ISSN: 2706-6495

المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي مقارنة بالقانون الإماراتي

Criminal responsibility for hacking the official websites of the state in the Saudi system compared to UAE law

إعداد الباحثة/ شيخة مسعد عبد الله البلوي

ماجستير شريعة وقانون، قسم الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية

Email: info@vjustice.sa

الملخص:

لما شكلت المواقع الإلكترونية مستودعاً لأسرار الدول، وأصبحت المعلومات متداولة في هذه المواقع عبر شبكات داخلية وخارجية، فقد مثّل ذلك فرصة للمجرمين المعلوماتيين للسطو على هذه البيانات والمعلومات، بوسائل متعددة وأساليب اختراقية أو احتيالية، ومن هنا فقد قامت الباحثة بإعداد هذه الدراسة نظراً لظهور مشكلة تتمثل في تزايد هجمات القراصنة الإلكترونيين على المواقع الرسمية للدول، التي أظهرت الحاجة لمناقشة علمية لحدود المسؤولية الجنائية عن هذا الفعل المؤثم، والعقوبات المقررة له، واتخذت أنظمة مكافحة الجريمة المعلوماتية السعودية أنموذجاً للدراسة، ومقارنتها بقوانين مكافحة الجريمة المعلوماتية الإماراتية. وتتمثل أهمية الدراسة في التوعية بأن هناك نظاماً يجرّم اختراق المواقع الإلكترونية للدولة في النظام السعودي والقانون الإماراتي، التصدي لجرائم اختراق المواقع الإلكترونية الرسمية لما لها أخطار أمنية وسياسية واجتماعية، الإسهام في الحفاظ على أمن المعلومات وأمن الحاسب الآلي لهذه المواقع.

استخدمت الباحثة المنهج الوصفي بطريقته العلمية القائمة على الاستقراء والتحليل والمقارنة لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها. وكانت حدود الدراسة الموضوعية في نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (79) ونظام التعاملات الإلكترونية بقرار مجلس الوزراء رقم (80) وتاريخ 1428/3/7هـ، ونظام الاتصالات السعودي الصادر بقرار مجلس الوزراء رقم (74) وتاريخ 1422/3/5هـ، والقانون الاتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية، وقانون المعاملات والتجارة الإلكترونية رقم (3) لعام 2002م، والقانون الاتحادي رقم (3) لسنة 2003م لتنظيم قطاع الاتصالات الإماراتية.

الكلمات المفتاحية: المسؤولية الجنائية، اختراق المواقع الإلكترونية، النظام السعودي، القانون الإماراتي، المواقع الإلكترونية الرسمية

ISSN: 2706-6495

Criminal responsibility for hacking the official websites of the state in the Saudi system compared to UAE law

Abstract:

When websites formed a repository of state secrets, and information circulated on these websites through internal and external networks, this represented an opportunity for cybercriminals to rob this data and information, using multiple means and hacking or fraudulent methods. Hence, the researcher prepared this study due to the emergence of a problem represented in the increase in hacker attacks on the official websites of countries, which showed the need for a scientific discussion of the limits of criminal responsibility for this sinful act, and the penalties for it.

The importance of the study is to raise awareness that there is a system that criminalizes hacking state websites in the Saudi system and UAE law, addressing the crimes of hacking official websites because they have security, political and social risks, and contributing to maintaining information and computer security for these websites.

The researcher used the descriptive approach in its scientific way based on induction, analysis and comparison to achieve the objectives of the study and answer its questions. The limits of the objective study were in the Saudi Information Crime Control System issued by Cabinet Resolution No. (79) and the Electronic Transactions System by Cabinet Resolution No. (80) dated 3/7/1428 AH, and the Saudi Communications System issued by Cabinet Resolution No. (74) dated 5/3 / 1422 AH, and Federal Law No. (5) of 2012 AD regarding combating information technology crimes in the United Arab Emirates, Law of Transactions and Electronic Commerce No. (3) of 2002 AD, and Federal Law No. (3) of 2003 AD regulating the UAE telecommunications sector.

Keywords: Criminal responsibility, Hacking websites, the Saudi system, UAE law, Official websites

ISSN: 2706-6495

1. المقدمة:

الحمد لله، والصلاة والسلام على رسول الله. وبعد:

فقد أصبحت الحاسبات الآلية والمواقع الإلكترونية مستودعاً لأسرار الأفراد والدول على حد سواء؛ ذلك أن اتجاه الدول لسياسة الحكومات الإلكترونية، وما يتبع ذلك من تناقل للبيانات والمعلومات عبر الشبكات المعلوماتية، سواء الداخلية منها والخارجية، وسواء ما كان من هذه البيانات سرياً أو متاحاً للجمهور عبر هذه الشبكات، مما شكّل ما يعرف بالثورة المعلوماتية.

وإذا كانت الفائدة المرجوّة من الثورة المعلوماتية في المجال الإلكتروني قد آتت أكلها، إلا أنه على الجانب الآخر ظهرت عدد من الجرائم المرتبطة بهذه الثورة المعلوماتية، ويعود ذلك للتطور المتسارع لشبكة الإنترنت، التي مثلت وسيلة مثلى للمجرمين المعلوماتيين لتنفيذ جرائمهم المتمثلة في الاعتداء على خصوصية الأفراد، بعيداً عن أعين الجهات الرقابية، وتجاوز هذا الاعتداء ليصل للاعتداء على المواقع الرسمية للدولة[1].

وهذا ما دفع الحكومات والدول إلى محاولة التصدي لها بإصدار الأنظمة والقوانين، والاتفاقيات كاتفاقية الإجرام السيبيري (الجرائم المعلوماتية) التي صدرت عن المجلس الأوروبي، ووُقِّعَت في العاصمة المجرية بودابست في 23 نوفمبر (2001م)، وقّعت عليها 30 دولة.

ومن هنا فإن الدراسة الحالية سوف تنصب على المسؤولية الجنائية عن اختراق المواقع الإلكترونية للدولة نظراً لما للاختراقات الإلكترونية من دور بارز في الحرب المعلوماتية المعاصرة.

1.1. مشكلة الدراسة:

على الرغم من التقدم التقني في مجال نقل المعلومات وتداولها، واتجاه عدد من الدول إلى الحكومة الإلكترونية، إلا أن إساءة استخدام التكنولوجيا شكلت تهديداً لخصوصية الحكومات، واعتداء على أسرارها بالعبث والتخريب تارة، وتسريبها ونشرها تارة أخرى، من خلال الاعتداء على المواقع الرسمية للدول.

ولما لم تكن الدول العربية بدعاً بين هذه الدول، فقد تعرضت مواقعها الإلكترونية الرسمية للاختراق والاقتحام، فقد ظهرت في الآونة الأخيرة العديد من جرائم الاختراق للمواقع الإلكترونية الرسمية في المملكة العربية السعودية ودولة الإمارات العربية، ولا أدلّ على ذلك مما حدث من محاولة اختراق لموقع أرامكو السعودية[2] وهيئة الآثار والسياحة، وموقع أبشر، وموقع جامعة الطائف.

(1) يوسف، صغير (2013). الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير (غير منشورة). جامعة مولود معمري، الجزائر: كلية الحقوق، قسم القانون الدولي، ص3.

(2) الغامدي، محمد (1434). محاولة اختراق أرامكو تهدف للإضرار بالاقتصاد الوطني ومنع تدفق الزيت الى الأسواق المحلية والعالمية، الرياض: جريدة الرياض، الاثنين 26 محرم، العدد 16240.

ISSN: 2706-6495

وكذلك محاولات الاختراق في دولة الإمارات من قراصنة من خارج البلاد يستهدفون مواقع إلكترونية لشركات وجهات حكومية[1].

ولما كانت هجمات القراصنة الإلكترونيين على المواقع الحكومية في الدولة تزداد عاماً بعد آخر، فقد رأت الباحثة الحاجة لمناقشة علمية قانونية لحدود المسؤولية الجنائية عن هذا النوع من الاختراقات، والعقوبات المقررة له، من خلال دراسة نصوص النظام السعودي ومقارنتها بنصوص القانون الإماراتي، ومن هنا تبلورت مشكلة الدراسة لدى الباحثة والتي تكمن في الإجابة على التساؤل الرئيس الآتي:

ما نطاق المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي؟

2.1. تساؤلات الدراسة:

1- ما مفهوم اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي؟

2- ما أهم الفروق التي تميز الجريمة المعلوماتية عن الجريمة التقليدية وسمات مرتكبي كل منهما؟

3- ما أهم صور اختراق المواقع الرسمية للدولة؟ وما الفروق التي تميز كلاً منها؟

4- ما مدى المسؤولية الجنائية لمقدم الخدمة، وبقية الأطراف ذات العلاقة بتقديم واستخدام الخدمة المعلوماتية؟

5- ما نوع القصد الجنائي المتطلب لترتب المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي؟

3.1. أهداف الدراسة:

1- توضيح مفهوم اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي.

2- بيان الفروق التي تميز الجريمة المعلوماتية عن الجريمة التقليدية، وسمات مرتكبي كل منهما.

3- مناقشة أهم صور اختراق المواقع الرسمية للدولة، والفروق التي تميز كلاً منها.

4- توضيح مدى تحقق المسؤولية الجنائية لمقدم الخدمة، وبقية الأطراف ذات العلاقة بتقديم واستخدام الخدمة المعلوماتية.

(1) العربي، يوسف (2013). الإمارات تحبط محاولات جديدة لاختراق مواقع إلكترونية حكومية، دبي: جريدة الاتحاد الإماراتية، الاثنين، 24يوليو.

ISSN: 2706-6495

4.1. أهمية الدراسة:

الأهمية العلمية:

1- تطمح الباحثة أن تكون هذه الدراسة إضافة إلى المكتبة العربية والإسلامية والعالمية لإفادة الباحثين وطالبي المعرفة في هذا المجال.

2- التنبيه على مقومات جريمة اختراق المواقع الإلكترونية الرسمية للدولة حتى يبتعد عن أركانها من يجهلها.

3- أن تكون الرسالة مرجعاً قانونياً متخصصاً في المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة.

الأهمية العملية:

1- توعية المجتمع بأن هناك نظاماً يجرّم اختراق المواقع الإلكترونية للدولة في النظام السعودي والقانون الإماراتي.

2- أن تكون الرسالة مرجعاً للعاملين في القطاعات الحكومية لتوعيتهم بما يترتب على اختراق المواقع.

3- التصدي لجرائم اختراق المواقع الإلكترونية الرسمية لما لها أخطار أمنية وسياسية واجتماعية.

4- الإسهام في الحفاظ على أمن المعلومات وأمن الحاسب الآلي لهذه المواقع.

5.1. حدود الدراسة:

تتمثل حدود هذه الدراسة فيما يأتي:

الحدود الموضوعية:

تتحدد الدراسة موضوعياً بدراسة نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (79) وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم (م/17) وتاريخ 1428/3/8هـ، ونظام التعاملات الإلكترونية بقرار مجلس الوزراء رقم (80) وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم (م/18) وتاريخ 1428/3/8هـ، ونظام الاتصالات السعودي الصادر بقرار مجلس الوزراء رقم (74) وتاريخ 1422/3/5هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم (م/12) وتاريخ 1422/3/12هـ، والقانون الاتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية، وقانون المعاملات والتجارة الإلكترونية رقم (3) لعام 2002م، والقانون الاتحادي رقم (3) لسنة 2003م لتنظيم قطاع الاتصالات الإماراتية.

6.1. منهج الدراسة:

اعتمدت الباحثة على المنهج الوصفي بطريقته العلمية القائمة على الاستقراء والتحليل والمقارنة لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها، حيث يعتمد هذا المنهج على الوصف والتفسير والتحليل، ويهتم بوصف الأحداث وصفاً واقعياً ودقيقاً،

وتعليلها وتحليلها وتطوراتها المتوقعة، ولا يتوقف المنهج الوصفي عند وصف الظاهرة فقط، بل يتعدى ذلك إلى التعرف على العلاقات بين المتغيرات التي تؤثر في الظاهرة والمقارنة بين الأشياء المختلفة[1].

7.1. مصطلحات الدراسة:

المسؤولية الجنائية:

المسؤولية لغة: من (سأل يسأل) أي: طلب يطلب، والسائل الطالب، والمسؤولية: مصدر صناعي من مسؤول وهو المطلوب[2]، ومنه قوله تعالى (**وَقِفُوهُمْ إِنَّهُمْ مَسْئُولُونَ**)[3].

والمسؤولية: التكليف، ومنه قوله صلى الله عليه وسلم: "كلكم راعٍ، فمسؤول عن رعيته..."[4] أي: كل شخص مكلف بما أوكل إليه ومحاسب عليه[5]، والمسؤولية: حالة أو صفة من يُسأل عن أمر تقع عليه تبعته[6].

المسؤولية في الاصطلاح القانوني: "التزام الفرد بواجباته أمام المجتمع، ويترتب عليه مسؤولية جنائية، أو مدنية أو غيرها"[7].

كما تعرف بأنها "إلزام الشخص الآهل بتحمل نتائج الأفعال، والأقوال التي تصدر منه بالمباشرة، أو بالتسبب"[8].

الجناية لغة: من (جنى يجني جناية)[9] أي: أذنب، وجنى على نفسه وجنى على قومه وجنى الذنب على فلان: جرّه إليه[10]، وجنى فلان جناية: اجترم[11]، والجناية: الذنب والجرم وما يفعله الإنسان مما يوجب عليه العقاب أو القصاص في الدنيا أو الآخرة[12].

