AL-NAHRAIN JOURNAL OF LEGAL SCIENCE Vol.27 2025, pp. 147-161

AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW

ISSN:3006- 0605 DOI:10.58255

عدد: مؤتمر (الفراهيدي) المجلد: ٢٧ تموز ٢٠٢٥ مجلة النهرين للعلوم القانونية

Received:1/3/2025 Accepted: 7/4/2025 Published: 1/6/2025

الجرائم الالكترونية المفهوم والاسباب في ظل التحولات الاقليمية والدولية

م.د . سيف ماجد كرم
جامعة الفراهيدي / كلية القانون

الملخص:
تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت مثل غرف الدردشة، والبريد الإلكتروني ،والموبايل، ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح (الجريمة الإلكترونية)
كما تتناول أسباب الجريمة الإلكترونية، حيث تم تصنيف هذه الأسباب على ثلاثة مستويات من النظم هي: النظام الشخصي، والنظام الوسيط والنظام الكلي. فقد انطلقت من أن الجرائم الإلكترونية هي الأفعال الإجرامية التي ترتكب بواسطة الحاسب أو النطاق التقني مثل الإنترنت والشبكات، أو التي يكون فيها الحاسب والحيز التقني مستهدف للجريمة الإلكترونية. وتشمل الجرائم الإلكترونية ضمن هذا التحديد وليس حصرا على الإرهاب الإلكتروني، والاحتيال وسرقة الهوية والملاحقة والتحرش، وبريد النفايات والفيروسات، وشم كلمات السر، والقنابل الذكية.
وتتلخص أسباب الجرائم الإلكترونية بانها ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي حيث انتقل نشاط الناس من الواقع الفعلي (المادي) إلى الواقع الافتراضي، وهي جريمة عابرة للحدود الوطنية. وقد سهل انتشار الجرائم الإلكترونية سهولة الوصول للمستهدفين وانخفاض الكلفة، والغفلة في تنفيذها وضعف الرقابة والسرعة في تنفيذها وتوظيف الاتصالات والتفاعلات في ارتكابها، وقلة الخطورة على الجناة، وسرعة الكسب غير المشروع، والفرص المتاحة لارتكابها، والضغوط الشخصية

والعامة على الجناة، وضعف الرقابة عامة. كما ساهمت عوامل التحضر السريع، والبطالة والرغبة بسرعة الثراء، وضعف التشريعات وضعف أدوات الحماية، وتوافر الفرصة لارتكابها وغياب الحراسة التقنية في انتشارها. وينفذها شباب يسعون للشهرة أو مجرمون محترفون يسعون للكسب والثراء، أو للاعمال الارهابية .

المقدمة : تميز القرن ٢١ باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسعت الإنترنت أضعافا مضاعفة. حاليا ، حوالي هناك ٨٢٠ مليون شخص يستخدمون الإنترنت ، بزيادة قدرها ١٢٦ في المئة من ٢٠٠٠ - ٢٠٠٥، .InternetWorldStats.com)لقد وفرت السهولة النسبية لاستخدام الإنترنت، والحصول على الإنترنت على نحو متزايد أكثر للإنترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة، كل ذلك مكّن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة ، والترفيه ، والتعلم ، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت. وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني ، والذي يعرف بأنه مكان لأجل غير مسمى حيث يتفاعل الأفراد والتجمعات " (٢ ٢٠٠٤)ويتصف الفضاء الإلكتروني بأنه مكان بلا حدود مادية أو اجتماعية تحرم الأفراد من العيش فيه.

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة. ولنا أن نتصور حجم التفاعلات التي تتم في الواقع الافتراضي سواء كانت شخصية أو مؤسسية أو في مجال الأعمال أو الخدمات أو الثقافة .

وللأسف، فان الفضاء الإلكتروني ينتج أنواعا جديدة من الجريمة تسمى الجريمة الإلكترونية (cyber crimes)من خلال خلق فرص جديدة للمجرمين (Wall). ، ٢٠٠٥ قد مكّنت مجرمي الفضاء الإلكتروني من تصفح الإنترنت وارتكاب جرائم مثل القرصنة، والاحتيال، والتخريب للكمبيوتر ، والاتجار بالمخدرات ، والتعامل في معلومات العدالة، والمواد الإباحية، والملاحقة (United Nations Crime and Justice 1999 information UNCJIN)دون القبض عليهم أو الكشف عن الجرائم. لقد تكونت أنماط جديدة من الجرائم من منها : لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم التي تخترق الحماية الأمنية في النظم القانونية ويتم تجنب العقاب فيها .

