كلية الشريعة والقانون بدمنهور

جامعة الأزهر

مجلة البحوث الفقهية والقانونية

مجلة علمية محكّمة
تصدرها كلية الشريعة والقانون بدمنهور

بحث مستل من

العدد الثالث والأربعين - "إصدار أكتوبر ٢٠٢٣م - ١٤٤٥هـ"

جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقاً للنظام السعودي (دراسة تحليلية تطبيقية)

Crimes Of Intentional Assault On The Integrity Of Electronic Information Systems According To The Saudi System (Applied Analytical Study)

الدكتـــور

عبدالله بن محمد الجربوع

عضو هيئة التدريس بكلية الأنظمة والدراسات القضائية
الجامعة الإسلامية بالمدينة المنورة

مجلـة البحـوث الفقهيـة والقانونيـة
مجلة علمية عالمية متخصصة ومُحكمة
من السادة أعضاء اللجنة العلمية الدائمة والقارئة
في كافة التخصصات والأقسام العلمية بجامعة الأزهر

المجلة مدرجة في الكشاف العربي للإستشهادات المرجعية ARABIC CITATION INDEX
على Clarivate Web of Science
المجلة مكشّفة في قاعدة معلومات العلوم الإسلامية والقانونية من ضمن قواعد بيانات دار المنظومة
المجلة حاصلة على تقييم ٧ من ٧ من المجلس الأعلى للجامعات
المجلة حاصلة على تصنيف Q3 في تقييم معامل "ارسيف Arcif" العالمية
المجلة حاصلة على تقييم ٨ من المكتبة الرقمية لجامعة الأزهر

رقم الإيداع
٦٣٥٩

الترقيم الدولي
(ISSN-P): (1110-3779) - (ISSN-O): (2636-2805)

للتواصل مع المجلة
+201221067852
journal.sha.law.dam@azhar.edu.eg

موقع المجلة على بنك المعرفة المصري
https://jlr.journals.ekb.eg

جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقاً للنظام السعودي
(دراسة تحليلية تطبيقية)

Crimes Of Intentional Assault On The Integrity Of Electronic Information Systems According To The Saudi System
(Applied Analytical Study)

الدكتـــــور

عبدالله بن محمد الجربوع

عضو هيئة التدريس بكلية الأنظمة والدراسات القضائية

الجامعة الإسلامية بالمدينة المنورة

جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقاً للنظام السعودي (دراسة تحليلية تطبيقية)

عبدالله بن محمد الجربوع
كلية الأنظمة والدراسات القضائية، الجامعة الإسلامية، المدينة المنورة، المملكة العربية السعودية.
البريد الإلكتروني: amsjsmu@gmail.com

ملخص البحث:

تناولت الدراسة تعريف الاعتداء على نظم المعلومات الإلكترونية وسرقتها، وتدمير المواقع وتشويهها، كما تعرضت الدراسة لحجب الخدمة ومحاكاة المواقع، وانتحال شخصية تلك المواقع، وإحداث خلل في سلامة النظم والمعلومات، وجرائم تزوير المستندات الإلكترونية، والاعتداء على التوقيع الإلكتروني، وأتبعت الدراسة المنهجين التحليلي والتطبيقي، ثم الاعتماد على مصادر جمع المعلومات الأولية والثانوية المتمثلة في الكتب والمراجع، وتمت المقارنة بين النظام السعودي وقانون العقوبات الفرنسي، وقانون التجارة الإلكتروني التونسي، في بعض المواضيع ذات العلاقة بنظم المعلومات وتدميرها، والدخول على منظومة التوقيع الإلكتروني لشخص آخر دون تفويض أو نسخها أو الاستيلاء عليها، وكانت أهم النتائج التي توصل إليها الباحث: أن المعلومات تصلح لأن تكون محلاً للحقوق الشخصية والمالية، لذلك يجب أن تحمى بالنظام، وأن المساس بالمعلومات الشخصية للأفراد قد يكون مصدره أشخاص مخربون، يقومون بالاعتداء على البيانات الشخصية للآخرين وانتهاكها بشتى الصور، وأن تزوير المستندات الإلكترونية هو تغيير الحقيقة في المستند الإلكتروني، بإحدى طرق التغيير، كالتوقيع والحذف، والإضافة،

والتعديل أو التغيير، كما أن النظام السعودي يعتبر أن تزوير المستندات المعالجة آلياً يدخل في مفهوم التزوير، وطبق بحق مرتكبيها العقوبات التي نص عليها النظام. ومن أهم التوصيات أن يتم تطوير الأنظمة بالتوسع في حماية المساس بالمعلومات الشخصية للأفراد من مخاطر الإنترنت، وأهمية أن يتم إصدار تشريع خاص بحماية المستندات الإلكترونية، وتشديد عقوبة تزويرها، والتوصية بتطوير مقررات كليات الأنظمة في الجامعات، بتدريس الأنظمة ذات العلاقة بالجرائم؛ لأهميتها ولمعرفة المستجدات والتطورات التي تحدث فيها.

الكلمات المفتاحية: اعتداء، نظم معلومات، نظام سعودي.

Crimes Of Intentional Assault On The Integrity Of Electronic Information Systems According To The Saudi System (Applied Analytical Study)

Abdullah bin Muhammad Al-Jarbou
College of Regulations and Judicial Studies, Islamic University, Medina, Kingdom of Saudi Arabia.
E-mail: amsjsmu@gmail.com

Abstract:

The study has addressed attacks on information systems, stealing it and destroying websites and distorting it, as well as blocking services, mimicking websites, website identity theft and causing deficiencies in systems and information, digital documents fraud and hacking log in accounts. The study followed the descriptive and analytic methodologies then referred to primary and secondary references like books and references. A comparison was made between the Saudi system and French penalty law and Tunisian e-commerce law in some subjects pertaining to information system destruction and digital identity theft and logging into other individual's accounts without permission, copying accounts, and or seizing it. The most important findings were that information can be regarded as personal and financial properties which is why it has to be protected by the system. Likewise, information can fall in the hands of malicious individuals who seek to take information to commit fraud by the various ways available. Forging electronic documents is changing the documents through adding signatures, omitting information or adding it or changing it. The Saudi system regards electronic forgery as fraud and individuals have been prosecuted according to the Saudi law. The study recommends developing systems in the area of personal information protection from the dangers of internet. It also highlights the importance of developing special

legislation to protect personal documents and introduce harsher penalties for violators. It is also recommended to develop curriculums for information Technology faculties that teaches systems that has to do with digital crimes in order be aware of any developments in the field.

Keywords: Assault, Information System, Saudi Law.

المقدمة:

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين.

أما بعد:

شهدت المجتمعات المعاصرة تطورات كبيرة في استخدام تكنولوجيا المعلومات، في جميع نواحي الحياة التجارية والاجتماعية وغيرها، ونتج عن ذلك ارتكاب البعض لجرائم ومخالفات سوء استخدام تلك التكنولوجيا، وبالتالي يهتم موضوع البحث بمعرفة جرائم الاعتداء المتعمد على نظم المعلومات الإلكترونية، وفقاً للتشريعات الجنائية، مقارنة بالنظام السعودي، في محاولة لبيان أحكام هذه التقنيات الجديدة، وبيان حكم الاعتداء عليها باستخدام الحاسب وشبكة الإنترنت، وغيرها من الموضوعات مما سيرد في البحث.

أهمية وأسباب اختيار البحث:

تبرز أهمية موضوع البحث وأسباب اختياره في عدة نقاط منها الآتي: ـ

أهمية البحث:

١ـ يكتسب هذا الموضوع أهمية كبيرة؛ بسبب انتشار الجرائم المعلوماتية والإلكترونية في الآونة الأخيرة، الأمر الذي أدى إلى ظهور تشريعات جديدة خاصة بمجال المعلوماتية في كثير من البلدان، مثل: تشريعات مكافحة جرائم المعلومات، وتشريعات التعاملات الإلكترونية، مما يتطلب معه دراستها وتمحيصها، لبيان مدى كفايتها لمحاربة الجرائم المعلوماتية.

٢ـ إيضاح جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي وما ينتج عنها.

٣- خطورة جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي على الفرد والمجتمع والامن العام.

٤- بيان المستجدات لجرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي.

٥- إيضاح الجهود المبذولة لمكافحة جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي **وذلك** من خلال عرض الأنظمة والتطبيقات.

٦- الاطلاع على حكم جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي من الناحية النظامية.

٧- حداثة جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي وتأثيرها بشكل كبير على **المجتمع**، الامر الذي يمثل تهديدا للأمن العام للمجتمع.

٨- ظهرت في مجتمعاتنا العديد من الانتهاكات التي تمس الناس في دينهم وأنفسهم وأعراضهم وأموالهم دون العلم بالحكم النظامي لها.

٩- دخول الاجهزة الالكترونية (سواء كانت تعمل عن طريق الشبكة العنكبوتية أم لا) أغلب جوانب الحياة اليومية والعملية، فاقتضت الضرورة بيان المسائل التي توضح استخدام الالكترونيات لأجل جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي.

١٠- عدم وجود دراسة قانونية متخصصة في هذا الموضوع لذا فإن المجال واسع لمثل هذه الدراسة لا سيما على كثرة التطورات اليومية في هذا الجانب.

١١ـ رغبة الباحث في دراسة هذا الموضوع من خلال **شرح جرائم** الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية؛ وفقاً للنظام السعودي.

هدف البحث:

يهدف البحث إلى دراسة جرائم الاعتداء المتعمد على نظم المعلومات الإلكترونية، ومعرفة القواعد القانونية التي تحكم مختلف جوانب الحماية الجنائية للمعلومات.

يرمي هذا المشروع البحثي لتحقيق مجموعة من الأهداف **منها**: ـ

١ – سيسهم في دراسة جرائم الاعتداء المتعمد على نظم المعلومات الإلكترونية من خلال دراسة وتحليل الجوانب النظامية، وذلك بالرجوع للأنظمة والكتب القانونية وغيرها من المصادر، وهذا ما يخص الجانب النظري.

٢ – كذلك من خلال البحث عن دراسة جرائم الاعتداء المتعمد على نظم المعلومات الإلكترونية في المملكة العربية **السعودية**، سوف نتوصل بإذن الله لنتائج تساعد في الحد من انتشار هذه الجريمة.

٣– أما الجانب التطبيقي فسأتناول تجربة المملكة العربية السعودية في مكافحة هذه الجريمة والاستفادة منها في اعداد توصيات يستفيد منها كل المهتمين بهذا المجال.

مشكلة البحث:

يثير هذا البحث العديد من المشكلات، على أن أهمها: مدى ملاءمة الأنظمة والقوانين الحديثة لحماية المعلومات، واستخدام التكنلوجيا من الاعتداء المتعمد على نظم المعلومات، وسرقة المعلومات نفسها، واتلافها، أو تدميرها، أو إعادة نشرها، ومحاولة التوصل إلى أجوبة قانونية، لجملة من التساؤلات الرئيسة مثل: مفهوم الاعتداء المتعمد على نظم المعلومات.

منهج البحث:

تم اتباع المنهج التحليلي التطبيقي، حيث تم تحليل ما ورد في أنظمة المملكة ذات العلاقة بالجرائم المعلوماتية والتعاملات الإلكترونية، وبيان تطبيقاتها القضائية.

تقسيم البحث:

مبحث تمهيدي: الأحكام العامة لجرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقا للنظام السعودي.

المطلب الأول: مفهوم جرائم الاعتداء المتعمد

أولاً: الجريمة

ثانيا: الاعتداء

ثالثا: المتعمد

المطلب الثاني: مفهوم نظم المعلومات الإلكترونية

أولاً: نظم

ثانياً: المعلومات

ثالثاً: الإلكترونية

المبحث الأول: جرائم الاعتداء على نظم المعلومات الإلكترونية.

المطلب الأول: سرقة المعلومات.

المطلب الثاني: تدمير المواقع وتشويهها.

المطلب الثالث: جريمة انتهاك سرية البيانات الإلكترونية والاستيلاء عليها.

المبحث الثاني: جرائم تزوير المستندات الإلكترونية والتوقيع والبريد الإلكتروني.

المطلب الاول: جريمة تزوير المستندات الإلكترونية.

المطلب الثاني: جريمة الاعتداء على التوقيع الإلكتروني.

المطلب الثالث: جرائم الاعتداء على البريد الإلكتروني.

