الجريمة المعلوماتية في النظام السعودي

د/أميرة محمد ابراهيم ساتي*

https://aif-doi.org/AJHSS/107504

*أستاذ القانون الجنائي المساعد
كلية الحقوق - القسم العام
جامعة دار العلوم

مستخلص البحث

يهدف هذا البحث إلى التعريف بالجريمة المعلوماتية في الأنظمة ذات العلاقة بما في ذلك نظام مكافحة جرائم المعلوماتية السعودي، كما تم تعريف أدوات الجريمة المعلوماتية وخصائصها، كما تعرضت الدراسة لبيان معايير وطرق ارتكاب الجريمة المعلوماتية، كما تعرضت الدراسة الى بيان الصعوبات المتعلقة بمكافحة الجريمة المعلوماتية في على المستوى الوطنى والدولى واتبعت الدراسة المنهج والتحليلي، ثم الاعتماد على مصادر جمع المعلومات الثانوية والأولية المتمثلة في الكتب والمراجع والمجلات، وكانت أهم النتائج التي توصل إليها الباحث منها أهمية معرفة طبيعة الجريمة المعلوماتية وخصائصها وبيان المعايير ووسائل وأساليب ارتكابها وبيان صعوباتها وتشجيع الباحثين على البحث في الجرائم المعلوماتية وفي تفسير وتطبيق قوانين مكافحة الجرائم المعلوماتية المستحدثة.

الكلمات المفتاحية: جريمة، معلوماتية، مكافحة الجرائم، الانترنت، تشريع سعودي.

Abstract

The aim of this research is to define information crime in the relevant systems، including the Saudi anti-informatics crime system، as well as the definition of information crime tools and their characteristics. The national and international level. The study followed the analytical approach، then relied on secondary and primary information collection sources represented in books، references، and magazines. The most important findings of the researcher were the importance of knowing the nature and characteristics of information crime، clarifying the criteria، means and methods of committing it، indicating its difficulties، and encouraging researchers to research information crimes. And in the interpretation and application of laws to combat information crimes developed.

Keywords: Crime، informatics، crime control، the Internet، Saudi legislation.

ISSN : 2410-1818

المقدمة

بسم الله والصلاة والسلام على نبيه الحبيب المصطفى خير خلق الله وخاتم أنبيائه والمرسلين، أما بعد.. شهد العالم تطوراً كبيراً ونقلة نوعية ضخمة في كيفية التواصل بين البشر في مختلف أنحاء العالم، بدءاً بالوسائل البسيطة من النار وورق الأشجار وصولاً إلى تطور هائل بالتكنولوجيا تمثل في ظهور الحواسيب والأجهزة المحمولة واستخدام الشبكة العنكبوتية في شتى مجالات الحياة مما أدى ذلك إلى انتشار شبكة ضخمة من المعلومات الإلكترونية وهي ما تعرف بشبكة الإنترنت، الأمر الذي أحدث فارقاً عظيماً نتج عنه فوائد لا تعد ولا تحصى إذ عمل هذا التطور على تقريب المسافات وسهولة الاتصال والتواصل بين أنحاء العالم وتكوين صداقات ومعارف جديدة خارج نطاق الأسرة، وإنجاز المهام والأعمال المهنية عن بعد، ولكن لا يكاد يخلو شيء من الثغرات وهذا حال ذلك التطور الذي أفضى إلى ظهور العديد من المشكلات والتي أصبحت تشكل عائقاً أمام تحقيق أهداف التطور والتقدم، ومن هذه المشكلات الجرائم المعلوماتية.

مشكلة البحث:

شهدت الجريمة المعلوماتية انتشاراً كبيراً وذلك اعتباراً لطبيعة هذا النوع من الجرائم، حيث إنها تعتبر جريمة عالمية عابرة للحدود الوطنية ويمكن ارتكابها من أي مكان في العالم، كما يصعب اكتشافها وضبط أدلتها وملاحقة مرتكبيها، مما يجعل كل ذلك محل تساؤلات ودراسات للعمل على مواجهة هذه المشكلة والحد منها، من هنا ثار التساؤل عن الجهود الوطنية المبذولة في محاولة مكافحة هذا النوع من الجرائم.

ويتفرع عن هذا التساؤل الرئيسى العديد من التساؤلات الفرعية التي يجب طرحها وتتمثل في الاتى :

1. ماهية الجريمة المعلوماتية وأركانها؟
2. ما هي الصعوبات التي تواجه التعاون الوطني والدولي المتعلقة بالجريمة المعلوماتية؟
3. كيفية التصدي أو مكافحة الجريمة المعلوماتية على الصعيد الوطني والدولي؟

أهمية البحث:

يستمد هذا البحث أهميته من كون أنه لا يكاد أحد في هذا العصر الحديث لا يستخدم التكنولوجيا الحديثة وتقنية المعلومات والإنترنت والهواتف النقالة والحواسيب بأنواعها، فمن المهم أن نسلط الضوء على مفهوم الجريمة المعلوماتية وأركانها باعتبارها من الجرائم المستحدثة ومن الجرائم التي تواجه الأجهزة والسلطات العدلية في الدول صعوبات في اكتشافها وضبط مرتكبيها، ومحاولة التصدي لهذا النوع من الجرائم نظراً لخطورتها التي باتت تؤثر على المجتمعات بشكل كبير.

ISSN : 2410-1818

أهداف البحث:

1. التوصل إلى طرق لمكافحة الجريمة المعلوماتية المستحدثة.
2. الخروج بتوصيات قد تساعد على الحد من ارتكاب الجرائم المعلوماتية.

منهج البحث:

طبيعة دراسة الجريمة المستحدثة تتطلب تحليل مفهوم الجريمة المعلوماتية، وما ورد في نصوص النظام في سبيل استخراج أحكامها وبيان أركانها وأساليبها وتجنبها وما يترتب عليها من آثار، لذلك سوف نستعمل المنهج التحليلي في بحثنا.

خطة البحث:

ومن أجل الإجابة على هذه الإشكالية قمنا بتقسيم البحث كالآتي:

المبحث الأول: ماهية الجريمة المعلوماتية وخصائصها

المطلب الأول: مفهوم الجريمة المعلوماتية

المطلب الثاني: خصائص الجريمة المعلوماتية

المبحث الثاني: الصعوبات التي تواجه التعاون الوطني والدولي المتعلقة بالجريمة المعلوماتية

المطلب الأول: الصعوبات على الصعيد الوطني

المطلب الثاني: الصعوبات على الصعيد الدولي

المبحث الثالث: مكافحة الجريمة المعلوماتية

المطلب الأول: مكافحة الجريمة على الصعيد الوطني

المطلب الثاني: مكافحة الجريمة على الصعيد الدولي

المبحث الأول: ماهية الجريمة المعلوماتية

بداية مما لا شك فيه أنه في وقتنا الحالي والتطور الملحوظ حاليًا خاصةً في مجال أجهزة الحاسب الآلي حيث أصبح بلا مبالغة هي الوسيلة الأولى والفكرة الأولى وأيضًا القرار الأول لجميع ما يريد فعله أي شخص، ولا شك أن لكل شيء ميزات بالإضافة إلى سلبيات ومشاكل عدة وهذا ما سنتطرق له في

ISSN : 2410-1818

بحثنا هذا، سنخصص مبحثنا على الجريمة الإلكترونية سنتطرق بدايةً في المطلب الأول إلى مفهومها بشكل واضح ودقيق وننتقل في المطلب الثاني إلى ماهية خصائص هذه الجريمة أيضًا بالتفصيل.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعتبر الجريمة الالكترونية من الظواهر الحديثة وقد أحاط بتعريفها الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، ولم يتفق الفقه إلى الآن إلى تعريف واحد لها.[1]

سنتطرق في مطلبنا هذا إلى عدة فروع نتناول في الأول التعريف وفقًا للاتجاه الضيق ثم في الفرع الثاني نتطرق إلى التعريف وفقًا للاتجاه الموسع وفي الفرع الثالث الى التعريف بشكل عام وأخيرًا في الفرع الرابع الى التعريف وفقًا للنظام السعودي.

