبة السياسية وذلك من خلال الاطلاع على القرارات السياسية التي تقوم بها الحكومة ونشرها وإيصالها إلى أكبر شريحة من المواطنين وزعزعة الاستقرار، وليس فقط قيام الأفراد بنشر المعلومات لكن السياسيون أيضا يلعبون دور محرك وسياسي في التأثير على الأفراد وذلك من خلال نشر السياسات والبيانات وتأثير على المواطنين وبث التفرقة ما بينهم وبين حكوماتهم، ايضا قد يتم القيام بالتهديد كتهديد شخصيات سياسية ومهمة في المجتمع بالقتل والابتزاز أو القيام بإلحاق الضرر بالشبكات المعلوماتية والأنظمة الالكترونية، كما يتم اختراق البريد الالكتروني لرؤساء الدول ومعرفة معلوماتهم والتجسس عليها ومعرفة مراسلاتهم الشخصية ومخاطباتهم ورسائلهم والاطلاع عليها للاستفادة منها في الجرائم أو التهديد بها. فأنها قد تصل الى حروب وصراعات بين الدول قد يتم فيه استخدام قدرات هجومية بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية ويتضمن هذا النوع توظيف أسلحة إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون مع قوى أخرى لتحقيق أهداف سياسية. ويتم ذلك من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية والعمل على اختراق الأمن الوطني للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك حدود الدول، كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسس، بما قد يكون له تأثيرات مدمرة على الدول[١٥] .

المبحث الثالث: الجهود الدولية المكافحة لجرائم نظم المعلومات : رؤية مستقبلية لأمن رقمي مستدام"

نظرا لحداثة الجرائم المعلوماتية وتطورها السريع وسهولة ارتكابها واتساع نطاقها، دفع الحكومات والمنظمات الدولية للتدخل لحماية المجتمع الدولي من هذه الظاهرة الإجرامية المستحدثة. لقد أضحت الجريمة المعلوماتية ظاهرة إجرامية متنامية وبات من الضروري أن تكثف جهود جميع الدولية لمكافحتها نظرا لطابعها المتجاوز الحدود الدولة الواحدة . ونظراً لهذه التحديات، استشعرت الدول والمنظمات الدولية أهمية تكثيف الجهود وتوحيد السياسات لمكافحة هذه الجرائم، بهدف تحقيق رؤية مستقبلية تضمن أمناً رقمياً مستداماً. ومن هنا، يأتي هذا المبحث لتحليل وتقييم الجهود الدولية في مواجهة الجرائم

[١٥] الأشقر(٢٠١٢) ، الأمن السيبراني التحديات ومستلزمات المواجهة، بيروت .جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

الإلكترونية وتحديات نظم المعلومات، والتعرف على مدى كفاءة هذه الجهود وفاعليتها في ظل التغيرات التقنية المتسارعة.

المطلب الاول: دور المنظمات الدولية

اولا: دور الامم المتحدة : لا شك ان الأمم المتحدة دور في مكافحة هذا النوع من الجرائم ومؤكده على وجوب تضافر جهود الدول والعمل المشترك الجماعي في مكافحة هذا النوع من الجرائم ومن اهم الجهود التي بذلتها الأمم المتحدة هو عقد العديد من المؤتمرات ومن اهم تلك المؤتمرات هي :[١٦]

١-المؤتمر السابع : المنع الجريمة ومعاملة المجرمين والذي انعقد في ميلانو الإيطالية في الفترة الممتدة ٩/٦ و ٢٦/١٠ ١٩٨٥ وحينها كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلي واعداد تقرير قصد عرضه على المؤتمر الثامن

٢- المؤتمر الثامن : عقد هذا المؤتمر في هافانا الكوبية عام ١٩٩٠م الذي أقر المعاهدة النموذجية التسلم المجرمين وتبادل المساعدات في المسائل الجنائية اما في مجال جرائم الحاسوب قد أشار إجراءات يستوجب على الدول اتخاذها :

أ- تحديث القوانين وأغراضها الجنائية من أجل تطبيق أفضل للقوانين الجنائية الراهنة وعلى نحو ملائم ، وإدخال تعديلات إن تطلب الأمر ذلك.