(1) أبو سليمان، عبد الوهاب إبراهيم (2006م). كتابة البحث العلمي (صياغة جديدة) ومصادر الدراسات القرآنية والسنة النبوية والعقيدة الإسلامية، ط3، جدة: دار الشروق، ص33.

(2) الفيومي، أحمد بن محمد (1987م). المصباح المنير، د. ط، بيروت: مكتبة لبنان، 403/1. وابن منظور، محمد بن مكرم (2008). لسان العرب، ط6، بيروت: دار صادر، 382/11.

(3) سورة الصافات: آية 24.

(4) البخاري، محمد بن إسماعيل (1428هـ). صحيح البخاري، د.ط، بيروت: دار الكتب العلمية، كتاب العتق، باب كراهية التطاول على الرقيق وقوله عبدي أو أمتي، حديث رقم 2554، ص510.

(5) ابن حجر، أحمد بن علي (1379م). فتح الباري شرح صحيح البخاري، د.ط، بيروت: دار المعرفة، باب العبد راع في مال سيده، ونسب النبي صلى الله عليه وسلم المال إلى السيد، 181/5.

(6) إبراهيم، مصطفى وآخرون (1380). المعجم الوسيط، القاهرة: مطبعة مصر، 411/1.

(7) إمام، محمد كمال الدين (1411هـ). المسؤولية الجنائية- أساسها وتطورها، ط2، بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع، ص81 .

(8) بهنسي، محمد فتحي (1409هـ). المسؤولية الجنائية، ط9، القاهرة: دار الشروق، ص69.

(9) الفيروز آبادي، مجد الدين محمد (د.ت). القاموس المحيط، د. ط، بيروت: مؤسسة الرسالة، ج4ص339. وابن منظور، محمد بن مكرم (2008). لسان العرب، مرجع سابق، ج14 ص190.

(10) إبراهيم، مصطفى وآخرون (1380هـ). المعجم الوسيط، مرجع سابق، ج 1ص141.

(11) الأصفهاني، الحسين بن محمد (د.ت). المفردات في غريب القرآن، القاهرة: مكتبة نزار مصطفى الباز، ص108.

(12) ابن منظور، محمد بن مكرم (2008). لسان العرب، مرجع سابق، ج14 ص190.

ISSN: 2706-6495

الجناية في الاصطلاح القانوني: هـي الجريمة المعاقب عليها بالإعدام، أو الأشغال الشاقة المؤبدة، أو المؤقتة، أو السجن في القوانين الوضعية[1].

الاختراق (Hacking):

لغة: أصله (خ ر ق) خرق الثوب وخرقه فانخرق وتخرق واخرورق، ويقال: في ثوبه خُرْق، ومصدره خَرْق [2]، وهو يأتي اللغة على معان منها:

المرور: ومنه الممر في الأرض عرضاً على غير طريق، واختراق الرياح: مرورها[3].

القطع: ومنه قوله تعالى: (**إِنَّكَ لَن تَخْرِقَ الْأَرْضَ**)[4] خرق الأرض يخرقها: قطعها حتى بلغ أقصاها، وخرقت الأرض أي: جبتها[5].

الكذب والاختلاق والافتراء: ومنه قوله عز وجل: (**وَخَرَقُوا لَهُ بَنِينَ وَبَنَاتٍ بِغَيْرِ عِلْمٍ**)[6] أي: افتعلوا ذلك كذباً وكفراً[7].

والذي نخلص إليه مما سبق أن الاختراق في اللغة يأتي على معان عدة تدور حول التجاوز بحق أو بغير حق.

المعنى في الاصطلاح القانوني:

عرفته الفقرة (7) السابعة من المادة (1) الأولى من نظام مكافحة الجرائم المعلوماتية السعودي بأنه "دخول غير مشروع من شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

المواقع الإلكترونية (Internet Websites):

التعريف في الاصطلاح: عرفت الفقرة (9) التاسعة من المادة (1) الأولى من نظام مكافحة الجرائم المعلوماتية السعودي الموقع الإلكتروني بأنه "مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان موحد".

التعريف الإجرائي: ترى الباحثة تعريف المواقع الإلكترونية لغايات هذه الدراسة بأنها مكان إتاحة البيانات الرسمية للدولة على الشبكة المعلوماتية من خلال عنوان محدد يميزها عن غيرها من المواقع الأخرى.

(1) سرور، أحمد فتحي (1972). أصول السياسة الجنائية، د. ط، القاهرة: (د. ن)، ص25. وأيضاً: الطويل، عبد الله بن محمد (2012). المسؤولية الجنائية عن تشغيل العمالة غير النظامية، (د. ط)، الرياض: جامعة نايف العربية للعلوم الأمنية، ص7 .
(2) الرازي، محمد بن أبي بكر (1415). مختار الصحاح، تحقيق: محمود خاطر، بيروت: مكتبة لبنان، كتاب الخاء (73/1).
(3) ابن منظور، محمد بن مكرم (2008). لسان العرب، مرجع سابق، (75/10).
(4) سورة الإسراء: من الآية 37.
(5) ابن منظور، محمد بن مكرم (2008). لسان العرب، مرجع سابق (75/10).
(6) سورة الأنعام: من الآية (100).
(7) ابن منظور، محمد بن مكرم (2008). لسان العرب، مرجع سابق (75/10).

2. الدراسات السابقة:

وفيما يأتي أهم الدراسات التي توصلت لها الباحثة:

الدراسة الأولى: دراسة العبيدي، خالد بن عبد الله (1430) بعنوان "الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية- دراسة تحليلية مقارنة"[1].وكان من نتائج الدراسة: أن جرائم الحاسب الآلي تختلف عن بقية الجرائم في أن لها طبيعة قانونية خاصة، لأن الاعتداء فيها ينصب على المعلومات، أن نظام مكافحة جرائم المعلومات السعودي يحدّ من الجرائم المعلوماتية بفرض الضوابط والعقوبات.

الدراسة الثانية: دراسة العُمَري، عبد الله بن ناصر (2010) بعنوان "الحماية الجنائية للبريد الإلكتروني- دراسة تأصيلية مقارنة"[2]. وكان من نتائج الدراسة: أن من أكثر الجرائم شيوعاً الواقعة على البريد الإلكتروني هي اختراق البريد الإلكتروني، وانتهاك سريته. أن التشريع الإسلامي والقوانين الوضعية تحمي خصوصية الفرد من خلال بريده الإلكتروني.

الدراسة الثالثة: دراسة الروقي، مروان بن مرزوق (1432) بعنوان "القصد الجنائي في الجرائم المعلوماتية-دراسة تأصيلية مقارنة"[3]. وكان من نتائج الدراسة: اختلاف القصد الجنائي في الجرائم المعلوماتية من جريمة لأخرى، أن الفرق بين القصد الجنائي والخطأ غير العمدي يكون في مقدار سيطرة الجاني على العناصر المادية للجريمة.

الدراسة الرابعة: دراسة مصطفى، خالد حامد (2013) بعنوان "المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي"[4]. وكان من نتائج الدراسة: عدم ملاءمة القواعد التقليدية في قانون العقوبات الإماراتي لمكافحة جرائم النشر الإلكتروني، عدم وضع تعريف موسع للناشر الإلكتروني في القانون الإماراتي.

الدراسة الخامسة: دراسة العجمي، عبد الله دغش (2014) بعنوان "المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة [5].وكان من نتائج الدراسة: أن الجرائم الإلكترونية تأخذ صوراً متعددة، وكل صورة منها تثير مشكلات موضوعية وإجرائية، أشارت الدراسة إلى عجز التشريع الجزائي الكويتي عن مواجهة الجرائم الإلكترونية مقارنة بالتشريع الأردني.

الدراسة السادسة: دراسة الفايز، عبد العزيز بن عبد الكريم (2014) بعنوان "العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي-دراسة مقارنة"[1].وكان من نتائج الدراسة: أن المصادرة في النظام السعودي عقوبة تكميلية جوازية للقاضي،

(1) العبيدي، خالد بن عبد الله بن معيض (1430). الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية-دراسة تحليلية مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.
(2) العمري، عبد الله بن ناصر بن أحمد (2010). الحماية الجنائية للبريد الإلكتروني-دراسة تأصيلية مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.
(3) الروقي، مروان بن مرزوق (1432). القصد الجنائي في الجرائم المعلوماتية-دراسة تأصيلية مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.
(4) مصطفى، خالد حامد (2013). المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي (بحث منشور). مجلة رؤى استراتيجية، دبي: مركز الإمارات للبحوث والدراسات الاستراتيجية، مارس.
(5) العجمي، عبد الله دغش (2014). المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة، رسالة ماجستير (غير منشورة). جامعة الشرق الأوسط، عمان: كلية الدراسات العليا، قسم القانون العام.

فيها سلطة تقديرية في الحكم بها أو عدم الحكم، مع مراعاة الغير حسني النية، بينما هي في القانون الإماراتي عقوبة وجوبية، وليس فيها سلطة للقاضي. أن عقوبة إغلاق المحل أو الموقع الإلكتروني في النظام السعودي عقوبة تكميلية جوازية، في حين هي عقوبة وجوبية في القانون الإماراتي.

التعقيب على الدراسات السابقة:

وهذا يعني سبق هذه الدراسة لهذا الموضوع، على الرغم من وجود عدد من الدراسات التي تناولت الجريمة المعلوماتية، فمنها ما تناول هذه الجريمة من منظور فقهي، ومنها ما تناول جزئية معينة من الجريمة المعلوماتية، دون تخصيص جرائم اختراق المواقع الرسمية للدولة، وهذا ما سيتضح من خلال بيان أوجه الشبه والاختلاف بين الدراسات السابقة والدراسة الحالية، وفيما يأتي بيان ذلك:

أوجه الشبه بين الدراسات السابقة والدراسة الحالية:

تتفق الدراسة الحالية مع الدراسات السابقة من حيث النطاق الموضوعي للدراسة؛ ذلك أن الدراسات السابقة قد تناولت الجريمة المعلوماتية في النظامين السعودي والإماراتي كدراسة الفايز (2014)، ودراسة الروقي (1432)، ودراسة العمري (2010)، وربما اقتصر بعضها على أحد النظامين كدراسة مصطفى (2013) التي اختصت بالقانون الإماراتي، ودراسة العبيدي (1430) التي تناولت النظام السعودي مقارناً بالأنظمة العربية والأجنبية.

كما تتشابه الدراسة الحالية مع بعض الدراسات السابقة من حيث تناولهما جزئيات في الجريمة المعلوماتية، كدراسة الفايز (2014) التي تناولت العقوبات التكميلية في النظام السعودي والقانون الإماراتي، وهو ما تناولت الدراسة الحالية جانباً منه في المبحث الثاني من الفصل الرابع (عقوبة المصادرة وعقوبة إغلاق المحل)، ودراسة العجمي (2014) التي تناولت المشكلات العملية والقانونية للجرائم الإلكترونية، وهو ما تناولت الدراسة الحالية جانباً منه في الفصل الثاني، ودراسة مصطفى (2013) التي تناولت المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها، وهو ما تناولت الدراسة الحالية جانباً منه في الفصل الثاني.

أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة:

1. أن الدراسة الحالية اختصت في نطاقها الموضوعي بدراسة جرائم اختراق المواقع الرسمية للدولة، دون بقية الجرائم المعلوماتية الأخرى، وهو ما لم تتوصل الباحثة لدراسة مماثلة له في أي من الدراسات السابقة أو الدراسات التي تناولت الأنظمة العربية الأخرى، ما يعني سبق الدراسة الحالية لهذا الموضوع، وجدّته.
2. على الرغم من أن بعض الدراسات السابقة تناولت الجريمة المعلوماتية إلا أنها لم تتطرق لجرائم اختراق المواقع الرسمية للدولة، ولم تخصص لها باباً يميزها، فاكتفت هذه الدراسات بالجرائم المعلوماتية، ومنها الاعتداء على المواقع والبريد الإلكتروني والشبكات، دون تخصيص المواقع الرسمية للدولة، حتى ما كان نطاقها الموضوعي النظام السعودي أو القانون الإماراتي.

(1) الفايز، عبد العزيز بن عبد الكريم (2014). العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي-دراسة مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية للعلوم الأمنية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.

ISSN: 2706-6495

3. النطاق الشخصي للمسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي

1.3. ماهية المجرم المعلوماتي (Cyber Criminal)

تمهيد وتقسيم:

يسمى العصر الحاضر بعصر التكنولوجيا والانفجار التقني والمعرفي، ويعرف أيضاً بعصر المعلومات؛ إذ تشهد البشرية تقدماً سريعاً ومطرداً في عدة مجالات متعلقة بحياة الإنسان؛ فأصبحت أجهزة الحاسب الآلي الوسيلة الأولى في حفظ المعلومة ونقلها حتى لا يكاد يستغنى عنها في أي مجال من مجالات الحياة المختلفة.

كما يطلق على العصر الحاضر أيضاً عصر الجريمة المنظمة التي تعددت أشكالها وطرقها، سواء أكانت جريمة تقليدية أو معلوماتية، ومن هذه الأنواع الجريمة المعلوماتية، وتعني السلوك غير المشروع المتعلق بالوصول للبيانات الآلية والتقنية وتداولها مما يشكل فعلاً إجرامياً أو غير أخلاقي بغض النظر عن السبب أو الدافع المؤدي لذلك أو الوسيلة المستخدمة فيه[1].