الفرع الأول: تعريف الجريمة المعلوماتية وفقًا للاتجاه الضيق

بدايةً حين توضيح التعريف الضيق للجريمة المعلوماتية نلاحظ أن الفقه أختلف أيضًا في المعيار المعتمد في هذا الاتجاه، منهم من اعتمد معيار الوسيلة ومنهم من اعتمد معيار توافر معرفة تقنية الحاسب الآلي ومنهم أيضًا من يرى أن الجريمة الالكترونية موضوعها المال المعلوماتي المعنوي، وسنتناول هذه الآراء كل رأي على حده:

أولًا: معيار وسيلة ارتكاب الجريمة

يرى الفقيه " Merwe " أن الجريمة المعلوماتية تتمثل في " الفعل غير المشروع الذي يشترط في ارتكابه استخدام الحاسب الآلي " [2]

وعرف الفقيه Leslie D.Ball الجريمة الالكترونية بأنها " كل فعل اجرامي يستخدم الحاسوب في ارتكابه كأداة أساسية " [3]

---

1) د. شاهين خضر، رضوان سعادة، الجريمة الالكترونية وإجراءات مواجهتها، رسالة ماجستير، ,كلية الحقوق .جامعة محمد بوضياف، 1441هـ، ص7.

2) د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت.2013 ,ص60

3) أحمد عبدالله المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، المركز القومي للإصدارات القانونية، ط1، القاهرة، 2017، ص27.

ISSN : 2410-1818

ومن التعريفات أيضًا التي وضعها أنصار هذا الاتجاه الضيق أن الجريمة الالكترونية هي: " التي تقع على جهاز الحاسوب أو داخل نظامه فقط، أو هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تلك التي يتم تحويلها عن طريقه ". وفقاً للنظام السعودي.

ومن التعريفات أيضًا التي وضعها أنصار هذا الاتجاه الضيق أن الجريمة الالكترونية هي: " التي تقع على جهاز الحاسوب أو داخل نظامه فقط، أو هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تلك التي يتم تحويلها عن طريقه ".[4]

ونرى مما ذكر أعلاه أن أصحاب هذا الرأي في الاتجاه الضيق اعتمدوا اعتمادًا كليًا على الوسيلة المرتكبة في هذه الجريمة، وأن الجريمة المعلوماتية تقوم باستخدام جهاز الحاسب الآلي سواءً كان هو الأداة الأساسية المستخدمة أو الأداة الثانوية.

ثانيًا: معيار موضوع الجريمة

يرى أصحاب هذا الرأي أن تعريف الجريمة الإلكترونية يرجع إلى موضوعها فقط وغير متعلقة بالوسيلة المستخدمة أو الفاعل. حيث يرى هؤلاء أن الجريمة الالكترونية هي التي تكون موضوعها المال المعلوماتي المعنوي، دون النظر فيما إذا كان الحاسب هو الأداة المستعملة في ارتكابه من عدمه. [5]

ثالثًا: معيار توفر المعرفة بالتقنية المعلوماتية

أما بالنسبة لأصحاب هذا الرأي فلا يستندون في تعريفهم للجريمة الإلكترونية إلى مدى توفر استخدام الحاسب الآلي بل يستندون على الشخص مستخدم هذا الحاسوب، حيث أنه ما يميز الجريمة الإلكترونية عن غيرها من الجرائم هو أن مرتكبيها يحيطون علمًا ومعرفة بتقنية المعلومات وفي غياب هذه المعرفة لا يمكنهم ارتكاب هذه الجرائم.

الفرع الثاني: تعريف الجريمة المعلوماتية وفقاً للاتجاه الموسع

لقد وجهت انتقادات عديدة للتعريفات السابقة المستخدمة وفقاً للاتجاه الضيق، حيث أنها من وجهة نظر الكثير قاصرة على شيء معين وغير كافية لتصبح تعريفًا شاملًا للجريمة الالكترونية ومن هنا انطلق أصحاب الاتجاه الموسع.

---

4) خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص43.

5) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، الطبعة الثانية، دار النهضة العربية، القاهرة , 2009 م. ص65

ISSN : 2410-1818

فقد عرف الجريمة الالكترونية أصحاب هذا الاتجاه بأنها: " كل سلوك إجرامي يتم بمساعدة الحاسوب " أو هي كل جريمة تتم في محيط أجهزة الحاسوب أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها.[6]

وفي ذات الاتجاه يرى الفقيهان Michel & Credo " " أن سوء استخدام الحاسوب أو جريمة الحاسوب تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به.[7]

ومما لا شك فيه أن الأخذ بهذا التعريف الموسع منتقد أيضًا من قبل الكثير، حيث أنه لا يمكن الاعتماد على الوسيلة أو المناسبة التي حدث فيها الاعتداء وإنما وجب البحث في العمل الأساسي المكون لها وليس لمجرد استخدام الحاسب الآلي في ارتكابها.

الفرع الثالث: تعريف الجريمة المعلوماتية وفقًا للاتجاه العام

بداية على الرغم من تباين التعريفات المتعددة حول الجريمة الالكترونية الا أنه من الممكن تعريفها بأنها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على الحاسب أو التي تحول عن طريقه كما تعرف بأنها كل فعل اجرامي متعمد أيًا كان صلته بالمعلومات وسينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل "[8]

كما يعرفها الدكتور مصطفى محمد موسى بأنها: " كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف " [9]

كما يمكن إجمالها بأنها: " الجريمة التي يكون محلها المعطيات المعالجة بلغة الأدلة أي المعلومات والبرامج، أو بالنظام المعلوماتي، إضافة إلى وسيلة ارتكابها الحاسوب أو أية وسيلة الكترونية لها نفس إمكاناته لأنه لا يمكن الدخول إلى النظام بدونه". [10]

---

6) خالد ممدوح إبراهيم، مرجع سابق، ص42.

7) علي جعفر، مرجع سابق، ص82.

8) سعيدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، ط1، الإسكندرية،2017، ص55.

9) سعيدي سليمة، بلال حجازي، المرجع السابق، ص56.

10) غنية باطلي،. الجريمة الالكترونية:دراسة مقارنة , العدد 1 , الجزائر: منشورات الدار الجزائرية, 2015 ,ص100

ISSN : 2410-1818

الفرع الرابع: تعريف الجريمة المعلوماتية وفقاً للنظام السعودي

بدايةً نصت المادة الأولى المعنية بالتعاريف في نظام مكافحة الجرائم المعلوماتية على أن الجريمة المعلوماتية هي : "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام. " [11]

ويتضح مما ذكر أعلاه أن نظام مكافحة الجرائم المعلوماتية قد وسع لنا في مفهوم الجريمة المعلوماتية فأدخل في نطاقها جميع الأفعال بدون حصر لها التي تستخدم بالحاسب الآلي أو الشبكة المعلوماتية أيًا منهما وتكون مخالفة بالطبع لأحكام النظام حتى تدخل في نطاق الجريمة، فيتضح لنا حرص المنظم السعودي في جعل التعريف مناسب لكل زمان ومكان ومع تطور الجرائم الذي من الممكن ان يحدث حاليًا أو مستقبلًا.