الخاتمة.

النتائج والتوصيات.

المصادر والمراجع.

مبحث تمهيدي:
الأحكام العامة لجرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقا للنظام السعودي
المطلب الأول:
مفهوم جرائم الاعتداء المتعمد

أولاً: الجريمة

تعريف الجريمة في اللغة مأخوذ من كلمة جرم ويدل على أربعة أمور، هي: القطع، والكسب، والذنب، والجَسَد. وَالجُمْعُ أَجْرامٌ وجُرُومٌ، وَهُوَ الجَرِيمَةُ، وقد جَرَمَ يجْرِمُ جَرْماً واجْتَرَمَ وأَجْرَم، فَهُوَ مجْرِم وجَرِيمٌ[(١)].

وفي اصطلاح الفقهاء نجد أن تعريف الجريمة له اتجاهان: عام/ وهو قولهم (الجريمة هي: فعل ما نهى الله عنه وزجر وعصيان ما أمر الله به). وخاص/ وهو قولهم (الجريمة هي: محظورات شرعية زجر الله تعالى عنها بحد أو تعزير)، أو الجزاء المقرر لمصلحة الجماعة على عصيان أمر الشارع.

أما تعريف الجريمة بالمفهوم القانوني: " هي أي انتهاك للقانون الجنائي وتعد عدوانا ضد المجتمع" فالجريمة: سلوك إنساني منحرف يمثل اعتداء على حق أو مصلحة من الحقوق أو المصالح التي يحميها الشرع أو القانون؛ بناء عليه وبتعريف أكثر دقة فإن الجريمة: كل سلوك إنساني غير مشروع إيجابياً كان أم سلبياً عمدياً كان أم غير عمدي يرتب له القانون جزاء جنائياً[(٢)].

---

(١) ابن منظور، محمد بن مكرم، لسان العرب، دار صادر، ط٣، بيروت، ١٩٩٣، ج١٢، ص٩١.

(٢) عودة، عبد القادر، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، ط١١، مؤسسة الرسالة، ج١،ص ٧٦.

وتجدر الإشارة إلى أن النظام في المملكة العربية السعودية مستمد من كتاب الله تعالى وسنة رسوله صلى الله عليه وسلم؛ كما نصت عليه المادة السابعة من النظام الأساسي للحكم؛ ولذلك نلحظ أن تعريف الجريمة في النظام السعودي هو ذات تعريف الجريمة عند الفقهاء.

ثانيا: الاعتداء

مأخوذ من كلمة عدا فيقال عَدا فلان عَدْواً وعُدْواناً وعداءً وتعدي أي ظلم ظلماً جاوز فيه القدر، والتعدي فيه مجاوزة الحد يقال: تعديت الحق واعتديته، ومنه الاعتداء والتعدي والعدوان. وقد قالت العرب: اعتدى فلان عن الحق واعتدى فوق الحق[١].

وفي اصطلاح الفقهاء يقصد به تجاوز الحد والقدر والحق الذي ينبغي الاقتصار عليه[٢].

ثالثا: المتعمد

أصله مأخوذ من كلمة عمد بفتح العين والميم: وهو ضد الخطأ وهو ما يكون غالباً في القتل وسائر الجنايات. ويقال تعمده وتعمد له وعمده عمداً وعمد إليه أي قصده، والعمد مصدره. والعمدة ما يعتمد عليه. واعتمدت على الشيء: اتكأت عليه[٣].

---

(١) ابن منظور، محمد بن مكرم، لسان العرب،١٩٩٣، ج١٥، ص ٣٣.

(٢) الموسوعة الفقهية الكويتية، وزارة الأوقاف والشؤون الإسلامية، الكويت، ط٣، ١٩٨٤م، ج٢٨، ص١٧٩

(٣) ابن منظور، محمد بن مكرم، لسان العرب،**١٩٩٣**، **ج٣**، ص ٣٠٣.

المطلب الثاني:
مفهوم نظم المعلومات الإلكترونية

أولاً: نظم

النظم في اللغة مأخوذ من قوله نظمه ينظمه نظماً ونظاما ونظمه فانتظم وتنظم، ويقصد بالنظم بفتح النون وتشديدها التأليف. ومنه نظمت اللؤلؤ أي جمعته في السلك، والتنظيم مثله، ومنه نظمت الشعر ونظمته، ونظم الأمر على المثل. وكل شيء قرنته بآخر أو ضممت بعضه إلى بعض فقد نظمته. والجمع أنظمة وأناظيم ونظم. ويقال ليس لأمرهم نظام أي ليس له هدي ولا متعلق ولا استقامة. والنظام بكسر النون وتشديدها العقد من الجوهر والخرز ونحوهما[١].

ويقصد بالنظم في الاصطلاح العلمي" أنه أي تركيب أو تصميم متكامل من أجزاء وأنظمة فرعية تؤدي مهمة أو أكثر لتحقيق هدف معين متفاعلة مع بعضها البعض"[٢].

ثانياً: المعلومات

المعلومات في اللغة أصلها مشتقة من كلمة علم بفتح العين وكسر اللام. **والعلم** نقيض الجهل، علم علما وعلم هو نفسه، ويقال رجل عالم وعليم، ويقصد به الإدراك والوعي والإحاطة ببواطن الأمور[٣].

ويعرف الفقه القانوني المعلومة بأنها **الحقائق**، أو **الرسائل**، أو **الإشارات**، أو المفاهيم التي تعرض بطريقة صالحة **للإبلاغ**، أو **التوصيل**، أو **التفسير بواسطة إنسان**، أو **أدوات**، أو معدات آلية[٤].

---

(١) ابن منظور، محمد بن مكرم، لسان العرب،**١٩٩٣**، **ج**١٢، ص ١٧٩.

(٢) الدسوقي، عبدالسميع، المحاسبة وتكنولوجيا المعلومات، دار النهضة، القاهرة، ١٩٩٨م، ص١٥٤

(٣) ابن منظور، محمد بن مكرم، لسان العرب،**١٩٩٣**، **ج**١٢، ص ٤١٧.

(٤) العريان، ٢٠٠٤م، ص٣٦.

وقد عرف علماء التقنية نظم المعلومات بأنها النظام الذي يتضمن مجموعة متجانسة ومترابطة من الأعمال والموارد تقوم بتجميع وتشغيل وإدارة البيانات بغرض إنتاج وتوصيل معلومات مفيدة لمستخدمي القرارات من خلال شبكة القنوات وخطوط الاتصال(١).

كما عرف نظام الجرائم المعلوماتية السعودي؛ النظام المعلوماتي بأنه مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية(٢).

ثالثاً: الإلكترونية

يقصد بكلمة إلكتروني" تقنية استعمال وسائل **كهربائية**، أو **كهرومغناطيسية**، أو **بصرية**، أو أي شكل آخر من وسائل التقنية المشابهة"(٣).

ويمكن تعريف نظم المعلومات الإلكترونية بأنها المكونات المادية والبرمجيات ووسائل الاتصالات عن بعد وإدارة قواعد البيانات وتقنيات معالجة المعلومات الأخرى المستخدمة في نظم المعلومات المعتمدة على الحاسب(٤).

---

(١) حسين، أحمد حسين علي، نظم المعلومات المحاسبية، الإطار الفكري والنظم التطبيقية، مكتبة الإشعاع الفنية، القاهرة، ١٩٩٨م، ص٢١

(٢) نظام مكافحة جرائم المعلوماتية، نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

(٣) نظام التعاملات **الإلكتروني** السعودي، ٢٠٠٧م بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٨ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

(٤) حلمي، يحيى مصطفى، أساسيات نظم المعلومات، مكتبة عين شمس، القاهرة، ٢٠٠٥م، ص٩٩

المبحث الأول:
جرائم الاعتداء على نظم المعلومات الإلكترونية

تمهيد:

أكثر الجرائم المعلوماتية التي يتم ارتكابها يكون الهدف منها الحصول على المعلومات الإلكترونية، التي تكون إما محفوظة على أجهزة الحاسب الآلي، أو منقولة عبر شبكة الإنترنت(١)، وغالباً ما يتم الاعتداء على هذه المعلومات بالاستيلاء عليها، أو تغييرها، أو حذفها، أو إلغائها نهائياً، ويكون الدافع من ذلك التنافس، أو الابتزاز، أو تحقيق مكاسب، أو الحصول على مزايا(٢).

فهذا المبحث ينقسم إلى ثلاثة مطالب:

المطلب الأول: جريمة سرقة المعلومات.

المطلب الثاني: تدمير المواقع وتشويهها.

المطلب الثالث: جريمة انتهاك سرية البيانات الإلكترونية والاستيلاء عليها.

---

(١) الجنبيهي، منير محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥م، ص١٦.

(٢) الغافري وآخرون، حسين الغافري و محمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، ٢٠٠٨م، ص٤٦

المطلب الأول:
جريمة سرقة المعلومات:

هذه الجريمة تقوم على ركنين أساسيين هما: الركن المادي ، والركن المعنوي.

أولا: الركن المادي.

يعرف بأنه هو كل العناصر الواقعية التي يتطلبها النص الجنائي لقيام الجريمة. وتعتبر ماهيته؛ كل ما يدخل في النموذج التشريعي للجريمة، وتكون له طبيعة مادية ملموسة، كما أن الركن المادي يمثل صلب كل جريمة لأن الشارع لا يجرم على مجرد التفكير في الجريمة أو على مجرد الدوافع والنزاعات النفسية الخالصة وإنما يستلزم أنْ تظهر تلك النزاعات والعوامل النفسية في صورة واقعة مادية هي الواقعة الاجرامية، فالمشرع لا يستطلع أعماق نفوس البشر ويفتش في تفكيرهم المجرد ليعاقبهم على ذلك، دون أن يتخذ هذا التفكير، وتلك العوامل النفسية مظهراً مادياً[1].

وللركن المادي ثلاثة عناصر أساسية لقيام الجريمة هي: السلوك الإجرامي والنتيجة الضارة وعلاقة السببية بين السلوك والنتيجة. فتمثل النتيجة في الركن المادي لمحل جريمة السرقة مال منقول مملوك للغير، والسلوك الاجرامي وهو النشاط المادي في جريمة السرقة يقصد به الاختلاس، وهو الاستيلاء على الحيازة الكاملة للمال بعنصريها المادي والمعنوي، بغير رضا مالكه أو حائزه، والاختلاس لا يقع إلا

---

(١) قورة، عادل، محاضرات في قانون العقوبات، القسم العام ص- ١٠٣) منتديات أستار تايمز، بتاريخ ٢٠١٤/ ١٢/ ٢٨ م،

https://www.startimes.com/f.aspx?t=36015683.

باجتماع عنصرين، الأول: الاستيلاء على الحيازة الكاملة، والثاني: انعدام رضا مالك الشيء أو حائزه[١].

وقد استقرت الأحكام القضائية على وقوع جريمة السرقة تامة بخروج الشيء المسروق من حيازة المجني عليه، إلى حيازة الجاني، أما قبل ذلك فإن الأمر يتعلق بشروع في السرقة إذا بدأ المتهم إخراج المال من حيازة المجني عليه، مع توفر نية التملك، وبذلك لا يتحقق وصف السرقة[٢].

هذه المعطيات التي استقر عليها فقه القانون، أثارت السؤال حول مدى إمكان اختلاس المعلومات ومدى إمكان تطبيق نصوص جريمة السرقة في حال سرقة المعلومات والبرامج؛ وقد اختلف الفقه والقضاء في اختلاس المعلومات الإلكترونية، فقد أيده البعض وعارضه البعض الآخر.

فذهب فريق إلى أن الاعتداء على البرامج والمعلومات المخزنة داخل جهاز الحاسب الآلي يشكل جريمة سرقة، إذا قام شخص بالدخول على جهاز الكمبيوتر، واطلع على البرامج أو المعلومات الموجودة بداخله، أو قام بنسخ هذه البرامج والمعلومات، فإن هذا الاعتداء يشكل جريمة سرقة، لأنه اعتداء على حق ملكية، ويستند هذا الرأي على: أن البرامج والمعلومات لها كيان مادي، يمكن رؤيته على الشاشة مترجم إلى أفكار، وأنه يمكن الاستحواذ على هذه البرامج والمعلومات عن طريق نسخها بأي طريقة كانت، كنسخها على ديسك أو "CD"، أو ما يسمى

---

(١) محمود، عبدالله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠١م، ص٢٦١

(٢) عطاالله، شيماء عبد الغني محمد، الأحكام الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة،٢٠٠٧، ص٤٥.

