مجلة الاجتهاد القضائي - المجلد 13 – العدد 01 - (العدد التسلسلي 26) - مارس 2021 (ص ص: 39 – 58)
مخبر أثر الاجتهاد القضائي على حركة التشريع - جامعة محمد خيضر بسكرة

الجرائم ذات التقنية العالية والحماية من الهجمات الإلكترونية في النظام السعودي

High-tech crimes and protection against cyber attacks in Saudi Law

د. محمد مكاوي محمد [1]
أستاذ
جامعة الملك فهد (السعودية)
mmakkawi@kfupm.edu.sa

د. دينا عبد الله صالح [2]
استاذ مساعد
جامعة تبوك (السعودية)
dabdullah@ut.edu.sa

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر
13 سبتمبر 2020	19 نوفمبر 2020	31 مارس 2021

الملخص:

تلقي هذه الدراسة الضوء على موضوع مخاطر الجرائم ذات التقنية العالية من خلال استعراض النظرة القانونية لنظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية، وما رتبه من عقوبات على تلك الجرائم، كما تبين لنا ذات الدراسة مدى كفاية هذا القانون للحد من هذه الجرائم في المملكة العربية السعودية، وتكمن أهمية هذه الدراسة في أهمية موضوعه حيث يتعرض للأنظمة السعودية في معرفة إبراز الجوانب القانونية التي تحكم الجرائم ذات التقنية العالية، مع بيان خصائصها ومفاهيمها وسمات مرتكبي هذه الجريمة وأشكالها وكيفية مكافحتها. وتوضيح الخطر الذي تشكله هذه الجرائم على الحواسيب والأجهزة الإلكترونية الأخرى وعلى المجتمع وكيفية حمايتها. ومن أهم النتائج التي تم التوصل إليها المساعدة على تحقيق الأمن المعلوماتي، وحماية المصلحة العامة، والأخلاق، والآداب العامة، وحماية الاقتصاد الوطني. ومن التوصيات نظراً لطبيعة الجرائم ذات التقنية العالية وطبيعتها المتعدية للحدود وما يمكن أن تثيره من إشكالات قانونية من حيث الاختصاص والإثبات يتعين على المملكة العربية السعودية إبرام اتفاقيات دولية جماعية أو ثنائية على حد سواء.

الكلمات المفتاحية: الجرائم، التقنية العالية، الأنظمة السعودية، أمن الإنترنت، الإثبات.

Abstract :

This study highlights the subject of high technology crimes risk by reviewing the legal perspective of the computer crimes control in Saudi Arabia and any penalties for such crimes. The same study also shows how far the law is effective on such offense in Saudi Arabia. The importance of this study is that it is subjected to Saudi laws is aware of highlighting the legal aspects that govern the crimes of High-tech. It also describes the characteristics, concepts and forms of the perpetrators of this crime and how to combat it and to illustrate the danger of these crimes to computers and other electronic devices and on the community and how to protect them. One of the most important results is to help achieve information security and protecting the public interest, morality, public morality and protecting the national economy. One recommendation is that, given the nature and trans boundary nature of high-tech crimes, the legal problems that it can raise in terms of competence and evidence, Saudi Arabia must conduct international conventions, both collective and bilateral.

key words :

High - tech crimes - Saudi Law – Secure information- prosecution.

[2] المؤلف المرسل: د. دينا عبد الله صالح ـــــــــــــ *Email: dina198465@gmail.com*

مقدمة:

إن التطور التكنولوجي السريع الذي يعيشه العالم الآن والذي يعرف بالعصر المعلوماتي أو عصر ثورة المعلومات، فظهور الحاسب الآلي والإنترنت، وتكنولوجيا المعلومات والاتصالات أدى إلى التقدم الإنساني والرفاهية في أغلب مناحي الحياة التعليمية والاقتصادية والعديد من المجالات الأخرى. فاستخدامات الحاسب تزيد يوماً بعد يوم في شتى الأعمال ومختلف المعاملات سواء كانت مالية أو دولية أو تدخل في اقتصاديات الدولة، فالتكنولوجيا الحديثة أصبح الاعتماد عليها كبيراً في مختلف أوجه الحياة.

غير أن هذه كل التكنولوجيا الحديثة ذاتها تحمل بين ثناياها خبراء جدد يتمتعون بالحرفية والخبرة في تطويع هذه التكنولوجيا للقيام بأعمال إجرامية جديدة تعتمد على التقنية الحديثة في تنفيذها وبأساليب مبتكرة، وطرق جديدة لم تكن معروفة من قبل، الأمر الذي يمثل خطراً كبيراً وأضراراً للفرد والمجتمع خاصة الخدمات والمعاملات. كما يجب التعرف على تلك وما تمثله من خطورة، واطلاق حملة للتوعية بها وكيفية مكافحتها لأن السواد الأعظم من الناس يجهلها.

تأتي أهمية الدراسة في كون أهمية موضوعه، من الناحية الاجتماعية؛ إن استخدام الأنترنت في جميع المعاملات أصبح الوسيلة الأمثل والمختصرة للوقت والجهد والمال مما جعل الكل يتجه لها، بيد أن لهذه العولمة آثار اتخذها البعض بطريقة مضادة للمجتمع بدافع إجرامي وإساءة سمعة الضحية سواء بطريقة مباشرة أو غير مباشرة.

كما تكمن أهداف هذه الدراسة في تحقيق الأهداف التالية:

1- توضيح لمعنى الجريمة وما يندمج فيها من مستجدات العصر الحديث.

2- تعريف العامة بالجرائم التي قد تنشأ في الفضاء الإلكتروني.

3- إبراز صور لبعض أنواع هذه الجرائم.

4- توضيح موقف المشرع السعودي من هذه الجرائم.

5- التعرف على العقوبات التي فرضتها المملكة العربية السعودية على هذه الجرائم.

6- نشر الوعي والتنبيه بخطورة هذه الجرائم والعقوبات المقررة على مرتكبيها.

إشكالية الدراسة تتمثل في أن الانتشار الكبير للكمبيوتر والإنترنت قد جلبا مجموعة من الجرائم التي لم تكن معروفة من قبل والتي أصبحت منتشرة في الوقت الحالي والتي يتم فيها استهداف البرامج والبيانات والمعلومات من قبل تلك الجرائم والتي قد تسبب مشكلات سواء اجتماعية أو خسائر للمؤسسات والحكومات. ومدى خطورتها على المجتمع والاقتصاد الوطني.

أتبعت في هذه الدراسة المنهج الاستقرائي التحليلي والوصفي وذلك بالرجوع إلى المصادر الشرعية والقانونية في هذا الشأن بتجميع المادة المطلوبة من مصادرها الأصلية وشرحها وبيانها بالتحليل والمقارنة. وقسمت الدراسة إلى مبحثين: تناولت في المبحث الأول مفهوم الجرائم ذات التقنية العالية وخصائصها وأنواعها، أم المبحث الثاني الإجراءات القانونية للجرائم ذات التقنية العالية في المملكة العربية السعودية وطرق إثباتها وعقوبتها.