وحتى تتضح لنا الصورة بشكل أفضل نلاحظ أن التعريف ذكر لنا " الحاسب الآلي أو الشبكة المعلوماتية " سنتطرق إذًا إلى مفهوم الحاسب الآلي بالإضافة إلى مفهوم الشبكة المعلوماتية.

مفهوم الحاسب الآلي: " أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له. "[12]

أما بالنسبة لمفهوم الشبكة المعلوماتية: " ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت) . " [13]

ونلاحظ مما ذكر أعلاه أن المنظم السعودي في نظام مكافحة الجرائم المعلوماتية لم يغفل عن الأساسيات وهي توضيح ماهية الجريمة المعلوماتية بالإضافة إلى جميع المصطلحات المشابهة لها التي قد تحدث لبس لدى الكثير أو الموضحة لها.

---

11) نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8 هـ.

12) سعيدي سليمة، بلال حجازي، مرجع سابق، ص56.

13) محمد محي الدين عوض – مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) – بحث مقدم الي المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد من 25 – 28 اكتوبر 1993 م.ص65

ISSN : 2410-1818

المطلب الثاني: خصائص الجريمة المعلوماتية

بدايةً أدى انتشار شبكة المعلومات إلى التغير التقني والمتعاظم في هذا المجال وإلى سهولة تداول المعلومات، بالإضافة إلى كون الجريمة المعلوماتية قد ترتكب في دولة ما أما بالنسبة للنتيجة الإجرامية لها قد تتحقق في دولة أخرى، فتصبح الجريمة المعلوماتية شكلًا جديدًا من الجرائم العابرة للحدود، مما جعلها تتخذ طابعًا يميزها عن غيرها من الجرائم. [14]

وبذلك يتضح لنا أن الجريمة المعلوماتية تتميز بعدة خصائص من أبرزها ما يلي:

1- تعتبر من الجرائم العالمية، وهذا قد يؤدي إلى تشتيت جهود التحري والتنسيق لمثل هذه الجرائم فهذه الجرائم بمثابة صورة صادقة من صور العولمة، فمن حيث المكان يمكن ارتكاب هذه الجريمة عن بعد، وقد يتعدد هذا المكان بين أكثر من دولة، ومن الناحية الزمانية تختلف المواقيت بين الدول، الأمر الذي يثير التساؤل حول القانون الواجب التطبيق.[15]

2- تعتبر أيضًا من الجرائم صعبة الإثبات، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية، والسبب في ذلك يعود إلى استخدام الجاني وسائل تقنية وفنية معقدة في كثير من الأحيان، كما تعتبر من السهل محو الدليل والتلاعب فيه كونها من الجرائم السريعة جدًا التي لا يستغرق الا بضع ثواني لإتمامها، لذلك معظم الجرائم الالكترونية تم اكتشافها بمحو الصدفة وبعد مرور وقت طويل على ارتكابها.[16]

3- تعد الجرائم المعلوماتية أقل عنفًا من الجرائم التقليدية أي أنها لا تحتاج لأي مجهود عضلي، بل تعتمد على القدرة الذهنية والتفكير العلمي المدروس المستند إلى المعرفة بتقنيات الحاسب الآلي. [17]

4- أن الباعث على اكاب الجرائم المعلوماتية يختلف عن الباعث في الجرائم التقليدية، ففي الجرائم المعلوماتية يتمثل دور الباعث في الرغبة في مخالفة النظام العام والخروج عن القوانين أكثر من استهداف

14) د. محمد بن أحمد علي المقصودي، الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيًا، المجلة العربية للدراسات الأمنية، المجلد33، العدد (70)، الرياض، 2017، ص 113.

15) د. محمد المقصودي، المرجع السابق ذكرة، ص113.

16) د. عادل يوسف عبدالنبي الشكرى – الجريمة المعلوماتية وازمة الشرعية الاجرائية – جامعة الكوفة – كلية القانون – منشور بمجلة مركز دراسات الكوفة العدد السابع 2008 , ص65

17) . عادل يوسف عبدالنبي الشكرى , المرجع السابق, ص66

ISSN : 2410-1818

الحصول على الربح في حين نجد أن الباعث في الجرائم التقليدية هو الحصول على الربح المادي السريع.[18]

5- تعتمد هذه الجرائم على قمة الذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض ومن الصعب اثباتها كما أن التحقيق فيها يختلف بتاتًا عن التحقيق في الجرائم التقليدية، والوصول إليها يستوجب الحصول على خبرة فنية وتقنية عالية جدًا. [19]

المبحث الثاني: الصعوبات التي تواجه التعاون الوطني والدولي المتعلقة بالجريمة المعلوماتية

تقع جرائم المعلوماتية وترتكب في إطار تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوماً بعد يوم في إدارة مختلفة المعاملات الاقتصادية والمالية والخدمية الوطنية والدولية على حد سواء – ويعتمد عليها في تسير معظم شؤن الحياة اليومية للأفراد.

وأيضاً في عالم مزدحم بالشبكات اتصالية دقيقة ومتطورة تنقل وتشغل البيانات والمعلومات من مناطق متباعدة باستخدام تقنيات لا تكفل لها آمناً متكاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرار فادحة، يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية ومن بينها جرائم الإنترنت أمراً محتماً.

ومع ضرورة هذا التعاون والمناداة، إلا أنه ثمة صعوبات ومعوقات تقف دون تحققه وتجعله صعب المنال ومن خلال هذا المبحث سوف نحاول أن نبرز أهم تلك الصعوبات وكيفية مواجهتها على النحو التالي [(20)].

18) د. فتوح الشاذلي، عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة و القانون – دراسة مقارنة – منشورات الحلبي الحقوقية , بيروت , 2015 ,ص97

19) دياب البدوي، الجرائم الإلكترونية المفهوم والأسباب، الملتقي العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، كلية العلوم الاستراتيجية، 2018.ص108

20) د. سليمان احمد محمد فضل، المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، بدون دار نشر، القاهرة 1428 هـ، ص 435.

ISSN : 2410-1818

المطلب الأول: الصعوبات على الصعيد الوطني

تتميز جرائم الإنترنت بمجموعة من الخصائص التي تؤدي إلى صعوبة التعامل معها وضبطها، حيث تواجه الأجهزة الأمنية عند مواجهتها لجرائم الإنترنت على المستوى الوطني العديد من الصعوبات أهمها:

الفرع الأول: إحجام الكثير من الجهات والأفراد عند الإبلاغ عن تلك الجرائم

في الواقع فإن إحجام المجني عليه عن الإبلاغ عن الجرائم المعلوماتية يبدو أكثر وضوحاً الجهات وخاصة البنوك أو المؤسسات الادخارية على عدم الكشف عما تعرضت له، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات، وبالتالي لأصول الأموال التي تتعامل معها، فتكتفي الجهة عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضت له السلطات المختصة، تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها، وبالتالي يجب تحديث الأساليب الإجرائية في مواجهة الجرائم المعلوماتية واستكمالها على نحو يكفل استجابتها بشكل كافي، حيث يضمن تعويض الأفراد لحقوقهم وحرياتهم دون التعرض لخطر المتطلبات العملية الإثباتية في مجال تقنية المعلومات والاتصالات [21].

الفرع الثاني: عدم كفاية القوانين القائمة

يقابل التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أم الخاصة واعتماد الجميع عليه في سائر شئونهم استغلال الجناة لتلك التقنية في ارتكاب جرائمهم، وهذا التطور المتلاحق في مجال المعلومات لا يقابله بذات الدرجة تطور في النصوص القانونية، كما سبق دراسته من خلال المواجهة التشريعية لهذه الجرائم [22]، فالقانون الجنائي بنصوصه الحالية لا يكفي لإمكانية مواجهة تلك الصور المستحدثة من الجرائم، حيث تتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة مما يتنافى مع الطبيعة المعلوماتية، وبالتالي تخرج تلك الصور من تحت طائلة العقاب [23].