1.1.3 مفهوم المجرم المعلوماتي (Cyber Criminal)

المجرم المعلوماتي ليس مجرماً عادياً أو تقليدياً، ذلك أنه يمتلك مهارات تقنية عالية، تجعل منه خبيراً بالمسائل المعلوماتية ونظم التشغيل للحاسب الآلي والأجهزة التقنية الحديثة، وهذا يعني أن هذا النوع من الإجرام يسمى إجرام الأذكياء إذا ما قيس بالإجرام التقليدي الذي يتسم في الغالب بالعنف[2].

المعنى اللغوي للجريمة والمجرم:

الجريمة لغة: "مأخوذة من (جَرَم) وهو بفتح الجيم: القطع، جرمه يجرمه جَرماً: قطعه، وشجرة جريمة أي: مقطوعة، و(الجُرم) بضم الجيم: التعدي والذنْب، والجمع أجرام وجروم، وهو الجريمة، وقد جَرم يجرُم جَرماً واجترم وأجرم فهو مجرم، وجَرَم عليهم وإليهم جريمة، أي: جنى جناية، وجمع الجريمة: جرائم"[3].

الجريمة اصطلاحاً (Crime): هي "محظور شرعي زجر الله تعالى عنه بحد أو تعزير"[1]. والمحظورات هي: "إما إتيان فعل منهي عنه، أو ترك فعل مأمور به، وقد وصفت المحظورات بأنها شرعية إشارة إلى أنه يجب في الجريمة أن تحظرها الشريعة"[2].

(1) قارة، آمال (2002). الجريمة المعلوماتية، رسالة ماجستير (غير منشورة). جامعة الجزائر، الجزائر: كلية الحقوق، قسم القانون الجنائي والعلوم الجنائية، ص113.

(2) سالم، محمد علي وهجيج، حسون عبيد (2007). الجريمة المعلوماتية، (بحث منشور). مجلة جامعة بابل، بغداد: العلوم الإنسانية، المجلد 14، العدد 2، ص 88.

(3) ابن منظور، محمد بن مكرم (2010م). لسان العرب، مرجع سابق، 124/2.

الجريمة المعلوماتية (Cyber Crime): ليس هناك اتفاق بين فقهاء القانون على استخدام مصطلح محدد لهذا المدلول، "فهناك من يسميها بهذا الاسم، وهناك من يسميها الجريمة الإلكترونية، وهناك من يطلق عليها جرائم المعلومات، ومن يسميها إساءة استخدام تكنولوجيا المعلومات والاتصال، ومن يطلق عليها جرائم الكمبيوتر والإنترنت، وفضل آخرون تسميتها الجرائم المستحدثة"[3].

المجرم لغة: اسم فاعل من الفعل (أجرم)، فهو من ارتكب الجُرم أو قام به.

المجرم المعلوماتي (Cyber Criminal): هو "كل شخص يقوم بأي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[4].

2.1.3. الفرق بين المجرم المعلوماتي والمجرم التقليدي

تتشابه في كثير من الأحيان الجريمة المعلوماتية والجريمة التقليدية في أمور، ولكنها تختلف في أمور أخرى، ومن هنا ترى الباحثة بعد استقراء الدراسات المتخصصة في هذا المجال بيان أوجه التشابه والاختلاف بين المجرم التقليدي والمجرم المعلوماتي من حيث: دوافع الجريمة، وأدلة الإثبات، والسمات الشخصية والفنية، ومحل الجريمة في كل منهما، وفق ما يأتي:

أولاً: دوافع الجريمة المعلوماتية (Cybercrime Motives):

يعرف الدافع بأنه "الباعث أو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام، فهو عبارة عن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة لأخرى باختلاف مرتكب الجريمة من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات"[5].

هناك دوافع إضافية للمجرم المعلوماتي لارتكاب جريمته، ومنها:

1. الولع بجمع المعلومات وتعلمها.
2. الدوافع الشخصية: غالبًا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالذات، وبقدرته على اقتحام النظام، فيندفع تحت تأثير الرغبة القوية في تحقيق الذات، أو بدافع المغامرة والإثارة.

---

(1) الماوردي، علي بن محمد بن حبيب (2012م). الأحكام السلطانية، ط2، القاهرة: مطبعة البابي الحلبي، ص11.

(2) عودة، عبد القادر (2013م). التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، ط2، بيروت: دار الكتاب العربي، 66/1 .

(3) الشكري، عادل يوسف عبد النبي (2008م). الجريمة المعلوماتية وأزمة الشرعية الجزائية، (بحث منشور). الكوفة: مجلة مركز دراسات الكوفة، العدد السابع، ص 112.

(4) بيومي، عبد الفتاح (2009). الأحداث والإنترنت: أثر الإنترنت في انحراف الأحداث، (د. ط)، الإسكندرية: دار الفكر العربي، ص25.

(5) الغافري، حسين بن سعيد (2009م). السياسة الجنائية في مواجهة جرائم الانترنت-دراسة مقارنة، القاهرة: دار النهضة العربية، ص55.

3. الإضرار بالأشخاص والجهات: وغالباً ما تكون هذه الجرائم بصورة ابتزاز أو تهديد، ويتمثل هذا الدافع في السطو على البريد الإلكتروني أو الموقع الخاص ببعض الفتيات مثلاً وسرقة صورهن الشخصية[1].

ثانياً: الكشف عن شخصية المجرم المعلوماتي (Disclosure Of Cyber Criminal Identity):

1. صعوبة إثبات وقوع الجريمة.
2. صعوبة تحديد المسؤول جنائيًا عن الفعل الإجرامي.
3. صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.
4. تنازع القوانين الجنائية من حيث المكان.
5. صعوبة التوصل إلى الجاني.
6. القصور في القوانين الجنائية القائمة.
7. افتراض العلم بقانون جميع دول العالم[2].

ثالثاً: سمات المجرم المعلوماتي (Traits Of Cyber Criminal):

وقد أشارت الدكتورة عطوي إلى مجموعة من الخصائص والسمات التي تميز المجرم المعلوماتي، ومنها:

1. أن المجرم المعلوماتي إنسان اجتماعي بطبعه: فهو يقوم بعمله في المجال المعلوماتي أو غيره من المجالات، ويمارس حقوقه الاجتماعية والسياسية دون عائق في حياته العملية.
2. أن المجرم المعلوماتي إنسان ذكي محترف: فهو يمارس ما يعرف بتقنيات التدمير الناعمة، يتلاعب بالبيانات والبرامج، ويعدل عليها، ويمحو ما استطاع، ويقوم بذلك بهدوء غير محسوس.
3. أنه مجرم متخصص في هذه الحاسبات والبرمجيات، وذلك حتى يستطيع تجاوز أنظمة الحماية التي تستخدمها الأجهزة والمواقع المستهدفة. كما يتمثل هذا التخصص في أنه لا يمارس أو يرتكب أية أفعال إجرامية من الجرائم التقليدية، بل هي محصورة في مجال البرمجيات والحاسبات.
4. أن المجرم المعلوماتي عائد إلى الإجرام: ذلك أن إصراره على قهر الأنظمة التشغيلية وبرامج الحماية التي تستخدمها الأجهزة والمواقع هو الدافع للجريمة في كثير من الأحيان، كما يدفعه لذلك جهله غالباً بالعقوبات المترتبة على الفعل الجرمي ونتائجه.

(1) الغافري، حسين بن سعيد (2009م). السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص58.

(2) حسني، محمود نجيب (1999م). شرح قانون العقوبات، القسم العام، ط1، القاهرة: دار النهضة العربية، ص105.

5. المجرم المعلوماتي غير عنيف: فجرائمه تعرف بجرائم الحيلة، وهذه لا تتطلب عنفاً، بل تتطلب ذكاء وتكيفاً اجتماعياً، بعكس المجرم التقليدي الذي يتسم بالانطواء والابتعاد عن الناس[1].

رابعاً: محل الجريمة (Crime Subject):

في الجريمة التقليدية غالباً ما يتم الاعتداء على النفس أو المال منقولاً كان أو غير منقول، ولكننا في الجريمة المعلوماتية أمام محل للجرم هو المعلومات غالباً، فقد تكون الجريمة واقعة على الكمبيوتر الذي يحتوي المعلومات بهدف تدميره أو سرقة ما بداخله، كما يمكن أن يكون أداة للجريمة، أو بيئة لها.

2.3. مقدم ومستهلك الخدمة (Internet Service Provider And Customer)

1.2.3. متعهد الخدمة (Internet Service Provider)

ماهية متعهد الخدمة:

تتألف شبكة الإنترنت من أعداد هائلة من أجهزة الحاسوب المتصلة ببعضها عن طريق أجهزة الاتصال التي تشكل الشبكة المعلوماتية، بما يتيح للعملاء مجالات مختلفة تتمثل في الدعاية والإعلان والتسويق، والاتصال والتبادل التجاري، وهذا بدوره يؤدي إلى تداخل أطراف عدة في عملية الاتصال هذه.

والدخول إلى الشبكة المعلوماتية لا يتم إلا عن طريق متعهد الخدمة الذي يتيح للمستخدم من مؤسسات وهيئات حكومية وغيرها الوصول للشبكة؛ فهو يقدم خدمات فنية تربط المشتركين بالمواقع أو المستخدمين الآخرين للشبكة، كونه هو من يدير آلية الاتصال بالإنترنت[2].

وهذا يعني من وجهة نظر الباحثة أن هذا الدور لا يقتصر على متعهدي الخدمة الذين ينحصر دورهم في توريد المحتوى المعلوماتي، والسلطة والرقابة على محتوى المعلومات، بل يشمل فئات أخرى تشترك في هذا الدور، وأدوار أخرى فنية وتقنية تتمثل في توصيل الخدمة للمستهلك، وتمكينه من الحصول على البيانات والمعلومات التي يريدها، ويكون متضامناً في المسؤولية المدنية في حالات كونه المورد للمحتوى، أو المنتج لها، في حال ثبوت قدرته على رقابة المحتوى وفحصه قبل نشره، ومثال ذلك:

أولاً: متعهد الوصول (Internet Service Provider):

يتمثل دوره في الجانب الفني بتوصيل المستهلك بشبكة الإنترنت- سواء أكان شخصاً معنوياً أو طبيعياً- فهو يربط المستهلك بالمواقع المختلفة، ولا دور له في المحتوى، ولا السيطرة على المواقع ولا مراقبة المعلومات،

(1) عطوي، مليكة (2012م). الجريمة المعلوماتية، مرجع سابق، ص12.

(2) كيلاني، عبد الفتاح محمود (2014). مدى المسؤولية القانونية لمقدمي خدمة الإنترنت، مرجع سابق، ص473.

ISSN: 2706-6495

ومثاله: شركة الاتصالات السعودية، وموبايلي وزين. ويطلق على هؤلاء متعهدي الوصول أو مقدمي خدمة الاتصالات مع شبكة الإنترنت أو مزودي خدمة الإنترنت، أو مقدمي خدمة الإنترنت[1].

ثانياً: مورد المعلومات (Content Provider):

هو شخص طبيعي أو معنوي يبث المعلومات والرسائل المتعلقة بموضوع معين على الإنترنت، بحيث يتمكن المستهلك من الحصول عليها مجاناً أو بمقابل مادي، وهو من يبث الحياة في الشبكة من خلال تزويدها بالمادة، وبالتالي فهو المسؤول الأول عن المعلومات؛ لأنه من يتحكم في نشرها وبثها على الإنترنت، من خلال تأليفها أو تجميعها واختيارها حتى تصل للمستهلك[2].

ثالثاً: متعهد الإيواء (Domain Host): هو شخص معنوي أو اعتباري يقوم بتخزين المعلومة، ويدير محتواها، بما يتيح لمورّد المعلومة عرضها على المستهلك[3].

الالتزامات الخاصة بمتعهد الخدمة:

أولاً: ضمان الاستخدام الأمثل لبنك المعلومات:

الأول: تقني: وهو يعني الالتزام بتذليل الصعوبات التي يواجهها مستهلك الخدمة، من خلال تطوير تقنياته ومعداته باستمرار، لضمان استجابة البنك للحد الأدنى من الطلبات التي التزم باستقبالها، والرد عليها في نفس الوقت، دون زيادة مقابل مادي أو أن يؤثر ذلك على نوعية الخدمة المقدمة.

الثاني: إعلامي: بما أن المورد التزم بتوصيل مستهلك الخدمة لبنك المعلومات فإنه يكفل له التأهيل المستمر الذي يتيح له التعامل مع النظام التقني بنجاح، وإعادة تأهيله عند تعديل الخدمة. وهذا يشمل مساعدته على إيجاد الشبكات والنهايات الطرفية الملحقة بالخدمة بما يسهل له الاستخدام الأمثل للتعامل مع البنك[4].

ثانياً: الاستجابة الفورية لاتصالات المستهلك النهائي:

الاستجابة الفورية تعني الرد على استفسارات المستهلك النهائي وطلباته بشكل فوري، ومعيار هذا الالتزام هو معيار موضوعي، يتمثل فيما جرت عليه العادة فيما يخص نوعية السؤال وحجمه، ومدى سهولة الحصول على المراجع المبرمجة في ذاكرة البنك[5].

(1) منصور، محمد حسين (2006). المسؤولية الإلكترونية، مرجع سابق، ص 175.

(2) كيلاني، عبد الفتاح محمود (2014). مدى المسؤولية القانونية لمقدمي خدمة الإنترنت، مرجع سابق، ص487.

(3) حوته، عادل أبو هشيمة محمود (2004). عقود خدمات المعلومات الإلكترونية في القانون الدولي الخاص، القاهرة: دار النهضة العربية، ص200.

(4) لطفي، حسام (2010). عقود خدمات المعلومات، ط2، القاهرة: دار الكتاب الجامعي، ص 92.