ب- مصادرة العائد والأصول من الأنشطة غير المشروعة.

ج-اتخاذ تدابير الأمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الانسان التأكيد على رفع الوعي لدى الجماهير والقضاة والأجهزة المعنية في هذا المجال بأهمية مكافحة هذا النوع من الجرائم ومحاكمة مرتكبيها، وذلك بتدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة.

ح-التعاون مع المنظمات المهتمة بهذا الموضوع ، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب.

خ- حماية مصالح وحقوق ضحايا جرائم الحاسوب.

٣- المؤتمر التاسع : المنعقد بالقاهرة المصرية في (٥/٥/١٩٩٥) أوصى هذا المؤتمر بوجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الاجراءات الضرورية والمناسبة

[١٦] بيدي امال، جهود الأمم المتحدة في مواجهة الجريمة السيبرانية ، مجلة البحوث في الحقوق والسياسية ، المجلد٨ ، العدد١، الجزائر،ص١٣.

٤-المؤتمر الثاني عشر : للأمم المتحدة حول منع الجريمة والعدالة والجنائية المنعقد في سلفادور البرازيلية في الفترة الممتدة ٢٠١٠ حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات في مجال مكافحة الجريمة لاسيما أن منظمة الأمم المتحدة تعد الإطار الأمثل لمكافحة الإجرام الالكتروني وقد وضعت مجموعة من القواعد الموضوعية والإجرائية لمواجهة هذا النوع من الجرائم وتأكيدا منها في هذا المؤتمر جاء البند ٤١ من تقريره بحث الدول على بناء قدرات سلطاتها الوطنية من أجل التعامل مع الجرائم الإلكترونية بما في ذلك المنع والكشف والتحقيق وملاحقة هذه الجريمة بكافة أشكالها وتعزيز الأمن في شبكات الكمبيوتر.

٥- المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة بقطر في الفترة الممتدة بين ٢٠١٥ ومن أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة الالكترونية ما يلي:[١٧]

أ – وجوب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة الالكترونية ومنعها ، حيث أن هذا النوع من الجرائم يتطلب من الدول أن تنمي قدرتها في جانب تدابير المنع والتحري المضادة.

ب- بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم الالكترونية والتحقق فيها

ج-الواضح أن الكثير من أجهزة إنفاذ القانون تواجه صعوبات في إمكانية الوصول إلى البيانات الموجودة خارج نطاق إقليمها أثناء التحري عن الجرائم الالكترونية وفي المقابل لابد من أن تكون ضمانات حقوق الإنسان وسيادة القانون وصون الحرمة الشخصية كافية لضمان أن يكون ذلك الوصول إلى البيانات من أجهزة إنفاذ القانون محددا وقابلا للتنبؤ ومتناسبا وخاضعا للرقابة.

ح- التأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة الالكترونية

ثانيا: منظمة التعاون الاقتصادي والتنمية:

بدأت هذه المنظمة الاهتمام بهذا النوع من الجرائم منذ ١٩٧٨ م حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنيات المعلومات ، وبعد الدليل المتعلق بحماية الخصوصية وقواعد البيانات أول الأدلة التي تم تبنيها من قبل مجلس المنظمة عام ١٩٨٠ م ، فأصدرت عام ١٩٨٣م بعنوان الجرائم المرتبطة بالحاسوب وتضمن التقرير مجموعة من الأفعال التي يجب على الدول تجريمها :[١٨]

١-الاستخدام او الدخول الى نظام ومصادر الحاسوب بنحو غير مصرح

---

[١٧] بيدي امال، المصدر السابق

[١٨] قطاف سليمان ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ، مجلة البحوث القانونية والاقتصادية ، المجلد، الجزائر، ٥، العدد ٢ ، ٢٠٢٢، ص ٧٥

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

٢- الافشاء غير المصرح به للمعلومات او منع او تعطيل استخدام الحاسوب او برامجه او البيانات المخزونة داخلة ..