ولكن المملكة العربية السعودية تعمل على الحد من هذه الفوضى ومحاربتها من خلال وضع نظام مكافحة الجرائم المعلوماتية في السعودية والذي تناول كافة الجرائم الالكترونية والعقوبات التي تترتب على تلك الجرائم، فرض نظام مكافحة الجرائم المعلوماتية في السعودية جملة من العقوبات تتناسب مع جسامة كل جريمة لتكون رادعاً لكل من سولت له نفسه أذية الناس والانتقاص من

21) د. سليمان احمد فضل، المرجع السابق.285

22) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، الناشر: دار النهضة العربية للنشر والتوزيع، القاهرة، 2009، ص655

23) د. حسين الغافري، المرجع السابق، ص 256.

ISSN : 2410-1818

حقوقهم وزرع الخوف والقلق في نفوسهم، ونستنتج أن نظام مكافحة الجرائم المعلوماتية في السعودية منصفاً للجميع. فنحن نعيش الآن في عصر الثورة التكنولوجية. وقد حققت هذه النهضة دون أدنى شك تطورات إيجابية في جميع الأصعدة، ولكن هناك مأزق حقيقي خلفته التكنولوجيا المعلوماتية نتيجة سوء الاستعمال الذي خلف آثار سلبية.

الفرع الثالث: صعوبة إثبات الجريمة المعلوماتية والتحقيق فيها

1. غياب الدليل المرئي الجرائم التي تقع على العمليات الإلكترونية المختلفة، كالتي تقع على عمليات التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، أو على أعمال الحكومة الإلكترونية، قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية، كجرائم السرقة، أو الاختلاس، أو الاستيلاء، أو الغش، أو التزوير، أو الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة.[24]

لا يوجد شك في إن إثبات الأمور المادية التي تترك آثاراً ملحوظة يكون سهلاً ميسوراً، بعكس إثبات الأمور المعنوية فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة، وكمثال لذلك نجد أن التجسس المعلوماتي بنسخ الملفات وسرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الافعال اكتشاف أمرها وملاحقة الجناة عنها، ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسبات، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة. فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات

24 د. عادل عامر، مظاهر صعوبة اثبات الجريمة الالكترونية، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم – الدكتور عادل عامر – جريدة الفراعنة(alfaraena.com)).

ISSN : 2410-1818

الجنائي التي تعتمد على الإثبات المادي للجريمة، ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع اي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية.[25]

2. سهولة إخفاء الدليل: كما سبق القول فإن الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من اخفاء الافعال غير المشروعة التي يقومون بها اثناء تشغيلهم لهذه الوسائل الإلكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها، كما وأن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الإلكترونية ويكون أمرها حكراً عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار، كما أنهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فإنه قد يقومون باختراق قواعد البيانات والتغيير في محتوياتها تحقيقا لمآرب خاصة، وقد يخربون الانظمة تخريبا منطقيا بحيث يمكن تمويهه.[26]

كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في انظمة التشغيل أو التصميم الكلي للنظام المعالج آليا للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون ان يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل [(27)]، ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه ان يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها.[28]

---

25) د. عبد القادر الجيرانى , الجريمة المعلوماتية ,مقال نشر بتاريخ 30 يوليو , 2017 ,

https://www.facebook.com/405355742894368/posts/1380377042058895/?paipv=0&eav=Afa6rS60EfpskuSqzvjOjN8tCWaWpbHC8m2QnFXxz8twszzUpPVvmWzm80_UF8Z49YA&_rdr

26) د. عبد القادر الجيرانى , الجريمة المعلوماتية , المقال السابق , ونشر بتاريخ 30 يوليو , 2017 .

/https://elbashayer.com/2084752/1056406

27) د. عادل عامر، مظاهر صعوبة اثبات الجريمة الالكترونية، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم :- الدكتور عادل عامر – جريدة الفراعنة(alfaraena.com)).

28) د. عادل عامر، المرجع السابق، الثلاثاء 2022/10/25م،

ISSN : 2410-1818

فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده. ويلاحظ أن المجني عليهم قد يساهمون بدورهم في عدم إماطة اللثام عن هذه الجرائم، فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من الآخرين، ولعل هذا الأمر قد تلجأ إليه عادة المؤسسات المالية كالبنوك والمؤسسات الادخارية وشركات الإقراض والسمسرة، حيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها على الثقة فيها من العملاء المتعاملين معها، مما قد يؤدي إلى انصرافهم عنها، وهو ما قد يصيبهم بأضرار قد تزيد بكثير عن كشف ستر هذه الجرائم وتقديم مرتكبيها إلى العدالة وإذا نظرنا إلى هذا الإحجام عند الإبلاغ عن مثل هذه الجرائم الفنية نجد أنه قد ترتب عليه نتائج تكون في منتهى الخطورة، فهو يزيد من الرقم مما يعوق رسم السياسة الجنائية السليمة لمواجهة الظاهر الإجرامية المستجدة واختيار افضل الوسائل لمكافحتها.[29]

3. إعاقة الوصول إلى الدليل: جناة الجرائم الإلكترونية من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، ولذلك نحد انهم وهم يرتكبون الجرائم الإلكترونية يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة كشف سرتهم وإزالة حجب الشر التي اصطنعوها بأيديهم، وكمثال لذلك نجد أنهم قد يستخدمون التشفير وكلمات السر التي تمكنهم من اخفاء الأدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم ان يفهم مقصودها، وقد يقوم هؤلاء ايضا بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها في منتهى الصعوبة.[30]

وليس بخافٍ كذلك أن هؤلاء الجناة قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فقد يستخدمون البريد الإلكتروني في إصدار تكليفاتهم بارتكاب جرائم القتل والاغتيالات والتخريب دون ان يتمكن أحد من تحديد اماكنهم أو تسجيل هذه التكليفات على النحو الذي كان يحدث في الاتصالات السلكية واللاسلكية، كذلك فإن مرتكبي جرائم الإنترنت يصعب ملاحقتهم لاستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها،

29) د. عادل عامر، مظاهر صعوبة اثبات الجريمة الالكترونية، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم :- الدكتور عادل عامر – جريدة الفراعنة

30) د. عادل عامر، مظاهر صعوبة اثبات الجريمة الالكترونية، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم :- الدكتور عادل عامر – جريدة الفراعنة (alfaraena.com)).

ISSN : 2410-1818

لأنهم في الغالب يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة ليس عن طريق ابواب حاسباتهم الآلية وانما عن طريق مقاهي الإنترنت. أيضا فإنه يلاحظ أن ملاحقة جرائم الإنترنت قد تتعلق ببيانات تكون مخزنة في داخل دولة اجنبية بواسطة شبكة الاتصال عن بعد ، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة.[31]

4. صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية لا شك في أن طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، بعكس الدليل القولي فإن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه وإدراك حقيقته ، وإذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الإلكترونية قد يتحصل من عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات الكترونية وعمليات أخرى غير مرئية ، فإن الوصول إليه وفهم مضمونه قد يكون في غاية الصعوبة ، فالطبيعة غير المادية للبيانات المخزنة بالحاسب الآلي، والطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الإثبات الجنائي، ومثال ذلك أن إثبات التدليس والذي قد يقع على نظام المعالجة الآلية للمعلومات يتطلب تمكين سلطة الاستدلال أو سلطة التحقيق من جميع المعطيات الضرورية التي تساعد على إجراء التحريات والتحقق من صحتها للتأكد عما إذا كانت هناك جريمة قد وقعت أم لا.