(5) لطفي، حسام (2010). عقود خدمات المعلومات، مرجع سابق، ص93.

ثالثاً: تقديم معلومات مشروعة وجديرة بالثقة:

تشمل المشروعية عدة أمور منها:

1. ألا تكون المعلومات مخالفة للتشريعات المعمول بها في الدولة، فلا تتعلق بأمن الدول كأسرار الدفاع والتسليح العسكري وغيرها من الأسرار التي تحرص الدول على سريتها وعدم إفشائها
2. التزام المورد بحقوق التأليف، وعدم نشر أي محتوى محميّ إلا بإذن مكتوب من المؤلف، وكذلك عدم استغلاله أو تخزينه أو استرجاعه.
3. عدم مخالفة المعلومات للآداب العامة، كأن تكون خاصة بإبرام عقود لتجارة السلاح أو المخدرات أو علاقات غير مشروعة[1].

2.2.3. مستهلك الخدمة (Internet Customer)

ماهية مستهلك الخدمة:

عرف نظام الاتصالات السعودي في الفقرة (16) السادسة عشرة من مادته (1) الأولى مستهلك الخدمة بأنه "الشخص ذو الصفة الطبيعية أو المعنوية الذي يستخدم خدمات الاتصالات". في حين غاب هذا التعريف في القانون الاتحادي لتنظيم قطاع الاتصالات في دولة الإمارات، كما غاب أيضاً عن نصوص القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

الالتزامات الخاصة بمستهلك الخدمة:

بناء على هذه العلاقة التعاقدية بين الطرفين فمن الواجب أن يلتزم مستهلك الخدمة بمجموعة من الالتزامات تجاه متعهد الخدمة والغير في ذات الوقت، باعتبارها جزءاً من العقد، وتمثل ضماناً للخدمة وكذلك مشروعية استخدامها ومشروعية الالتزام بما يترتب على العقد من واجبات متبادلة بين الطرفين، ومنها ما يؤثر على حقوق الغير، ومن هذه الالتزامات:

أولاً: سداد المقابل المادي:

يعد هذا الالتزام من أهم التزامات مستهلك الخدمة، بحكم العلاقة التعاقدية بين الطرفين، حتى يرى بعض فقهاء القانون أنه الالتزام الوحيد من قبل مستهلك الخدمة، ويستند هذا المقابل المادي إلى مدة الاتصال وحجم البيانات المستخدمة، ويتمثل هذا المقابل المادي في اشتراك شهري أو سنوي متفق عليه[2].

(1) حوته، عادل أبو هشيمة محمود (2004). عقود خدمات المعلومات الإلكترونية في القانون الدولي الخاص، مرجع سابق، ص 202-203.

(2) حوته، عادل أبو هشيمة محمود (2004). عقود خدمات المعلومات، مرجع سابق، ص 208.

ثانياً: ضمان سرية التعامل:

يقابل هذا الالتزامَ التزامٌ مثله من قبل متعهد الخدمة، فهو التزام متبادل بين الطرفين، وهو يوجب على مستهلك الخدمة أن يتخذ التدابير اللازمة للمحافظة على كود الاستعمال، وتغييره عند شعوره بتسريبه[1].

ثالثاً: الالتزام باحترام حقوق الملكية الفكرية:

تعدّ قواعد المعلومات الإلكترونية من المصنفات المحمية، بموجب قوانين حماية الملكية الفكرية، فأصحابها يتمتعون بالحقوق الأدبية والمالية عليها مقابل جهودهم في اختيار محتواها، وتأليفها وعرضها، وفي هذه الحالة يكون صاحب هذه الحقوق هو مؤلف المعلومة، وقد يكون متعهد الخدمة هو صاحب هذه الحقوق في حال حصوله على ترخيص من مؤلفها أو منتجها[2].

رابعاً: احترام الغرض من الاستخدام الوارد في العقد: المستهلك قد يكون منتجاً للمعلومة، ويكون العقد معه على أساس هذه المهمة، وبالتالي فإنه يكون مسؤولاً عن الفعل الضار الذي سبّبه للغير باعتباره منتجاً للمعلومة، كأن يتضمن المحتوى تشهيراً بالغير أو شتماً أو انتهاكاً لخصوصيتهم، من منطلق قيام المسؤولية تجاه من أنتج المعلومة[3].

أهمية التزامات متعهد الخدمة ومستهلك الخدمة وتحدياتها: تأتي أهمية التزامات كل من متعهد الخدمة ومستهلك الخدمة في التعامل مع البيانات في الإنترنت أكثر من غيرها من الأمور المادية، وخاصة ما يتعلق منها بالخصوصية بسبب ما يفرضه عالم الشبكات المعلوماتية من تحديات ومعوقات لحماية الخصوصية.

وسائل حماية التزامات متعهد الخدمة ومستهلك الخدمة:

إن حماية هذه الالتزامات بين طرفي الخدمة المعلوماتية (المتعهد والمستهلك) تستلزم مجموعة من الوسائل والإجراءات التقنية والتنظيمية والتشريعية، وفيما يأتي تفصيل كل منها:

1. الوسائل التقنية: تعني هذه الطريقة إخضاع النظم الآلية لإشراف الدولة، وفق ضوابط معينة، وتمكين الطرفين من الاطلاع على المعلومات الخاصة بكل منهما للتأكد من سلامتها، وتصحيح ما يعترضها من أخطاء، كتشفير المعلومات.
2. وسائل التنظيم الداخلي: تعني هذه الوسيلة وضع القواعد السلوكية وعقود نقل البيانات لضمان الالتزام بها، ومثال هذه العقود النماذج التي أقرتها غرفة التجارة الدولية لعقود نقل البيانات، ومنها تسجيل المستخدم وبياناته قبل الدخول للمواقع.
3. الوسائل التشريعية: تعني هذه الوسيلة حرص الدول على صيانة الخصوصية الخاصة ببيانات أفرادها ومؤسساتها، من خلال النصوص القانونية والأنظمة الدستورية التي تنص على هذه الحقوق والالتزامات[4].

(1) حوته، عادل أبو هشيمة محمود (2004). عقود خدمات المعلومات، مرجع سابق، ص 211.

(2) عبد الصادق، محمد سامي (2008). التحديات التشريعية في عصر تكنولوجيا المعلومات والاتصالات، مرجع سابق، ص 31.

(3) الحسبان، ياسين محمد (2010). المسؤولية المدنية لمزودي الخدمات عبر الإنترنت في القانون الأردني، رسالة ماجستير (غير منشورة). جامعة عمان العربية، عمّان: كلية القانون، قسم القانون الخاص، ص 106.

(4) الأستاذ، سوزان عدنان (2013). انتهاك حرمة الحياة الخاصة عبر الإنترنت، مرجع سابق، ص443- 445.

4. النطاق الموضوعي للمسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة

تمهيد وتقسيم:

يتناول هذا الفصل من الدراسة توضيح ما يتضمنه النطاق الموضوعي للمسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي، لتوضيح السلوك الذي يرتب المسؤولية الجنائية لمرتكب جريمة الاختراق؛ حيث يتم تقسيمه إلى مبحثين: يتناول الأول منهما بيان ماهية اختراق المواقع الإلكترونية الرسمية للدولة، ويعكف المبحث الثاني على دراسة صور اختراق المواقع الإلكترونية الرسمية للدولة.

1.4. ماهية اختراق المواقع الإلكترونية الرسمية للدولة

1.1.4. مفهوم المواقع الإلكترونية الرسمية للدولة

عرّف نظام مكافحة الجرائم المعلوماتية السعودي في الفقرة (9) التاسعة من المادة (1) الأولى الموقع الإلكتروني بأنه "مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد". ولا يختلف هذا التعريف عما جاء في الفقرة (9) التاسعة من المادة (1) الأولى من قانون مكافحة جرائم تقنية المعلومات الإماراتي من تعريف الموقع الإلكتروني بأنه "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية".

وقد جاءت تعريفات عدة للمواقع الإلكترونية، ومنها:

"عبارة عن مجموعة من الموضوعات والملفات الموجودة على خادم الويب، وهو عبارة عن مساحات إلكترونية يتم شراؤها من قبل الشركات المتخصصة في هذا المجال، وهو يعد وسيلة مملوكة للجهة التي تتولى الإنفاق عليه، وبذلك يصبح وسيلة تستخدم لخدمة مصالح هذه الجهة التي تتولى الإشراف عليه"[(1)].

أقسام المواقع الإلكترونية:

تنقسم المواقع الإلكترونية إلى أنواع متعددة، حسب الهدف منها، فمنها مواقع تجارية تهدف للربح والتعريف بالمنتجات، وهناك المواقع التعليمية ذات الهدف التعليمي، وهناك مواقع التواصل الاجتماعي التي تهدف للتواصل بين أفراد المجتمعات على اختلاف أماكنهم ولغاتهم[(2)].

مكونات المواقع الإلكترونية:

يتكون الموقع الإلكتروني من مجموعة من العناصر التي تميزه عن غيره، وتسهل التعرف عليه لمن أراد الوصول إليه، ومنها:

(1) قشقوش، هدى (1992). جرائم الحاسب الإلكتروني في التشريع المقارن، القاهرة: دار النهضة العربية، ص2.

(2) حسين، محمد مصطفى (2010). تقييم جودة المواقع الإلكترونية، مرجع سابق، ص 38.

1. بروتوكول نقل النص التشعبي (Hypertext Transfer Protocol- Http) التي تعني مجموعة المقاييس المتفق عليها لاستخدامها بين الحاسبات التي تتم من خلالها عملية الاتصال ومشاركة الملفات.
2. اسم فريد (Uniform Resource Locator- URL) ويمنح هذا الاسم من قبل مركز معلومات الشبكة.
3. ينتهي كل عنوان بحروف توضح نوع نشاط الموقع.
4. الوصلات والروابط التشعبية، وهي عبارة عن أيقونات للتنقل بين صفحات الموقع الرئيسة والفرعية، وقد تحمل كل أيقونة منها صورة أو عبارة تنقل المستخدم للرابط التشعبي[1].

استخدامات المواقع الإلكترونية:

وفي نطاق هذه الدراسة فإن استخدام المواقع الإلكترونية الرسمية للدول ينحصر في الاستخدامات الإيجابية، ومنها:

1. خدمة التواصل:
2. خدمة البحوث
3. خدمة التعليم
4. الخدمات الحكومية
5. الخدمات الأمنية
6. خدمات الإعلام.

2.1.4. مفهوم اختراق المواقع الإلكترونية الرسمية للدولة

مع تحول أغلب الحكومات الدولية للنظام الإلكتروني الذي يعرف بالحكومة الإلكترونية، تحولت المعلومات والأوراق التقليدية ونقل البيانات وتداولها إلى معلومات رقمية يمكن تداولها عبر الفضاء الإلكتروني، اعتماداً على نظم تشغيلية ومواقع إلكترونية خاصة بهذه الجهات والدول، كما تحوّل الأشخاص الذين يسعون للحصول على هذه البيانات إلى استخدام هذه الوسيلة المتطورة للحصول عليها.

أما في قانون مكافحة جرائم المعلومات الإماراتي فقد غاب هذا التعريف، ولم يتطرق القانون لتعريف الاختراق أو الاعتداء على البيانات أو وسائل تناقلها، أو أي مما يتعلق بها من الأنشطة الجرمية.

أولاً: استهداف البنية الأساسية:

تستهدف عمليات اختراق المواقع الرسمية للدول التأثير على الاقتصاد العالمي، واقتصاد الدول المستهدفة بشكل خاص، وذلك بسبب المناخ السياسي والعداوات بين الدول والجماعات التي تشكل تهديداً لها؛ فتستهدف عمليات القرصنة البنية التحتية للدولة المستهدفة بالتدمير، ويرى الخبراء أن مثل هذه الأعمال التخريبية لا تسعى لتحقيق الربح المادي بقدر ما تسعى لتحميل الدول المستهدفة خسائر مادية والإضرار بها،

(1) دولة، زهير مصطفى؛ واشتيوي، عماد محمد (2006). القائم بالاتصال في المواقع الإلكترونية الإخبارية الفلسطينية، مرجع سابق، ص23.

ثانياً: استهداف الأمن:

تمثل جريمة اختراق مواقع الدولة الرسمية خطراً على أمن الدولة وسرية معلوماتها وبصفة خاصة المعلومات الأمنية ، فقد تتمثل جريمة الاختراق في الإرهاب الذي يعرف بأنه "كل عمل يرتكب بوسيلة فتاكة، يبعث على الذعر، ويشكل خطراً عاماً يهدد أكثر من شخص". كما يعرف الإرهاب الإلكتروني بأنه "استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو مهاجمة نظم المعلومات على خلفية سياسية أو اقتصادية أو أمنية أو عرقية أو دينية"[1] وتتسم هذه الجريمة باستخدامها المكثف لوسائل الاتصال الحديثة، وأهمها الإنترنت، مستهدفة بأعمالها غير المشروعة أهدافاً متنوعة، ومنها الإنترنت والمواقع الإلكترونية للدول المستهدفة، حتى صار الإنترنت من أهم وسائلها لتحقيق أهدافها غير المشروعة[2].

ثالثاً: طابع التنظيم:

تعد جريمة اختراق المواقع الرسمية للدولة جريمة منظمة على أعلى مستويات التنظيم، وتعرف الجريمة المنظمة بأنها "التنظيم الإجرامي الذي يضم أفراداً أو مجموعات، ينشطون بشكل منظم للحصول على فوائد مالية من خلال ممارسة أنشطة غير قانونية، يعمل أعضاؤه من خلال بناء تنظيمي دقيق ومعقد، يشبه ما عليه الحال في المؤسسات الاقتصادية، ويخضعون لنظام جزاءات داخلية رادعة".[3].