المبحث الأول: مفهوم الجرائم ذات التقنية العالية وخصائصها وأنواعها

يشهد العالم المعاصر تطوراً كبيراً ومتلاحقاً في مجال التكنولوجيا عامة والتكنولوجيا الرقمية خاصةً، وبسرعة مهولة نجد انفسنا كل يوم في تطور جديد وتقنية واستحداثات جديدة، وأن الجرائم ذات التقنية العالية خلقت عالماً جديداً لا يعترف بالحدود الجغرافية، التي فقدت كل آثر لها في بيئة افتراضية متشعبة العلاقات. وجميعها من مظاهر العولمة وشبكة الإنترنت، والتي بالرغم من فوائدها الكبيرة إلا إن لها سلبيات عديدة ساعدت على أنتشار ظاهرة الإجرام، بحيث سهلت عمليات الاتصال بالإنترنت إيصال المعلومات بين المجرمين والجماعات العاملة في عمليات التهريب والإتجار بالمخدرات، وكذلك عمليات النسخ غير المباشر لنظم وتشغيل الحاسب الآلي مما يؤدي لخسارة منتجي تلك النظم والبرامج، كذلك عمليات التزييف الإلكتروني على شبكة الإنترنت وغيرها من الجرائم، خاصة من خلال التلاعب بالأشخاص لأداء أفعال أو الإقرار بمعلومات حساسة وهو ما يعرف بالهندسة الاجتماعية (*social engineering*) وكل هذا يدلل على أن طرق وآليات الجريمة التقنية قد تطورت وخرجت عن طور التقليد.

غير أن التكنولوجيا الحديثة أعطت مجالاً للتوسع في التعامل مع الجريمة وفي الإثبات الجنائي سواء في مجال الأجهزة المتطورة أو في مجال العلوم المختلفة المساعدة في عملية التحقيق وصولاً لإثبات التهمة، بالإضافة إلى تطوير وتأهيل العاملين في مجال التحقيق الجنائي للقيام بدورهم على أفضل وجه. وفي المطلب الأول من هذا المبحث سيتم التطرق لمفهوم الجريمة بشكل عام ومن ثم لمفهوم الجرائم ذات التقنية العالية بشكل خاص واركناها وخصائصها وبعضاً من صورها.

المطلب الأول: مفهوم الجريمة بصفة عامة

للجريمة عدة تعاريف تختلف من تشريع إلى آخر، ومن علم إلى آخر، مع أن فكرة الجريمة لا تتغير في جوهرها بل تتغير صورها وتتعدد بحسب المصدر الذي وضع الأوامر والأنظمة. وعليه فإن للجريمة مفاهيم متعددة فقد تم تعريفها في الشريعة الإسلامية بأنها" إتيان فعل محرم معاقب على فعله، أو ترك فعل واجب معاقب على تركه"[1]، وتعرف الجريمة

لغة بأنها "الذنب والتعدي، يقال جَرَمَ فُلان جَرْما أي أَذْنَب. وهي مشتقة من الجرم بمعنى القطع والكسب، واستعملت بمعنى التعدي والذنب والحمل على الفصل حملاً آثماً[2]، أما من المنظور القانوني فقد تم تعريفها بأنها "كل سلوك إيجابي أو سلبي يقع بالمخالفة لأحكام القانون".

أما تعريف الجريمة في النظام السعودي، لم يتطرق النظام السعودي لتعريف الجريمة بصفة عامة، وإنما اكتفى بتعريفها على ما ورد في الفقه الإسلامي؛ بأنها "إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم". أو هي "فعل أو ترك ما نصت الشريعة على تحريمه والعقاب عليه"[3]. وخلاصة القول أن الجريمة هي كل فعل إيجابي أو سلبي صادر عن إرادة إجرامية، يقرر له المنظم عقوبة أو تدبير احترازي. ولا نجد اختلاف في تعريف الجريمة في النظام السعودي عن تعريف الجريمة في الشريعة الإسلامية. وتوجد عدة عوامل دافعه لارتكاب الجريمة منها ما هو داخلي مثل الوراثة والجنس والنوع والأمراض العضوية والعقلية، ومنها ما هو خارجي مثل العوامل الاجتماعية والبيئة الأسرية والأصدقاء وغيرها.

المطلب الثاني: مفهوم الجرائم ذات التقنية العالية وأركانها وخصائصها

لقد شاع استخدام مصطلح الجرائم ذات التقنية العالية في السنوات الأخيرة، وهي الجريمة التي تلعب فيها التقنية الرقمية بيانات الحاسب الآلي والبرامج المعلوماتية دوراً مهماً[4]، إذن هي تتمثل في كل فعل أو سلوك غير مشروع مرتبطة بأي جهة أو شكل بجهاز الحاسوب أو شبكاته، وغالباً يكون الهدف من تلك الجرائم هو سرقة المعلومات الموجودة في الأجهزة الحاسوبية وغيرها من الوسائط التكنولوجية الأخرى أو هدف أخر غير مباشر ألا وهو الأشخاص أو جهات معنية مرتبطة بتلك المعلومات التي تم سرقتها. فالتغيرات التطويرية للعالم وحداثتها واختلاف الثقافات أدى كذلك إلى حداثة الجريمة ذات التقنية العالية ومن ثم لاختلاف مفهومها بين الدول، وهذه الجرائم من هذا النوع لها مسميات عديدة منها:

- الجرائم التي تخص الكمبيوتر والإنترنت.
- الجرائم التي تكون على مستوي عالي من التقنية.
- جرائم الياقات البيضاء.
- والجريمة الإلكترونية.

وللبحث في أي فرع من فروع المعرفة لابد لنا أولاً أن نبين مفهوم الجريمة ذات التقنية العالية وذلك من خلال إبراز السمات الأساسية للجريمة ذات التقنية العالية ومفهومها وخصائصها وتصنيفاتها وصورها.

الفرع الأول: تعريف الجرائم ذات التقنية العالية وفقاً لنظام مكافحة الجرائم المعلوماتية السعودي

نصت المادة الأولى من نظام مكافحة جرائم المعلوماتية بأن الجريمة المعلوماتية هي " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" [5]. كما عرفت نفس المادة التقنية [6]. كما تعرف بأنها: "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات، التي تصلح لأن تكون محلاً للتبادل والاتصال، أو التفسير أو التأويل، أو للمعالجة، سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة" [7].

ونحن نرى أن المشرع السعودي جانبه الصواب بوضعه تعريف جامع مانع للجريمة المعلوماتية، حيث كان من الأجدى به أن يترك ذلك للفقه والقضاء من جهة، ومن جهة ثانية بقيت عدم حصر الجريمة المعلوماتية في إطار أفعال محددة تحسباً للتطور التكنولوجي والتقني في المستقبل الذي من الممكن أن يفرز أخرى قد لا يشملها التعريف الذي وضعه القانون، ومن المعلوم أن الفقه والقضاء عادةً يتفادى التسرع في وضع تعاريف للمفاهيم والظاهرة القانونية الجديدة لكونها متطورة وقابلة للتغير. فيكون التعريف والحال هكذا بمثابة مجازفة لا تسلم من المخاطر.