ومثل هذا الأمر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس [(32)]، وقد يستعصى هذا الأمر فهما على سلطة الاستدلال لعدم قدرتها على فك رموز الكثير من المسائل الفنية الدقيقة التي من خلال ثناياها قد يتولد الدليل المتحصل من الوسائل الإلكترونية كذلك فإن الكثير من العمليات الآلية للبيانات التي قد يقوم بها الحاسب الآلي بطريقة آلية دون الحاجة إلى عمليات إدخال كما هو الحال في احتساب الفائدة على الايداعات البنكية والتي تقيد آليا بأرصدة حسابات العملاء على ضوء الشروط المتفق عليها مسبقا والمخزنة في برنامج الحاسب، قد يكون من السهل اختراقها وارتكاب جرائم تزوير واستيلاء تقع عليها عن طريق إدخال بيانات غير معتمدة في نظام الحاسب أو اجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة.

وبالنظر إلى أن طبيعة هذه العمليات يصعب أن تخلف وراءها آثار مادية ملموسة تكشف عنها ، فإن ذلك سيزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي تتمخض عن هذه العمليات

31) د. عبد القادر الجيراني , الجريمة المعلوماتية ,مقال نشر بتاريخ 30 يوليو , 2017 ,

https://www.facebook.com/405355742894368/posts/1380377042058895/?paipv=0&eav=Afa6rS60EfpskuSqzvjOjN8tCWaWpbHC8m2QnFXxz8twszzUpPVvmWzm80_UF8Z49YA&_rdr

32) حسين بن سعيد الغافري، مرجع سابق.655

ISSN : 2410-1818

الإلكترونية، فقد يستعصى عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها وصعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات أيضا فإن فهم الدليل الموصل إلى اثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية قد يزداد صعوبة، في تلك الحالات التي يتصل فيها الحاسب الآلي بشبكة الاتصالات العالمية، ففي مثل هذه الحالات فإن فهم مثل هذا الدليل يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل السبل لضبطه، وبالنظر إلى أهمية الخبرة في فك غموض الجرائم التي تقع بالوسائل الإلكترونية، فإن ذلك يكشف لنا عن الاهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الإلكترونية الدقيقة وإعداد تقاريرهم الفنية فيها والتي تكون ذات اهمية بالنسبة لقضاء الحكم الذي غالبا ما يتخذ منها سندا يرتكن إليه في المسائل الفنية البحتة.[33]

ولا يغيب عن الذهن إن فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات سلطة الاستدلال وسلطة التحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها الجرائم الإلكترونية، والعمل على المامهم بمكونات الحاسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها، والتي تعتمد على المختصرات خاصة وان الجرائم التي تقع باستخدام الوسائل الإلكترونية في الغالب ما تعتمد على رموز تكون معروفة عند أهل العلم والخبرة [(34)].

المطلب الثاني: الصعوبات على الصعيد الدولي

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المتعلقة بشبكة الإنترنت وإن كان يعد مطلباً تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، ثمة صعوبات ومعوقات دون تحقيقه أهمها ما يلي:

الفرع الأول: مشكلة الاختصاص في الجرائم المعلوماتية

تعد الجريمة المعلوماتية من أهم الجرائم العابرة للحدود الإقليمية لكونها تتميز بمجموعة من الخصوصيات ومن أهمها البعد الدولي، والمتمثل في تعدي النشاط الإجرامي لعدد من الدول، وهو ما يثير العديد من الصعوبات في مجال التعاون الدولي خصوصا إشكالية الاختصاص القضائي بين الدول، وذلك نتيجة لاختلاف التشريعات في المعايير والمبادئ المطبقة في تحديد القانون الواجب التطبيق.

---

33) د/ عادل عامر , مظاهر صعوبة اثبات الجريمة الالكترونية , نشر في مجلة صنعاء نيوز , نشر بتاريخ 17 سبتمبر 2018

34) مرجع سابق، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم :- الدكتور عادل عامر – جريدة الفراعنة(alfaraena.com)).

ISSN : 2410-1818

والجرائم المتعلقة بالإنترنت من أكبر المشاكل التي تثير مسألة الاختصاص على مستوى محلي أو دولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانوناً لذلك، ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود [35]، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى "مبدأ الإقليمية" وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ "الاختصاص الشخصية"، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عند إذن في اختصاصها استناداً إلى "مبدأ العينة" [36].

الفرع الثاني: الصعوبات الخاصة بالمساعدات القضائية الدولية

نعلم أن الأ صل بالنسبة لطلبات الإنابة الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبسط والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، هو الأمر الذي انعكس على جرائم المتعلقة بالإنترنت. كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث إن الدولة متلقيه الطلب غالباً ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب. هو محبط شطب القضية لعدم تلبيه طلب بسيط في الوقت المناسب [37].

تعرف الإنابة القضائية: هو الأجراء الذي تكلف به أفراد الهيئة العدلية المتمثلين في الضباط، وهو قرار يصدر من الجهة العليا وهي القضائية المحقق في الأمر إلى الجهة التنفيذية التي تليها [38]، يتضح من تعريف الإنابة القضائية بأنها نقل مهام من سلطة إلى أخرى لتقوم كل هيئة بالدور المكلف به، وبتلك الصورة تتطبق المواد القانونية بشكل منظم. إلى جانب هذا تقوم الإنابة القضائية على تقديم طلبات رسمية من المحاكم الداخلية إلى المحاكم الأجنبية أو الدولية بغرض الاطلاع على أدلة وتحقيقات أخرى.

35) هلالي عبدالله أحمد، "الجرائم المعلوماتية عابرة الحدود"، دار النهضة العربية، القاهرة، الطبعة الأولى،2007 ص530.

36) هلالي عبدالله أحمد، "الجوانب الموضوعية والإجرائية للجرائم المعلوماتية"، دار النهضة العربية، القاهرة، 2003.ص350.

37) د. حسين بن سعيد الغافري، مرجع سابق. ص655

38) باسنت هاشم، "تعريف الإنابة القضائية وأحكامها وقوانينها، الثلاثاء 2022/10/25م، (تعريف الإنابة القضائية واحكامها وقوانينها – موسوعة(mosoah.com)).

ISSN : 2410-1818

تعد المملكة العربية السعودية من ضمن ستة وسبعين دولة التي أقرت بمعاهدة لاهاي، حيث تعتمد المعاهدة على مساعدة الدول لبعضها عند القيام بالتحقيق في قضية ما وذلك من خلال توفير الأدلة اللازمة وطلب الشهود من الدولة وتعاونها في التحقيق والبحث إلى أن تصل للحقيقة.

وعقدت المؤتمر في قصر السلام بمدينة لاهاي وتواجد العديد من الوزارات والحكومات والوفود الدولية من مختلف دول العالم لمناقشة بنود المعاهدة بشكل كامل، اجتمعت الدول في عام 2019م من أجل البحث في مواد المعاهدة ولتنفيذ أحكامها المتعلقة بالجانب المدني والجانب القضائي، تعد تلك المعاهدة من أهم المعاهدات التي أجرتها الدول مع بعضها حيث تعتمد على نشر الأمان وعدم زعزعة استقرار المجتمعات والمواطنين، بل من خلالها سوف يطبق القانون الدولي لحماية الأفراد بشكل شامل.[39]

الفرع الثالث: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب

تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات. ومن الصعوبات أيضاً التي قد تهدد التعاون في مجال التدريب ما يتعلق بالفروق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين. أيضاً من الصعوبات التي قد تؤثر على العملية التدريبية على التعامل الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية. عن طريق عدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلاً تاماً ومتقناً، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية [(40)].