أولاً - أهمية البحث:

نظراً لانتشار تطبيقات الجرائم الالكترونية في مجتمعاتنا وما ينتج عن هذا الانتشار من تزايد الجرائم المتعلقة بتلك الجرائم فكان ضرورياً بحث الجرائم الالكترونية المفهوم والاسباب في ظل التحولات الاقليمية والدولية المسؤولية الجنائية عن تلك الجرائم المرتكبة ، كما ترجع أهمية البحث أيضاً في الإجابة عن تساؤل،وهو هل من الضروري إعطاء الشخصية القانونية لكيان الجرائم الالكترونية من أجل الوصول إلى مسؤوليتهم الجنائية عن الجرائم المرتكبة طرفهم؟ .فمع هذا التطور الرهيب في تطوير أنظمة الجرائم الالكترونية ازدادت في الفترة الاخيرة . وهذا ما دفعنا إلى التطرق إلى هذا البحث لإلقاء الضوء على تلك المشاكل والوقوف على أبعادها.

ثانياً - أهداف البحث :

يستهدف البحث التطرق إلى قواعد المسؤولية الجنائية والعقاب على الجرائم الالكترونية للوقوف على من هو المسؤول الحقيقي عن الجرائم التي قد تنشأ عن استخدام التطبيقات الالكترونية في حياتنا. فمن خلال البحث نتناول التعرف على اهم تلك الجرائم اومجالاتها

ومميزاتها وتسليط الضوء على تناول القانون الجنائي للمسؤولية الجنائية لتلك الجرائم من حيث القواعد القانونية المقترحة والعقوبات المناسبة ونظراً لتسارع كافة دول العالم في استغلال لمثل هذه الجرائم بكافة مناحي الحياة، لذا يجب الموازنة بين التشجيع على تطويره من جانب وبين وضع القواعد القانونية التي تحمى المجتمع من الاستغلال السيّئ لتلك الجرائم.

ثالثاً ـ إشكاليات البحث:

من أهم الصعوبات التي واجهت البحث تناوله لموضوعات حديثة وليس لها تنظيم قانوني ففي البداية يجب تعريف ماهية الجرائم الالكترونية ، ثم يثور التساؤل حول مفهوم هذه الجرائم والأسباب في ظل التحولات الدولية والإقليمية من المسؤول جنائياً عن الجرائم الناشئة عن هذه الجزيمة ، وما هي مفهومها وبيان مسؤولية مرتكبيها ؟

بالإضافة إلى ذلك يثار التساؤل حول القانون الواجب التطبيق على تلك الاعمال الجنائية، هل يمكن الرجوع إلى القواعد العامة للقانون الجنائي لتطبيقها على تلك الاعمال ؟ أم أنها غير ملائمة لمواجهة هذا التطور في إجرام الذكاء الاصطناعي، بالتالي يجب تشريع قواعد قانونية خاصة لمواجهة الجرائم الناشئة عن تلك الجرائم؟ لكى تتناسب مع طبيعته المختلفة، وتتلائم مع تطورات العصر الحديث.

رابعاً ـ منهج البحث : سوف نعتمد في هذه الدراسة على المنهج الوصفي التحليلي من خلال وصف الأفكار وطرح الاحتمالات التي يرجع سببها إلى أنظمة الذكاء الاصطناعي ثم تحليل الموقف التشريعي من خلال تقديم الاستنتاجات والتكيف القانوني الأقرب للتطبيق.

المبحث الأول : مفهوم الجريمة الالكترونية

لقد أصبحت الجريمة الإلكترونية وجرائم الحاسوب ونظمها ، بلا حدود، وهي عالمية، التحقيق فيها والحكم عليها عملية معقدة. وترتكب هذه الجرائم من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب وشبكات المعلومات. كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة.

المطلب الأول : ما هي الجريمة الالكترونية:

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية. وكما يقول فان دير هلست و ونيف " هناك غياب لتعريف عام واطار نظري متسق في هذا الحقل من الجريمة . وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية ١٨./٢٠٠٨" والرقمية وكلها تعكس فجوات مهمة في التعري تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية (PAC). ، ٢٠٠٨،١) وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

تتكون الجريمة الإلكترونية أو الافتراضية cyber crimes من مقطعين هما الجريمة (crime)والإلكترونية (.(cyberويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت مثل غرف الدردشة، والبريد)(Halder & Taishankar ٢٠١١( )الإلكتروني، والموبايل

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح. وتشمل عدداً محدداً من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة . ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق

مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". UNODC).، ٢٠١٣)

ولقد خلص فان دير هولست ونفيه ١٩ . (Van der Hulst and Neve, 2008, p إلى أن: "حقل علم الجريمة يفتقر إلى التعريف المشترك والإطار المفاهيمي المتسق. ويستخدم ترسانة حية من المصطلحات وتكون أحيانا فيكون على شكل تركيبة مع البادئات (Prefixesمثل الإنترنت والكمبيوتر، والبريد والإنترنت، أو المعلومات الرقمية، حيث انتشرت هذه المصطلحات، وطبقت بشكل عشوائي، وهذا يعكس التداخل في المحتوى أو يعكس فجوات مهمة.