"USB"، كما أن اختلاس المعلومات يتحقق بالنشاط المادي الصادر من الجاني، سواء بتشغيله الجهاز للحصول على المعلومة، أو الاستحواذ عليها[١].

وذهب فريق ثان إلى التفرقة بين حالتين، الأولى: تتمثل في سرقة (CD) أو ديسك مسجل عليه معلومات أو برامج، وفي هذه الحالة يشكل الفعل جريمة سرقة تخضع لأحكام قانون العقوبات. والثانية: سرقة برنامج من على ديسك أو (CD) وذلك عن طريق نسخه، ويشكل الفعل جريمة تقليد للمصنف، يحميها قانون حماية المؤلف، وأما الاطلاع على المعلومة أو نسخها، فلا يشكل جريمة سرقة، وإنما جريمة إفشاء الأسرار في حال ما كانت المعلومة سرية، أما إن كانت المعلومة متاحة للجمهور مجاناً، فلا جريمة وإن كانت متاحة بمقابل فإن الاعتداء عليها سرقة منفعة ولا عقاب على ذلك إلا في حال وجود نص يعاقب على سرقة المنفعة[٢].

ويستندون في ذلك إلى: أن الاختلاس اللازم لوقوع السرقة بمعناه المعروف غير متحقق في حالة سرقة المعلومات؛ لأنه لا ينطوي على تبديل للحيازة، بل أنه ينحصر في الحصول على منفعة الشيء فقط دون أصله الذي يبقي في حيازة صاحبه، كما يذهب أنصار هذا الاتجاه إلى: أن السرقة تقتضي اختلاس مال مادي، أما سرقة المعلومات فهي مجرد نسخ للمعلومات، التي تظل في حيازة صاحبها الشرعي، وإنما فقط يتقاسم الاطلاع على هذه المعلومات مع مالكها.

---

(١) الرومي، محمد أمين، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٣م، ص ٤٦

(٢) المرجع السابق، ص٤٧.

فيما ذهب فريق ثالث إلى أن المعلومات المختزنة في الحاسب الآلي، وإن كانت لا تعتبر في ذاتها أشياء مادية، فلا يتصور انتزاع حيازتها ولا تكون بذلك محلاً للسرقة، إلا أن السندات المثبتة لها، أو التي تكون وسيلة تسجل عليها تصلح موضوعاً للسرقة؛ لأنها كياناً مادياً، فإذا ما تجسدت المعلومات المختزنة في الحاسب الآلي على ركيزة، سواء كانت ملفاً أو شريطاً ممغنطاً، فإننا نكون بصدد شيء مادي يصلح موضوعاً للسرقة(١).

وفي حكم قضية شهيرة يطلق عليها "Logabax": أن المال المعلوماتي هو الذى سمح بوصف سرقة الوثيقة، وتتلخص وقائع هذا الحكم في: أن أجيراً والذى بمقتضى وظيفته كان له مطلق التصرف، وقام بتصوير وثائق للمنشأة التي يعمل بها، ومن بين الوثائق التي تم تصويرها وثيقة سرية تتعلق بالعمل، وجاء في حيثيات الحكم أن التقاط صور الوثائق محل الإدعاء، ولأغراض شخصية، وضد إرادة وبدون علم مالك هذه الوثائق، فإن المتهم لم يفعل سوى الحيازة المادية، وأنه حاز بطريق الغش، وأثناء الوقت المخصص لإنتاج هذه الوثيقة، وهكذا نسبت المحكمة جريمة السرقة إلى العامل، بمجرد التقاطه صور للوثيقة، باعتبار أن الأمر ينطوي على اختلاس قانوني، ففي هذه القضية فإن المعلومة بمفردها هي التي سمحت بوصف الاختلاس، وقصد الغش، فواقعة انتقال الصورة بموجبه تحقق فعل الاختلاس، وذلك بسبب المعلومة التي تحملها الصورة، ومن ثم فإن اختلاس المعلومة هو ما أدى إلى اختلاس الوثيقة(٢).

---

(١) محمود، عبدالله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، ص٢٨١

(٢) المرجع السابق، ص٢٩٤.

والعنصر الثالث من الركن المادي وهو علاقة السببية بين السلوك والنتيجة وبه يكتمل الركن المادي للجريمة.

ثانيا: الركن المعنوي.

ويمثل الركن المعنوي لهذه الجريمة ، القصد العام و القصد الخاص ، فالقصد العام معلوم و هو العلم و الإرادة اما القصد الخاص فقد ثارت صعوبة تتعلق به في هذه الجريمة (السرقة المعلوماتية)، ذلك أن القصد الخاص لا يتوفر في حق المتهم بهذه الجريمة، إلا إذا توافرت إليه نية التملك، وذلك بالإضافة لتوافر القصد العام من علم وإرادة، وذلك لا يتوفر إلا بقصد حرمان المجني عليه نهائياً من المال محل للسرقة، وتثور الشكوك حول نية التملك في حالة سرقة المعلومات، إذا توفر لدى الجاني نية النسخ ورد الشيء، وليس نية التملك، إذ يترتب على تخلف نية التملك نتيجة قانونية هامة، تتمثل في انتفاء وصف السرقة، وبالتالي يقع الفعل في معنى الاستعارة، فقد صدرت أحكام للقضاء الأمريكي التي استبعدت فيها وقوع جريمة السرقة، ممن قام بنسخ برامج من حاسب آلي مملوك للغير، وذلك عن بُعد، كما استبعدت هذه الاحكام وقوع السرقة على معلومات سرية تخص مرضى إحدى المستشفيات، قام المتهم بنسخها عن بُعد من أجهزة المستشفى[1].

وحيث أن محل السرقة يتعين أن يكون مادياً، فإذا تعلق الأمر بما يسمى بالأموال غير المادية، كالأفكار فإنه يتعين أن تكون مضمنة في شيء مادي، حتى يمكن السيطرة عليه

(١) عطا الله، شيماء عبد الغني محمد، الأحكام الحماية الجنائية للتعاملات الإلكترونية، ص٥٣.

ويتحقق اختلاسه، لذلك يرى جانب من الفقه الفرنسي، أن المعلومات يمكن أن تكون محلاً للسرقة، إذا تم نقل هذه المعلومات إلى ذمة مالية أخرى[١].

وقد جرم المشرع الفرنسي في الفقرتين (٥،٦) من المادة (٤٦٢) من قانون (١٩٨٨م) استخدام المستندات المعلوماتية بدون إذن صاحبها، وتطبيقاً لذلك اتجه القضاء الفرنسي إلى وقوع جريمة السرقة بتصوير المستندات بدون موافقة صاحبها، على الرغم من ترك المستندات الأصلية، واتجهت أحكام القضاء الأوربي نفس الوجهة التي تبناها القضاء الفرنسي، عندما اعتبر نسخ المعلومات صورة من صور جريمة السرقة[٢].

أما ما يتعلق بالنظام السعودي، فإنه لم ينحاز لرأي قانوني معين فيما يتعلق بالجدل السائد حول الطبيعة القانونية لسرقة المعلومات الإلكترونية، لكنه في المقابل أسبغ على تلك المعلومات المثبتة من خلال الشبكة المعلوماتية أهمية قصوى، وحرمة خاصة؛ فقد أعتبر أن الدخول غير المشروع إلى كل موقع إلكتروني أو نظام معلوماتي بحد ذاته يشكل جريمة، فضلًا عن القيام بسرقتها، ويتجلى ذلك بالاطلاع على (المادة الخامسة) من نظام مكافحة الجرائم المعلوماتية، والتي عاقبت بالسجن مدة لا تزيد عن أربع سنوات، وغرامة مالية لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل من يقوم بالدخول غير المشروع لموقع إلكتروني، أياً كان الهدف من ذلك الدخول، ما دام أنه مخالفاً للنظام، ولم يكن بطريقة مشروعة، وقد أضافت المادة

---

(١) رمضان، مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م، ص١٤١.

(٢) عطا الله، شيماء عبد الغني محمد، الأحكام الحماية الجنائية للتعاملات الإلكترونية، ص٤٧.

الرابعة من النظام المشار إليه عقوبة السجن والغرامة على كل من يستولي على نفسه أو لغيره على مال منقول أو حصوله دون مسوغ نظامي على معلومات[١].

يتضح مما سبق ومن خلال ما ورد في النظام السعودي ان الطبيعة القانونية لسرقة المعلومات الإلكترونية هو (الدخول غير المشروع إلى كل موقع إلكتروني أو نظام معلوماتي بحد ذاته يشكل جريمة، فضلًا عن القيام بسرقتها) وهذا يدل على دقة النظام السعودي في وصفه هذه الجريمة.

(١) نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

المطلب الثاني:
جريمة تدمير المواقع وتشويهها:

من المعلوم أن تدمير المواقع الإلكترونية أو تشويهها في نطاق الجرائم المعلوماتية يدخل في مفهوم الإتلاف، الذي ينصب على معطيات الحاسب، من بيانات ومعلومات مخزنة في نظم الحواسب والبرامج، وكذلك يشمل جميع المعطيات المتبادلة بين شبكات الحواسب، وعبر شبكات المعلومات، وبالتالي ينتج عنه إما محو كلي للمعطيات أو تشويه من شأنه إتلاف أجراء منها، يمنع استخدام النظام أو البرنامج على نحو طبيعي، وذلك بسبب غياب التكامل المطلوب بين عناصر ومعطيات النظام(١).

ومن أشهر الأمثلة على ذلك: تدمير المواقع، ويقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام(٢).

وتقوم جريمة تدمير المواقع الإلكترونية من خلال توافر الركن المادي، المتمثل في فن التعطيل، الذي يندرج ضمن إعاقة النظام، أياً كانت تلك الوسيلة المستخدمة في ذلك، ومنها ما يتحقق باستخدام البرامج الخبيثة ذات الأثر التدميري، التي تستهدف كل ملفات وبرامج الموقع أو جزء منها، وكذلك المعطيات المخزنة فتصيبه بالشلل

---

(١) فتح الله، محمود رجب، الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩م، ص ٣٦٤.

(٢) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٠٩م، ص٣٨٣.

التام، ومن أشهر تلك البرامج الخبيثة ما يطلق عليه: القنابل الموقوتة، وبرنامج الدودة، والفيروسات الإلكترونية وأحصنة طروادة[١].

ومن الوسائل المستخدمة في تدمير المواقع ما يكون بطريقة فنية، دون استخدام البرامج الخبيثة، مثل: ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع المستهدف؛ للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة فيه، فتنتقل إلى جهاز المعتدي[٢].

وتجدر الإشارة أن إتلاف أجهزة الحاسب الآلي، أو البرامج والمعلومات، سواء بمحوها كلياً، أو جزئياً، أو بالتأثير على نتائجها وعملها، بأن تخرج هذه البرامج نتائج غير صحيحة، أو غير منطقية، لا يجوز من الوجهة الشرعية، لما فيه من الاعتداء على الغير، ولما فيه من الضرر الذي جاءت الشريعة الإسلامية بتحريمه والنهي عنه[٣].

وقد يكون الإتلاف بطريق تشويه الموقع، عن طريق اختراقه، وتغيير الصفحة الرئيسة للموقع بصفحة أخرى، يعلن فيها المخترق انتصاره على نظام مزود ويب،

---

(١) أحمد، هلالى عبدالله، جرائم المعلوماتية التقليدية والمستحدثة، دار النهضة العربية، مصر، الطبعة الأولى، ٢٠١٣م، ص ٢٥٧.

(٢) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٠٩م، ص٣٨٤.

(٣) السند، عبدالرحمن بن عبدالله، الأحكام الفقهية للتعاملات الإلكترونية "الحاسب الآلي وشبكة المعلومات، الإنترنت"، دار الوراق، دار النيرين للطباعة والنشر والتوزيع، بيروت، الطبعة الثالثة، ٢٠٠٦م، ص٣٥٠.

والإجراءات الأمنية للشبكة، ويقصد من وراء ذلك إلى إبراز قدراته التقنية، وإعلان تحديه للمشرفين على نظم مزودات ويب، ليثبت لنفسه، أو لغيره، امتلاكه المقدرة التقنية على كسر نظام الحماية في هذه المزودات، الأمر الذي يتطلب معرفة معمقة لطريقة عمل الإنترنت وبروتوكولاته، وقد تتضمن الصفحة الجديدة أحياناً رسالة يرغب الشخص الذي قام بعملية التشويه إيصالها للعالم(١).