الفرع الثاني: أركان الجريمة ذات التقنية العالية

أولاً - الركن المادي:

ويمثل هذا الركن كيان الجريمة، وهو وجود بيئة رقمية واتصال بالإنترنت ومن خلالها يقوم المجرم المعلوماتي بتحميل الحاسب الآلي ببرامج الاختراق أو إعداده لهذه البرامج المخترقة بصورة يمكن إثباتها كجريمة، وبه يتحقق الاعتداء على المصلحة المراد حمايتها وهذا الفعل يمثل النشاط الذي يصدر عن الجاني مرتكب الجريمة.

ثانياً- الركن المعنوي:

يعبر عن إرادة المجرم المعلوماتي (القصد الجنائي men's rea) والعلاقة التي تربطهُ بماديات الجريمة وشخصيته، فلابد أن يرتكب هذا الفعل المُجَرّم بعلم وإرادته الفعلية طواعية ورغبة وعن إدراك لأهداف التخريبية.

ثالثاً- خصائص الجرائم ذات التقنية العالية وتصنيفاتها:

1 - خصائصها:

تتميز الجرائم ذات التقنية العالية بعدة خصائص بحيث أنها تختلف عن الجريمة التقليدية وذلك لارتباطها بتقنية وتكنولوجيا المعلومات[8]، ويمكن توضيح هذه الخصائص كما يلي[9]:

أ – أنها من الجرائم الناعمة أي التي لا تتطلب عنفاً كالجريمة التقليدية مثل جرائم السرقة أو الجرائم التي تتطلب احتكاكا مع رجال الشرطة، ونعومتها تتمثل في أنها عبارة عن سطو إلكتروني، حيث أن نقل البيانات من حاسب لأخر أو قرصنة حاسوب يتم دون عنف.

ب – يصعب إثباتها، نسبةً لافتقاد الأدلة التي تدل على الجاني وغياب البصمات أو الشواهد التي تتوافر لدى الجرائم التقليدية.

ج – تعتبر من الجرائم العابرة للحدود الدولية (*Transnational*) فالطفرة في الاتصالات حولت العالم إلى قرية كونية صغيرة، وربطت بين الشعوب المتباعدة، فأصبحت عملية تبادل المعلومات والمعارف سهلة وميسورة فالعالم كله أصبح مربوط بشبكة من الاتصالات عن طريق الأقمار الصناعية والإنترنت، مما سهل الجريمة التقنية وانتشارها فهي لا تعرف الحدود بين الدول ولا تعرف مكاناً أو زماناً.

د– السرعة في التنفيذ: أي السهولة في تنفيذ الجريمة ذات التقنية العالية بضغطة زر واحدة يمكن نقل ملايين العملات خاصة ما يُعرف ب (*bitcoins*) من مكان لآخر بعد الإعداد لتنفيذها واستخدام البرامج المعينة والمعدات للسرقة الإلكترونية.

و– الديمومة: المعدات والبرامج المسروقة التي يمكن أن تستخدم لفترة طويلة.

ه – القيمة: معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم ذات القيمة.

ت– الإزالة: الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها وحذفها فقط.

الفرع الثالث: تصنيف الجرائم ذات التقنية العالية

تختلف الجرائم ذات التقنية العالية عن بعضها البعض باختلاف كيفية التنفيذ، والهدف من الجريمة لذا يمكن تصنيفها حسب التالي:

أولاً – تصنف الجرائم وفقاً لنوع الجريمة ومحلها:

وهذا النوع من الجرائم يشمل نوعين منها ما هو متعلق بالحاسوب أو معلوماته كتشويه البيانات أو إتلافها وذلك عن طريق الفيروسات أو جرائم تقع على ما تمثله المعلومات من أموال وأصول وتلاعب في المعلومات المخزنة داخل الحاسب الآلي. كذلك الجرائم التي تكون متعلقة بالمتعلقات الشخصية أو الحياة الخاصة بالإنسان كبياناته ومعلوماته مثال الصور والفيديوهات. والجرائم التي تمس الشخص بحقوقه سواء المملوكة له أو الفكرية المتعلقة ببرامج الكمبيوتر وأنظمته أي جملةً بمعني قرصنة البرمجيات.

ثانياً– تصنيف حسب المهمة التي قام بها الحاسوب ودوره في الجريمة

وتضم العناصر السرية والنظم كالدخول غير المصرح به وغير القانوني مثل أن يخترق شخص شبكة حواسيب مرتبطة بالأنترنت واختراق نظام الأمن والدخول للمحتويات والكشف

عنها. وكذلك العمل على تدمير كل محتويات الجهاز الذي تم الدخول عليه ويقوم الشخص المخترق بدحض البيانات ومسحها أو يعمل على تعطيلها أو تشويشها وتعطيل برامجها لكي يجعلها غير قابلة للاستخدام. والعمل على اعتراض أنظمة الحاسب. وعدم معرفة استخدام جهاز الكمبيوتر واستخدامه بسوء أو الإساءة إليه.

ثالثاً- تصنيف حسب الهدف الذي كان من أجله الجريمة أو دوافعه لذلك:

ويكون من هذه الأهداف المعلومات؛ والوصول لهذه المعلومات بطريقة غير شرعية، كذلك بالنسبة للبنوك أو الشركات الكبيرة والحكومات يكون الهدف سرقة المعلومات السرية سواء لهدف سياسي أو من أجل الهدف المادي. كذلك يكون الغرض من أجل تعطيل خادم الذي يوفر المعلومات عن طريق شبكة الأنترنت والتلاعب بها. أيضاً الكسب غير المشروع سواء كان مادي أو معنوي أو سياسي وذلك، إما بالعمل على تزوير البطاقات الائتمانية لسرقة الحسابات البنكية.

المطلب الثالث: صور لبعض الجرائم ذات التقنية العالية في المملكة العربية السعودية

تتعدد صور الجرائم التقنية وتتفرع كما ذكرنا سابقاً في أنواعها، ونحدد في هذا المطلب الجرائم ذات التقنية العالية الأكثر انتشاراً في المملكة العربية السعودية كما يلي:

1- الجرائم الجنسية والممارسات غير الأخلاقية: تؤكد عدد من الدراسات أن الجرائم الجنسية والتردد علي المواقع الإباحية بصورة متواصلة، تتصدر القائمة في المملكة العربية السعودية، وهذا يؤدي إلى انحرافات أخلاقية غير مرغوبة وسلوكيات شاذة تضر بالمجتمع، مما يترتب عليه انتشار الجريمة وأن تشيع الفاحشة.

2- جرائم الاختراقات أو الدخول غير المصرح به: (*unauthorized access*) لموقع إلكتروني أو إلى نظام معلوماتي أو زراعة الفيروسات[10] لتدمير المعطيات والملفات المخزنة أو لتعديلها، أو يكون الاختراق إما للابتزاز (*extortion*) أو لتهديد شخص، أو لحمله على القيام بفعل أو الامتناع عن فعل ويقع هذا الفعل ضمن التصرفات غير القانونية.