وهناك مقياس طور من قبل برنامج سايبر الجريمة الإلكترونية التابع للشرطة الهولندية (Programma Aanpak Cybercrime)فمن الواضح أنه في هولندا، هناك فروق ذات دلالة موجود في نطاق التعاريف المستخدمة للجريمة الإلكترونية، وفي أنواع الجريمة الإلكترونية التي تقع ضمنها والتي لا تقع ضمنها. وتتراوح التعريفات، على سبيل

المثال، من أي نوع من الجريمة التي ترتبط بأنظمة الكمبيوتر والتي لا ترتبط بمعانيها، إلى كل جريمة ناتجة من استخدام المكون الرقمي (PAC). ، ٢٠٠٨,١فمن الواضح أن هذه التعاريف تختلف إلى حد ما في طبيعتها. فالتعريف الأول تعريف ضيق: الجرائم التي ترتكب فقط على أنظمة الحاسب على سبيل المثال، شملت القرصنة ونشر الفيروسات، في حين أن جرائم مثل الاحتيال والمطاردة عبر الإنترنت لم يشملها. أما التعريف الثاني فواسع : فشمل الجرائم التي استخدم الجاني فيها مجرد هاتف محمول أو نظام الملاحة عبر الأقمار الصناعية لارتكاب الجريمة.

كمصطلح عام " " (Leukfeldt, Veenstra & Stol 2013)ولقد عرفها ليوكفيلدت وفنسترا وستول لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات (ICT)دوراً أساسياً. وهنا تقع الكثير من الجرائم ضمن هذا التعريف. لقد قدم ليوكفيلدت وآخرون ((٢٠١٢) . (Leukfeldt et alقائمة ب ٢٨ جريمة بدءا من قرصنة الأنظمة الرقمية، وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية.

المطلب الثاني: مصطلح التعريف الدولي للجريمة الالكترونية

تعتمد "تعريفات" للجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح هنالك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الإلكترونية أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية، وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي بعض التعاريف تحتاج إلى جوهر أفعال الجريمة الإلكترونية، ومع ذلك، فإن أي تعريف للجريمة الإلكترونية ليس ذا صلة لأغراض أخرى، مثل تعريف نطاق التحقيق المتخصص وقوى التعاون الدولي، والتي من الأفضل أن تركز على الأدلة الإلكترونية على بناء مفاهيمي عام ومصطنع هو الجريمة الإلكترونية

مصطلح " الجريمة الإلكترونية"

حاولت العديد من الأعمال الأكاديمية تعريف " الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية مهتمة بتعرف دقيق للمصطلح. فمن أصل حوالي ٢٠٠ مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، استخدم أقل من خمسة في المئة كلمة " جرائم الإلكترونية " في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعاً في التشريعات هو لمصطلح "جرائم الكمبيوتر"، و"الاتصالات الإلكترونية"، و"تكنولوجيا المعلومات"، أو الجريمة ذات التقنية العالية. وفي الممارسة العملية ، فإن العديد من هذه المفردات من التشريعات التي إنشاؤها للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية ، مثل الدخول غير المصرح به لنظام الكمبيوتر ، أو التدخل في نظام الكمبيوتر أو البيانات. حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح الجريمة الإلكترونية في عنوان فعل أو قانون (مثل " قانون الجرائم الإلكترونية ") ، ومن النادر أن يتضمن جزء التعريفات تعريف الجريمة، وعندما يضمن مصطلح الجريمة الإلكترونية كتعريف قانون كان التعريف العام له ببساطة باسم " الجرائم المشار إليها في هذه القانون وبطريقة مماثلة فأن عدد قليل جدا من الصكوك القانونية الدولية أو الإقليمية تعريف الجريمة الإلكترونية فلا اتفاقية مجلس أوروبا للجرائم الإلكترونية (Council of Europe Cybercrime Convention)، واتفاقية جامعة الدول Draft African(ولا مشروع اتفاقية الاتحاد الأفريقي ، League of Arab States Convention) العربية)(، على سبيل المثال ، تضمنت تعريفاً للجريمة الإلكترونية لأغراض الصك.

الاتجاهات التي وسعت تعريف المعدات إلى التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، البعض أضاف للتعريف بيانات الحاسوب التي تتم معالجتها من قبل النظام. وحيث إن مصطلح " نظام الحاسوب " أو " نظام المعلومات " يستثني المعلومات المخزنة في النظام أو في أجهزة التخزين الأخرى، وغالبا ما يتم التعامل معها بشكل منفصل في الأحكام القانونية الموضوعية. في حين أن بعض الصكوك تعرف كل " الحاسوب و " نظام الحاسوب "، وتضمن الأخير عادة السابق، وسياق استخدام كل المصطلحين دوم فرق بينهما في الممارسة.