وتعتبر جريمة تدمير المواقع الإلكترونية أو تشويهها جريمة عمدية، يتخذ ركنها المعنوي صورة القصد الجنائي، وبالتالي فإنه لا تتم الجريمة إلا عند توافر القصد الجنائي، بعنصرية العلم والإرادة، ولا حاجة إلى ركن خاص أو مفترض، كالإضرار بالمصلحة العامة، ويعني ذلك أن الجريمة لا تكون تامة بمجرد الإهمال، أو عدم أخذ الحيطة والحذر، الذي أدى لإيقاف الشبكة، أو تعطيلها، أو الإضرار ببرامجها، أو بياناتها، بأي صورة، ولابد من الإشارة إلى أن العلم المقصود به سلوك الجاني في إتلاف الشبكة، أو تدميرها، وتشويهها، أو الإضرار بها في أي صورة كانت، مما يجرمه القانون، كما أنه يلزم للاعتداد بالإرادة أن تكون إرادة واعية ومدركة، طبقاً للقواعد العامة، لكن لا يشكل جهل الجاني بنص التجريم نفي القصد الجنائي طبقاً للقواعد العامة(٢).

وقد جرّم المشرع الفرنسي في قانون العقوبات المعدل والصادر في (١٩٩٤م) جريمة التعطيل، أو الإفساد عن عمد، كل ما يتعلق بتشغيل نظام المعالجة الآلية للبيانات، أو

---

(١) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٣٨٥.

(٢) الشاذلي، فتوح عبدالله، جرائم التعزير المنظمة في المملكة العربية السعودية، مكتبة الرشد، الرياض، الطبعة الرابعة، ٢٠٢٠م، ص ٥٩٢.

محو وتعديل البيانات المعالجة آلياً، أو التدخل في طرق معالجتها، في الفقرتين (٤،٣) من المادة (٤٦٢) وعاقب عليه بالحبس لمدة تتراوح بين ثلاثة أشهر وثلاث سنوات، أو الغرامة المالية التي تتراوح بين عشرة الآف فرنك ومئتي ألف فرنك[١].

وباستقراء النظام السعودي فقد شدد في وجوب تحقيق الأمن المعلوماتي، وحماية المصلحة العامة، طبقاً لما نصت عليه (المادة الثانية) من نظام مكافحة الجرائم المعلوماتية لسنة (١٤٢٨هـ) وأما ما يتعلق بتدمير المواقع وتشويها فقد فصّلت (المادة الخامسة) من النظام المشار إليه بعقوبة الجاني، والتي تصل إلى السجن لمدة أربعة سنوات، وبغرامة تصل إلى ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، وذلك لكل من يرتكب جريمة الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها، أو إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها بأي وسيله كانت[٢].

ومن التطبيقات القضائية الحديثة للقضاء السعودي، ما ذهبت إليه محكمة الاستئناف في تأييد المحكمة الجزائية بمنطقة الأحساء بإدانة متهم بالدخول غير المشروع لأحد المواقع الإلكترونية، وهو عبارة عن صحيفة إلكترونية، وتغيير بياناته الخاصة، وإتلافه

---

(١) حجازي، عبدالفتاح بيومي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، منشأة المعرف، الإسكندرية، الطبعة الأولى، ٢٠٠٩م، ص ٧٣.

(٢) نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

وتدميره وتغيير التصميم لصور فاضحة، وقد تم الحكم عليه بالسجن لمدة ستة أشهر[١].

يتضح مما سبق ان النظام السعودي قد شدد في وجوب تحقيق الأمن المعلوماتي، وحماية المصلحة العامة.

(١) مجموعة الأحكام القضائية، المجلد الرابع والعشرون، وزارة العدل السعودية، مركز البحوث، ٢٠١٢، ص ٨٤.

المطلب الثالث:
جريمة انتهاك سرية البيانات الإلكترونية والاستيلاء عليها:

عُرّفت البيانات الشخصية بأنها: كل بيان يتعلق بشخص محدد أو قابل للتحديد، بصورة مباشرة أو غير مباشرة، ومنها ما قد يتعلق بحرمة الحياة الخاصة للإنسان، ومنها ما يسمح برسم صورة لاتجاهاته وميوله، ومنها تلك التي تتعلق باتجاهاته السياسية، ومعتقداته الدينية، وتعاملاته المالية والبنكية، وجنسيته، وهواياته، وحالته العضوية، أو النفسية، أو العقلية والاقتصادية، أو الثقافية، أو الاجتماعية(١).

وقد عرّف نظام مكافحة الجرائم المعلوماتية البيانات الإلكترونية بأنها: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه، بواسطة الحاسب الآلي، كالأرقام والحروف والرموز(٢).

إنَّ موضوع الحماية فيما يتعلق بالبيانات الإلكترونية لا يقصد بها مجرد المعلومات المخزنة بحد ذاتها، إنما تتمثل في المصالح التي تهددها هذه المعلومات، وبما أنّ الإنترنت أصبح شبكية عالمية، فإنه يمكن الربط بسهولة بين المعلومات الشخصية التي تُجمع عن المستخدم، سواء تمَّ الحصول على هذه البيانات من خلال الاستمارات الإلكترونية التي تعبأ من قبل المستخدم، أومن خلال استخدام برمجيات خاصة بالتجسس، تجمع معلومات مختصرة عن طريق استخدام الإنترنت، متضمنة

---

(١) رمضان، مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، ص٨٢.

(٢) نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

معلومات حسَّاسة، مثل: أرقام بطاقات الائتمان الخاصة، أو تستخدم مثل تلك البيانات لانتحال شخصية صاحب الحق في هذه البيانات، واستخدامها بشكل غير مشروع[١].

وهناك صوراً عديدة للاعتداء على البيانات الإلكترونية من خلال الحاسب الآلي وشبكة الإنترنت، عالجتها الأنظمة في عدة جرائم، مثل: جريمة دخول المواقع وأنظمة المعلومات المملوكة للغير، وجريمة التنصت، أو التقاط، أو اعتراض الرسائل، وجريمة انتهاك المعتقدات الدينية، أو حرمة الحياة الخاصة[٢].

ويرى البعض أن تعبير حماية البيانات الإلكترونية الخاصة يجب أن يفهم على أساس حماية الأشخاص ضد نوعين من الاعتداءات، الأول: الاعتداء على سرية الحياة الخاصة، مثل إفشاء الحياة الخاصة، بمعنى تعريف العامة أو عدد غير محدود من الأشخاص بعناصر تتصل بالحياة الشخصية، أو العائلية، أو التحري عن الحياة الخاصة، أو التجسس عليها، والثاني: هو الاعتداء على سرية المعلومات والبيانات الشخصية الخاصة ويعنى ذلك أن الأنظمة تحاول وضع سياج للاستقلال، تنعم بداخله الحياة الخاصة، بحريتها ويمتنع على الآخرين اختراقه، سواءً تعلق ذلك بالحياة الشخصية للفرد، أو بياناته الإلكترونية السرية[٣].

---

(١) الشوابكة، محمد أمين، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الاردن، ٢٠٠٩،ص٦٤.

(٢) الشاذلي، فتوح عبدالله، جرائم التعزير المنظمة في المملكة العربية السعودية، ص ٥٩٥.

(٣) دياب، صلاح محمد أحمد، الحماية القانونية للحياة الخاصة للعامل وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية- مصر- ص١٨.

وقد حاول الفقه القانوني إيضاح معنى الدخول في إطار المعلوماتية بصفة عامة، حيث إنه يشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي، والإحاطة أو السيطرة على المعطيات التي يتكون منها، أو الخدمات التي يقدمها[١].

وقد يتم انتهاك تلك البيانات الإلكترونية الخاصة، والاستيلاء عليها بالدخول غير المصرح إلى النظام، عن طريق توجيه هجمات إلى معلومات الحاسب الآلي، أو خدماته، بقصد المساس بالسرية، أو السلامة، أو المحتوى، أو تعطيل قدرة وكفاءة الأنظمة للقيام بأعمالها، وقد يكون الدخول بواسطة الاختراق، وهو عملية دخول غير مصرح بها إلى أجهزة الغير وشبكاتهم الإلكترونية، ويتم الاختراق بواسطة برامج متطورة يستخدمها من يمتلك خبرة في استخدامها[٢].

وتختلف وسائل الدخول التي يمكن اللجوء إليها لتنفيذ جريمة انتهاك سرية البيانات الإلكترونية، ولكن لا بد من الإشارة إلى أنه في بعض الصور الإجرامية لا تتطلب الجريمة العبث أو تخريب تلك البيانات الإلكترونية، أو سرقتها، ولكنها تتم بمجرد الدخول غير المشروع والمصرح به قانوناً لقيام الجريمة، وغالباً ما قد يتطلب تنفيذ الجريمة إلى قدرة فنية خاصة، وخبرة تقنية عالية، للحصول على شفرات خاصة بالدخول غير المصرح به، بغرض انتهاك سرية تلك البيانات، والذي يشكل جريمة بحد ذاته[٣].

---

(١) فريد، نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، الطبعة الأولى،٢٠٠٥، ص٣٣٢.

(٢) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٤٤٢.

(٣) فريد، نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، ص٣١٥.

وقد يكون القصد من انتحال شخصية الموقع هو الاستيلاء على معلومات الهوية، وذلك مثل أرقام بطاقات الائتمان، أو رقم الضمان الاجتماعي، كإنشاء موقع يتطلب الدخول إليه اشتراك باستخدام بطاقة الائتمان، فيقوم المجني عليه باستخدام بطاقة الائتمان، وبالتالي يقع في شبكة احتيال، أو أن يقوم المجني عليه بملء استمارة ما، تتضمن بيانات هويته، ويقوم الجاني باستخدام هذه البيانات في الاحتيال على آخرين(١).

وقد تمكن أحد المحتالين من الحصول على أسماء وأرقام التأمين الاجتماعي لمجموعة كبيرة من العسكريين الأمريكيين، والقيام باستخدامها احتيالاً على أحد المصارف(٢).

وقد يتم الاستيلاء بأسلوب ما يسمى محاكاة الموقع، وغالباً ما يستخدم هذا الأسلوب في السطو على أرقام البطاقات الائتمانية، وأرقام الحسابات، والأعمال التجارية، وفكرته تقوم على تقليد أحد المواقع الحقيقة، التي غالباً ما تكون مواقع تجارية بكافة تفاصيل الموقع، من تخطيط وألوان وغيرها، وجعل الموقع المقلد يقوم بنسخ بعض محتويات الموقع الأصلي، ثم تقديم منتج بسعر مغرٍ، لحث الناس على إدخال معلوماتهم الائتمانية(٣).

---

(١) الشناوي، محمد، جرائم النصب المستحدثة (الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)، دار الكتب القانونية، مصر المحلة الكبرى، ٢٠٠٨م، ص٩١.

(٢) المرجع السابق، ص٣٢.

(٣) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٣٩٠.

وقد تتم هذه الجريمة من خلال انتحال شخصية الموقع، الذي يتم بموجب هجوم يشنه الجاني على الموقع للسيطرة عليه، أو يحاول اختراق موقع أحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك، مما يؤدى إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور[١].

ومن أمثلة ذلك عندما وقعت عدة شركات كبرى ضحية عمليات نصب عديدة، فمثلاً: في عام (١٩٩٥م) كان عنوان موقع الإنترنت (www.mcdonalds.com) المملوك للشركة الأمريكية العالمية العملاقة McDonald's المتخصصة في تقديم الوجبات السريعة مسجلاً بطريق الاستيلاء عليه من قبل صحفي يعمل بمجلة Wired الأمريكية، وقد تمكنت هذه الشركة، وبعد مساومات مالية كبيرة من استرجاع هذا العنوان الخاص بها[٢].