3- التنصت والتسجيل سواء المرئي أو الصوت: (*wiretapping*) زراعة برامج في جهاز المعتدى عليه للاطلاع على محادثاته ومراسلاته.

4- الابتزاز: وهو الحصول على مكاسب مادية أو معنوية عن طريق الإكراه أو التهديد، وتعد خطورة الابتزاز في أن توفر الإنترنت يساعد المبتزين بعدة أوجه[11]، لأنه يمكنهم من تحديد الهدف نسبة لأن الإنترنت ملئ بالمعلومات التي تساعد على ذلك، كما أنه وسيلة لتهديد الضحية بتهديده بنشر ما لديه من صور أو مستندات أو بيانات سرية أو تسجيلات صوتية وفيديوهات على الشبكة لابتزاز الضحية مقابل طلب تحويل مبالغ مالية أو لحمله على القيام بأفعال مخلة بالآداب العامة وذلك دون معرفة حساب أو هوية المبتز[12].

5- الاعتداء على سلامة الشبكة المعلوماتية (القرصنة الإلكترونية):[13] وتعني أفعال غير مشروعة الغرض منها التحايل على أنظمة المعالجة الآلية للبيانات بغرض إتلاف أي مستند معالج إلكترونياً ويكون ذلك من خلال قرصنة الكتابة، باستخدام برامج جاهزة هدفها مهاجمة أجهزة الحاسب الآلي وتدميره. أو بسبب تحقيق مكاسب مالية لأغراض شخصية كسرقة بيانات أو معالجة إلكترونية للبيانات الخاصة بها إجراء بدون وجه حق، أو عقد صفقات لترويج المخدرات وأنشطة الشبكات الإباحية ونحوها[14].

6- جرائم الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكتروني: حيث يتم اختراق النظام المعلوماتي لأحد البنوك بغرض تحويل مبالغ مالية من حسابات العملاء إلى الحاسب الخاص للمجرم المعلوماتي[15]. ومثال لذلك البطاقات البنكية أو الائتمانية فبعض المخترقين لأجهزة الحاسوب أو المقرصنين يعملوا على ابتزاز الشركات العالمية وتهديد أصحابها والعمل على نشر معلومات خاصه وسرية بها إذا لم تستجيب وترضخ لطلباتهم وذلك بتحويل مبالغ مالية كبيرة لهم. وكذلك اختراق النظام المعلوماتي للغير بغرض التجسس على المؤسسات الهامة في الدولة[16] أو لتدمير ثرواتها المعلوماتية كلها أو جزء منها، أو التجسس على الأسرار الشخصية للأفراد أو التلاعب في بياناتهم الشخصية بالحذف أو الإضافة أو التعديل.

7- العمل على استغلال واستهداف القصر والأطفال في المحتويات الإباحية: وهي الفئة ما دون سن الثامنة عشر سنة حيث يتم استغلال هذه الفئة بعدة صور من خلال عرض أفلام ذات طبيعية إباحية متضمنه مشاهد جنسية عبر تلك المشاهدات أو الأفلام أو الصور الموحية باعتداءات جنسيه تتم من خلال أجهزة الحاسب الآلي ومواقع التواصل الاجتماعي، علماً بأن هذا الاستغلال يعد تجارة غير مشروعة يُعاقب عليها القانون في دول كثيرة.

8- الملاحقات الإلكترونية: وتتم باستخدام الشبكة العنكبوتية ومواقع التواصل الاجتماعي وذلك بجمع بيانات عن الضحية التي سوف يتم ملاحقته أو مطاردته وذلك بمعرفة اسمه أو جمع بيانات ومعلومات عن اسم عائلته وأرقام اتصالاته ومعرفة موقع عمله ومكان إقامته والدخول على صفحاته ومراقبة حساباته الشخصية ومحادثاته وذلك لإحراجه أو لسرقة أمواله أو مضايقته.

9- برامج الفيروسات: (*viruses*) تعني كلمة فيروس في اللغة تلك الكائنات الدقيقة التي لا ترى بالمجهر العادي وتنفذ من الراشحات البكتيرية وتحدث بعض الأمراض[17]. والفيروس عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تمكنه من القدرة على ربط نفسه ذاتياً ببرامج أخرى، ثم يتوالد ويتكاثر تلقائياً وينتشر داخل البرامج المختلفة أو بين مواقع معينة من ذاكرة الحاسب وغيره من الوسائط الأخرى حتى يحقق الأهداف المتوخاة منه[18]. حيث يتم

التعدي على البرامج أو الأجهزة بواسطة البرمجيات الضارة (الفيروسات) وهذه البرامج يصممها مجرمين يكونوا على درجة عالية من الاحتراف بهدف تدمير مواقع في الإنترنت أو تدمير أجهزة حواسيب وغيرها من الوسائط الإلكترونية، بعمل فيروسات وبرامج تكون قادرة على الاندماج والانتشار وربط نفسه مع برنامج ثاني يعرف باسم (الحاضن) فالفيروسات لا يمكن أن تتكون لوحدها من نفسها ويمكن تداولها من جهاز حاسوب متضرر منها لجهاز حاسوب سليم فتقوم بالانتشار فيه.

فأسهل طريقة لانتشار تلك الفيروسات هي الشبكات العنكبوتية لأنها اسهل طريق لانتقالها من حاسوب لحاسوب آخر طالما لا يوجد في الحاسوب السليم برنامج يعمل علي حمايته من تلك الفيروسات وتنزيل برنامج يمنع المخترقين ويحمي الفيروسات من الانتشار والانتقال. وتتعدد أنواع فيروسات الحاسب الآلي، بيد أن أكثرها شيوعاً هو فيروس الفدية (*ran som war*) وحصان طروادة وفيروس القنبلة المعلوماتية الموقوتة (*time bomb*) وفيروس الدودة المعلوماتية (*warm*)[19].فعلى المستخدم العمل على حماية جهازه بحفظ أغراضه بوسائل الحفظ والتخزين الأخرى مثل الأقراص الضوئية والفلاشات وكذلك بأرسالها إلى بريده الإلكتروني، فجميعها وسائل يمكن للشخص حماية معلوماته من الاختراق.

10- الاحتيال والنصب: (*fraud*) عن طريق الإنترنت من خلال البطاقات الائتمانية هذه الأفعال انتشرت وأصبحت من الوسائل التي تكون عبر الإنترنت من خلال المواقع التي يتم التواصل فيها من قبل الأشخاص، ومن صور ذلك أن يعمل المحتال على استخدام وسائل وأساليب يستدرج بها الشخص الذي يريد أن يوقعه بالفخ ويستدرجه، لأن الغالبية من الناس أصبحوا يستخدموا تلك المواقع، كذلك أن يرسل المحتال رسائل إلكترونية للضحية تحتوي على بيانات معينة، توحي له بتقديم خدمات معينه من خلال روابط يصممها للإيقاع بضحيته، كذلك العمل على مواقع مموهة تكون باسم شركات عالمية معروفة لسرقة البيانات وكل المعلومات التي تفيد الشخص المحتال.كما أن وسائل النصب أصبحت باحترافية عالية في حالة الشراء من على بعض المواقع لأي منتج أو خدمة عبر الشبكة العنكبوتية، فعلى الشخص توخي الحذر والتأكد من مصداقية تلك الشركات.