يستلزم مثل هذه الجرائم وجود تعاون دولي فعال والذي يعتبر ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقنية نظم المعلومات ما يعرف بالمعلومات المختبئة والتي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات، لأجل ذلك كان لا بد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيين، وهذا لن يتحقق إلا بالتدريب، فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها لا بد وأن ترتكز على كيفية تطوير العملية

39) سعيدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، ط1، الإسكندرية،2017 .

40) د. سليمان أحمد فضل، "المرجع السابق" ص450.

ISSN : 2410-1818

التدريبية والارتقاء بها والنهوض بأساليب تحقيقها لأهدافها، من هذا المنطلق كانت الدعوى إلى وجوب تأهيل القائمين على هذه الأجهزة وحيث أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال العدالة الجزائية.[41]

والتدريب المقصود هنا ليس التدريب التقليدي فحسب فلا يكفي أن تتوافر لدي رجال العدالة الجزائية الخلفية القانونية أو أركان العمل الشرطي وإنما لا بد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية. وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، ويلاحظ هنا أنه من الأسهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الادعاء العام [(42)].

ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي، وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي مع ذكر لمفاهيم معالجة البيانات وتحديد نوعية وأنماط الجرائم المعلوماتية، وبيان لأهم الصفات التي يتميز بها المجرم المعلوماتي، والدوافع وراء ارتكاب الجرائم المعلوماتية.

وفيما يتعلق بمنهج التحقيق فإنه لا بد وأن يشتمل على: 1. إجراءات التحقيق، 2. التخطيط للتحقيق، 3. تجميع المعلومات وتحليلها، 4. أساليب المواجهة والاستجواب، 5. مراجعة النظم الفنية للبيانات، 6. أساليب المعمل الجنائي، بالإضافة إلى ذلك لا بد وإن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على أدلة الاتهام وما يخص الملاحقة الدولية والتعاون المشترك.[43]

41) د. محمد صادق إسماعيل , التعاون الدولي في مجال مكافحة الجريمة المعلوماتية ,مقال منشور على موقع المرجع الالكترونى للمعلومات , نشرت بتاريخ 2022/9/25 ,ص344-358

42) د. حسين بن سعيد الغافري، مرجع سابق.ص.ص : 655-670

43) خالد على نزال , التحقيق الجنائى في الجرائم الإلكترونية , بحث مقدم لإستيقاء درجة الحصول على الدكتوراة , الجزء الأول ,العدد 72 , مجلة البحوث القانونية والاقتصادية ,كلية الحقوق , جامعة المنصورة ,مصر ,2020. ص.ص 18:6

ISSN : 2410-1818

المبحث الثالث: مكافحة الجريمة المعلوماتية

المطلب الأول: مكافحة الجريمة على الصعيد الوطني

بيّنت المملكة العربية السعودية جهودها إزاء مكافحة الجرائم المعلوماتية حيث قامت بإنشاء منصة إلكترونية لمكافحة الجرائم المعلوماتية وهي عبارة عن خدمة إلكترونية تقدمها الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر تمكن مكافحة الجرائم المعلوماتية، سواء عن طريق الحصول على معلومات أو محادثات أو صور لحياة إنسان خاصة، ونشرها على وسائل تقنية المعلومات لغرض التشهير أو إلحاق الضرر به.[44]

فالمملكة العربية السعودية: أصدرت في عام 2007 أولي قوانينها في مجال المكافحة التشريعية لجرائم تقنية المعلومات تحت عنوان نظام مكافحة الجرائم المعلوماتية، وأقره مجلس الوزراء بالقرار رقم 79 بتاريخ 1428/3/7 هـ .، وتم التصديق عليه بالمرسوم الملكي رقم 17م بتاريخ 1824/3/8 هـ، وصدر بالقرار رقم 11567 / ب - بتاريخ 1428/3/9 هـ، وكان الهدف منه الحد من نشوء هذه الجرائم المعلوماتية، فقد جاء في المادة الثانية من هذا النظام يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، بما يؤدي إلى ما يلي: (١- المساعدة على تحقيق الأمن المعلوماتى. ٢- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية. ٣- حماية المصلحة العامة، والأخلاق والآداب العامة. ٤- حماية الاقتصاد الوطني).[45]

وقد نظم الأمن العام بالتعاون ورشة عمل عن الجرائم المعلوماتية خلال الفترة من 17 إلى 18 شباط (فبراير) 2014 في مدينة الرياض واستهدفت الورشة توضيح النماذج والأنماط المتعددة للجرائم المعلوماتية، والآثار السلبية المترتبة عنها اقتصادياً واجتماعياً وأمنياً، بما في ذلك سبل الوقاية والعلاج[46]

ونجحت الورشة في استقطاب عدد لا بأس به من الخبراء والمختصين في مجال مكافحة الجرائم المعلوماتية من مختلف القطاعات والأنشطة الأمنية والمالية بما في ذلك قطاع الاتصالات وتقنية المعلومات، باعتبارها القطاعات الأكثر اتساقا واحتكاكاً بالمعلومة، وكونها أيضاً تستخدم أحدث التقنيات

44) محمد محي الدين عوض – مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) – بحث مقدم الي المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد من 25 – 28 اكتوبر 1993 م. ص65

45) قرار مجلس الوزراء بالقرار رقم 79 بتاريخ 1428/3/7 هـ .، وتم التصديق عليه بالمرسوم الملكي رقم 17م بتاريخ 1824/3/8 هـ،

46) محمد سامي دسوقى، ثورة المعلومات وانعكاسها على الواقع العملي، ندوة الابتزاز المفهوم والواقع والعلاج، جامعة الملك سعود، 2011 م. ص75

ISSN : 2410-1818

المتوافرة على مستوى العالم لمعالجة المعلومة ونقلها من مكان إلى آخر وبين أفراد المجتمع بكل شرائحه وطبقاته و خَلُصت الورشة إلى أن السعودية، كبيئة مالية واستثمارية وأمنية لا تعيش، ولله الحمد، ظاهرة أو حالة من ظواهر الجرائم المعلوماتية على الرغم من انتشار استخدام وسائل وأدوات التكنولوجيا الحديثة في الاتصال وتقنية المعلومات في المملكة، إذ تشير المعلومات إلى أن عدد الاشتراكات في خدمات الاتصالات المتنقلة قد بلغ نحو 51 مليون اشتراك بنهاية الربع الثالث من العام الماضي، وبنسبة نمو "انتشار" لخدمات الاتصالات المتنقلة على مستوى السكان بلغت نحو 170 في المائة. [47]

وما ساهم بشكل كبير في الحد من انتشار الجرائم المعلوماتية في المملكة، إقرار الحكومة السعودية لنظام صارم لمكافحة الجرائم المعلوماتية في السعودية، الذي عرف الجريمة المعلوماتية على أنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام النظام و وقد حدد النظام عدداً من أنماط ونماذج الجريمة المعلوماتية، التي من بينها على سبيل المثال لا الحصر، التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه، أو الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، حتى ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً. [48]

ومن بين النماذج أيضاً للجرائم المعلوماتية، الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني بهدف تغيير تصاميم الموقع، أو إتلافه أو تعديله أو شغل عنوانه. وأخيراً حدد النظام من بين أنواع الجرائم المعلوماتية، المساس بالحياة الخاصة بالناس عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرات، أو ما في حكمها، إضافة إلى التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة .[49]

ومن بين جهود المملكة في مكافحة انتشار الجرائم المعلوماتية، إطلاق هيئة الاتصالات وتقنية المعلومات بالأمس القريب، لحملة توعوية على مستوى المملكة، استهدفت التعريف بنظام مكافحة الجرائم المعلوماتية والرفع من مستوى الوعي بسبل المكافحة والوقاية والعلاج، بما في ذلك تبيان حقوق

47) يونس خالد عرب مصطفي – جرائم الحاسوب " دراسة مقارنة" – رسالة ماجستير – كلية الحقوق الجامعة الاردنية – عمان 1994 م ص52.