ثالثا: الاتحاد الدولي للاتصالات : اعتمد المؤتمر العالمي لتنمية الاتصالات لعام ٢٠٠٦ القرار رقم (٤٥) الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلوماتي ومكافحة الرسائل الاقتحامية، وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين العام ٢٠٠٦، وقد تم تبنى مجموعة من التوصيات في مجال الأمن المعلوماتي والرسائل الاقتحامية، كما أطلق الأمين العام للاتحاد في أيار ٢٠٠٧ ، جدول أعمال الأمن المعلوماتي العالمي لوضع إطار المواجهة ، لتحديات المتزايدة لأمن الإنترنت، ولإيجاد حلول لتعزيز الثقة والأمن في مجتمع المعلومات، وفي أكتوبر ٢٠٠٧ أنشئ فريق من الخبراء رفيع المستوى (HLEG) ضم أكثر من مائة خبير قدموا التقارير والتوصيات في حزيران ٢٠٠٨ حيث نشرت الاستراتيجية العالمية في ٢٠٠٨/١١/١٢ وقد اشتملت الإستراتيجية على المجالات التالية التدابير[١٩].

المطلب الثاني: الاتفاقيات الدولية

تعد الاتفاقيات والمعاهدات من اهم صور التعاون الدولي بصفة عام وفي مكافحة هذا النوع من الجرائم بصفة خاصة ، ومن بين المعاهدات الدولية في مكافحة هذا النوع من الجرائم هي اتفاقية بودابست و قانون تالين :

١_**اتفاقية بودابست** : تم إبرام أول المعاهدات المتعلقة بمكافحة الجريمة الالكترونية أو جرائم الانترنيت، وكان هذا عام ٢٠٠١، بعاصمة المجرية بودابست فقد تم صياغة المعاهدة من طرف عدد كبير من الخبراء المختصين في القانون في مجلس أوروبا، وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطع الكمبيوتر على مستوى العالم، هذا ما أدى في النهاية إلى توقيع عليها من قبل ٣٠ دولة بتاريخ ٢٣ نوفمبر ٢٠٠١، في العاصمة المجرية بودابست. تعد هذه الاتفاقية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الالكترونية لقد وقعت على هذه الاتفاقيات العديد من الدول الغير الأعضاء في مجلس أوروبا مثل كندا واليابان وجنوب إفريقيا كما صادقت عليها الولايات المتحدة الأمريكية، فهي في الأصل أوروبية المنشأ، إلا أنها دولية الطابع لأنها مفتوحة للانضمام لدول الأخرى غير دول المجموعة الأوروبية طبقاً لنص المادة ٤٨ ، وتتضمن هذه الاتفاقية : الطائفة الأولى : الجرائم التي تستهدف عناصر امن المعلومات

[١٩] قطاف سليمان ، مصدر سابق ، ص ٧٩

مجلة دجلة • المجلد ٨، العدد ١ ملحق، (٢٠٢٥)، ص: ٤٠ - ٥٧
ISSN: 2222-6583

الالكترونية ، الطائفة الثانية الجرائم المرتبطة بالحاسوب ، الطائفة الثالثة الجرائم بالمحتوى الالكتروني، الطائفة الرابعة الجرائم السيبرانية[٢٠].

٢ – **قانون تالين** : تداعيات الهجمات الالكترونية التي استهدفت البنية التحتية الرقمية لإستونيا عام ٢٠٠٧، وأيضاً الهجمات الالكترونية ضد جورجيا خلال نزاعها المسلح مع روسيا عام ٢٠٠٨ إلى سعي، حلف شمال الأطلسي (الناتو) للتصدي للهجمات الالكترونية ، فقد عمد إلى إنشاء مركز الدفاع الإلكتروني التعاوني للتميز. وفي الفترة ما بين سنتي ٢٠٠٩ و ٢٠١٢ ، وبطلب من مركز الدفاع الإلكتروني التعاوني للتميز، قامت ، من الخبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات الالكترونية وتم تتويج هذه الجهود بنشر دليل يعرف باسم "دليل" تالين(Manuel de Tallinn) وهو وثيقة قانونية غير ملزمة تنظم قواعد الاشتباك عبر الانترنت وقد تم صدور إصدارين له الإصدار الأول عام ٢٠١٣ ويتكون من ٩٥ قاعدة قانونية ويركز على أشد الهجمات الالكترونية خطورة أي تلك الهجمات التي تنتهك حظر استخدام القوة في العلاقات الدولية، وتخول الدول ممارسة حق الدفاع عن النفس، و/ أو الهجمات التي تحدث أثناء النزاع المسلح ويطبق عليها قواعد القانون الدولي الإنساني. الإصدار الثاني عام ٢٠١٧ المعروف باسم (Tallinn ٢.٠) ويتكون من ١٥٤ قاعدة قانونية ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات الالكترونية الأخرى التي تحدث يومياً خلال وقت السلم، والتي تقل عن عتبة استخدام القوة أو النزاع المسلح، ويتناول القضايا التي يصبح في فيها الهجوم الرقمي انتهاكاً للقانون الدولي في الفضاء السيبراني[٢١] .