وبالنظر إلى التنظيم الدقيق الذي تتمتع به جريمة اختراق المواقع الرسمية للدولة فإن لها مجموعة من الخصائص التنظيمية التي تميزها عن غيرها في ذلك، ومنها:

1. **من حيث الهيكل التنظيمي:**

تربط هذه الجريمة بين أعضائها برباط محكم، قائم على اعتماد القوة والفعالية، بما يحقق التنسيق الكامل بينهم، وفق نظام قيادي يتخذ القرارات، ويوزع الأدوار استعانة بذوي الكفاءة والاختصاص، بما يحقق أهداف الجماعة، والحماية أثناء ممارسة أنطتهم، مع الحفاظ في الوقت نفسه على الشكل الهرمي للمستويات الوظيفية.

(1) الكبيجي، بهاء فهمي (2013). مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير (غير منشورة). جامعة الشرق الأوسط، عمّان: كلية الحقوق، قسم القانون العام، ص84.

(2) مؤمن، طاهر شوقي (2014). مشروعية الرقابة على الإنترنت، الرياض: ورقة عمل في المؤتمر العلمي حول دور الإعلام العربي في التصدي لظاهرة الإرهاب، 24-26 محرم، ص7.

(3) فنور، حاسين (2013). المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، رسالة ماجستير (غير منشورة). جامعة الجزائر، الجزائر: كلية الحقوق، قسم القانون الدولي، ص54.

2. من حيث طبيعة النشاط:

يمتاز نشاط هذه الجريمة بالاحتراف والتخصص، اعتماداً على ما يمتلكه منتسبوها من مهارات فائقة في الإجرام المعلوماتي، كما يمتاز بالاستمرارية في السلوك الإجرامي، ولا ينتهي نشاطها إلا بانتهاء الجماعة نفسها، يساعدها في ذلك ما تمتاز به من مرونة وهيكلية متنقلة لتفادي السلطات التنفيذية والقضائية، مستخدمة في ذلك العنف[1].

3. من حيث الأهداف والغايات:

تمتاز هذه الجريمة بقدرة أفرادها على تدويل الجريمة، وجعلها عابرة للحدود، وممارسة أعمالها على نطاق واسع في دول عدة، من خلال قدرتهم على توظيف أطراف جديدة، وابتزاز أطراف أخرى بما يخدم أغراضهم، ويحقق لهم المكاسب المادية والمعنوية[2].

رابعاً: فئات المخترقين (Types Of Hackers):

قسمت الدراسات والبحوث فئات المجرمين المعلوماتيين بحسب السن والأهداف كما مرّ في المطلب الأول من المبحث الأول من الفصل الثاني، فإذا كانت تلك خصائص عامة تميز المجرم المعلوماتي بشكل عام، فإن لمخترقي المواقع الإلكترونية الرسمية للدولة خصائص تميزهم عن غيرهم من فئات المجرمين المعلوماتيين والمجرمين التقليدين.

خامساً: تعاظم آثارها:

تمتاز جريمة اختراق المواقع الإلكترونية بعظم آثارها مقارنة بغيرها من الجرائم التقليدية أو الجرائم المعلوماتية التي تشكل انتهاكاً لحرمة الحياة الخاصة أو الاعتداء على الأشخاص،

التي يعرفها فقهاء القانون بأنها "جرائم تقوم بالاعتداء على الحياة الخاصة للشخص، وما ينبغي أن تحاط به من حرمة وقدسية، ومن أمثلتها استراق السمع إلى حديث خاص، والتقاط صور لشخص في مكان خاص"[3].

2.4. صور اختراق المواقع الإلكترونية الرسمية للدولة (Types Of Government Websites Hacking)

1.2.4. الأساليب الاقتحامية (Hacking Methods)

يعرف الاقتحام لغة بأنه الدخول فجأة وبلا رويّة، ومنه قولهم: "قَحَم في الأمر: رمى بنفسه فيه فجأة بلا رويّة، ومنه الفعل اقتحم. واقتحم المنزل: هجَمَه. وأقحم فرسه النهر: أدخله فيه"[1].

(1) فنور، حاسين (2013). المنظمة الدولية للشرطة الجنائية، مرجع سابق، ص65.

(2) فنور، حاسين (2013). المنظمة الدولية للشرطة الجنائية، المرجع السابق، ص 66.

(3) مجمع اللغة العربية (1999). معجم القانون، القاهرة: الهيئة العامة لشؤون المطابع الأميرية، ص54.

والاقتحام هو لب الاختراق بما فيه من فجأة الفعل بخلاف الاحتيال الذي قد يستغرق مدة زمنية أطول للتفعيل، ويعرف الدخول غير المشروع لدى بعض فقهاء القانون بأنه "الولوج غير المصرح به إلى نظام معالجة آلية للبيانات باستخدام الحاسوب، بحيث يتحقق الدخول غير المشروع بالوصول إلى المعلومات والبيانات المخزنة داخل النظام المعلوماتي، دون رضاً من المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها"[2].

1. الاختراق البسيط (Simple Hacking):

اختارت الباحثة هذه التسمية؛ لأن الوصف فيها يدل على الفعل، وهي تعني أن المخترق يدخل للجهاز وهو في حالة التشغيل، أو يقوم هو بتشغيله ببساطة،

وهذا ما أكده الدكتور الدسوقي من أن بعض الحالات لا تحتاج سوى للضغط على زر التشغيل في الحاسب الآلي، والدخول إليه، وغالباً ما يتم في الأجهزة التي لا يتنبه القائمون عليها لتثبيت رمز للدخول لها[3].

2. التجربة العشوائية لكلمات السر:

يلجأ المخترق بحسب هذا الأسلوب إلى تجربة كلمات سر عشوائية، في محاولة للدخول لهذه الأجهزة بطريقة التخمين، وقد تستغرق هذه العملية ساعات أو دقائق، كما قد تفشل بحسب قوة كلمة المرور أو سهولتها[4].

3. الاختراق بإلغاء الخدمة أو تعطيلها:

يتمثل ذلك في إرسال عدد هائل من الرسائل للموقع أو البريد الإلكتروني للجهة المستهدفة، بطرق فنية، فيعيق عملها، أو يعطل أجهزتها أو شبكتها، وهو ما يعرف بالإغراق بالرسائل[5].

وقد عرّفت هيئة الاتصالات وتقنية المعلومات السعودية الرسائل الاقتحامية بأنها "أي رسالة إلكترونية ترسل دون موافقة مسبقة من المستلم لها، وذلك بوساطة أيّ وسيلة اتصال إلكترونية بما في ذلك على سبيل المثال لا الحصر البريد الإلكتروني، والرسائل النصية (SMS) أو رسائل الوسائط المتعددة (MMS) والبلوتوث والفاكس"[6]

(1) الفيروز آبادي، مجد الدين محمد بن يعقوب (2008). القاموس المحيط، تحقيق: أنس الشامي؛ وزكريا جابر، القاهرة: دار الحديث، ص1291.

(2) الدسوقي، محمد كمال محمود (2015). الحماية الجنائية لسرية المعلومات الإلكترونية- دراسة مقارنة، مرجع سابق، ص59.

(3) الدسوقي، محمد كمال محمود (2015): الحماية الجنائية لسرية المعلومات الإلكترونية- دراسة مقارنة، مرجع سابق، ص62.

(4) الدسوقي، محمد كمال محمود (2015): الحماية الجنائية لسرية المعلومات الإلكترونية- دراسة مقارنة، مرجع سابق، ص62.

(5) إبراهيم، خالد ممدوح (2009). الجرائم المعلوماتية، مرجع سابق، ص248.

(6) هيئة الاتصالات وتقنية المعلومات السعودية (د. ت): ضوابط الحد من الرسائل الاقتحامية، الرياض: منشورات هيئة الاتصالات، ص4.

4. التلاعب في مرحلتي إدخال البيانات وإخراجها:

يعد هذا الأسلوب أكثر حالات الاختراق حدوثاً؛ ذلك أنه يتمثل في تزويد الجهاز بالبيانات المغلوطة، أو المزورة؛ سواء أكان ذلك بحسن نية أو بسوء نية؛ وهذا ينبني على علمه بتزوير هذه البرامج أو عدم علمه به[1].

ويمثل هذا الأسلوب جريمة خطيرة لتأثيره على سلامة ووجود النظام والبيانات، فقد تتم عملية التلاعب بالبيانات بالتغيير أو الإضافة أو الحذف، بشكل دائم أو مؤقت، وهذا كله يدرج تحت جريمة الإضرار بالممتلكات.

5. التلاعب بالبرامج:

يتميز هذا الأسلوب عن سابقه بتعقيده؛ إذ يحتاج إلى خبرة برمجية وفنية؛ ولذلك فإنه يعدّ أخطر من سابقه أيضاً؛ وتستخدم في هذا الأسلوب طريقتان:

أ. تتمثل هذه الطريقة في إدخال برمجيات غير مرخص بها على الأجهزة، سواء أكانت هذه البرمجية نسخة مقلدة أو قديمة غير محدّثة، وما يتبع ذلك من آثار وأضرار لاستخدامها.

ب. تطبيق برامج إضافية غير مسموح لها بالتواجد على الأجهزة المشغلة للمواقع الرسمية للدولة، إذ تعمد كثير من الجهات الرسمية لتخصيص أجهزة بعينها ذات مواصفات خاصة، وبرامج محددة لتشغيل المواقع الإلكترونية[2].

6. الفيروسات (Viruses):

تعد الفيروسات من أخطر ما تواجهه المواقع الإلكترونية والأجهزة والأنظمة المشغلة لها من أساليب الاختراق، ويعرف الفيروس في علوم الحاسبات بأنه "برنامج حاسوبي كأيّ برنامج آخر، وله القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه، حتى يبدو كأنه يتكاثر ويتوالد ذاتياً، ويقوم بالانتشار بين برامج الحاسب الآلي المختلفة، وبين مواقع مختلفة في ذاكرة الجهاز"[3].

7. برنامج حصان طروادة (Trojan Horse Program):

لكي يتم الاختراق لا بد من وجود برامج تصمم لاختراق الأجهزة أو المواقع الإلكترونية على شبكة الإنترنت، وقد صممت العديد من البرامج لهذه الغاية، غير أن أغلبها تحتوي على نقطة ضعف تمكّن برامج المكافحة من اكتشافها والتصدي لها،

(1) ابن عفون، حمزة (2012). السلوك الإجرامي للمجرم المعلوماتي، مرجع سابق، ص61-62. والكبيجي، بهاء فهمي (2013). مدى توافق أحكام جرائم أنظمة المعلومات، مرجع سابق، ص20.

(2) ابن عفون، حمزة (2012). السلوك الإجرامي للمجرم المعلوماتي، مرجع سابق، ص65-66.

(3) حجازي، عبد الفتاح بيومي (2009). نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، مرجع سابق، ص329-330. والكبيجي، بهاء فهمي (2013). مدى توافق أحكام جرائم أنظمة المعلومات، مرجع سابق، ص41.

إلا أن هناك بعض البرامج التي كانت تحتاج إلى دقة فنية أكثر بجانب بعض الصعوبات التي تواجه اكتشافها، ومثال ذلك ما يعرف بحصان طروادة[1].

2.2.4. الأساليب الاحتيالية (Fraudulent Methods)

يعرف الاحتيال لغة بأنه "الحذق وجودة النظر، والقدرة على التصرف"[2].

ويعرف الاحتيال اصطلاحاً بأنه "ما يُتوصل به إلى مقصود بطريق خفي، وهو سلوك الطرق الخفية التي يُتوصل بها إلى حصول غرض لا يتفطن له إلا بنوع من الذكاء والفطنة"[3].

5. القصد الجنائي والعقوبات المقررة في النظام السعودي والقانون الإماراتي

1.5. تمهيد وتقسيم:

يتناول هذا الفصل من الدراسة توضيح ما يتضمنه القصد الجنائي والعقوبات المترتبة على توافره بجريمة اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي والقانون الإماراتي؛ حيث يتم تقسيمه إلى مبحثين: يتناول الأول منهما بيان القصد الجنائي، ويعكف المبحث الثاني على دراسة العقوبات المترتبة على توافره في جريمة اختراق المواقع الإلكترونية الرسمية للدولة.

2.5. القصد الجنائي

تمهيد وتقسيم:

القصد لغة: يطلق على معانٍ عدة، منها إتيان شيء وأَمُّه[4]، وقصدتُ الشيءَ: طلبتُه بعينه، وأُقصده السهم: إذا أصابه، فقُتِل مكانَه، وقيل ذلك لأنه لم يحدْ عنه[5]. وقيل: هو الاعتماد وإتيان الشيء، أو هو الاعتزام والتوجه والنهوض نحو الشيء على اعتدال[6].

(1) الجنبيهي، منير وممدوح محمد (2006). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية: دار الفكر الجامعي، ص46-47.

(2) الفيروز آبادي، مجد الدين محمد بن يعقوب (2008). القاموس المحيط، مرجع سابق، ص 425.

(3) عبادي، ماجد عمر (2014). جريمة الاحتيال عبر البريد الإلكتروني- دراسة مقارنة، بحث تخرج (غير منشور). جامعة النجاح، نابلس: كلية الحقوق، قسم القانون المقارن، ص10.

(4) ابن فارس، أبو الحسن أحمد (1420). معجم مقاييس اللغة، تحقيق: عبد السلام هارون، الرياض- بيروت: شركة الرياض للنشر والتوزيع، ودار الجيل، 95/5.