48) د. عادل يوسف عبدالنبي الشكرى – الجريمة المعلوماتية وازمة الشرعية الاجرائية – جامعة الكوفة – كلية القانون – منشور بمجلة مركز دراسات الكوفة العدد السابع 2008, ص65

49)خالد على نزال , التحقيق الجنائى في الجرائم الإلكترونية , بحث مقدم لإستيقاء درجة الحصول على الدكتوراة , الجزء الأول ,العدد 72 , مجلة البحوث القانونية والاقتصادية ,كلية الحقوق , جامعة المنصورة ,مصر ,2020. ص69

ISSN : 2410-1818

المستخدمين وفق ما كفله النظام لهم، إضافة إلى التوعية بسبل الوقاية من خطر الوقوع ضحايا لأي نوع من هذه الجرائم .وهدفت الحملة أيضاً، إلى لفت انتباه مستخدمي خدمات الاتصالات وتقنية المعلومات في المجتمع السعودي إلى خطورة الجرائم المعلوماتية، والتحذير من التساهل أو الإهمال أثناء التعامل مع المعلومات، مع إيضاح المهمات للجهات المعنية بمكافحة الجرائم المعلوماتية، إضافة إلى إيضاح المسؤوليات والعقوبات المترتبة على مرتكب الجريمة المعلوماتية، وكذلك التعريف بسبل التقاضي، وآليات الشكوى لمن يقعون ضحايا لمثل هذا النوع من الجرائم. [50]

وللقطاع المصرفي السعودي أيضاً جهود ملحوظة وملموسة في مكافحة الجرائم المعلوماتية بأنواعها المختلفة، خاصة التي تعتمد على استخدام وسائل التكنولوجيا والتقنية الحديثة في الاتصالات ونقل المعلومات، ولا سيما أن القطاع المصرفي السعودي قد شهد خلال السنوات القليلة تحولاً ملحوظاً وملموساً إلى التعاملات الإلكترونية، التي تعتمد بشكل كبير على استخدام وسائل تقنية الاتصالات الحديثة. من هذا المنطلق حرصت جميع البنوك التجارية العاملة في المملكة على تحصين أنظمتها المعلوماتية الداخلية بما في ذلك أنظمتها المعلوماتية المتعلقة بحسابات العملاء، باستخدام أفضل برامج الحماية المتوافرة على مستوى العالم، مثل المعيار الخاص بحماية بيانات عمليات بطاقات الدفع بهدف التقليل من مخاطر الاحتيال، الذي يعرف بالمعيار الأمني لصناعة بطاقات الدفع والذي أقره مجلس المعايير الأمنية لصناعة بطاقات الدفع المعني بوضع المعايير الأمنية لبطاقات المدفوعات عالمياً و دون أدنى شك أن السعودية تبذل جهوداً كبيرة في سبيل مكافحة الجرائم المعلوماتية بأنواعها وأنماطها وأشكالها المختلفة، ولكن لأن تنجح هذه الجهود وتأتي بأكلها وتحقق الأهداف المنشودة منها وكما اتفقت جميع أوراق العمل التي قدمت بالورشة سالفة الذكر، فلابد من تعاون جميع أفراد المجتمع مع تلك الجهود، من خلال الحرص عند استخدام وسائل الاتصالات وتقنية المعلومات الحديثة من عدم إساءة استخدامها من جهة أو من الوقوع ضحية لإساءة استخدامها من قبل الآخرين من جهة أخرى.[51]

50) سعيدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، ط1، الإسكندرية،2017 . ص105

51) ليندة شرابشة , السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية والاتجاهات الدولية في مكافحة الجريمة الالكترونية , جامعة زيان عاشور الجلفة , المجلد 2009، العدد 1 (30 إبريل/نيسان 2009 , الجزائر , ص248

ISSN : 2410-1818

المطلب الثاني: مكافحة الجريمة على الصعيد الدولي [52]

تضافرت الجهود من أجل كبح هذه الظاهرة بنجاعة وفعالية ، وفي إطار الجهد المبذول فان هناك العديد من الهيئات الدولية التي تلعب دورا ملحوظا في هذا المجال على رأسها منظمة الأمم المتحدة التي بذلت جهودا لا يستهان بها ، مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشار الجريمة المعلوماتية ، وهذا من خلال مؤتمراتها لمنع الجريمة ومعاملة المجرمين بدءا بالمؤتمر السابع عام 1985 إلى غاية المؤتمر الثاني عشر عام 2010 .إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات وذلك تحت إشراف الأمم المتحدة عام 1994 ، الذي نتج عنه عدة توصيات وقرارات ذات صلة بالجرائم المعلوماتية ، وقد تضمنت شقين اثنين واحد موضوعي يتناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، وثاني إجرائي يتضمن الإجراءات الواجب إتباعها لتطبيق القواعد الموضوعية.

كما كان للمنظمة العالمية للملكية الفكرية دور بارز في هذا المجال، وذلك من خلال خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الآلي وهذا من خلال المادة 04 و 05 من اتفاقية تريبس، هذا إلى جانب الجهد الكبير المبذول من قبل الاتحاد الدولي للاتصالات وهذا في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبل الأمين العام للاتحاد عام 2007، و الذي يرمي إلى تحقيق عدة أهداف أبرزها استحداث تشريع نموذجي لمكافحة الجريمة المعلوماتية يمكن تطبيقه عالميا ويكون قابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

أما المنظمات الإقليمية فقد كان للاتحاد الأوروبي دور فعال في هذا المجال حيث أثمرت جهوده عن ميلاد أولى المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية بالعاصمة المجرية بودابست عام 2001 ، و قد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية ببعضها البعض، وتعزيز قدرات القضاء وكذا تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات الجرائم المعلوماتية في إطار القوانين المحلية، كما أنشأ الإتحاد الأوروبي أجهزة تساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوروبول والمركز الأوروبي لمكافحة الجريمة المعلوماتية والذي أفتتح في جانفي 2013م.[53]

---

52) أيمن قادري، بحث مكافحة الجرائم المعلوماتية في القانون الدولي، العدد 1, مجلة جامعة جيلالي ليابس , الجزائر , ديسمبر-٢٠١٤.ص 13

53) ليندة شرابشة , السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية والاتجاهات الدولية في مكافحة الجريمة الالكترونية , جامعة زيان عاشور الجلفة , المجلد 2009، العدد 1 (30 إبريل/نيسان 2009 , الجزائر , ص248

ISSN : 2410-1818

هذا عن الجهود الغربية أما الجهود العربية فقد أسفرت هي أيضاً عن ميلاد اتفاقية عربية لمكافحة جرائم تقنية المعلومات، وهذا كنتيجة للاجتماع المشترك لمجلسا وزراء الداخلية والعدل العرب والمنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة وذلك في ديسمبر 2010م وهذا بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات.[54]

الخاتمة

تناول هذا البحث موضوع الجرائم المعلوماتية، ويرجع السبب في اختيار هذا الموضوع هو التطور التكنولوجي الهائل في وسائل التواصل الاجتماعي والاقبال المتزايد عليها، مما تسبب ذلك في استهداف العديد من الفئات المجتمعية المختلفة وايقاعهم ضحايا لمرتكبي هذا النوع من الجرائم، وتطرقنا في موضوعنا إلى ثلاثة مباحث، تناولنا في المبحث الأول ماهية الجريمة المعلوماتية وأركانها، وتحدثنا في المبحث الثاني عن الصعوبات التي تواجه التعاون الوطني والدولي المتعلقة بالجريمة المعلوماتية، والمبحث الثالث مكافحة الجريمة المعلوماتية، ومن خلال هذا البحث توصلنا إلى العديد من النتائج والتوصيات نذكر أهمها.