كما قد تتحقق هذه الجريمة عندما يقوم الجاني بأي عمل يؤدى إلى إرباك سير النظام، بحيث لا يؤدى نفس الوظيفة المعتادة له، كأن يصبح عاجزاً عن العمل كلية، أو يعمل ولكن بطريقة بطيئة عن المعتاد، وتطبيقاً لذلك قضت إحدى المحاكم الفرنسية بتوافر جريمة الإخلال بالنظام، من المتهم الذي قام بإرسال رسائل كثيرة إلى أحد الأجهزة الخاصة بإحدى الشركات المنافسة، موهماً نظام هذه الشركة أن الرسائل تصل إليه من أجهزة متعددة، وتتضمن طلبيات شراء من الشركة، وقد كانت تلك الطلبيات غير جدية، وكان هدف المتهم منها أن يملئ الأجهزة الخاصة بهذه الشركة،

---

(١) الحسن، عزة على محمد، الجريمة المعلوماتية في القانون السوداني، الزيتونة للطباعة،٢٠٠٩، ص٦٢.

(٢) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٣٩١.

حتى تكون عاجزة عن تلقي طلبات جديدة، وبالتالي يضر بها في النهاية لذا قضت المحكمة بتوافر هذه الجريمة في هذه الحالة[١].

كذلك قد يقوم الجاني بالاستيلاء على مواقع المؤسسات والكيانات المعروفة، وانتهاك خصوصيتها، باستخدام اسماء حقول الانترنت، أو ما يسمى (الدومين)، ومن أبرز الأمثلة على ذلك: عندما سطا شخص يدعى "جون ويليامز راسين" على موقع "الجزيرة نت" أثناء الحرب على العراق، ولم يستخدم المعتدي لغات برمجة أو برامج معقدة لاعتراض البيانات، بل قام بذلك من خلال الحصول على بطاقة هوية هاتفية، وتزوير توقيع، وإرسال طلب بالفاكس بالتوقيع المزور إلى شركة " Netwok Solution" وهي أكبر شركة لحجز أسماء الحقول على شبكة الإنترنت تابعة لمؤسسة "Verision" التي تمنح شهادات الضمان الأمني للمواقع التجارية، يطلب فيه إعادة تخصيص بيانات التحكم باسم الحقل القديم ببيانات حديثة، فقامت الشركة بإعادة تخصيص الموقع إلى الجاني، واضطرت قناة الجزيرة للدخول في دوامة إدارية وفنية وقانونية حتى تستعيد موقعها مرة أخرى[٢].

وقد عاقب قانون العقوبات الفرنسي على انتهاك سرية البيانات الإلكترونية، أو الاستيلاء عليها، أو إعاقتها، أو تحريف تشغيل نظم معالجة البيانات، حيث جاء في المادة (٣٢٣-٢) منه يعاقب بالحبس لمدة ثلاث سنوات وغرامة مقدارها ٣٠٠.٠٠٠

---

(١) عطاالله، شيماء عبد الغني محمد، الأحكام الحماية الجنائية للتعاملات الإلكترونية، ص٤٧.

(٢) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٣٩٠.

ألف فرنك فرنسي كل من قام انتهاك خصوصية البيانات، أو الاستيلاء عليها، أو بإعاقتها، أو إفساد تشغيل نظام معالجة البيانات[١].

ومن التطبيقات القضائية الحديثة للقضاء السعودي، ما ذهبت إليه محكمة الاستئناف في تأييد حكم المحكمة الجزائية بمنطقة الرياض بإدانة متهم باختراق غير مشروع لأجهزة المحاسبة الإدارية بالشؤون الإدارية والمالية بإحدى المدارس، والاستيلاء على معلومات شخصية تتعلق بمسيرات رواتب العاملات، ونشرها على الانترنت، بقصد إلحاق الضرر، وقد تم تطبيق عقوبة السجن والغرامة المالية بحقه[٢].

وبمقارنة النظام الفرنسي مع ما ورد في نظام مكافحة جرائم المعلوماتية السعودي، يلاحظ التقارب بين القانونين، في مدة عقوبة الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، حيث فرض النظام السعودي عقوبة السجن، التي قد تصل إلى أربعة سنوات، وبغرامة لا تزيد على ٣ ملايين ريال، أو بإحدى العقوبتين.

---

(١) حجازي، عبدالفتاح بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية/ دار النهضة العربية، القاهرة، الطبعة الأولى ٢٠٠٩م، ص٣٦٢.

(٢) الحقباني، رايز بن سالم، مهارات البحث والتحقيق في الجرائم المعلوماتية، كلية الملك فهد الأمنية، الرياض، ٢٠١٤، ص ١٧٩.

المبحث الثاني:
جريمة تزوير المستندات الإلكترونية وجريمة الاعتداء على التوقيع والبريد الإلكتروني

تمهيد:

سنتناول في هذا المبحث عدد من الجرائم التي تشكل **اعتداء** على سلامة التقنية المعلوماتية، وهذه الجرائم تتمثل في جريمة تزوير المستندات الإلكترونية، وكذلك جريمة الاعتداء على التوقيع الإلكتروني، وختاماً سنفصل الحديث عن جريمة الاعتداء على البريد الإلكتروني؛ وذلك على النحو التالي:

فهذا المبحث ينقسم إلى ثلاثة مطالب:

المطلب الأول: جريمة تزوير المستندات الإلكترونية.

المطلب الثاني: جريمة الاعتداء على التوقيع الإلكتروني.

المطلب الثالث: جرائم الاعتداء على البريد الإلكتروني.

المطلب الأول:
جريمة تزوير المستندات الإلكترونية:

لا شك أن خطورة انتشار جريمة التزوير بشكل عام في مجتمع ما أثر بالغ في ضياع الحقوق، وإضعاف المراكز القانونية بشكل عام، وتتعاظم هذه الجريمة إذا اتصلت بالنظام المعلوماتي، أو ما يتعلق بالتقنية الحديثة، وسببه سهولة إنتاج نسخ مزورة، عن طريق التقنية الحديثة بكميات كبيرة وبزمن قياسي، خاصة مع توفر القدرة الفائقة العالية في كافة المجالات التقنية، وكذلك تطور الطابعات الحديثة، كوسيلة إخراج التي توصل بجهاز الكمبيوتر، حيث تتفاعل معه، ومن ثم يتم إخراج المحرر المزور بالطريقة التي يريدها الجاني من تلك الجريمة[١].

ويقصد بجريمة تزوير المستندات الإلكترونية في الفقه القانوني: هو تغيير الحقيقة في المستند الإلكتروني، بإحدى طرق التغيير، كالتوقيع والحذف، والإضافة، والتعديل أو التغيير، وأن يترتب على هذا التغيير ضرر للغير[٢].

وقد عرّف النظام الجزائي السعودي جريمة التزوير بأنها: كل تغيير للحقيقة بإحدى الطرق المنصوص عليها نظاماً، حدث بسوء نية قصداً للاستعمال فيما يحميه النظام،

---

(١) رضوان، هلال محمد، بحوث وآراء جديدة في مجال كشف التزييف والتزوير، عالم الكتب، ١٩٩٣م، ص ٧٩.

(٢) السند، عبدالرحمن بن عبدالله، الأحكام الفقهية للتعاملات الإلكترونية "الحاسب الآلي وشبكة المعلومات، الإنترنت، ص٣٧٦.

من محرر، أو خاتم، أو علامة، أو طابع، وكان من شأن هذا التغيير أن يتسبب في ضرر مادي، أو معنوي، أو اجتماعي، لأي شخص ذي صفة طبيعية، أو اعتبارية[١].

وفي ذات السياق كذلك عرّف النظام الجزائي السعودي المشار إليه المحرر بأنه: كل مسطور يتضمن حروفاً، أو علامات، ينتقل بقراءتها الفكر إلى معنى معين، بصرف النظر عن الوعاء الذي كتبت أو حفظت فيه، بما في ذلك وسائل تقنية **المعلومات**.

ولا شك أن جريمة التزوير الإلكتروني تعتبر جريمة غير تقليدية، غالباً ما تحتاج إلى معارف ومهارات فنية متقدمة في مجال تقنية الانترنت والحاسب الآلي، وبالتالي فهي لا ترتكب بطريقة عشوائية، بل إنها تحتاج إلى درجة عالية من التخصص والكفاءة، بالإضافة إلى قدرة عالية في الحيلة والخداع[٢].

ولا يخفى أن تزوير المستندات الإلكترونية قد يقع من اختلاق أو تعديل غير مصرح به للبيانات المسجلة، بطريقة من شأنها أن تحوز هذه البيانات قيمة دامغة، ومن ثم تكون موضوعاً للخداع، وقد يتخذ التزوير المعلوماتي صورة إدخال غير مصرح لبيانات صحيحة أو غير صحيحة على السواء، ومن شأن كل ذلك أن يخلق موقفاً يماثل عمل محرر مزور، كذلك قد يتخذ التزوير المعلوماتي صورة التعديل أو التغيير الجزئي أو

---

(١) النظام الجزائي لجرائم التزوير لسنة ١٤٣٥هـ بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١١ وتاريخ ١٨/ ٢/ ١٤٣٥هـ.

(٢) عباس، ٢٠١٥م، ص٥٣.

المحو، كواقعة خروج البيانات المحملة على دعامة، والطمس، كواقعة حفظ وإخفاء بيانات يساوي ذلك بشكل عام تزوير محرر صحيح[١].

ويلاحظ أنه يوجد تشابه كبير بين جرائم التزوير وجرائم الاحتيال، وذلك من حيث قيامهما على تغيير الحقيقة، غير أنهما بطبيعة الحال يختلفان من عدة زوايا أهمها: أن جريمة تزوير المحررات سواء أكانت إلكترونية أو تقليدية، لا بد أن تقع على محرر، وهذا لا يشترط في جريمة الاحتيال، بالإضافة لذلك لابد من ثبوت الضرر في جريمة التزوير، وغالباً ما تجتمع جريمتا الاحتيال والتزوير في جريمة واحدة، ونكون حينئذ أمام حالة التعدد المادي للجرائم[٢].

وهذه الجريمة تشترط لتحققها توافر الركن المادي، والذي يتمثل في تغيير الحقيقة في المستندات المستخرجة، من خلال الحاسب الآلي، سواء أكانت محولة أو مرسلة بطريق الانترنت، أو المطبوعة بالطرق التقليدية، أو الدعامات كالشرائط الممغنطة والمسجلة، وهو ما يطلق عليه لفظ (CD)، وذلك شريطة وجود الضرر الذي يتمثل في اهتزاز الثقة المفروضة في المحررات الرسمية أو العرفية، وذلك مثل عمليات الدفع الإلكتروني، والفواتير، وجميع العمليات البنكية، والشركات، والمؤسسات مهما كان حجمها، ولا بد من الإشارة إلى أن التزوير المعلوماتي لا يتم فقط من قبل مشغل الحاسب الآلي وحسب، بل من الممكن أن يتم توجيه الاتهام بمثل هذه القضية إلى

---

(١) أحمد، هلالي عبدالله، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣/ ١١/ ٢٠٠١م، دار النهضة العربية، القاهرة، الطبعة الأولي ٢٠٠٣، ص١١٠.

(٢) فتح الله، محمود رجب، الوسيط في الجرائم المعلوماتية، ص٣٥٧.

كل شخص طبيعي ليس لديه أي قدر من المهارة الفنية بتقنية المعلومات، مادام أنه هو من طلب من المبرمج تزوير تلك المستندات، مع توفر الركن المعنوي بحقه[١].

وعلى ذلك؛ فإن تغيير الحقيقة كعنصر من عناصر الركن المادي في جريمة تزوير المستندات تقع على البيانات والمعلومات، بأي لغة وبأي طريقة كانت، ويستوي أن يكون التغيير مادياً أو معنوياً، كما يستوي شكلها، أو المادة التي كانت عليها كالصور، والرموز، والعلامات، ما دام أنه ينصب على محرر معين، وله حجية وصلاحية للتمسك به في مواجهة الغير[٢].

أما ما يتعلق بالركن المعنوي لهذه الجريمة، فإنه يتخذ صورة القصد الجنائي، ولكن لا يكفي لقيامه القصد العام بعنصرية العلم بأركان الجريمة، واتجاه الإرادة من الجاني إلى القيام بالفعل، وتحقيق نتيجته، بل أيضاً تتطلب هذه الجريمة توافر قصد جنائي خاص، يتمثل بنية استعمال المحرر المزور فيما زور من أجله، وذلك أن من شرط قيام الجريمة كما ذكر آنفاً: أن يكون هنالك تعمد لتغيير الحقيقة في محرر يسبب ضرراً للآخرين وأن تتوجه النية لاستعماله[٣].