(5) الفيومي، أحمد المقري (1414). المصباح المنير في غريب شرح الكبير، تحقيق: مصطفى الرافعي، ط4، بيروت: دار الكتب العلمية، 776/2.

(6) ابن منظور، محمد بن مكرم (2010م): لسان العرب، مرجع سابق، 188/3.

ISSN: 2706-6495

القصد شرعاً: عرفه ابن عابدين بأنه "الإرادة المقترنة بالفعل"[1]. كما عرفه الغزالي بأنه "حالة لا بد منها لإيجاد الفعل، وهو صفة للقلب يكتنفها أمران: علم وعمل، العلم يقدمه؛ لأنه أصله وركنه، والعمل يتبعه؛ لأنه ثمرته وفرعه"[2]. كما يعرف بأنه "نوع من الإرادة بلغت في قوتها درجة الجزم، فالإرادة لا تكون قصداً إلا إذا كانت جازمة"[3].

التعريف الإجرائي للقصد الجنائي: ترى الباحثة تعريف القصد الجنائي لغايات هذه الدراسة بأنه إحاطة المجرم المعلوماتي بالعناصر المادية لجريمة اختراق المواقع الرسمية للدولة، واتجاه إرادته إلى تحقيق هذه العناصر المتمثلة في الفعل ونتيجته.

1.2.5. القصد الجنائي العام

مفهوم القصد الجنائي العام:

يتحقق القصد الجنائي العام بتوافر اتجاه إرادة الجاني إلى مباشرة الركن المادي للجريمة مع العلم به وبسائر ما يتطلبه النص القانوني من عناصر الجريمة[4].

وقد بيّن كلٌّ من نظام مكافحة الجرائم المعلوماتية السعودي وقانون مكافحة جرائم تقنية المعلومات الإماراتي الأفعالَ المجرّمة في مجال الجريمة المعلوماتية، وحدّدا لها عقوبات منظمة بناءً على توافر الركن المعنوي للمجرم المعلوماتي المتمثل في القصد الجنائي العام للجرائم العمدية المنصوص عليها، وستقوم الباحثة في هذا المطلب باستجلاء القصد الجنائي العام المتطلب لذلك في النظام السعودي، ومقارنته بالقانون الإماراتي، من خلال تفصيل الجرائم التي اشتملت على هذا القصد، وفيما يأتي أبرزها:

أولاً: التنصّت على المراسلات أو التقاطها أو اعتراضها:

جاء في الفقرة (1) الأولى من المادة (3) الثالثة من نظام مكافحة الجرائم المعلوماتية السعودي ما نصه "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي– دون مسوغ نظامي صحيح– أو التقاطه أو اعتراضه".

ثانياً: الدخول غير المشروع:

جاء النص على هذه الجريمة في أكثر من مادة من مواد نظام مكافحة الجرائم المعلوماتية السعودي؛ ومنها ما جاء في الفقرة (2) الثانية من المادة (3) الثالثة منه ما نصه "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال،

(1) ابن عابدين، محمد أمين (1404). حاشية رد المحتار على الدر المختار شرح تنوير الأنصار، ط3، القاهرة: مطبعة مصطفى البابي الحلبي، 169/6.

(2) الغزالي، أبو حامد محمد بن محمد (1412). إحياء علوم الدين، تحقيق: سيد إبراهيم، القاهرة: دار الكتاب الحديث، 558/2.

(3) الأشقر، عمر سليمان (1990). مقاصد المكلفين فيما يُتعبد به لرب العالمين، ط2، عمّان: دار النفائس، ص19.

(4) ربيع، حسن (د.ت). شرح قانون العقوبات المصري، القسم العام– المبادئ العامة للجريمة والعقوبة، القاهرة: (د. ن)، ص 274.

أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً".

ثالثاً: الإضرار بالشبكات الإلكترونية والبيانات:

نصت الفقرة (2) الثانية من المادة (5) الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي على أن "يعاقب... كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٢- 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".

رابعاً: إعاقة الوصول للخدمة:

نصت الفقرة (3) الثالثة من المادة (5) الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي على أن " يعاقب... كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت".

2.2.5. القصد الجنائي الخاص

مفهوم القصد الجنائي الخاص:

هو اتجاه إرادة الجاني إلى ارتكاب الركن المادي للجريمة بناءً على علمه بعناصر الجريمة الواردة بالنص، مع توافر نية الإضرار[1].

وقد أشار كلٌّ من نظام مكافحة الجرائم المعلوماتية السعودي وقانون مكافحة جرائم تقنية المعلومات الإماراتي إلى الأفعالَ المجرّمة في مجال الجريمة المعلوماتية، وستقوم الباحثة في هذا المطلب باستعراض المواد القانونية التي حدّدت هذه الجرائم التي تشتمل على القصد الجنائي الخاص في النظام السعودي، ومقارنتها بالقانون الإماراتي، مشيرة إلى علاقة هذه الجرائم بنطاق هذه الدراسة.

أولاً: الدخول للمواقع الإلكترونية للحصول على بيانات حكومية ومعلومات سرية:

نصت الفقرة (2) الثانية من المادة (7) السابعة من نظام مكافحة جرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٢- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".

كما نصت المادة (4) الرابعة من قانون مكافحة جرائم تقنية المعلومات الإماراتي على هذه الجريمة، وجاء فيها:

(1) ربيع، حسن (د.ت). شرح قانون العقوبات المصري، القسم العام– المبادئ العامة للجريمة والعقوبة، مرجع سابق، ص 275.

1- يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء أكان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية.

2- وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر".

وفي نطاق موضوع هذه الدراسة فإن القصد الجنائي الخاص للمجرم يتمثل في نية الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني مع توافر القصد الجنائي العام بداية بعلم الجاني بأن دخوله أصلاً غير مشروع[1]. وتعد هذه الجريمة امتداداً لجريمة الدخول غير المشروع بهدف أو قصد خاص، وهو الحصول على البيانات الحكومية التي تمس الأمن الداخلي أو الخارجي للدولة.

وترى الباحثة أن القانون الإماراتي قد شدد العقوبة في حال تعرضت البيانات للحذف أو الإلغاء، على الرغم من أن حذف البيانات الحكومية أو إتلافها أقل ضرراً من إفشاء هذه المعلومات التي قد يستفيد منها العدو، خاصة في أعمال التجسس على التسليح العسكري حسبما ترى الباحثة.

ثانياً: الدخول لموقع إلكتروني بغير تصريح لتغيير تصميمه أو إتلافه أو تعديله أو إلغائه:

نصت الفقرة (3) الثالثة من المادة (3) الثالثة من نظام مكافحة جرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه".

كما نصت المادة (5) الخامسة من قانون مكافحة جرائم تقنية المعلومات الإماراتي على هذه الجريمة، وجاء فيها: " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه".

ويتمثل القصد الجنائي الخاص في هذه الجريمة بأن تتجه نية الجاني إلى هذا السلوك الإجرامي بقصد تغيير تصميمه أو إتلافه أو تعديله أو شغل عنوانه، مع توافر عناصر القصد الجنائي العام أولاً لتوافر علمه وإرادته المسبقة والتي توجهت إلى الدخول غير المسموح به [2].

(1) الروقي، مروان بن مرزوق (2011). القصد الجنائي في الجرائم المعلوماتية، مرجع سابق، ص75، 93.

(2) الروقي، مروان بن مرزوق (2011). القصد الجنائي في الجرائم المعلوماتية، مرجع سابق، ص71، 89.

ويلحظ على النظام السعودي أنه قد ميّز في هذه الفقرة بين دخولين: أحدهما الدخول غير المشروع، والثاني الدخول المشروع؛ وهذا يثير تساؤلاً لدى الباحثة عن ارتباط العقوبة المقررة في هذه المادة بالقصد الجنائي الخاص من الدخول "تغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه"، أهو مرتبط بالدخول الثاني فقط دون الأول؟ أم هو مرتبط بكليهما؟ أما ارتباطه بالأول فقط فقد استبعدته الباحثة لاستحالة المعنى بدونه، وهذا يعني في نظر الباحثة أن هذه الفقرة القانونية بحاجة لإعادة صياغة لما تثيره من إشكال كما وضحتْه.

كما نصت الفقرة (1) الأولى من المادة (5) الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها".

وترى الباحثة أن النظام السعودي قد اقتصر في التجريم في هذه الفقرة على الدخول غير المشروع فقط، دون التصريح بالمدخول إليه كما في الفقرة الثالثة من المادة نفسها التي وضحت المدخول إليه بأنه الموقع الإلكتروني، وهو ما يعني أن المدخول إليه قد يكون جهازاً أو نظاماً معلوماتياً أو موقعاً إلكترونياً، والأخير هو ما يدخل ضمن نطاق هذه الدراسة بشكل مباشر؛ أما الدخول للأول (الجهاز) فقد يكون وسيلة للدخول للموقع الرسمي للدولة أو المواقع الشخصية.

ثالثاً: التحايل على العنوان البروتوكولي للإنترنت بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها.

نصت المادة (4) الرابعة من نظام مكافحة الجرائم المعلوماتية السعودي على أنه: "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة".

رابعاً: الحصول بدون تصريح على رقم سري أو شيفرة للدخول إلى وسيلة تقنية معلومات:

نصت المادة (14) الرابعة عشرة من قانون مكافحة جرائم تقنية المعلومات الإماراتي على هذه الجريمة، وجاء فيها: " 1- يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل، بدون تصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو معلومات إلكترونية".

خامساً: الابتزاز أو التهديد للقيام بفعل أو الامتناع عنه:

نصت الفقرة (2) الثانية من المادة (3) الثالثة من نظام مكافحة جرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛

كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا".

سادساً: الاعتداء على خصوصية شخص للتشهير به:

نصت الفقرة (5) الخامسة من المادة (3) الثالثة من نظام مكافحة جرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛

كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة".

سابعاً: استغلال الوظيفة لكشف معلومات سرية:

نصت الفقرة (2) الثانية من المادة (8) الثامنة من نظام مكافحة جرائم المعلوماتية السعودي على أن " لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية: ٢- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه".

ثامناً: الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها:

نصت الفقرة (1) الأولى من المادة (5) الخامسة من نظام مكافحة جرائم المعلوماتية السعودي على أن "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها".

3.5. العقوبات المترتبة على اختراق المواقع الإلكترونية الرسمية للدولة

تمهيد وتقسيم:

اتسمت مكافحة جرائم المعلوماتية في المملكة العربية السعودية باعتمادها على القواعد العامة الموضوعية والإجرائية حتى صدور نظام مكافحة جرائم تقنية المعلومات؛ فقد كانت قبل هذا النظام تعتمد على ما توفره النصوص الشرعية والأنظمة الجزائية من تجريم الأفعال المؤثمة كالسرقة وخيانة الأمانة، وبصدور هذا النظام أصبحت لهذه الأفعال عقوبات محددة.

وتعرف العقوبة في اصطلاح فقهاء القانون بأنها "جزاء تقويمي تنطوي على إيلام مقصود، تنزل بمرتكب جريمة ذي أهليه لتحمّلها، بناء على حكم قضائي يستند إلى نص قانوني يحددها، ويترتب عليها إهدار حق لمرتكب الجريمة أو مصلحة له أو ينقصهما أو يعطل استعمالهما"[(1)].

(1) الصيفي، عبد الفتاح مصطفى (1995). الأحكام العامة للنظام الجزائي، الرياض: مطبوعات جامعة الملك سعود، ص483.

ISSN: 2706-6495

1.3.5. العقوبات الأصلية

مفهوم العقوبة الأصلية:

تعرف العقوبة الأصلية في الشريعة الإسلامية بأنها "العقوبات المقررة أصلاً للجريمة، كالقصاص للقتل، والقطع للسرقة"[1]. كما تعرف بأنها "العقوبات المقررة أصلاً، حددها المشرع الحكيم، ونصّ على لزومها لمن أتى جريمة معينة، كالقصاص للقتل، والقطع للسرقة، والجلد لشارب الخمر"[2].

وفيما يأتي تفصيل العقوبات الأصلية في نظام مكافحة جرائم المعلومات السعودي وقانون مكافحة الجرائم المعلوماتية الإماراتي الخاصة بنطاق موضوع هذه الدراسة، وهي جرائم اختراق المواقع الرسمية للدولة:

أولاً: عقوبة السجن:

تعرف عقوبة السجن بأنها "عقوبة مقررة للجنايات، وتتمثل في وضع المحكوم عليه في أحد السجون العمومية، وتشغيله داخل السجن أو خارجه في الأعمال التي تعينها الحكومة للمدة المحكوم بها عليه"[3].

ووفقاً لأنظمة المملكة العربية السعودية تم تعريفها بأنها: "عقوبة تعزيرية يحكم بها شرعاً، أو توقعها الجهة المختصة ذات الولاية بالفصل في الدعاوى الجزائية"[4].

وترى الباحثة تقسيم هذه العقوبة (السجن) بحسب ما ورد في النظام السعودي والقانون الإماراتي إلى أربعة أقسام:

القسم الأول: عقوبة السجن في حدها الأعلى:

وفيما يأتي تقسيم عقوبات السجن في نظام جرائم المعلومات السعودي وقانون مكافحة جرائم المعلوماتية الإماراتي في حدها الأعلى:

المجموعة الأولى: السجن بما لا يزيد على سنة واحدة:

ضمت هذه العقوبة مجموعة من الجرائم المعلوماتية، كما ورد في المادة (3) الثالثة من نظام جرائم المعلوماتية السعودي التي جاء فيها: " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.