النتائج:

1. تتعدد التعريفات حول الجريمة المعلوماتية وحتى وقتنا الحالي لم يتوصل الفقهاء إلى تعريف شامل ودقيق لهذه الجريمة.

2. تختلف الجريمة المعلوماتية اختلافاً كلي عن الجريمة التقليدية.

3.تعتبر الجرائم المعلوماتية من الجرائم التي يصعب اكتشافها، فهمي تعتبر جريمة ناعمة عابرة للحدود.

4.تعتبر الجرائم المعلوماتية من الجرائم الخطرة لأنها تمثل تهديداً مباشراً للأمن والاستقرار وعائق للتطوير والتنمية الاجتماعية.

5. أن مكافحة جريمة المعلوماتية تقتضي توحيد التشريعات المختلفة من ناحية، وأن يكون نظام الإثبات بالدليل الإلكتروني واحد بين الدول التي وقعت فيها الجريمة من ناحية أخرى.

6. أهمية وجود تشريع قضائي محلي خاص بكل دولة يعالج مثل هذه الجرائم، على أن يراعي هذا التشريع إمكانية استغلال سمة عبر الوطنية لتلك الجرائم، مع اقتراحها ما يسمى بالتحقيق الدولي

54) ديباجة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة بتاريخ 21 ديسمبر 2010

ISSN : 2410-1818

المشترك لهذه الجرائم، بحيث يمكن من خلال إرسال معلومات مفصلة عن تلك الجريمة إلى أي من الدول مطالبتها باتخاذ الإجراءات القضائية المناسبة.

7. أهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات والتي منها تلك الجرائم التي تقع بسبب ثورة الاتصالات عن بعد.

التوصيات:

1. ضرورة وجود تعاون دولي لمكافحة الجرائم المعلوماتية.
2. دعوة الاعلام لإبراز التشريعات العقابية الصادرة بشأن مرتكبي الجرائم المعلوماتية.
3. عقد اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت، بالإضافة إلى تحديث القوانين الجنائية الموضوعية فيها والإجرائية بما يتناسب مع التطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.
4. "بالمساعدات القضائية الدولية" والتباطؤ في الرد ، نوصي بإيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلاً أو بالسماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة.
5. " مجال التدريب" نوصي باتخاذ المزيد من الإجراءات في الحملات التوعوية للتبنية بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبالمزيد من التنسيق مع الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية تناسب جميع الجهات.
6. بالإضافة إلى قيام بعض العمليات المشتركة والتي من شانها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر من شأنها.

ISSN : 2410-1818

قائمة المراجع

أولا: الكتب

- أحمد عبدالله المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، المركز القومي للإصدارات القانونية، ط1، القاهرة، 2017.
- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، الناشر: دار النهضة العربية للنشر والتوزيع، القاهرة، 2009.
- خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008.
- د. محمد صادق إسماعيل، التعاون الدولي في مجال مكافحة الجريمة المعلوماتية،مقال منشور على موقع المرجع الالكترونى للمعلومات، نشرت بتاريخ 2022/9/25.
- دياب البدوي، الجرائم الإلكترونية المفهوم والأسباب، الملتقي العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، كلية العلوم الاستراتيجية، 2018.
- سعيدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، ط1، الإسكندرية، 2017.
- سليمان احمد محمد فضل، المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، بدون دار نشر، القاهرة 1428هـ.
- عادل يوسف عبدالنبي الشكرى – الجريمة المعلوماتية وازمة الشرعية الاجرائية – جامعة الكوفة – كلية القانون – منشور بمجلة مركز دراسات الكوفة العدد السابع 2008.
- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت.2013 .
- غنية باطلي، الجريمة الالكترونية: دراسة مقارنة، العدد 1، الجزائر: منشورات الدار الجزائرية، 2015 .
- محمد بن أحمد علي المقصودي، الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيًا، المجلة العربية للدراسات الأمنية، المجلد33، العدد (70)، الرياض، 2017.
- محمد سامي دسوقى، ثورة المعلومات وانعكاسها على الواقع العملي، ندوة الابتزاز المفهوم والواقع والعلاج، جامعة الملك سعود، 2011 م.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، 2009 م.
- هلالي عبدالله أحمد، "الجرائم المعلوماتية عابرة الحدود"، دار النهضة العربية، القاهرة، الطبعة الأولى، 2007.

ISSN : 2410-1818

- هلالي عبدالله أحمد، "الجوانب الموضوعية والإجرائية للجرائم المعلوماتية"، دار النهضة العربية، القاهرة، 2003.

ثانيا : الأبحاث العلمية

- أيمن قادري، بحث مكافحة الجرائم المعلوماتية في القانون الدولي، العدد 1، مجلة جامعة جيلالي ليابس، الجزائر، ديسمبر-2014.
- خالد على نزال، التحقيق الجنائي في الجرائم الإلكترونية، بحث مقدم لاستيفاء درجة الحصول على الدكتوراة، الجزء الأول،العدد 72، مجلة البحوث القانونية والاقتصادية،كلية الحقوق، جامعة المنصورة،مصر،2020.
- د. فتوح الشاذلي، عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة و القانون - دراسة مقارنة - منشورات الحلبي الحقوقية، بيروت، 2015 .
- ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية والاتجاهات الدولية في مكافحة الجريمة الالكترونية، جامعة زيان عاشور الجلفة، المجلد 2009، العدد 1 (30 إبريل/نيسان 2009، الجزائر.
- محمد محي الدين عوض – مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) – بحث مقدم الي المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد من 25 – 28 اكتوبر 1993 م.

ثالثا: رسائل الماجستير والدكتوراة

- د. شاهين خضر، رضوان سعادة، الجريمة الالكترونية وإجراءات مواجهتها، رسالة ماجستير، ، كلية الحقوق .جامعة محمد بوضياف، 1441هـ
- يونس خالد عرب مصطفي – جرائم الحاسوب " دراسة مقارنة" – رسالة ماجستير – كلية الحقوق الجامعة الاردنية – عمان 1994 م

رابعا : القوانين والأنظمة

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة بتاريخ 21 ديسمبر 2010.
- قرار مجلس الوزراء السعودى رقم 79 بتاريخ 1428/3/7 هـ ، وتم التصديق عليه بالمرسوم الملكي رقم 17م بتاريخ 1824/3/8 هـ،
- نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8 هـ.

ISSN : 2410-1818

خامسا :مواقع الانترنت

- د. عادل عامر، مظاهر صعوبة اثبات الجريمة الالكترونية، الثلاثاء 2022/10/25م، (مظاهر صعوبة اثبات الجريمة الالكترونية بقلم - الدكتور عادل عامر - جريدة الفراعنة (alfaraena.com)).
- د. عبد القادر الجيرانى، الجريمة المعلوماتية،مقال نشر بتاريخ 30 يوليو، 2017،

https://www.facebook.com/405355742894368/posts/1380377042058895/?paipv=0&eav=Afa6rS60EfpskuSqzvjOjN8tCWaWpbHC8m2QnFXxz8twszzUpPVvmWzm80_UF8Z49YA&_rdr

- باسنت هاشم، "تعريف الإنابة القضائية وأحكامها وقوانينها، الثلاثاء 2022/10/5م؛ (تعريف الإنابة القضائية واحكامها وقوانينها - موسوعة(mosoah.com)).