وقد قامت مختلف الدول في السنوات الأخيرة بإجراء تعديلات جوهرية على قوانينها الجزائية؛ من أجل الاستجابة للتطورات التي أنتجتها التقنية الحديثة والحاسب الآلي،

---

(١) حجازي، عبدالفتاح بيومي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٢م، ص ٢٤٦.

(٢) الحكيمي، عبدالباسط محمد سيف، النظرية العامة للجرائم ذات الخط العام، رسالة دكتوراه، بغداد، ٢٠٠٠، ص ٦٨.

(٣) عبدالله، فهد بن سعد، الأحكام الشرعية والنظامية لجرائم تزوير المحررات الرسمية، مذكرة لنيل رسالة الماجستير، المعهد العالي للعلوم الأمنية، الرياض، ١٩٩٦، ص ٢٩٣.

ويتضح ذلك بالنظر إلى القانون الفرنسي، حيث أن قانون العقوبات الجديد لسنة (١٩٩٤م) قد نص على تجريم التزوير في المحررات الرسمية والعرفية بأي طريقة كانت، وبالتالي أصبح هذا النص بإطلاقه يغطي جرائم التزوير التقليدية والمعلوماتية، حيث نصت المادة (٤٤١) في الفقرة الأولى منها على أنه: يعد تزويراً كل تغيير تدليسي للحقيقة، يكون من شأنه أن يحدث ضرراً، ويقع بأي وسيلة كانت سواء، وقع في محرر، أو سند، معبراً عن الرأي، أياً كان موضوعه، والذي أعد مسبقاً كأداة لإنشاء حق، أو ترتيب أثر قانوني معين، وقد عاقب على ثبوت جريمة تزوير المحرر واستعماله بالسجن ثلاث سنوات، والغرامة التي لا تزيد على ٣٠٠ ألف فرنك[١].

وبالرجوع إلى النظام السعودي يلاحظ أن تزوير المستندات المعالجة آلياً يدخل في مفهوم التزوير، وينطبق عليه النظام الجزائي لجرائم التزوير، الذي اعتبر أن كل تزوير بطريق تقنية المعلومات داخل في العقوبات الواردة في النظام، وعلى ذلك فقد عاقب النظام المشار إليه تزوير المستندات والمحررات المنسوبة إلى جهة عامة بالسجن من سنة إلى خمس سنوات، وبغرامة لا تزيد على خمسمائة ألف ريال، أما تزوير المستندات والمحررات العرفية فعاقب عليها بالسجن مدة لا تتجاوز ثلاث سنوات، وبغرامة لا تزيد على ثلاثمائة ألف ريال، أو بإحدى هاتين العقوبتين[٢].

ومن التطبيقات القضائية الحديثة للقضاء السعودي، ما ذهبت إليه محكمة الاستئناف في تأييد حكم المحكمة الجزائية بإدانة متهم بتزوير مستند إلكتروني، عبارة عن شهادة

---

(١) قانون العقوبات الفرنسي المعدل الصادر ١٩٩٤م.

(٢) النظام الجزائي لجرائم التزوير لسنة ١٤٣٥هـ بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١١ وتاريخ ١٨/ ٢/ ١٤٣٥هـ.

البكالوريوس وتقديمها لبرنامج **ابتعاث خادم الحرمين من أجل استكمال دراسة مرحلة الماجستير**، وقد تم تطبيق عقوبة السجن والغرامة المالية بحقه، بعد ثبوت جريمة التزوير واستعمال المحرر المزور[1].

(١) مجموعة المبادئ والأحكام الجزائية، ١٤٣٦هـ.

المطلب الثاني:
جريمة الاعتداء على التوقيع الإلكتروني:

عرّف بعض فقهاء القانون التوقيع الإلكتروني، بأنه: حروف أو أرقام أو رموز أو إشارات لها طابع متفرد، تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره[١].

وقد عُرّف التوقيع الإلكتروني من وجهة نظر القانون الخاص على أنه: ما يوضع على محرر إلكتروني (شريحة إلكترونية) ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع مميز ومنفرد يسمح بتحديد شخص الموقِّع ويميزه عن غيره[٢]،

كما عرّفه نظام التعاملات الإلكترونية السعودي بأنه: بيانات إلكترونية، مدرجة في تعامل إلكتروني، أو مضافة إليه، أو مرتبطة به منطقياً، تستخدم لإثبات هوية الموقع وموافقته على التعامل الإلكتروني، واكتشاف أي تعديل يطرأ على هذا التعامل بعد التوقيع عليه[٣].

ومن خلال التعريفات المشار إليها آنفاً يتضح أن: التوقيع الإلكتروني يتميز عن التوقيع التقليدي بأنه لا يتخذ صورة واحدة أو شكل معين، بل يمكن أن يتم بأي شكل يميّز صاحب التوقيع ويحدد هويته، ويظهر رغبته في إقرار العمل القانوني، أو الرضا

---

(١) السند، عبدالرحمن بن عبدالله، الأحكام الفقهية للتعاملات الإلكترونية "الحاسب الآلي وشبكة المعلومات، الإنترنت، ص١٤٦.

(٢) يوسف، أمير فرج، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية،٢٠٠٨، ص١٤.

(٣) الفقرة الرابعة عشر من المادة الأولى من نظام التعاملات الإلكترونية لسنة ٢٠٠٧م بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٨ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

بمضمونه، سواء كان في هيئة صورة، أو حرف، أو رقم، أو رمز، أو إشارة، أو صوت، كما أن التوقيع التقليدي يكون في الغالب على ورقة يوضع عليها التوقيع أو الختم أو البصمة، بخلاف التوقيع الإلكتروني الذي يكون على أجهزة الحاسب الآلي وعبر شبكة الإنترنت[١].

كما يتميز التوقيع الإلكتروني عن التوقيع الكتابي التقليدي بأنه: لا يتم إلا بوسيلة واحدة محددة سلفاً، وتكون وفقاً لإجراءات تقنية آمنة، وذلك لتتمكن من التعرف على شخصية الموقع وتضمن سلامة المحرر من العبث أو التحريف، وبالتالي فإن التوقيع الإلكتروني يعطي لتلك الوثيقة الموقعة صفة المحرر الأصلي، فيكون بذلك دليلاً مقبولاً في حالة وجود أي نزاع بين أطراف العقد الموقع، والذي تم استخدام التوقيع الإلكتروني فيه[٢].

وتجد الإشارة إلى أن التوقيع الإلكتروني يتخذ صوراً متعددة، منها ما يسمى نقل التوقيع العادي إلى توقيع إلكتروني بواسطة الماسح الضوئي، ولكن يعيب هذا النوع أنه غير آمن على الإطلاق، وبالتالي يستطيع كل من يستعمل ذلك الجهاز الاستيلاء عليه، ولذلك نجد أن هذا النوع لا يستخدم على نطاق واسع، وغالباً لا يعترف به، وهناك نوع آخر يطلق عليه التوقيع الإلكتروني بواسطة رمز سري، ويتم التوقيع عبر إدخال بطاقة ممغنطة في آلة معدة لذلك مع إدخال الرقم السري والضغط بالموافقة

---

(١) عبدالحميد، ثروت، التوقيع الإلكتروني، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠٢م، ص ٥١.

(٢) الأباصيري، فاروق محمد أحمد، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٢م، ص ٧٩.

على إتمام العملية، وغالباً يتم ذلك على أجهزة الصرف الآلي أو سحب مبالغ أو تحويلات مالية[١].

ومن أشهر أنواع التوقيع الإلكتروني، ما يتم بإعطاء الموافقة على إتمام العقد بطريق استخدام شبكة الانترنت، وهو شائع الاستخدام في التسوق الإلكتروني، ومن تلك الصور ما يسمى التوقيع البيومتري؛ والذي يعتمد على الخصائص الذاتية للإنسان، كبصمة الإصبع، أو شبكية العين، أو الصوت، أو شكل الشفاه، أو الحمض النووي الجيني، ومن أكثر أنواع التوقيعات الإلكترونية أمناً وآخر ما توصلت إليه التكنولوجيا التقنية، هو التوقيع الرقمي الذي يقوم على وسائل التشفير الرقمي معتمداً على خوارزميات أو معادلات حسابية؛ لضمان سرية المعلومات والاتصالات بطريقة آمنة عبر تحويلها إلى معادلة رياضية، يتم قراءتها من صاحب المفتاح الذي يملك شفرتها[٢].

وتقوم جريمة الاعتداء على التوقيع الإلكتروني بتوافر الركن المادي للجريمة، والذي يتمثل في تغيير الحقيقة وذلك بالتلاعب في توقيع مخزن على الحاسب الآلي، أو التوقيع الإلكتروني الذي يتم إدخاله عن طريق الحاسب، ويكون ذلك بدون موافقة أو

---

(١) جميعي، حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٣٧.

(٢) الأباصيري، فاروق محمد أحمد، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، ص ٨٤.

علم صاحبه، مما يؤدي إلى إلحاق الضرر به أياً كانت صورته، وهو بذلك يشبه إلى حد كبير جريمة تزوير المستندات الإلكترونية[١].

وتحرص تشريعات التجارة الإلكترونية على تنظيم أحكام التوقيع الإلكتروني بما فيها الحماية الجنائية المقررة له، حيث أنه أمر لازم في التعاملات الإلكترونية، بما فيها عمليات التجارة الإلكترونية، وكذلك لئلا يتم انتهاك سرية البيانات والمعلومات الخاصة بها، ولهذا فقد أسبغ قانون التجارة الإلكتروني التونسي الصادر في عام (٢٠٠٠م) حماية جنائية على التوقيع الإلكتروني، وعاقب المخالفين بالسجن والغرامة، إذ نصت المادة (٤٧) منه على معاقبة الجاني بالسجن لمدة تتراوح بين ستة أشهر وعامين، والغرامة بين ألف وعشرة آلاف دينار، أو بإحدى هاتين العقوبتين، متى ما استعمل بصفة غير مشروعة عناصر التشفير الخاصة بإمضاء أو توقيع غيره[٢].

وعند مقارنة ما نص عليه القانون التونسي بالنظام السعودي نلحظ أن: النظام السعودي أكثر تشدداً في العقوبة، حيث نص نظام التعاملات الإلكترونية السعودي لسنة (١٤٢٨هـ) في (المادة الثالثة والعشرون) على مخالفة الدخول على منظومة توقيع إلكتروني لشخص آخر، دون تفويض صحيح أو نسخها أو إعادة تكوينها، أو الاستيلاء عليها، وفي (المادة الرابعة والعشرون) من ذات النظام فرض عقوبة السجن مدة لا تزيد على خمس سنوات أو الغرامة التي لا تزيد على خمسة ملايين ريال، أو بهما معا، مع

---

(١) القهوجي، علي عبدالقادر، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسة مقدمة لمؤتمر كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، في موضوع (القانون والكمبيوتر والانترنت)، في الفترة من ١-٣ لسنة ٢٠٠٠م، ص ٦٣.

(٢) حجازي، عبدالفتاح بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية/ دار النهضة العربية، القاهرة، الطبعة الأولى ٢٠٠٩م، ص٣٣٠.

إمكانية الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة[١].

(١) نظام التعاملات الإلكترونية لسنة ٢٠٠٧م بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٨ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

المطلب الثالث:
جريمة الاعتداء على البريد الإلكتروني:

فالخصوصية وإن لم تكن قضية تكنولوجية، فإنها تعتبر اليوم من أبرز القضايا الاجتماعية والأخلاقية في عصر تكنولوجيا الإعلام الآلي والانترنت، والاختراق يعد بمثابة انتهاك صريح للخصوصية أو ما يسمى بالخصوصية الإلكترونية وإن لم يكن هناك اتفاق حول مفهوم الخصوصية سواء على المستوى التشريعي أو الفقهي فإن الأمر الأكيد أن المراسلات بمختلف أنواعها تعتبر من بين الأمور الخصوصية للشخص، والتي لا يحق للغير **الاطلاع** عليها أو اعتراضها بأي وجه من الأوجه، ولا أدل على ذلك مما تم إقراره في مؤتمر رجال القانون الذي انعقد بستوكهولم في ماي١٩٦٧م فقد عرف الحق في الخصوصية بأنه حق المرء في أن يترك ليعيش حياته الخاصة بأقل درجات التدخل وحمايته من: مراقبة مراسلاته، والاستخدام السيئ لاتصالاته الشخصية الكتابية والشفوية، واستخدام المعلومات المأخوذة أو المعطاة بواسطته في حالات الثقة المهنية[1].