(1) عودة، عبد القادر (د.ت). التشريع الجنائي مقارناً بالقانون الوضعي، بيروت: دار الكتاب العربي، ص632.

(2) العاني، محمد شلال؛ والعمري، عيسى صالح (1998). فقه العقوبات في الشريعة الإسلامية، عمّان: دار المسيرة للنشر والتوزيع، ص82.

(3) الشاذلي، فتوح عبد الله (2011). علم الإجرام وعلم العقاب، مرجع سابق، ص356.

(4) وزارة الداخلية- الإدارة العامة للحقوق (د. ت). مرشد الإجراءات الجنائية، الحقوق العامة، د.ط، الرياض: مطابع الأمن العام، ص 248.

ISSN: 2706-6495

المجموعة الثانية: السجن بما لا يزيد على ثلاث سنوات:

1-الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2- الوصول- دون مسوغ نظامي صحيح- إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات".

المجموعة الثالثة: السجن بما لا يزيد على أربع سنوات:

1- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

2- 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.

3-إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت".

المجموعة الرابعة: السجن بما لا يزيد على عشر سنوات:

ضمت هذه العقوبة مجموعة من الجرائم التي تتسم بخطورة أكبر من سابقتها لارتباطها بالإرهاب والمساس بالأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني

المجموعة الخامسة: السجن بما لا يقل عن نصف الحد الأعلى للعقوبة المقررة:

1- ارتكاب الجاني الجريمة من خلال عصابة منظمة.

2- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

3- التغرير بالقصّر ومن في حكمهم، واستغلالهم.

4- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة".

وهذا يعني أن التشديد تمثل في رفع الحد الأدنى للعقوبة- وهو غير محدد في الجرائم المعلوماتية- إلى نصف الحد الأعلى المقرر لها في حال توافر الظرف المشدد.

المجموعة السادسة: السجن بما لا يتجاوز نصف الحد الأعلى من العقوبة:

ارتبطت هذه العقوبة بفعل التحريض على الجريمة أو المساعدة فيها أو الاتفاق على تنفيذها في حال عدم تنفيذها، فجاء في المادة (9) التاسعة من النظام السعودي ما نصه: "يعاقب كل من حرَّض غيره، أو ساعده،

أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية".

القسم الثاني: عقوبة السجن في حدها الأدنى:

1. الفقرة (2) الثانية من المادة (4) الرابعة: "وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر"

2. الفقرة (1) الأولى من المادة (10) العاشرة: "يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامجاً معلوماتياً إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات".

القسم الثالث: عقوبة السجن (دون حد أعلى ولا أدنى):

ويلحظ أيضاً على عقوبات هذا القسم أنها خاصة بالقانون الإماراتي دون النظام السعودي الذي اكتفى بتحديد هذه العقوبة في حدها الأعلى كما مرّ في القسم الأول من هذه العقوبة السالبة للحرية.

القسم الرابع: عقوبة السجن المؤقت:

لم ترد هذه العقوبة في نظام مكافحة جرائم المعلومات السعودي، بل جاء النص عليها في قانون مكافحة جرائم المعلوماتية الإماراتي، وفيما يأتي تفصيل الجرائم التي جاءت هذه العقوبة جزاء عليها:

1. الفقرة (1) الأولى من المادة (4) الرابعة: "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء أكان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية".

2. المادة (7) السابعة: يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدّل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات، وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية.

ثانياً: عقوبة الحبس:

تعرف عقوبة الحبس بأنها "عقوبة مقررة للجنح، تتمثل في وضع المحكوم عليه في أحد السجون المركزية أو العمومية للمدة المحكوم بها عليه"[1].

كما عرف قانون العقوبات الإماراتي عقوبة الحبس بموجب نص المادة (69) التاسعة والستين؛ حيث جاء فيها أن "الحبس هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانوناً لهذا الغرض،

وذلك للمدة المحكوم بها. ولا يجوز أن يقل الحد الأدنى للحبس عن شهر، ولا أن يزيد حده الأقصى على ثلاث ولا أن يزيد حده الأقصى على ثلاث سنوات، ما لم ينص القانون على خلاف ذلك".

ويلاحظ على هذه العقوبة أنها خاصة بقانون مكافحة جرائم المعلومات الإماراتي دون نظام مكافحة جرائم المعلومات السعودي الذي لم ينص على هذه العقوبة، ما يعني أنه لم يفرق في العقوبة باعتبار الجريمة جناية أو جنحة.

ثالثاً: عقوبة الغرامة المالية:

تعرف عقوبة الغرامة المالية بأنها "شكل من أشكال العقوبات التي تصيب الذمة المالية للمحكوم عليه، عن طريق الزيادة في عناصرها السلبية"[2].

كما عرف قانون العقوبات الإماراتي الغرامة في المادة (71) الحادية والسبعين بأنها "عبارة عن إلزام المحكوم عليه بأن يدفع إلى خزينة الدولة مبلغاً من المال يحدده القاضي في حكمه كعقوبة على ارتكاب الجريمة".

وترى الباحثة تقسيم هذه العقوبة بحسب ما ورد في النظام السعودي والقانون الإماراتي إلى ثلاثة أقسام:

القسم الأول: عقوبة الغرامة المالية في حدها الأعلى:

وفيما يأتي تقسيم عقوبات الغرامة المالية في نظام جرائم المعلومات السعودي وقانون مكافحة جرائم المعلوماتية الإماراتي في حدها الأعلى:

- الغرامة بما لا يزيد على مئات الآلاف
- الغرامة بما لا تزيد على مليون أو مليوني ريال/ درهم
- الغرامة بما لا يزيد على ثلاثة ملايين ريال/ درهم
- الغرامة بما لا يزيد على خمسة ملايين ريال/ درهم
- الغرامة بما لا يقل عن نصف الحد الأعلى للعقوبة المقررة

(1) الشاذلي، فتوح عبد الله (2011). علم الإجرام وعلم العقاب، مرجع سابق، ص356.

(2) الشاذلي، فتوح عبد الله (2011). علم الإجرام وعلم العقاب، مرجع سابق، ص334.

- الغرامة بما لا يتجاوز نصف الحد الأعلى من العقوبة

القسم الثاني: عقوبة الغرامة في حدها الأعلى والأدنى

مما يحسب للقانون الإماراتي في تنظيم هذه العقوبة أنه قد حدّها بحد أعلى لا تتجاوزه أو تزيد عليه، وبحد أدنى لا تقل عنه، ويلحظ على هذه العقوبة أنها خاصة بالقانون الإماراتي فقط؛ ذلك أن هذه العقوبة لم ترد في نظام مكافحة جرائم المعلومات السعودي الذي اكتفى ببيان العقوبة في حدها الأعلى كما سبق في القسم الأول.

القسم الثالث: عقوبة الغرامة (دون حد أعلى ولا أدنى):

ويلحظ أيضاً على عقوبات هذا القسم أنها خاصة بالقانون الإماراتي دون النظام السعودي الذي اكتفى بتحديد هذه العقوبة في حدها الأعلى كما مرّ في القسم الأول من هذه العقوبة.

2.3.5. العقوبات التكميلية والتبعية

مفهوم العقوبة التكميلية:

تعرف العقوبة التكميلية في اصطلاح فقهاء القانون بأنها "العقوبة التي لا تتقرر إلا مع العقوبة الأصلية، فلا يمكن تطبيقها إلا مع العقوبة الأصلية، وبنص القانون، بل لا بد لتطبيقها من ذكر صريح لها في حكم القاضي، وتنقسم العقوبة التكميلية إلى قسمين: الأول: وجوبية: يتعين أن ينطق بها القاضي، وإلا كان حكمه باطلاً قابلاً للطعن فيه. والثاني: جوازية: يكون النطق بها متوقفاً على تقدير القاضي؛ بحيث إذا أغفل ذكرها كان معنى ذلك عدم استحقاقها، ولا يعتبر حكمه باطلاً[1].

وفيما يأتي أهم العقوبات التكميلية كما وردت في نظام مكافحة جرائم المعلومات السعودي، وقانون مكافحة الجرائم المعلوماتية الإماراتي:

- عقوبة الغرامة.

- عقوبة المصادرة.

- عقوبة إغلاق المحل أو الموقع الإلكتروني.

- عقوبة محو البيانات.

- العزل من الوظيفة.

- وضع المحكوم عليه تحت المراقبة أو الإشراف، أو حرمانه من استخدام شبكة معلوماتية أو نظام المعلومات.

(1) رستم، هشام فريد (2006). شرح قانون العقوبات المصري-القسم العام، القاهرة: دار النهضة العربية، ص416.

تعريف العقوبات التبعية:

تعرف العقوبات التبعية في اصطلاح فقهاء القانون بأنها "العقوبة التي لا تتقرر إلا مع العقوبة الأصلية، فلا يمكن تطبيقها حيث لا توجد عقوبة أصلية، وتتميز بأنها تُستحق مع العقوبة الأصلية بنص القانون، ودون الحاجة إلى ذكرها في حكم القاضي، وتعدّ العقوبة تبعية إذا كان القانون يقضي بها كأثر حتمي للحكم بالعقوبة الأصلية"[1].

وفيما يأتي أهم العقوبات التبعية كما وردت في قانون مكافحة جرائم المعلوماتية الإماراتي؛ ذلك أن نظام مكافحة جرائم المعلومات السعودي لم ينص صراحة على أي من العقوبات التبعية، ولكنه أشار لها في المادة (12) الثانية عشرة بقوله: "لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة":

أولاً: الإبعاد:

يعد إبعاد الأجنبي أحد التدابير الاحترازية التي تهدف لكفّ خطورته عن الدولة، وهو يمثل أحد عناصر سيادة الدولة على إقليمها، حتى لا يرتكب جرائم جديدة أو يؤثر في أبناء الإقليم، وهو قاصر على الأجانب دون المواطنين، الذين لا تجيز الدساتير إبعادهم عن بلدانهم[2].

ثانياً: الفصل/ العزل من الوظيفة:

لم ينص نظام مكافحة جرائم المعلومات السعودي على هذه العقوبة صراحة، ولكنه أشار إليها في نظام تأديب الموظفين الذي نص في المادة (44) الرابعة والأربعين منه على أن "الموظف الذي صدر حكم بحبسه يعرض أمره على هيئة الرقابة والتحقيق للنظر في مسؤوليته التأديبية".

6. نتائج الدراسة وتوصياتها ومقترحاتها

1.6. نتائج الدراسة:

1. يعرف المجرم المعلوماتي بأنه كل شخص يقوم بأي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.
2. يمكن تقسيم أصناف المجرمين المعلوماتيين إلى تقسيمات متعددة، منها تقسيمهم إلى: مجرمين مبتدئين في الجريمة المعلوماتية بناء على معرفة ضئيلة، لا ترقى إلى الخبرة، وذوي الكفاءة والخبرة الفنية والتقنية في الحاسوب واستخداماته ويستطيعون وبمهارة إخفاء أي آثار جرمية لفعلهم.

(1) حسني، محمود نجيب (1982). شرح قانون العقوبات المصري-القسم العام، القاهرة: دار النهضة العربية، ص492.

(2) الشاذلي، فتوح عبد الله (2011). علم الإجرام وعلم العقاب، مرجع سابق، ص391.

3. يعتبر متعهد الخدمة مصدر التدفق المعلوماتي، وهو بمثابة ناشر للموقع؛ لأنه المسؤول الأول عن تبادل المعلومات عبر الشبكة، وهو المسؤول عن تدقيق ومراقبة كل ما يبث عبر الشبكة من معلومات، كونه المخوّل الوحيد بهذه السلطة.
4. لم يشر المشرع السعودي ولا الإماراتي لمسؤولية مقدم الخدمة عن ارتكاب الجريمة المعلوماتية، بعكس بعض التشريعات الدولية والعربية التي أشارت لهذا الدور؛ فقد أوجب المشرع الأوروبي مسؤوليته عما ينشره
5. تعرف المواقع الإلكترونية الرسمية للدولة بأنها أماكن على الشبكة المعلوماتية مملوكة لجهات حكومية من خلال عنوان محدد خاص بكل جهة يميزها عن غيرها، ويتيح لها نقل البيانات أو تداولها عبر هذه الشبكة، وتتولى الإشراف عليها وتحديث بياناتها أو تعديلها بمقابل مادي تدفعه للجهة المستضيفة للموقع.
6. تعاني كثير من المواقع الرسمية للدول من نقص الخبرة في التعامل معها، مما يتسبب في كثرة الأعطال والبطء، مما يجعلها قاصرة عن الارتقاء لمستوى الكفاءة المنشود في تقديم الخدمات الإلكترونية. كما تعاني من ضعف أنظمة الحماية.
7. يعني اختراق المواقع الإلكترونية الرسمية للدولة: الدخول غير المشروع لمواقع الحكومة الإلكترونية، أو التعدي على البيانات الشخصية في نطاق الحكومة الإلكترونية، أو انتهاك سرية وخصوصية البيانات
8. تتنوع الأساليب الاقتحامية للمواقع الرسمية للدول ما بين: الاختراق البسيط، والتجربة العشوائية لكلمة السر، وإلغاء الخدمة أو تعطيلها، والتلاعب في مرحلتي إدخال البيانات وإخراجها، والتلاعب بالبرامج، والفيروسات، وبرنامج حصان طروادة.
9. تتنوع الأساليب الاحتيالية لاختراق المواقع الرسمية للدول بين: الاحتيال باستغلال الثغرات الأمنية، والاحتيال بالالتقاط السلكي، والاحتيال باستراق الأمواج، والاحتيال بانتحال صلاحيات شخص مفوض، والاحتيال على بروتوكولات الإنترنت، والاحتيال بمخلفات التقنية، والاحتيال بالتقاط كلمات السر، والاحتيال باستغلال المزايا الإضافية.
10. لم يميز المشرع السعودي بين كون الجريمة المعلوماتية جنحة أو جناية، في حين ميز القانون الإماراتي الجنحة عن الجناية، فجعل عقوبة الحبس للجنحة، وجعل عقوبة السجن والسجن المؤقت للجناية.
11. تعرف العقوبات التكميلية في نطاق هذه الدراسة بأنها العقوبات الموقعة على المجرم المعلوماتي في اختراق المواقع الإلكترونية الرسمية للدولة، ولا تتقرر إلا مع العقوبة الأصلية، ولا يمكن تطبيقها إلا مع العقوبة الأصلية

2.6. توصيات الدراسة:

بناء على النتائج السابقة التي توصلت لها الباحثة، فإنها توصي بما يأتي:

1. الإشارة إلى مسؤولية مقدم الخدمة في النظام السعودي والقانون الإماراتي؛ ذلك أن أياً منهما لم ينص على مسؤوليته، أسوة بالأنظمة الدولية التي تشير إلى مسؤوليته، كالقانون المصري الذي أعطاه فرصة سبعة أيام من اكتشافه المخالفة للتوقف عن بثّ المعلومة.
2. ضرورة تفعيل الأنظمة الدولية المتعلقة بوجوب المسؤولية الجنائية عن اختراق المواقع الرسمية للدول.