ومن الشائع وصف بيانات الحاسوب" أو "معلومات الحاسوب كتمثيل للحقائق، والمعلومات أو المفاهيم التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب. توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر التزم الصمت بشأن هذه النقطة. ومن المحتمل أن يكون الفرق ذا دلالة فقط بين بين تركيبات "المقروءة آليا" و "يمكن قراءتها ومعالجتها أو تخزينها بواسطة نظام الحاسوب (أو نظام المعلومات). ففي الممارسة العملية من المرجح أن تتضمن بيانات الحاسوب أو المعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة، و USBأو بطاقات فلاش للتخزين) أو البيانات أو المعلومات المخزنة في ذاكرة الحاسوب أو نظام بث نظام المعلومات أو البيانات أو المعلومات (سواء السلكية أو البصرية، أو تردد الراديو) ويعرض ماديا للبيانات أو المعلومات، مثل على شكل نسخة مطبوعة أو على شاشة.

حجم مشكلة الجرائم الإلكترونية:

هناك حوالي ٨٠٪ من أعمال الجريمة الإلكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الإلكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، وفيروسات الكمبيوتر، وإدارة الروبوتات، وحصاد البيانات المالية، وبيع البيانات، وقبض ثمن المعلومات المالية. لم يعد يحتاج مجرمو الجرائم الإلكترونية مهارات أو تقنيات معقدة.

وعلى الصعيد العالمي، تظهر أفعال الجريمة الإلكترونية انتشاراً واسعاً عبر أعمال مدفوعة ماليا، وأعمال ذات صلة بمحتوى الكمبيوتر، وكذلك العمل ضد السرية والسلامة والوصول إلى أنظمة الكمبيوتر.

تختلف تصورات المخاطر والتهديد النسبي بين الحكومات ومؤسسات القطاع الخاص. حاليا، لا تمثل إحصاءات الجريمة المسجلة لدى الشرطة أساسا سليما لإجراء مقارنات عبر الوطنية، على الرغم من أن هذه الإحصاءات غالبا ما تكون هامة لرسم السياسات على المستوى الوطني. يرى ثلثا الدول أن أنظمتها غير كافية لإحصاءات الشرطة في تسجيل الجريمة الإلكترونية. وترتبط سجلات الشرطة للجريمة الإلكترونية مع مستويات الدولة التنموية وقدرة الشرطة المتخصصة.

المبحث الثاني: أسباب الجريمة الالكترونية

هناك عدد من الأسباب التي يمكن حصرها بوصفها أسباباً للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما ان أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه فردي، مجتمعي ، كوني). فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية...الخ.

المطلب الأول : اساب الجريمة على المستوى الفردي

اولاً: البحث عن التقدير

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام. وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

ثانياً الفرصة: (Opportunity). لقد وفرت التقنيات الحديثة والإنترنت فرصاً غير مسبوقة لانتشار الجريمة الإلكترونية. أن الفرصة تنتج الجريمة ١٩٩٨ Felson & Clark). وتلعب البيئة وترتيباتها دوراً كبيراً في إنتاج الجريمة، والخروج على قواعد الاجتماعية. فوقت الانحراف عن قواعد الامتثال ليلاً ونهاراً وفي ايّ مكان، وعدم وجود رقابة كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية. وقد تشكل المعلومات هدفاً سهل المنال، ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها، أو سرقة محتوياتها، فهي فرصة مربحة .)2002(Rice & Smith) وقليلة المخاطر، واحتمالية الكشف للفاعل فيها ضئيلة ان تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للإنترنت قد خلق فرص جديدة للمجرمين وسهلت نمو الجريمة. أن جرائم الإنترنت تمثل شكلا جديداً ومميزاً للجريمة، وقد خلقت تحديات لتوقع التطورات والوقاية منها (٢٠١٣ UNODC،).