الخاتمة

أصبحت الجرائم المعلوماتية ظاهرة إجرامية حديثة نسبياً، ما دفع حكومات الدول إلى إدراك حجم مخاطرها وخسائرها، كونها تستهدف الاعتداء على البيانات بمفهومها التقني الواسع. ويرتكب هذه الجرائم أفراد يتمتعون بذكاء عالٍ ومعرفة تقنية متقدمة، مما يمكنهم من اختراق الخصوصية والاعتداء على المعلومات المخزنة أو المنقولة عبر أنظمة وشبكات الإنترنت. وتكمن خطورة هذه الجرائم في تأثيرها المباشر على الحياة الخاصة للأفراد، وتهديدها للأمن القومي والسيادة الوطنية. ونظراً للآثار السلبية لهذه الجرائم، بات من الضروري أن تمنح الدول اهتماماً استثنائياً لمواجهتها والحد من مخاطرها الاقتصادية، الأمنية، الاجتماعية والثقافية. ولا يمكن تحقيق ذلك إلا من خلال تعاون دولي فعال، باعتباره الوسيلة

[٢٠] الظاهر باكر ، مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية ، مجلة الصدى للدراسات القانونية والسياسية المجلد٤،الجزائر ، العدد ١ ، ٢٠٢٢، ص ٢١.

[٢١] السبعري و الزرقي(٢٠١٩)، انتقال التهديدات من الواقع إلى العالم الافتراضي، العراق .مجلة بابل للعلوم الإنسانية ، المجلد٤ : العدد ٢٧ ، ص ص ٤٢٧-٤٣٧.

الأكثر كفاءة في مكافحة هذه الجرائم، خاصة وأنها غالباً ما تُرتكب عبر حدود مختلفة. لذا، فإن التعاون الدولي لم يعد مجرد خيار، بل أصبح ضرورة حتمية لضمان الوقاية من هذه التهديدات ومنع مرتكبيها من الإفلات من العقاب.

الاستنتاجات:

١. تُعد جرائم نظم المعلومات من الجرائم الحديثة التي تُرتكب في العالم الافتراضي، بخلاف الجرائم التقليدية التي تحدث في الواقع المادي، وهي جرائم عابرة للحدود يرتكبها أشخاص يتمتعون بخبرة ومهارة عالية في تقنيات المعلومات والاتصالات.

٢. تنطوي هذه الجرائم على آثار جسيمة تمس الدول والأفراد، وذلك نتيجة التحول الرقمي المتسارع والاعتماد المتزايد على المعاملات الإلكترونية، مما أتاح المجال لاستغلالها وظهور هذا النوع من الجرائم.

٣. رغم وجود العديد من الجهود الدولية للحد من هذه الجرائم، والتي تمثلت في دور المنظمات العالمية مثل الأمم المتحدة والاتفاقيات الدولية، إلا أنها لا تزال تُرتكب نظراً للخصائص الفريدة التي تميزها وتجعل مكافحتها أكثر تعقيداً.

المقترحات:

١.تعزيز التشريعات الوطنية والدولية: من الضروري تحديث التشريعات المحلية بما يتماشى مع التطورات التقنية المستمرة، والعمل على مواءمتها مع الاتفاقيات الدولية لضمان تكامل الجهود في مكافحة الجرائم المعلوماتية.

٢. نشر الوعي المجتمعي: تعزيز الوعي الرقمي لدى الأفراد والمؤسسات حول أساليب الوقاية من الجرائم المعلوماتية، من خلال حملات إعلامية وتثقيفية دورية.