ومن أشهر جرائم انتهاك الخصوصية (**جرائم** البريد الإلكتروني) التي تمس الحياة الخاصة للأفراد، وسنتناول في هذا المطلب أهم الجرائم الواقعة على البريد الإلكتروني، وهما: جريمة انتهاك سرية رسائل البريد الإلكتروني، وجريمة تضخم البريد الإلكتروني.

---

(١) مشري، عبد الحليم، ضرورة تجريم الاعتداء على البريد الإلكتروني، مجلة العلوم القانونية،٢٠١٦م، ص٢٩٧.

الفرع الأول:
جريمة انتهاك سرية رسائل البريد الإلكتروني:

يُعرّف البريد الإلكتروني بأنه: تلك الرسالة التي تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل، كلياً أو جزئياً بوسيلة إلكترونية أو رقمية، وقد عرّفه القانون العربي النموذجي الموحد بأنه: نظام للتراسل باستخدام الحاسب لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقمياً في صندوق خاص وشخصي للمستخدم لا يمكن الدخول إليه إلا عن طريق كلمة مرور(١).

وبذلك فإن مجرد الدخول إلى موقع البريد الإلكتروني، والاطلاع على الرسائل الموجودة بداخله، بدون إذن من صاحبه، يعتبر انتهاكا لسرية المراسلات المكفولة بنصوص القانون(٢).

فالقانون يقر حماية المراسلات ويكفل سريتها، ومنها البريد الإلكتروني، فنتيجة الانتشار السريع لتكنولوجيا المعلومات وزيادة الاعتماد عليها في كافة نواحي الحياة، وبصفة خاصة في التجارة والمعاملات الإلكترونية، ازداد الاهتمام بسرية وخصوصية المعلومات الشخصية، ونتيجة تضخم حجم البيانات المتبادلة عبر البريد الإلكتروني ظهرت الحاجة الملحة لحماية البيانات والمعلومات، وتأمين تداولها عبر شبكة الإنترنت، وتختلف جريمة انتهاك سرية البريد الإلكتروني عن جريمة انتحال صفة شخصية صاحب البريد الإلكتروني، ذلك أنه إذا صاحب انتهاك سرية البريد

---

(١) فتح الله، محمود رجب، الوسيط في الجرائم المعلوماتية، ص٤٨٩.

(٢) كامل، حسام الدين، الحق في احترام الحياة الخاصة، دار النهضة العربية، القاهرة، ٢٠١٣، ص ١٣.

الإلكتروني مخاطبة الغير، أو توجيه أو استقبال مراسلات على البريد الإلكتروني المخترق، فهو يعتبر انتحال شخصية[١].

وبمراجعة نظام مكافحة الجرائم المعلوماتية السعودي نجد أنه لم يشر إلى تعريف محدد للبريد الالكتروني، أو بيان عقوبته بشكل خاص، ولكن ينطبق بحقه إدخاله في نطاق الموقع الإلكتروني، والذي عرّفه في الفقرة (العاشرة) من (المادة الأولى) بأنه مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد، وقد عاقب النظام المشار إليه مجرد الدخول غير المشروع إلى بريد إلكتروني، أو تغييره بأي شكل، أو التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو تهديد شخص، أو ابتزازه عن طريق البريد الالكتروني، أو أيّ موقع إلكتروني، بعقوبة السجن مدة لا تزيد على سنة، وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين[٢].

ومن ثم فإن الباحث يرى أن اختراق البريد الإلكتروني يُعد من مظاهر انتهاك الحق في الخصوصية، وعليه يستحق المخالف العقوبة المقررة نظاماً بحقه، وإن كان من الأولى تعديل النظام، وإضافة مادة تجرم انتهاك سرية البريد الالكتروني، وبيان عقوبتها بشكل مفصل في نظام مكافحة الجرائم المعلوماتية السعودي.

---

(١) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، ص٢٨٦.

(٢) نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

الفرع الثاني:
جريمة تضخم البريد الإلكتروني SPAM:

يعرّف مصطلح تضخيم البريد الإلكتروني أو ما يسمى (SPAM) بأنه: إرسال نسخ مكررة بعدد كبير من نفس الرسالة عبر البريد الإلكتروني، بما يترتب عليه عدم انتظام سير النظام المعلوماتي[١].

وعرفه آخرون بأنه: إرسال المجرم عشرات الرسائل دفعة واحدة لنظام البريد الإلكتروني عبر شبكة الانترنت، من خلال استعمال برامج تتمكن من التعرف على عناوين البريد الإلكتروني الموجودة في مختلف المواقع ومن ثم إرسالها للأفراد[٢].

وتتم جريمة تضخيم البريد الإلكتروني عن طريق وصول عدد ضخم من الرسائل مجهولة المصدر إلى حساب البريد الإلكتروني للمستلم النهائي، ويستخدم في إرسالها برامج معدة خصيصاً لذلك، وهى برامج متطورة لكونها تهدد قواعد البيانات بتضخيم قاعدة عمل البريد الإلكتروني، حيث يجد صاحبها نفسه أمام سيل منهمر من الرسائل الإلكترونية عديمة الفائدة، والتي قد يصاحبها فيروسات، أو صور، أو ملفات كبيرة الحجم، مما يترتب عليه إلغاء صندوق البريد على أثر تضخمه وتحميله فوق طاقته، مما قد يترتب عليه خسائر اقتصادية ضخمة، خاصة بالنسبة للشركات

---

(١) المكاوي، محمد محمود، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر، مصر، ٢٠١٠، ص١٣٢.

(٢) إبراهيم، خالد ممدوح، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية،، ٢٠٠٨، ص ١٤٠.

والمؤسسات العاملة في مجال التجارة الإلكترونية والتي تنتظر مئات الرسائل الإلكترونية يومياً بغرض إبرام الصفقات التجارية[١].

ويعد العدوان بتضخيم البريد الإلكتروني من أخطر صور الجرائم الواقعة على البريد الإلكتروني، إذ يؤدى إلى تعطل الشبكة، وعدم إمكانية استقبال أي رسائل، فضلاً عن إمكانية انقطاع الخدمة، أو يسبب حالة من عدم التوازن في التعامل التقني، من حيث حركة استدعائه والتعامل معه[٢].

ولا شك أن هذه الجريمة يكمن خطرها في تعطيل الميزة الأساسية للبريد الإلكتروني؛ ألا وهي السرعة العالية في إرسال البيانات واستقبالها في أي مكان في العالم يتوافر فيه شبكة للإنترنت، ولذلك فإن قيام الجاني بأي سلوك مادي للتعدي على البريد الإلكتروني بتضخيمه بأي طريقة كانت، بصورة عمدية تتحقق معها هذه الجريمة، وتتمثل في أي فعل يرتكبه الجاني، فيؤدي ذلك إلى تعطيله أو إيقافه عن العمل[٣].

وهناك العديد من الأمثلة لقوانين تجرم تضخيم البريد الإلكتروني، مثل: قانون ولاية أوهايو في أمريكا الصادر سنة (٢٠٠٢م) والذي نص على: تجريم رسائل البريد

---

(١) فريد، نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، ص٤٥.

(٢) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، ٢٠٠٩، ص ١٨٧.

(٣) حماد، حمزة عبدالكريم، جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية في القانون الإماراتي، مجلة جامعة الشارقة، الشارقة، المجلد ١٦، العدد ١، ٢٠١٩ص ٢٠٧.

مجهولة المصدر، واشترط أن تحتوي الرسائل الإلكترونية على اسم المرسل، وعنوانه الجغرافي، وعنوان بريده الإلكتروني[١].

أما يتعلق بالمنظم السعودي، فقد جرّم الاعتداء على تضخيم البريد الإلكتروني، من خلال (المادة الثانية) من نظام مكافحة الجرائم المعلوماتية، الذي يرمي إلى تحقيق الأمن المعلوماتي وحماية المصالح العامة والأخلاق، والآداب العامة، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية، والشبكات المعلوماتية، وعرّف الجريمة المعلوماتية بأنها: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية، لذلك نجد أن المنظم في الفقرة (العاشرة) من (المادة الأولى) التي عرفت الالتقاط بقولها: مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح، وبالتالي يتم معاقبة كل من يقوم بهذه الجريمة استناداً للمادة الثالثة من النظام المشار إليه، والتي تعاقب بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحداهما، كل من يقوم بمجرد الدخول غير المشروع إلى أيّ موقع إلكتروني، أو إلحاق الضرر به عبر وسائل تقنيات المعلومات المختلفة، أو التنصت على ما هو مرسل عن طريق الانترنت دون مسوغ نظامي صحيح، أو التقاطه، أو اعتراضه، ولا شك أن جريمة تضخيم البريد الإلكتروني داخلة في هذه الأفعال

---

(١) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٠٩م، ص٢٩٢.

الإجرامية، فإذا تحققت مع وجود القصد الجنائي بعنصريه: العلم والإرادة، فإن الجاني سيتعرض للعقوبة الواردة في (المادة الثالثة) من نظام الجرائم المعلوماتية[١].

(١) نظام مكافحة جرائم المعلوماتية لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

الخاتمة:

تناولت الدراسة موضوع جرائم الاعتداء المتعمد على نظم المعلومات، ومعرفة القواعد القانونية التي تحكم مختلف جوانب الحماية الجنائية المقررة لها، ومن ثم التوصل للنتائج والتوصيات التالية:

أولاً: النتائج:

(١) المعلومات تصلح لأن تكون محلاً للحقوق الشخصية والمالية، لذلك يجب أن تحمى بالنظام، وذلك للحفاظ قدر الإمكان على خصوصية المعلومات الخاصة بالأفراد من مخاطر الإنترنت واستخداماته.

(٢) نظام الجرائم المعلوماتية السعودي يجرم الدخول غير مشروع إلى كل موقع إلكتروني أو نظام معلوماتي؛ ويعاقب بالسجن والغرامة على كل من يخالف ذلك.

(٣) تظهر مخاطر تهديد جمع المعلومات عن الحياة الخاصة في أن الكثير من المؤسسات تجمع عن الأفراد بيانات عديدة، ومفصلة، تتعلق بالوضع المادي، أو الصحي، أو العائلي، أو العادات الاجتماعية عن الفرد، وتستخدم الحاسب الآلي وشبكات الاتصال في تخزينها، ومعالجتها، وتحليلها، والربط بينها، واسترجاعها، ومقارنتها، ونقلها، وهوما يجعل فرص الوصول إلى هذه البيانات على وجه غير مأذون به أو بطريق التحايل ممكناً.

(٤) المساس بالمعلومات الشخصية للأفراد قد يكون مصدره أشخاص مخربون يقومون بالاعتداء على البيانات الشخصية للآخرين وانتهاكها بشتى الصور.

(٥) يهدف النظام السعودي إلى الحد من وقوع الجرائم المعلوماتية، من خلال سن الأنظمة الحازمة، للمساعدة في تحقيق الأمن المعلوماتي، وحماية المصالح العامة، والأخلاق، والآداب العامة.

(٦) مجرد الدخول إلى موقع البريد الإلكتروني والاطلاع على الرسائل الموجودة بداخله، بدون إذن من صاحبه يعتبر انتهاكاً لسرية المراسلات المكفولة بنصوص النظام.

(٧) تتعدد صور جرائم البريد الإلكتروني التي تمس الحياة الخاصة للأفراد، منها: تهديد الغير من خلال البريد الإلكتروني، والتزوير.

(٨) تزوير المستندات الإلكترونية هو تغيير الحقيقة في المستند الإلكتروني، بإحدى طرق التغيير، كالتوقيع والحذف، والإضافة، والتعديل أو التغيير.

(٩) النظام السعودي يعتبر تزوير المستندات المعالجة آلياً يدخل في مفهوم التزوير، ويطبق بحق مرتكبيها العقوبات التي نص عليها النظام.

ثانياً: التوصيات:

(١) مراجعة نظام مكافحة الجرائم المعلوماتية السعودي الذي مضى على إصداره ما يقرب خمسة عشر عاماً؛ وذلك نظراً لتطور التقنيات والأجهزة الحديثة، مما يستلزم معه مواكبة النظام لهذا التطور؛ لحماية مستخدمي التقنية وردع المخالفين، خاصة مع وجود أشكال جديدة من السلوك الإجرامي المعلوماتي.