11- التشهير المعلوماتي: وهو أن الفاعل يعمل على الحاق ضرر بشخص ما عبر وسائل التقنية الحديثة والوسائط الإلكترونية المختلفة، أو تشويه سمعته.

المبحث الثاني: الإجراءات القانونية للجرائم ذات التقنية العالية في المملكة العربية السعودية وطرق إثباتها وعقوبتها

يعيش عالمنا المعاصر ثورة علمية ومعرفية هائلة ويشهد تغيرات تكنولوجية واجتماعية متسارعة، مهدت لظهور مجتمع المعرفة الذي تتسابق فيه الدول وتتصارع حول تملك وحيازة أكبر قدر من المعارف والمعلومات، وقد أدى انتشار المعلومات السريع عبر وسائل الاتصال المختلفة إلى تدفق هائل في المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية، يعجز الإنسان بقدراته العادية عن متابعتها والإلمام بها في عمرهِ القصير[20]

كذلك حدثت طفرة في تقنية المعلومات تمثلت في اختراع الحاسب الآلي الذي أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات ومعالجتها بسرعة خيالية لم تكم تخطر على باله من قبل، وهكذا تتضح إيجابيات الثورة المعلوماتية والتكنولوجية التي جاء بها الحاسب الآلي وقدرتها على تغيير أوجه الحياة إلى الأفضل. غير أن هذه الثورة المعلوماتية ذاتها (*per se*) تحمل في طياتها بذور الشر المتمثلة في الاستخدام غير المشروع لنظام الحاسب الآلي والوسائط التكنولوجية الأخرى[21].

حيث ترتب على ذلك أن ظهرت أنواع جديدة من الجرائم الحديثة عالية التقنية تتم من خلال الحاسوب، والتي أصبحت ظاهرة إجرامية جديدة ومستحدثة تقرع أجراس الخطر وتنبه المجتمعات الحديثة لحجم المخاطر والخسائر التي قد تنجم عن جرائم الحاسوب (الجرائم المعلوماتية *Cyber Crime*)، وهذه الجرائم هي تقنية ناتجة عن استخدام التكنولوجيا الرقمية كأداة لتحقيق غايات غير قانونية تنشأ في الخفاء ويقترفها أناس أذكياء (*hackers*) يمتلكون أدوات المعرفة التقنية الحديثة، وبالمقابل لابد من تطوير وسائل إثبات بما يواكب هذه الطفرة التي حدثت في طرق ارتكابها. ومن هذه الجرائم انتهاك الخصوصية (*invasion of privacy*) وانتحال الشخصية، والعمل على سرقة الملكية الفكرية، وكذلك سرقة الهويات(*theft identity*، والإتجار بالمواد الإباحية (*pornography*)، وتسريب المعلومات والمواد الإلكترونية المملوكة للمؤسسات والشركات سواء الحكومية أو الخاصة وتدميرها عن طريق فيروس (*virus*)، وغيرها من الجرائم التي تكون فيها الأجهزة والشبكات المحوسبة مسرحاً أو وسيلة لتنفيذها. حيث اتضح أن جرائم الاختراقات هي الأولى في المملكة العربية السعودية من بين تلك الجرائم والتي أخذت ما نسبته 5,6 ٪ لاختراقات مواقع حكومية، و3,5 ٪ اختراقات لمواقع تجارية[22] ونتيجة طبيعية لظهور مثل هذه الجرائم التي تسبب ضرراً على الأفراد والمجتمع والبيئة التكنولوجية، أصدر المنظم السعودي نظام مكافحة الجرائم المعلوماتية رقم (م/17) بتاريخ 1428/3/8ه والمعدل بتاريخ 1436ه.

المطلب الأول: إثبات الجرائم ذات التقنية العالية

أن للجرائم ذات التقنية العالية طبيعة خاصة تكمن في أن لشبكة المعلومات قدرة على نقل وتبادل المعلومات، وهذه المعلومات إما أن تكون معلومات ذات طابع شخصي ويكون الاعتداء فيها على الخصوصية، أو معلومات ذات طابع عام. لذا لابد من معرفة كيفية إثبات هذه الجرائم، والنظام القانوني الواجب تطبيقه على كل من يحاول استخدام هذه التقنية لغرض غير مشروع ويحاول التعدي على الأخرين إلكترونياً، فالدول المتقدمة تكنولوجياً مثل المملكة العربية السعودية وضعت قواعد موضوعية لمواجهة الاستخدام غير المشروع للحاسب الآلي والإنترنت، وأجرت المملكة تعديلات على قوانينها الإجرائية تكفل مكافحة هذه الجرائم في إطار الشرعية الجنائية، ولأن المملكة أدركت أن هذه الجرائم تُرتكب بتقنيات حديثة في عالم يختلف عن العالم المادي الذي عادة ما تُرتكب فيه الجرائم بالطرق التقليدية وإجراءاتها، والتي ترتكب عن طريق المجابهة بين الأشخاص كالقتل والإيذاء والسرقة، فالقانون الجنائي التقليدي بشقيه (الإجرائي والموضوعي) تم وضعه لمكافحة الاعتداءات المادية والمواجهة بين الأشخاص وجهاً لوجه[23]، وإثبات الإدانة بإقامة الأدلة التي تثبت وقوع الجريمة.

بيد أن الجرائم التقنية مختلفة عن هذه الجرائم التقليدية، فهي ترتكب في عالم افتراضي (*virtual*) وعلى مسافات بعيدة؛ ويتطلب وجود بيئة رقمية واتصال بالإنترنت ومعرفة النشاط وما ينطوي عنه، ونتيجته، لذلك يعد الأثبات من أهم التحديات التي تواجه الأجهزة الأمنية[24]. فالأثبات هو تأكيد حق متنازع فيه له اثر قانوني بالدليل الذي أباحه القانون لإثبات ذلك الحق[25]. وعرفه الدكتور عبد الرزاق السنهوري بقوله (هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتب عليها آثارها) [26]، أما وسائل الإثبات فهي كثيرة ومتنوعة منها على سبيل المثال لا الحصر، البينة والإقرار والقرائن والكتابة واليمين، والخبرة والمحررات أو الدليل الكتابي، غير أن للخبرة دوراً بارزاً في مجال الجرائم ذات التقنية العالية، وهي إجراء يتعلق بموضوع يتطلب إلماماً بعلم معين لإمكان استخلاص الدليل منه، فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منها الخبير رأيه[27]. ويعد تقرير الخبير من الأدلة، إما إجراء ندبه فهو إجراءات جمع الأدلة من شأن المعاينة والتفتيش وضبط الأشياء. والخبرة تشمل معاينة القاضي وخبرة المتخصصين والمتمرسين في استخدام الحاسب الآلي والإنترنت وغيرها مما يحتاج إلى مزيد من علم ومعرفة وخبرة وتجربة في كثير من المجالات خصوصاً في مجال الإلكترونيات مما لا يستطيع القاضي أو الإنسان العادي معرفتها بمجرد معلوماته العامة.