ثالثاً : ضبط الذات المنخفض : تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل إجرامي .) Gottfredson & Hirschi, 1990) تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض. وقد عرف كل من ،، جتفردستون وهيرشي السلوك الطائش بأنه كل فعل يقوم على القوة والخداع لتحقيق الرغبات الذاتية. وبناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش من خصائص الأشخاص، فإن السلوك الطائش يعد مظهراً من مظاهر الضبط الذاتي المنخفض، وكما في نظرية الضبط الاجتماعي لهيرشي ، فالدوافع لارتكاب السلوك الطائش ليست متغيرة. وذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش. فالسلوك الطائش يُعد عملاً سهلاً وقد يحقق المصالح الخاصة بسرعة مثل الرشوة، السرقة ونحوهما من الأعمال الإجرامية التي تتحقق بسرعة وسهولة دون انتظار أو بذل جهد، ولكن الاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المنحرف البداينة والرشيد والمهيزع (٢٠٠٥). إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثرين في ارتكاب السلوك الطائش، فتأثير هذين العاملين يكون نتيجة لاتحادهما، والتفاعل بينهما هو المؤدي للسلوك الطائش. وقد حاول كل جتفردستون وهيرشي عزو الاختلاف بين المجرمين وغيرهم إلى الاختلافات في مستوى ضبط الذات. إن نقص ضبط الذات قوة طبيعية تظهر في غياب الخطوات من أجل تطويره، أي أنه نتاج للتنشئة الاجتماعية الناقصة، حيث يفشل الآباء في مراقبة سلوك

الطفل، ولا يلاحظون السلوك المنحرف عندما يحدث، وإهمال معاقبة الطفل عندما يقترف سلوكاً منحرفاً. وعندما يتكون الضبط الذاتي في المراحل الأولى عند الأفراد، فإن الاختلافات في ضبط الذات تبقى ثابتة بشكل معقول من الوقت الذي تم تحديده عبر أطوار الحياة غير متأثر بالمؤسسات الاجتماعية البداينة والرشيد والمهيزع، (٢٠٠٥). بل على العكس فإن ضبط الذات قد يؤثر على أداء الأفراد في هذه المؤسسات، مثل المدرسة والعمل والزواج. والأشخاص ذوو الضبط المنخفض لا يميلون إلى السلوكيات المنحرفة فقط، بل إنهم في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج (البداينة والتوايهة، ٢٠١٠)

أظهرت الدراسات أيضا أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل، وهذا قد ينطبق على الأفعال التي يمكن إن تسهيل أو تتعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت. بالإضافة إلى ذلك، يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلا للانخراط في الجريمة الإلكترونية. ونظرية التعلم الاجتماعي " نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية ، فالمجرمين غالبا ما تحتاجون إلى تعلم تقنيات الكمبيوتر والإجراءات. فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي، تريان إن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي.

رابعاً :الضغوطات العامة : (General Strain). ترجع نظرية الضغوط العامة الانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجاباته النفس اجتماعية للحوادث والظروف والتي تعمل بوصفها ضغوطات أو مقلقات خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعياً (١٩٣٨ ، Merton 1992 ,Agnew)، وأن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة (Mazerolle, 1994 & Paternoster). كما قد تلعب العوامل الاجتماعية والاقتصادية أيضا دوراً هاماً في زيادة الجريمة الإلكترونية. فالضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف يمكن أن يؤدي، على سبيل المثال، إلى تخفيضات في الأمن، وإلى فرص لاستغلال ثغرات وضعف تكنولوجيا المعلومات والاتصالات والشركات مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، أو يصبح هناك موظفين ساخطين بسبب انخفاض الأجور والخوف من فقدان الوظيفة، والخطر يزداد من الأعمال الإجرامية والنفوذ من قبل منظمة إجرامية

خامسا: النشاط الروتيني. ويمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية. فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة ... الخ . إن التغيرات في أنشطة الناس الروتينية، من مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك، والايميل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفزين مع وجود اهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.

المطلب الثاني : أسباب الجزيمة على المستوى المجتمعي:

التحضر (Urbanization). يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهضة التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية. وكنتيجة يجد الناس انفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير والتي تعرف أولا الياهو "Yahoo Boys" وكما يرى ميك ٢٠١٢ Meke). فأن التحضر سبب رئيس للجرائم الإلكترونية في نيجيريا، وان التحضر بدون الجريمة مستحيل، وكنتيجة فان الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة الإلكترونية مربحة .

البطالة (Unemployment). ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة. وتتركز البطالة بين قطاعات كبيرة من الشباب. وكما يقول المثل النيجيري (العقل العاطل عن العمل هو ورشة عمل للشيطان) ولذا فان الشباب الذين يملكون المعرفة والمعرة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.

الضغوط العامة (Strains). تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.

البحث عن الثراء (Quest for Wealth). يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي ١٩٩٠ Gottfredson and Hirschi)، ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنومي لميرتون. فالرغبة في الثراء يواجها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية، ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية (lack of law enforcement and implementation). هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها. وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحالي على المستوى الدولي. فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية. وغالباً ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.

أسباب الجريمة على المستوى الكوني.