3. ضرورة تطوير خبرات القائمين على تشغيل المواقع الإلكترونية للدول بما يتماشى مع مهارات القائمين على المواقع الإلكترونية للجهات الخاصة كالبنوك والمؤسسات التجارية التي تهتم بتطوير موظفيها والمتعاملين معها، بما يحقق لها مكاسب ربحية.
4. ضرورة تطوير المواقع الرسمية للدولة وأنظمة حمايتها؛ لتقليل تعرضها للاختراق عند محاولات لا تتصف بالمهارة الكافية لاختراق المواقع ذات التأمين الجيد.
5. ضرورة استحداث التصنيفات العلمية الدورية الدقيقة لهذه المواقع الرسمية بحسب معايير الجودة، والاستجابة، لتحقيق الكفاءة المطلوبة.
6. ضرورة إصدار لائحة تنظيمية تفسر مواد نظام مكافحة الجرائم المعلوماتية السعودي، وأخرى لتفسير مواد قانون مكافحة الجريمة المعلوماتية الإماراتي.
7. توعية مستهلك الخدمة في الدول العربية بحقوقه والتزاماته، ومدى مسؤوليته الجنائية عن الجريمة المعلوماتية بشكل عام، واختراق المواقع الرسمية للدولة بشكل خاص.
8. ضرورة تبادل الخبرات وتوحيد الجهود بين الدول العربية والإقليمية والأجنبية، وتكوين قواعد بيانات في مجال جرائم المعلومات بشكل عام، وجرائم اختراق المواقع الرسمية بشكل خاص، والأساليب الإجرامية، وآثار الجريمة.

7. قائمة المراجع

القرآن الكريم.

إبراهيم، خالد ممدوح. (2009). الجرائم المعلوماتية، الإسكندرية: دار الفكر الجامعي.

إبراهيم، مصطفى وآخرون. (1380). المعجم الوسيط، القاهرة: مطبعة مصر.

الأستاذ، سوزان عدنان. (2013). انتهاك حرمة الحياة الخاصة عبر الانترنت-دراسة مقارنة، (بحث منشور). دمشق: مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلد 29، العدد الثالث.

الأشقر، عمر سليمان. (1990). مقاصد المكلفين فيما يُتعبد به لرب العالمين، ط2، عمّان: دار النفائس.

الأصفهاني، الحسين بن محمد. (د.ت) المفردات في غريب القرآن، القاهرة: مكتبة نزار مصطفى الباز.

إمام، محمد كمال الدين. (1411هـ). المسؤولية الجنائية-أساسها وتطورها، ط2، بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع.

البخاري، محمد بن إسماعيل. (1428هـ). صحيح البخاري، (د. ط)، بيروت: دار الكتب العلمية.

بلعيد، جميلة. (2012). التحكيم التجاري الدولي بين النظام الداخلي والنظام العام الدولي، القاهرة: مطبعة مصر المعاصرة.

بهنسي، محمد فتحي. (1409هـ). المسؤولية الجنائية، ط9، القاهرة: دار الشروق.

بيومي، عبد الفتاح. (2009). الأحداث والإنترنت: أثر الإنترنت في انحراف الأحداث، (د. ط)، الإسكندرية: دار الفكر العربي.

جعفر، علي عبود. (2013م). جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، صيدا: منشورات زين الحقوقية.

الجنبيهي، منير وممدوح محمد. (2006). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية: دار الفكر الجامعي.

الجندي، حسني. (1993). ضمانات حرمة الحياة الخاصة في الإسلام، ط1، القاهرة: دار النهضة العربية.

أبو حبيب، سعدي. (1988). القاموس الفقهي لغة واصطلاحاً، دمشق: دار الفكر.

حجازي، عبد الفتاح بيومي. (2004). التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول: نظام التجارة الإلكترونية وحمايتها مدنياً، الإسكندرية: دار الفكر الجامعي.

حجازي، عبد الفتاح بيومي. (2009). نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الزقازيق: بهجات للطباعة والتجليد.

ابن حجر، أحمد بن علي. (1379م). فتح الباري شرح صحيح البخاري، د.ط، بيروت: دار المعرفة.

الحمامي، عمر أبو الفتوح عبد العظيم. (2010م). الحماية الجنائية للمعلومات المسجلة الكترونياً، القاهرة: دار النهضة العربية.

سالم، محمد علي وهجيج، حسون عبيد. (2007). الجريمة المعلوماتية، (بحث منشور). مجلة جامعة بابل، بغداد: العلوم الإنسانية، المجلد 14، العدد الثاني.

سرور، أحمد فتحي. (2010). الوسيط في قانون العقوبات-القسم العام، القاهرة: مطابع الأهرام التجارية.

سرور، أحمد فتحي. (1972). أصول السياسة الجنائية، د. ط، القاهرة: (د. ن).

سليمان، عبد الحميد عثمان محمد. (2006). مسؤولية مزود الخدمة المعلوماتية، القاهرة: منشورات المنظمة العربية للتنمية الإدارية.

أبو سليمان، عبد الوهاب إبراهيم. (2006م). كتابة البحث العلمي (صياغة جديدة) ومصادر الدراسات القرآنية والسنة النبوية والعقيدة الإسلامية، ط3، جدة: دار الشروق.

السنباطي، إيهاب ماهر. (2007). الجرائم الإلكترونية- الجرائم السيبيرية، المغرب: ورقة عمل مقدمة لأعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 نيسان.

الشاذلي، فتوح عبد الله. (2011). علم الإجرام وعلم العقاب، الإسكندرية، دار المطبوعات الجامعية.

الشكري، عادل يوسف عبد النبي. (2008م). الجريمة المعلوماتية وأزمة الشرعية الجزائية، (بحث منشور). الكوفة: مجلة مركز دراسات الكوفة، العدد السابع.

الشمري، خالد طعمة صعفك. (2005). القانون الجنائي الدولي، ط2، الكويت: (د.ن).

الصيفي، عبد الفتاح مصطفى. (1995). الأحكام العامة للنظام الجزائي، الرياض: مطبوعات جامعة الملك سعود.

صغير، يوسف. (2013). الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير (غير منشورة). جامعة مولود معمري، الجزائر: كلية الحقوق، قسم القانون الدولي للأعمال.

الطويل، عبد الله بن محمد. (2012). المسؤولية الجنائية عن تشغيل العمالة غير النظامية، (د. ط)، الرياض: جامعة نايف العربية للعلوم الأمنية.

ابن عابدين، محمد أمين. (1404). حاشية رد المحتار على الدر المختار شرح تنوير الأنصار، ط3، القاهرة: مطبعة مصطفى البابي الحلبي.

العاني، محمد شلال؛ والعمري، عيسى صالح. (1998). فقه العقوبات في الشريعة الإسلامية، عمّان: دار المسيرة للنشر والتوزيع.

عبابنة، محمود أحمد. (2009). جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، عمّان: دار الثقافة للنشر والتوزيع.

عبادي، ماجد عمر. (2014). جريمة الاحتيال عبر البريد الإلكتروني-دراسة مقارنة، بحث تخرج (غير منشور). جامعة النجاح، نابلس: كلية الحقوق، قسم القانون المقارن.

عبد الحفيظ، أيمن. (2011م). الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، ط2، القاهرة: دار ضاحي للنشر.

عبد الحفيظ، أيمن. (2006). مكافحة الجرائم المستحدثة، دبي: مؤسسة البيان للصحافة والطباعة.

عبد الصادق، محمد سامي. (2008). التحديات التشريعية في عصر تكنولوجيا المعلومات والاتصالات، القاهرة: ورقة عمل مقدمة لمؤتمر القاهرة للتحديات التشريعية في عصر التكنولوجيا، في الفترة من 14-15، أبريل.

العبيدي، خالد بن عبد الله بن معيض. (1430). الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية-دراسة تحليلية مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.

العجمي، عبد الله دغش. (2014). المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة، رسالة ماجستير (غير منشورة). جامعة الشرق الأوسط، عمان: كلية الدراسات العليا، قسم القانون العام.

العربي، يوسف. (2013). الإمارات تحبط محاولات جديدة لاختراق مواقع إلكترونية حكومية، دبي: جريدة الاتحاد الإماراتية، الاثنين، 24يوليو.

عطوي، مليكة. (2012م). الجريمة المعلوماتية، الجزائر: (بحث منشور). الجزائر: حوليات جامعة الجزائر، العدد 21، جوان (يناير).

العيني، بدر الدين محمود أحمد. (2006). عمدة القاري، شرح صحيح البخاري، ط2، بيروت: دار إحياء التراث.

الغافري، حسين بن سعيد. (2009م). السياسة الجنائية في مواجهة جرائم الانترنت-دراسة مقارنة، القاهرة: دار النهضة العربية.

الغامدي، محمد. (1434). محاولة اختراق أرامكو تهدف للإضرار بالاقتصاد الوطني ومنع تدفق الزيت الى الأسواق المحلية والعالمية، الرياض: جريدة الرياض، الاثنين 26 محرم، العدد 16240.

الغزالي، أبو حامد محمد بن محمد. (1412). إحياء علوم الدين، تحقيق: سيد إبراهيم، القاهرة: دار الكتاب الحديث.

ابن فارس، أبو الحسن أحمد. (1420). معجم مقاييس اللغة، تحقيق: عبد السلام هارون، الرياض-بيروت: شركة الرياض للنشر والتوزيع، ودار الجيل.

الفايز، عبد العزيز بن عبد الكريم. (2014). العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي-دراسة مقارنة، رسالة ماجستير (غير منشورة). جامعة نايف العربية للعلوم الأمنية، الرياض: كلية الدراسات العليا، قسم العدالة الجنائية.

فرغلي، عبد الناصر محمد محمود؛ والمسماري، محمد عبيد سيف. (2007). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، الرياض: جامعة نايف العربية للعلوم الأمنية.

فنور، حاسين. (2013). المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، رسالة ماجستير (غير منشورة). جامعة الجزائر، الجزائر: كلية الحقوق، قسم القانون الدولي.

الفيروز آبادي، مجد الدين محمد. (د.ت). القاموس المحيط، د. ط، بيروت: مؤسسة الرسالة.

الفيومي، أحمد بن محمد. (1987م). المصباح المنير، د. ط، بيروت: مكتبة لبنان.

الفيومي، أحمد المقري. (1414). المصباح المنير في غريب شرح الكبير، تحقيق: مصطفى الرافعي، ط4، بيروت: دار الكتب العلمية.

قارة، آمال. (2002). الجريمة المعلوماتية، رسالة ماجستير (غير منشورة). جامعة الجزائر، الجزائر: كلية الحقوق، قسم القانون الجنائي والعلوم الجنائية.

المواقع الإلكترونية:

http://www.alarabiya.net/ar/saudi-today/2013/05/17

http://www.alittihad.ae/details.php?id=69638&y=22/7/2013

https://www.moi.gov.sa

https://www.moi.gov.ae/ar/eservices

http://www.cpmo.com.sa

http://www.government.ae

http://www.nauss.edu.sa

http://www.998.gov.sa

http://www.dcd.gov.ae

http://www.bbc.com/arabic/business/2012/12/121209_aramco_hacking.shtml

http://www.alittihad.ae/details.php?id=69638&y=2013

www.policemc.gov.bh

الأنظمة والقوانين:

قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، الأمم المتحدة (2000). نيويورك: منشورات الأمم المتحدة.

القانون الاتحادي لدولة الإمارات رقم (3) لسنة 2003 بشأن تنظيم قطاع الاتصالات.

القانون النموذجي العربي الموحد لسنة 2000م، اعتمده مجلس وزراء العدل العرب كقانون نموذجي استرشادي في دورته السادسة عشرة بالقرار رقم 365- د 6- 2000/11/16م.

القانون الاتحادي رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية.

قانون المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة رقم (3) لعام 2002م.

القانون الاتحادي رقم (3) لسنة 2003م لتنظيم قطاع الاتصالات الإماراتية.

نظام الاتصالات السعودي الصادر بقرار مجلس الوزراء رقم (74) وتاريخ 1422/3/5هـ، المقر بموجب المرسوم الملكي رقم (م/12) وتاريخ 1422/3/12هـ.

نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (79)