وإثبات الجرائم ذات التقنية العالية يصعب اكتشافها وإثباتها، وذلك يرجع لخصائص هذه التقنية ذاتها وخاصة السرعة الفائقة التي ترتكب بها، والسمات التي يتصف بها المجرم من حيلٍ وغش عند استخدامه لتقنيات معلوماتية ذات كفاءة عالية، ومحو آثارها وطمسها قبل أن يتم اكتشافها، فالمجرم التقني لا يترك أثراً ملموساً لأنها تتم بتقنيات عالية، والجُناة يكونون على مستوى عالي من الذكاء، كما يمكنهم العمل على تدمير وسائل الإثبات بعد ارتكابهم للجريمة، لأنه حتى الضحايا من الممكن ألا يكون في مصلحتهم إثبات أو القيام بشكوى للسلطات المعنية حتى يحفظوا ربما حياتهم الخاصة وخوفهم من أن تنتشر ويشهر بهم داخل الرأي العام، لذلك مسألة الإثبات تبقى جد صعبة.

لذا يصعب إثبات الجرائم ذات التقنية العالية نسبة لطبيعتها الفنية المعقدة، ولكن توجد عدة طرق لجمع الأدلة عن الجرائم ذات التقنية العالية وفي نفس الوقت تعد من طرق الإثبات حتى يتم الوصول إلى الحقيقة، وهي المعاينة ومشاهدة الآثار المادية إن وجدت وعلى الرغم من أهمية المعاينة في إثبات حالة الجريمة لكن ربما لا تكون فعالة للضبط، كذلك التفتيش وهو البحث والاستقصاء والهدف منه ضبط أدلة الجريمة وكل ما يفيد في كشف الحقيقة[28]، والشهادة والخبرة كما أسلفنا، والإثبات بجميع وسائل الإثبات إذا الأمر يتعلق بواقعة مادية للبيئة التقنية فإن الأمر لا يثير أي صعوبة، أي أن الضبط يرد بالأساس على الأشياء المادية محل الجريمة[29] مثل الأثبات بالشهود ولكن في الأغلب على حسب ما يتم العمل به في جرائم الصحافة وجرائم أخرى متعلقة بجرائم القذف أو التشهير غالباً ما يتم الإثبات بتقنية تصوير الشاشة أو الاعتماد على أمر قضائي بمعاينة الصفحة الإلكترونية ومعاينة موضوع القذف أو التشهير وما شابه ذلك.

كما يمكن الإثبات عن طريق الدليل الرقمي ويكون هذا الدليل في شكل مجالات ونبضات مغناطيسية أو كهربائية، والذي يتم أخذها من أجهزة الحاسوب والعمل على جمعها وتحليلها باستخدام برامج تكنولوجية خاصة وتطبيقات، وهي مكون رقمي لتقديم معلومات إما أن تكون في شكل صور ورسومات أو أصوات أو نصوص كتابية. فالدليل الرقمي يمتاز عن الدليل المادي؛ فالبرامج والتطبيقات الصحيحة التي سيتم استخدامها ستحدد العبث أو التعديل الذي تم مقارنته بالأصل. كذلك يمكن رصد معلومات عن الجاني من خلال الدليل الرقمي الذي يسجل تحركاته وبعض الأمور الشخصية والعمل على تحليلها في ذات الوقت.

فنرى أن رؤية المسرح الحقيقي المادي للجريمة والمسرح المعلوماتي الرقمي واستخلاص وسائل الاستدلال يمكن أن تكون ثرية جداً بما تحتويه من معلومات للكشف عن المجرم، لابد أن يتحرى القاضي جيداً عن الأدلة الجرمية الرقمية وان يكون ملماً بالعمليات الإلكترونية وكل ما

يتعلق بالجرائم التقنية وأن يستعين بأصحاب الخبرة والاختصاص التي تمكنه من اكتشاف الأدلة، لأن الأدلة التي يتحصل عليها من الوسائل الإلكترونية وما قد يصاحب الحصول عليها من خطوات معقدة فإن قبولها في الإثبات قد يثير الكثير من المشكلات والتلاعب والتغيير فيها.

وخلاصة القول يتبين أن الدليل الإلكتروني مثله مثل الدليل التقليدي، وسيلة من وسائل الإثبات حيث لا تقوم الجريمة الإلكترونية إلا في وجود دليل إلكتروني، غير أن الدليل الإلكتروني يختلف بعض الشيء عن الدليل التقليدي، حيث انه دليلا فنيا بحتا0 وقد يكون في شكل رسالة أو أرقام أو شفرات أو معلومات أو بيانات مشفرة أو حتى صور. كما أنه دليلاً وهمياً غير ملموس يسهل طمسه وإزالته واختراقه حتى بعد أن يتم العثور عليه، لذلك لابد من التعامل معه بشكل تقني عالي جداً.

المطلب الثاني: العقوبات المقررة لارتكاب الجرائم ذات التقنية العالية

فرض نظام مكافحة الجرائم المعلوماتية السعودي جملة من العقوبات تتناسب مع جسامة كل جريمة للحد من حدوثها، ولتكون رادعاً لكل من تسول له نفسه الاعتداء على الناس والانتقاص من حقوقهم وزرع الخوف والقلق في نفوسهم، وذلك بالسجن لفترات وغرامات مختلفة بحسب الجريمة ونوعها ومقدار ما تسببه من ضرر، سواء اجتمعت الغرامتان معاً، أو تم توقيع أي منهما بشكل منفرد بقوله (أو بإحدى هاتين العقوبتين)، وذلك وفق التوصيف التالي:

نصت المادة الثالثة من قانون مكافحة الجرائم المعلوماتية على أنه يعاقب بالسجن مدة أقصاها عام واحد، بالإضافة إلى غرامة مالية لا تتجاوز خمسمائة ألف ريال سعودي، أو بأي من هاتين العقوبتين كل من يرتكب أيا من الجرائم المعلوماتية الآتية:

- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه،أو تعديله، أو تشغيل عنوانه.

تنص المادة الربعة، على أن يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات، وبغرامة مالية حدها الأقصى مليونين ريال سعودي، أو بإحدى هاتين العقوبتين، كل من يرتكب أيا من الجرائم المعلوماتية الآتية:

- الاستيلاء للنفس أو للغير على الأموال المنقولة أو تلك التي تكون على سند من جراء الاحتيال أو انتحال أي من الملفات غير الصحيحة أو اتخاذ اسم كاذب.