التحول للمجتمع الرقمي. إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسة : (١) تغيرات كمية في مقدار المعلومات المتدفقة ونوعيها، فبفعل تكنولوجيا الاتصالات والمواصلات فأن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة. (٢) إرسال المعلومات إلى العديد من الأطراف (البشر والمعدات) فالمعلومات توجه الصاروخ والصحفي يرسل التقرير، والبث المباشر من مكان الحدث. (٣) وجود الشبكات)

(Networking حيث يتم تداول المعلومات بين جميع الأطراف من مثل البريد الإلكتروني، الجوال، ... الخ) كوهين، ٢٠٠١) (البداينة، (٢٠٠٨). ففي الفضاء الافتراضي، تكونت التفاعلات الافتراضية وحلت محل
التفاعل وجها لوجه وتكونت السلوكيات الافتراضية والشخصية الافتراضية والمجتمع المحلي الافتراضي.
لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الافتراضي). فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني، ينشؤون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية، وهم على تواصل مع ما يجري في العالم الخارجي، والقيام ببعض الأعمال. كل من هذه الأنشطة قد جعلت من الممكن للجميع وبوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة. وبعبارة أخرى ، فإن شبكة الإنترنت هي من خلقت ما يعرف الآن باسم الفضاء الإلكتروني، أو العالم الافتراض. يحتاج المجتمع لكي يقوم بوظائفه إلى أن يعم الأمن والأمان وان يتحقق النظام والاستمرارية.

العولمة:

إن ظهور الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن. ضمن الفضاء الإلكتروني، قد يظهر الأشخاص الفروق في امتثالهم الخاص (القانوني) وعدم الامتثال (غير القانوني مقارنة مع السلوك سلوكهم في العالم المادي. فالأشخاص، على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم. بالإضافة إلى ذلك، فمرونة الهوية (identity flexibility)، وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي (UNODC، ٢٠١٣).

انكشاف البنية التحتية المعلوماتية الكونية

تتفاوت البنى التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري، وسوء التصرف الإنساني. حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة (PCCIP، ١٩٩٧) خمسة قطاعات بناءً على الخصائص المشتركة لها ، وهذه القطاعات هي :

١. قطاع الاتصالات والمعلومات (Information and Communication)، وتشمل شبكات الاتصالات العامة (PTN)، والإنترنت، والحاسبات في المنازل، والاستخدام الأكاديمي، والحكومي، والتجاري.

٢. قطاع التوزيع المادي (الفيزيقي) (Physical Distribution)، ويشمل الطرق السريعة للمواصلات وخطوط السكك الحديدية، والموانئ وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع

٣.قطاع الطاقة (Energy)، وتشمل الصناعات التي تنتج الطاقة، وتوزع الطاقة الكهربائية، والبترول، والغاز الطبيعي.

٤.قطاع المال والبنوك (Banking and Finance)، وتشمل البنوك وشركات الخدمات المالية من غير البنوك، ونظم الرواتب، وشركات الاستثمار، والقروض المتبادلة، والتبادلات الأمنية والمادية.

٥-قطاع الخدمات الإنسانية الحيوية (Vital Human Services)، وتشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة، والضمان الاجتماعي، وتعويض الإعاقات، وإدارة سجلات المواليد ... الخ.).

أسباب تتعلق بخصائص الجريمة الإلكترونية:

فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية.

١.الازالة (Removable). الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.

٤. المتعة (Enjoyable). كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.

٥. الديمومة (Durable. المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

٦. سرعة التنفيذ : لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر . وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

٧.التنفيذ عن بُعد : لا تتطلب الجريمة الإلكترونية في أغلبها إلا جرائم سرقة معدات الحاسب وجود الفاعل في مكان الجريمة. بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب. الخ

٨.إخفاء الجريمة إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) جرائم

مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.

٩. الجاذبية نظراً لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات. ...إلخ.

١٠. عابرة للحدود الدولية (Transnational): إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكناً وشائعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، أصبحت ساحتها العالم أجمع (البداينة، ١٩٩٨ "ج"). (البداينة، ١٩٩٩ "د").

١١. جرائم ناعمة تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحياناً كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح. إلا أن الجريمة الإلكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً، فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن (سليم، (١٩٩٧).

١٢. صعوبة إثباتها : تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة (البحر، (١٩٩٩).

اهم طرق الجريمة الالكترونية :

١.تخريب المعلومات وإساءة استخدامها. ويشمل ذلك قواعد المعلومات المكتبات، تمزيق الكتب تحريف المعلومات، تحريف السجلات الرسمية... الخ.

٢. تزييف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

٣. انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.