٣. تطوير البنية التحتية التقنية: دعم تطوير أنظمة الحماية والرقابة الإلكترونية، وتحديث آليات كشف التهديدات الأمنية في المؤسسات الحكومية والخاصة.

٤. تعزيز التعاون الدولي: تشجيع تبادل المعلومات والخبرات بين الدول، وإنشاء مراكز تنسيق إقليمية لمكافحة الجرائم السيبرانية وتسهيل تسليم المجرمين الرقميين.

٥. تشجيع البحث العلمي: دعم الدراسات والبحوث المتخصصة في مجال الجرائم المعلوماتية للوقوف على أسبابها، وتطوراتها، وسبل الحد منها.

قائمة المصادر والمراجع:

أولاً: الكتب العربية والمترجمة

١. جورج بوردو، ترجمة سليم حداد، الدولة، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر، بيروت، ١٩٨٥.
٢. محمد الباهي، الفكر الإسلامي والمجتمع المعاصر، دار الكتب اللبنانية، بيروت، ٢٥، ١٩٧٥.
٣. خيري عبد القوي، دراسة في السياسة العامة، دار ذات السلاسل للطباعة والنشر، الكويت، ١٩٨٩.
٤. جيمس أندرسون، ترجمة عامر الكبيسي، صنع السياسات العامة، عمان، دار الميسرة للنشر والتوزيع والطباعة، ١٩٩٩.
٥. محمد علي سكيكر، الجرائم الإلكترونية وكيفية مواجهتها، دار مطالع الجمهورية للنشر، ٢٠١٠.
٦. نهلة عبد القادر المومني، الجرائم الإلكترونية، الطبعة الأولى ط.، دار الثقافة للنشر والتوزيع، ٢٠٠٨.
٧. جعفر حسن جاسم الطاير، جرائم تقنية المعلومات: رؤية جديدة للجرائم الإلكترونية، الطبعة الأولى، دار البداية، عمان، ٢٠١٢.

ثانيًا: الدوريات (البحوث المحكمة والمؤتمرات)

١. علاء نوري شنيف، أحمد رضا توحيدي، "صور الجرائم الإلكترونية ومواجهتها بالتشريعات القانونية"، مجلة إكليل للدراسات الإنسانية، العدد ١١، ٢٠٢٢.
٢. دقيش جمال سارة كريمة، "الأبعاد الاقتصادية للجرائم الإلكترونية"، مجلة دراسات التسويق وإدارة الأعمال، المجلد ٢، العدد ١، ٢٠١٨.
٣. علي الأشقر جنور، "الأمن السيبراني: التحديات ومتطلبات مواجهته"، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٢.
٤. بيدي أمل، "جهود الأمم المتحدة في مكافحة الجرائم الإلكترونية"، مجلة البحوث في القانون والسياسة، المجلد ٨، العدد ١، الجزائر.
٥. قطاف سليمان، مواجهة الجريمة الإلكترونية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد ٢، الجزائر، ٢٠٢٢.
٦. الزهير بكر، مكافحة الجريمة الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، المجلد ٤، العدد ١، الجزائر، ٢٠٢٢.
٧. بهاء عدنان الصابري وعماد عبد القادر الزرقي، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة بابل للعلوم الإنسانية، المجلد ٤، العدد ٢٧، العراق، ٢٠١٩.

ثالثًا: المواقع الإلكترونية

١. مريم عبد الرحمن، مفهوم الجريمة الإلكترونية ومراحلها التاريخية، بحث منشور بتاريخ ١ يوليو ٢٠٢٠، على الرابط: http://alhiwarmagazine.blogspot.com/2020/07/blog-post_10.html?m=1، تاريخ الولوج: ٢٨ يناير ٢٠٢٥.
٢. حسين بن سعيد الغافري، جهود سلطنة عُمان في مكافحة الجرائم الإلكترونية، تاريخ الولوج: ٢٨ يناير ٢٠٢٥. http://hussain-alghfri.blogspot
٣. منى شاكر فرج آل علي، أثر الجريمة الإلكترونية على الجوانب الاقتصادية، تاريخ الولوج: ٢٨ يناير ٢٠٢٥.