- التوصل إلى أي من البيانات البنكية أو الائتمانية من دون مسوغ نظامي، أو تلك البيانات التي تتعلق بملكية الأوراق المالية، من أجل الحصول على المعلومات أو الأموال أو ما تتضمنه من خدمات.

تنص المادة الخامسة على أن يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعديلها، أو تعطيلها بأي وسيلة.
- تنص المادة السادسة على أن يعاقب بالسجن مدة لا تتجاوز الخمس سنوات، إضافة إلى غرامة مالية حدها الأقصى ثلاثة ملايين ريال سعودي، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:
- إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة، أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية، أو أجهزة الحاسب الآلي.
- يؤسس أو ينشر أي موقع على أجهزة الحاسوب أو شبكة الإنترنت المعلوماتية وذلك للإتجار أو تسهيل الإتجار بالجنس البشري.
- تأسيس أو نشر أي من المواقع على الشبكة المعلوماتية الإلكترونية أو على أي من أجهزة الحاسوب وذلك للإتجار أو الترويج أو نشر طرق التعاطي أو تيسير التعامل من خلالها بالنسبة إلى أنواع المخدرات، فضلا عن المؤثرات العقلية المختلفة.
- نشر أو إنشاء أو ترويج أي من البينات والمعلومات التي تتعلق بالشبكة الإباحية، أو أي من أنشطة الميسر التي من شأنها الاختلال بالآداب العامة.

تنص المادة السابعة على أن يعاقب بالسجن مدة لا تزيد على عشر سنوات، إضافة إلى غرامة مالية لا تتجاوز خمسة ملايين ريال سعودي أو بأي منهما، لأي من مرتكبي الجرائم التالية:

- العمل على تأسيس أو نشر أي من المواقع للمنظمات الإرهابية والتي من شأنها تسهيل الوصول إلى المنظمات الإرهابية وقياداتها أو أعضائها أو العمل على الترويج إليها ولأفكارها أو تمويلها،

إضافة إلى نشر طريقة إعداد المتفجرات أو أي من الأجهزة أو مختلف الأدوات التي يتم استخدامها في العديد من العمليات الإرهابية.

- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشر، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

المادة الثامنة تنص على أن لا تقل عقوبة السجن أو الغرامة عن نصف حده الأعلى أذا اقترنت الجريمة بأي من الحالات الموضحة التالية:

- اذا شغل الجاني أي من الوظائف العامة أو الاتصال بين وظيفته والجريمة التي ارتكبها أو في حال ارتكابه الجريمة مستغلا سلطته أو نفوذه.
- اذا ارتكب الجاني أي من الجرائم من خلال العصابات المنظمة.
- صدور أحكام أجنبية أو محلية سابقة بالإدانة بحق الجاني في جرائم مماثلة.
- العمل على التغرير بالقصر، أو من في حكمهم والعمل على استغلالهم.

تنص المادة التاسعة على أن يعاقب كل من حرض غيره أو ساعده أو اتفق معه ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، اذا وقعت الجريمة بناء على هذا أو الاتفاق أو التحريض أو المساعدة، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها اذا لم تقع الجريمة الأصلية.

المادة العاشرة تنص على أن يعاقب كل من يشرع في القيام بأي من الجرائن المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

المادة الحادية عشر تنص على أن للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وان كان الإبلاغ بعد العلم بالجريمة وتعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

آلية التبليغ عن الجرائم ذات التقنية العالية:

1- يتم التبليغ عن الجرائم ذات التقنية العالية في المملكة العربية السعودية من خلال الدخول لمنصة أبشر الإليكترونية، ثم الدخول إلى خدمات الأمن العام، ومن بعد ذلك إلى خدمة بلاغ الجرائم الإلكترونية ومن ثم تحديد نوع البلاغ والقيام باستيفاء كافة الحقول المطلوبة، يتم بعد ذلك النقر على حقل إرسال. أخيراً وبعد إرسال البلاغ يتم تزويد المستخدم بالرقم المرجعي الخاص بالبلاغ.

2- أتاحت المملكة رقما موحداً يتم من خلاله تلقي مختلف بلاغات الجرائم الإلكترونية، إضافة إلى توفير خدمة التوعية والتوجيه من خلال الاتصال على الرقم (1909).

خاتمة:

بعد دراستنا لموضوع الجرائم ذات التقنية العالية والحماية من الهجمات الإلكترونية وفقا للنظام السعودي ذلك بالوقوف على أوجه الحماية التي وفرها النظام السعودي لحماية المجتمع من هذه الهجمات، وما ورد في النظام بهذا الخصوص. فقد توصلنا من خلال الدراسة للعديد من النتائج ولكن قبل عرضها لابد من توضيح أن ما تم التوصل إليه من نتائج متعلقة من إثبات الجرائم ذات التقنية العالية تشكل صعوبة لأنها متغيرة ومتطورة، لأن التقنية دائما تتطور بشكل كبير في هذا العالم الافتراضي وبسرعة مهولة.

أولاً- النتائج:

1- وضح لنا الإسلام بأن نحفظ الضرورات الخمس التي وصتنا بها الشريعة الإسلامية وهي الكليات الخمس حفظ الدين.

2- لكي تستقيم الحياة لابد من توفر الوعي الكافي للبعض والتعرف على جميع أنواع تلك الجرائم ومواكبة تطورات العصر وخاصة ما يحدث من تطورات مرتكبي الجرائم ذات التقنية العالية.

3- يجب العمل والاشتغال على معالجة أي خلل قد يُحدث ثغرة قد تؤدي بتلك الجرائم أو خللاً بالمجتمع؛ لذا لابد من العمل على توعيته بصورة دائمة وتثقيفية بالوسائل والطرق التي يستخدمها مجرمي التقنية.

4- يعد إثبات الجرائم ذات التقنية العالية من أهم التحديات التي تواجه الأجهزة الأمنية، فإثبات هذه الجرائم أمر يستلزم الكثير من الجهد والخبرات الفنية المتدربة على أعلى المستويات والتأهيل، فنقص الخبرة يشكل عائقاً أمام الإثبات.

5- العمل بشكل دوري على حماية حواسيبنا الشخصية بعمل برامج الحماية القوية.

6- عدم حفظ أي شيء مهم سواء صور شخصية أو ملفات مهمة قد تؤدي إلى مشارف الهلاك.

7- إن معرفة الأسباب التي تجعل وجوداً لي أي خلل في حواسيبنا بكل أشكاله تسهل وتوفر علي المختصين بسرعة الحماية وتكثيف الجهود والتوصل بسرعة لمرتكب الجريمة ومعرفة الهدف.

ثانيا- الاقتراحات:

في ضوء النتائج التي قد تم التوصل إليها، يمكن حصر عدد من التوصيات التي قد تساهم في تفعيل إثبات الجرائم ذات التقنية العالية وذلك كما يلي:

1- الاهتمام بتطوير الخبراء الفنيين لما لهم من دور أساسي وفعال في إثبات الجرائم ذات التقنية العالية، وإتقانهم لهذا المجال والتمكن من نقل الأدلة دون تدميرها أو إتلافها وكل ما هو مسجل على دعامة ممغنطة.