٤.سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات الطابع التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها...الخ.
٥.تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.
٦.التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
٧.التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
٨.التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.
٩.السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
١٠.سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
١١. الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
١٢ قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
١٣ قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
١٤.خلاعة الأطفال وتشمل نشر صور خاصة للأطفال الجنس السياحي" للأطفال خاصة، وللإناث بشكل عام، ونشر الجنس التخيلي (Cyber Six) على الشبكات.
١٥.القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونياً.
١٦. إفشاء الأسرار، وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.
١٧. الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف ... الخ.
١٨ سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
١٩. التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة أو المحادثة، أو الملامسة.
٢٠. المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.
٢١.الإرهاب الإلكتروني، ويشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

الخاتمة:

بعد ما انتهينا بحمد الله وتوفيقه من دراسة موضوعنا الجرائم الالكترونية المفهوم والأسباب في ظل التحولات الإقليمية والدولية الذي تناولنا فيه مفهوم الجريمة الالكترونية وماهيتها وأسباب الحريمة الالكترونية،وتعرضنا لمجموعة الإشكالات العديدة التي طرحتها المواجهة الإجرائية لهذا النوع من الجرائم وخلصنا في الأخير لمجموعة من النتائج التي تعتبر إجابة عن هذه التساؤلات المطروحة سابقا، تتمثل أهمها:

النتائج:

١.نظرا لأن الدور الوقائي في التصدي للجرائم أهم وأسبق من متابعتها بعد وقوعها، اتجهت جهود الدول إلى الوقاية من هذه التهديدات والحيلولة دون وقوعها، عن طريق ممارستها لوظيفتي الضبط الإداري والضبط القضائي، إذ تضطلع سلطات الضبط الإداري بمهمة المحافظة على النظام العام والوقاية من مختلف أشكال التهديدات بما فيها الاعتداءات الإلكترونية، في حين تختص سلطات الضبط القضائي بردع هذه الجرائم ومتابعتها قضائيا.

٢.كما أن دور المؤسسات الخاصة بتنظيم البريد والمواصلات السلكية واللاسلكية يبرز بشكل كبير في مجال الوقاية من الجرائم المتعلقة بالمحتوى الرقمي نظرا لطبيعة هذه الأخيرة وعلاقتها بشبكة الاتصالات العالمية ومختلف التكنولوجيات الناتجة عنها، وذلك من خلال تحسين الخدمات والاتصالات الإلكترونية المشاركة في تحديد عناصر الإطار القانوني والتنظيمي للحفاظ على الحقوق والحريات الأساسية في الفضاء السيبراني واحترام أخلاقيات تكنولوجيات الإعلام والاتصال.

٣.تبين من خلال الدراسة أنه برغم فعالية الإجراءات المستحدثة والخاصة في مواجهة الجريمة الإلكترونية إلا أنها تشكل خطرا كبيرا يهدد الحق في الخصوصية الذي كفلته الدساتير والقوانين نظرا لما تتيحه هذه الإجراءات السلطات البحث والتحري من إمكانية الاطلاع على أسرار وخصوصيات الأفراد هذا ما جعل المشرع الجزائي يحيطها بجملة من الضوابط والشروط المهمة

٤ . يجب تبيان حصر حالات اللجوء لهذه الإجراءات في الحالات الضرورية للتحري والتحقيق وغيرها، فضلا عن ضرورة الحصول على إذن مسبق من السلطة المختصة قبل مباشرة هذه الإجراءات، لتكون ضمانات تحمي المشتبه فيه أو المتهم من تعسف سلطات التحري والتحقيق عند مباشرته لهذه الإجراءات .

التوصيات :

١.العمل بنتائج البحوث العلمية والدراسات الخاصة بهذه الجرائم وأخذها بعين الاعتبار عند وضع السياسة الجنائية من طرف المشرع الجنائي.

٢. العمل على نشر الوعي والثقافة الإلكترونية، عن طريق تفعيل دور الإعلام في نشر التوعية الوقائية من الجرائم الإلكترونية، وتفعيل دور المجتمع المدني من خلال تنظيم الندوات والملتقيات والأيام الدراسية لبيان بخطورة هذه الجرائم وتفاديها.

٣. تضمين المناهج الدراسية أساسيات وأخلاقيات استخدام الإنترنت، وكذلك استحداث مقياس حول مواضيع الإجرام الإلكتروني وآليات مكافحته، يدرس على مستوى الجامعات العربية خاصة على مستوى كليات الحقوق والعلوم القانونية.

٤. العمل على إنشاء أجهزة ووحدات أمنية متخصصة في التحقيق في هذه الجرائم، يكون لديها الخبرة والإلمام الكافي بالجوانب التقنية والفنية عن طريق تكثيف البرامج والدورات التدريبية وعدم اقتصارها على المستوى الوطني فقط بل إتاحة المشاركة في الدورات المنعقدة في الدول الأجنبية.