2- التوعية ونشر العلوم الشرعية المستنبطة من الكتاب والسنه والبعد بقدر المستطاع وتوضيح العقوبات الإسلامية للسرقة أو التشهير أو التجسس.

3- أصبح الإرهاب عبر وسائل الاتصال من أكثر صور الجرائم ذات التقنية العالية، فاصبح الاختراق سهلا لهم فلابد لنا أن لانفتح أي ثغرة لهذا الاستغلال وان نحمي مجتمعنا من أي فكر دخيل أو مصدر منحرف لمنع الفساد ومحاربة كل مصدر فيه إجرام.

4- العمل على التنسيق الدائم والمستمر ما بين الجهات القضائية والجهات الأمنية والجهات التي لها علاقة بالتكنولوجيا لمعرفة كل ما هو مستجد من تقنيات.

5- الدورات المستمرة للقضاء وتعريفهم بكل ما هو جديد في مجال التقنية الحديثة من أساليب وأنواع.

الهوامش:

---

[1]- عبد القادر عودة، التشريع الجنائي الإسلامي مقارنة بالقانون الوضعي، مؤسسة الرسالة، بيروت، المجلد الأول، 1401ه، القسم الأول، ص 40.

[2]- خالد بن سعود البشر، مكافحة الجريمة في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض 1424ه، ص 21.

[3]. عبد القادر عودة، التشريع الجنائي الإسلامي مقارنة بالقانون الوضعي، مؤسسة الرسالة، بيروت، المجلد الأول، 1401ه، ص 66.

[4]- زكريا احمد عمار، الحلقة العلمية: الدليل الرقمي والتحقيق في الجرائم الإلكترونية، كلية علوم الأدلة الجنائية: جامعة نايف العربية للعلوم الأمنية، 1429ه، ص 15.

[5]- تعريف المجرم التقني *hacker*: شخص يتسم بصفات وسمات لا تتوافر في المجرم العادي، فهو شخص لديه خبره ومعرفة كافية بالمسائل التقنية والدراية الكافية بالحاسوب والبرامج والبيانات والنظام المعلوماتي، والتلاعب بالمعلومات وكذلك يمكن أن يكون محل الجريمة إتلاف الحاسب نفسه أو قد يكون وحدة المعالجة المركزية[(5)]. فيتضح لنا أن من يقوم بارتكاب الجريمة التقنية قد يكون فاعلاً اصلياً أو شريكاً في الجرم سواء وسطاء أو شركاء.

[6]- فتعريف المعلوماتية لا يوجد نص قانوني يعطي تعريفاً جامعاً مانعاً لها حيث يشير القانون الفرنسي الخاص بالاتصالات السمعية والبصرية لسنة 1982م إلى تعريف عام للمعلومة بأنها رنيناً وصوراً للوثائق والبيانات أو الرسائل من أي نوع كان.

[7]- تعريف التقنية العالية لغة هي التقنية في الوضع الأكثر تقدما المتوفر حاليا، وهي الصناعة أو تطبيق المهارات والمعرفة التي تتعلق بعالم الحوسبة، ويمكن أن تشمل التقنية الإلكترونيات والبيوتكنولوجيا وعدة مجالات أخرى.

[8]- (الجرائم التقليدية وهي كل الجرائم ماعدا الجرائم الناشئة عن الحاسب الآلي).

[9]- أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، 2000م، ص 125.

[10]- ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس الكمبيوتر ووسائل حمايتها. دار النهضة العربية، القاهرة، 1989م، ص 122.

(الفيروسات هي عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تمكنه من ربط نفسه ذاتياً ببرامج أخرى، ثم يتوالد ويتكاثر تلقائياً وينتشر داخل البرامج المختلفة أو بين مواقع معينة من ذاكرة الحاسب حتى يحقق الأهداف المتوخاة، والواقع أن هناك وجهاً للشبه بين الفيروس الذي يصيب الإنسان وذاك الذي يصيب الحاسب الآلي).

[11]- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي،القاهرة، 2006م، ص 187.

[12]- مروان مرزوق الروقي، القصد الجنائي في الجرائم المعلوماتية، دراسة تأيلية مقارنة، مكتبة القانون والاقتصاد، الرياض، 1434ه، ص 64.

[13]- محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، رسالة ماجستير قسم العلوم الشرعية، أكاديمية نايف للعلوم الأمنية، الرياض 1434ه-2003، ص 119.

(14) -*Computer bank, Bankers Review Security procedures after Virus Attack.Vol. 6 no.1, January 188 P.8.*

[15]- خالد المختار الفار/ إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب، دار عزة للنشر والتوزيع، الخرطوم 2010، ص 165.

(16) -*Mathew(J.Gray: An ounce of prevention fights Computer Viruses from electronic vandalism is vital" Tutoriel, LAN time, vol. 7,No.14, Nov. 1990 p.69.*

[17]- المعجم الوسيط، مجمع اللغة العربية، الإدارة العامة للمعجمات وإحياء التراث، ط 5، القاهرة،2011م.، ص 486.

[18]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية: دراسة مقارنة، 2006، ص ص 8-9.

[19]- المرجع نفسه، ص ص 7-8.

[20]- زهير الكرمي، العلم ومشكلات الإنسان المعاصر، ط 5، سلسلة عالم المعرفة، الكويت، 1978م، ص 21.

[21]- (يجب ملاحظة أن الحاسب الآلي يشمل أيضاً جميع وسائل الاتصال الحديثة بأنواعها المختلفة).

[22]- محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، أطروحة ماجستير، قسم العلوم الشرعية، أكاديمية نايف للعلوم الأمنية، الرياض، 1434ه-2003م.

[23]- وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية، ورقة بحثية.

[24]- أحمد الطاهر النور، أساليب إجرامية بالتقنية الرقمية، الندوة العربية القانونية المصاحبة لاجتماع مجلس وزراء العدل العرب، جامعة الخرطوم كلية القانون: الخرطوم في الفترة من 3-6 مارس 2003.

[25]- طالب محمد جواد-عبد الجبار ضاحي عواد، جرائم تقنية المعلومات وإثباتها، مجلة كلية الرافدين الجامعة للعلوم، العراق، 28 السنة الثالثة عشر، 2011م، ص ص 53-69.

[26]– محمد مصطفى الزحيلي، وسائل الإثبات في الشريعة الإسلامية في المعاملات المدنية والأحوال الشخصية، الطبعة الأولى، دار البيان، دمشق1402ه– 1982م، ص 22.

[27]– مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، كلية الحقوق الجامعية الليبية ببنغازي، الطبعة الأولى، ليبيا الجامعة الليبية، 1971م، ص 306.

[28]– فيصل بن معيض، هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية 1999، ص 24.

[29]– عبد الفتاح مصطفى الصيفي، تأصيل الإجراءات الجنائية، الإسكندرية 2002م، دار المعرفة الجامعية، ص 119.