فهرست المصادر :

المراجع العربية

١.الجـرائم الإلكترونيـة_المفهوم والأسـباب.البحر ، عبـد الـرحمن (١٩٩٩) معوقـات التحقيـق في جرائم الأنترنت رسالة ماجستير غير منشورة".
٢.الريـاض: أكاديميـة نـايف العربيـة للعلـوم الأمنية.البدايئـة، ذيـاب (٢٠١٣) الرصـد والتحليـل العلمـي لمحتويـات الشـبكات الاجتماعيـة فـي مجـال الإرهـاب. - ورقـة مقدمـة فـي النـدوة العلميـة توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب.
٣.البدايئـة، ذيـاب (٢٠١١) اسـتخدامات الإنترنـت فـي بـرامج الوقايـة مـن سـوء اسـتخدام المخـدرات. ورقـة مقدمـة فـي النـدوة العلميـة استخدام الإنترنـت فـي مكافحـة المخـدرات، جامعـة نايف العربية للعلوم الأمنية، الرياض السعودية، ٢٠١١
٤.البداينـة، ذيـاب والتوايهـه، مـريم، والعـوران حسـن (٢٠١٠). العلاقـة بـين مسـتوى ضـبط الـذات المـنخفض والسـلوك الطـائش لـدى طلبـة المـدارس فـي الأردن مجلـة العلـوم الإنسـانية والاجتماعية. جامعة الشارقة.
٥. ذيـاب (ب) (٢٠٠٩). الجريمـة الافتراضـية. ورقـة مقدمـة فـي الملتقـى الـدولي التنظـيم القـانوني للإنترنـت والجريمـة الإلكترونيـة بجامعـة عاشـور زيـان بالجلفـة الجلفـة بـالجزائر فـي الفترة٢٠٠٤
٦. ذيـاب(٢٠٠٣). الإعـلام الأمنـي فـي عصـر المعلومـات بحـث مقـدم إلـى النـدوة العلميـة العمـل الإعلامـي الأمنـي : المشـكلات والحلـول. جامعـة مؤتـة بالتعـاون مـع أكاديميـة نـايف العربية للعلوم
الأمنية خلال الفترة من ٢٠٠٣.
٧. جـرائم الحاسـب والإنترنـت فـي مركـز الدراسـات والبحـوث ص ص ٩٣-١٢٦ الظـواهر الاجرامية المستحدثة وسبل مواجهتها. الرياض:.
٨. جـرائم الحاسـب والانترنـت فـي مركـز الدراسـات والبحـوث ص ص ٩٣-١٢٦ الظـواهر الإجرامية المستحدثة وسبل مواجهتها .
٩. جـرائم الحاسـب والانترنـت فـي مركـز الدراسـات والبحـوث ص ص ٩٣-١٢٦ الظـواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض:.
١٠. هنـدرة الثقافـة الأمنيـة والتحصـين الاجتمـاعي ضـد الجريمـة الفكـر الشـرطي، م ، ع، ٢، ص ص ٩-٢٥

المصادر باللغة الانكليزية :

1-AABS (Assurance and Advisory Business Services), (1998). 2nd Annual Global Information Security Survey. Ernst& Young. http://www. Ey.com/security (also a PDF file).
2-Adeniran, A.I., 2008. The Internet and Emergence of Yahooboys sub-Culture. International Journal of Cyber Criminology, 2 (2):368-381؛
3-Al Badayneh, D. (2013). Human Behavior: When and where virtual Society meets physical Society?. European Journal of Science and Theology, February 2013, Vol.9, No.1, 3-17
4-Alshalan, A. (2006). Cyber-crime and Victimization. Unpublished Ph.D Dissertation in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology, and Social WorkMississippi State University
5-Anti-Defamation League. (1999). CyberTerrorism - Terrorism Update." http://206.3.178.10/ terror/focus/16 focus a2.html. 1999.

6-Aransiola, J.O., Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ. Cyberpsychology, Behaviour and Social Networking, 14(12):759.
7-Arneklev, B. J., Grasmick, H. G., Tittle, C. R. and Bursik, R. J. Jr. (1993). Low Self-Control and Imprudent Behavior. Journal of Quantitative Criminology, Vol. 9, No. 3, pp. 225-247.
8-Arquilla, John, Ronfeldt, David and Michele Zanini. "Networks, Netwar and Information-Age Terrorism." in Zalmay M. Khalilzhad and John P. White (eds.). The Changing Role of Information in Warfare. Santa Monica, California, Rand, 1999.
9-BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. Organised Crime in the Digital Age. Exploring Internet Crimes and Criminal Behaviour. Boca Raton, FL: CRC Press, Taylor & Francis Group.
10-Benson, M. L. and Moore, E. (1992). Are White-Collar and Common Offenders the Same? An Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime. Journal of Research in Crime and Delinquency, Vol. 29, No. 3, pp. 251-272.