(٢) تطوير الأنظمة بالتوسع في حماية كل ما يمس المعلومات الشخصية للأفراد، من أجل تجنب مخاطر الإنترنت واستخداماته.

(٣) إصدار تشريع خاص بحماية المستندات الإلكترونية وتشديد عقوبة تزويرها.

(٤) تطوير مقررات كليات الأنظمة في الجامعات، بتدريس الأنظمة ذات العلاقة بالجرائم؛ لأهميتها، ولمعرفة المستجدات والتطورات التي تحدث فيها.

(٥) نشر الأحكام القضائية المكتسبة للقطعية المتعلقة بمخالفة أنظمة مكافحة الجرائم المعلوماتية، وذلك على نطاق واسع في وسائل التواصل الاجتماعي بكافة صوره؛ لتوعية المجتمع وردع المخالفين.

(٦) ضرورة إعداد كوادر أمنية متخصصة من الناحية الفنية والقانونية في الكشف والتحري والتحقيق في قضايا مكافحة الجرائم المعلوماتية، وما يلزم ذلك، من إنشاء مراكز متخصصة في هذا الشأن؛ لتطوير القائمين عليه.

(٧) جمع الأنظمة المتعلقة بالجرائم المعلوماتية والتعاملات الإلكترونية وحماية المعلومات الشخصية في نظام واحد؛ ليسهل تطبيقها، ومن ثم مكافحتها وعرضها على العامة وفهمها من قبل المختصين.

(٨) حث الجميع من خلال الوزارات المعنية في السعودية، وبخاصة وزارة التعليم، على تثقيف منسوبيها وطلابها بخطر جرائم الانترنت، وعدم الاستخدام السيئ له، وأن من يخالف ذلك سيتعرض للعقوبة والجزاء الرادع.

(٩) ضرورة التعاون بين الدول العربية والخليجية لمواجهة خطر إساءة استخدام الانترنت، وذلك بإقرار أنظمة وعقوبات موحدة رادعة للمخالفين، وتبادل الخبرات المعلوماتية والتحقيقية؛ للحد من آثارها المدمرة على الاقتصاد والأمن والمصلحة العامة.

(١٠) إلزام شركات الإنترنت بعدم نشر قاعدة بيانات المستفيدين لديهم، وتجريم ذلك، ومعاقبة المخالفين، حتى لا يتم استعمالها في الإضرار بالأفراد والمؤسسات بشكل خاطئ.

فهرس المصادر والمراجع:

١) **ابن منظور**، محمد بن مكرم، لسان العرب، دار صادر، ط٣، بيروت، ١٩٩٣م، ج١٢، ج١٥.

٢) **الأباصيري**، فاروق محمد أحمد، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٢م.

٣) **إبراهيم**، خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٠٩م.

٤) **إبراهيم**، خالد ممدوح، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م.

٥) **أحمد**، هلالى عبدالله، جرائم المعلوماتية التقليدية والمستحدثة، دار النهضة العربية، مصر، الطبعة الأولى، ٢٠١٣م.

٦) **أحمد**، هلالي عبدالله، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في ٢٣/ ١١/ ٢٠٠١م، دار النهضة العربية، القاهرة، الطبعة الأولي ٢٠٠٣م.

٧) **أيوب**، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، ٢٠٠٩.

٨) **جميعي**، حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م.

٩) **الجنبيهي**، منير محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥م.

١٠) **الدسوقي**، عبدالسميع، المحاسبة وتكنولوجيا المعلومات، دار النهضة، القاهرة، ١٩٩٣م.

١١) **حلمي**، يحيى مصطفى، أساسيات نظم المعلومات، مكتبة عين شمس، القاهرة، ٢٠٠٥م.

١٢) **حجازي**، عبدالفتاح بيومي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٢م.

١٣) **حجازي**، عبدالفتاح بيومي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، منشأة المعرف، الإسكندرية، الطبعة الأولى، ٢٠٠٩م.

١٤) **حجازي**، عبدالفتاح بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الاسكندرية/ دار النهضة العربية، القاهرة، الطبعة الأولى ٢٠٠٩م.

١٥) **الحسن**، عزة على محمد، الجريمة المعلوماتية في القانون السوداني، الزيتونة للطباعة، ٢٠٠٩م.

١٦) **حسين**، أحمد حسين علي، نظم المعلومات المحاسبية، الإطار الفكري والنظم التطبيقية، مكتبة الإشعاع الفنية، القاهرة، ١٩٨٨م.

١٧) **الحقباني**، رايز بن سالم، مهارات البحث والتحقيق في الجرائم المعلوماتية، كلية الملك فهد الأمنية، الرياض، ٢٠١٤.

١٨) **الحكيمي**، عبدالباسط محمد سيف، النظرية العامة للجرائم ذات الخط العام، رسالة دكتوراه، بغداد، ٢٠٠٠م.

١٩) **حماد**، حمزة عبدالكريم، جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية في القانون الإماراتي، مجلة جامعة الشارقة، الشارقة، المجلد ١٦، العدد ١، ٢٠١٩م.

٢٠) **دياب**، صلاح محمد أحمد، الحماية القانونية للحياة الخاصة للعامل وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية- مصر- ٢٠١٠م.

٢١) **رضوان**، هلال محمد، بحوث وآراء جديدة في مجال كشف التزييف والتزوير، عالم الكتب، ١٩٩٣م.

٢٢) **رمضان**، مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م.

٢٣) **الرومي**، محمد أمين، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٣م.

٢٤) **السند**، عبدالرحمن بن عبدالله، الأحكام الفقهية للتعاملات الإلكترونية "الحاسب الآلي وشبكة المعلومات، الإنترنت"، دار الوراق، دار النيرين للطباعة والنشر والتوزيع، بيروت، الطبعة الثالثة، ٢٠٠٦م.

٢٥) **الشاذلي**، فتوح عبدالله، جرائم التعزير المنظمة في المملكة العربية السعودية، مكتبة الرشد، الرياض، الطبعة الرابعة، ٢٠٢٠م.

٢٦) **الشناوي**، محمد، جرائم النصب المستحدثة (الإنترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)، دار الكتب القانونية، مصر المحلة الكبرى، ٢٠٠٨م.

٢٧) **الشوابكة**، محمد أمين، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الاردن،٢٠٠٩م.

٢٨) **عبدالحميد**، ثروت، التوقيع الإلكتروني، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠٢م.

٢٩) **عبدالله**، فهد بن سعد، الأحكام الشرعية والنظامية لجرائم تزوير المحررات الرسمية، مذكرة لنيل رسالة الماجستير، المعهد العالي للعلوم الأمنية، الرياض، ١٩٩٦م.

٣٠) **عطا الله**، شيماء عبد الغني محمد، الأحكام الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، ٢٠٠٧م.

٣١) **عودة**، عبدالقادر، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، ط١١، مؤسسة الرسالة، ج١.

٣٢) **الغافري وآخرون**، حسين الغافري و محمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، ٢٠٠٨م.

٣٣) **فتح الله**، محمود رجب، الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩م.

٣٤) **فريد**، نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، الطبعة الأولى، ٢٠٠٥م.

٣٥) قانون العقوبات الفرنسي المعدل الصادر ١٩٩٤م.

٣٦) قانون المبادلات والتجارة الإلكترونية التونسي **رقم** (١) **قانون عدد** (٨٣) **لسنة ٢٠٠٠م**.

٣٧) قورة، **عادل**، **محاضرات في قانون العقوبات**، **القسم العام ص**ـ ١٠٣) **منتديات** أستار **تايمز**، **بتاريخ** ٢٠١٤/ ١٢/ ٢٨ م،

https://www.startimes.com/f.aspx?t=36015683.

٣٨) **القهوجي**، علي عبدالقادر، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسة مقدمة لمؤتمر كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، في موضوع (القانون والكمبيوتر والانترنت)، في الفترة من ١-٣ لسنة ٢٠٠٠م.

٣٩) **كامل**، حسام الدين، الحق في احترام الحياة الخاصة، دار النهضة العربية، القاهرة، ٢٠١٣م.

٤٠) **مجموعة الأحكام القضائية**، المجلد الرابع والعشرون، وزارة العدل السعودية، مركز البحوث، ٢٠١٢م.

٤١) **الموسوعة الفقهية الكويتية**، وزارة الأوقاف والشؤون الإسلامية، الكويت، ط٣، ١٩٨٤م.

٤٢) **محمود**، عبدالله حسين علي، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠١م.

٤٣) **المكاوي**، محمد محمود، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر، مصر، ٢٠١٠.

٤٤) **مشري**، عبد الحليم، ضرورة تجريم الاعتداء على البريد الإلكتروني، مجلة العلوم القانونية، ٢٠١٦م.

٤٥) نظام التعاملات الإلكترونية **لسنة ٢٠٠٧م بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/١٨ بتاريخ ١٤٢٨/٣/٨هـ.**

٤٦) النظام الجزائي لجرائم التزوير **لسنة ١٤٣٥هـ بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/١١ وتاريخ ١٤٣٥/٢/١٨هـ.**

٤٧) **نظام مكافحة جرائم المعلوماتية** لسنة ٢٠٠٧م، بالمملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨هـ.

٤٨) **يوسف**، أمير فرج، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٨م.

References:

• ebn manzur, muhamad bin mukram, lisan alearabi, dar sadir, ta3, birut, 1993m, ji12, ji15.

• al'abasiri, faruq muhamad 'ahmadu, eaqad alaishtirak fi qawaeid almaelumat eabr shabakat alaintirnti, dar aljamieat aljadidati, al'iiskandiriat, 2002m.

• 'iibrahim, khalid mamduhin, aljarayim almaelumatiatu, dar alfikr aljamieii, al'iiskandiriati, altabeat al'uwlaa, 2009m.

• 'iibrahim, khalid mamduhi, hijiat albarid al'iiliktrunii fi al'iithbati, dar alfikr aljamieii, al'iiskandiriati, 2008m.

• 'ahmadu, halalaa eabdallah, jarayim almaelumatiat altaqlidiat walmustahdathatun, dar alnahdat alearabiati, masira, altabeat al'uwlaa, 2013m.

• 'ahmadu, halali eabdallah, aljawanib almawdueiat wal'iijrayiyat lijarayim almaelumatia (ealaa daw' aitifaqiat budabist almuaqaeat fi 23/11/2001m, dar alnahdat alearabiati, alqahirati, altabeat al'awalii 2003m.

• ayubi, bulin 'antunius, alhimayat alqanuniat lilhayaat alshakhsiat fi majal almaelumatiati, manshurat alhalabi alhuquqiati, lubnan, altabeat al'uwlaa ،2009.

• jamiei, hasan eabd albastu, 'iithbat altasarufat alqanuniat alati yatimu 'iibramuha ean tariq alaintirnti, dar alnahdat alearabiati, alqahirat, 2000m.

• aljinbihi, munir muhamad, jarayim al'iintirnit walhasib alali wawasayil mukafahataha, dar alfikr aljamieii, al'iiskandiriati, 2005m.

• aldisuqi, eabdalsamiei, almuhasibat watiknulujia almaelumati, dar alnahdati, alqahirati, 1993m.

• hilmi, yahyaa mustafaa ،'asasiaat nazam almaelumati, maktabat eayn shamsa, alqahirati, 2005m.

• hjazi, eabdalfataah biumi, altijarat al'iiliktiruniat wahimayatuha aljinayiyatu, dar alfikr aljamieii, al'iiskandiriati, 2002m.

• hijazi, eabdalfataah biumi, aljarayim almustahdathat fi nitaq tiknulujia alaitisalat alhadithati, munsha'at almaerifi, al'iiskandariati, altabeat al'uwlaa, 2009m.

• hjazi, eabdalfataah biumi, nahw siaghat nazariat eamat fi eilm aljarimat walmujrim almaelumati, munsha'at almaearifi,

alaskandiriati/dar alnahdat alearabiat, alqahirati, altabeat al'uwlaa 2009m.

• alhasani, eazat ealaa muhamad, aljarimat almaelumatiat fi alqanun alsuwdanii, alzaytunat liltibaeati, 2009m.

• hsin, 'ahmad husayn ealay, nazam almaelumat almuhasabiati, al'iitar alfikria walnuzum altatbiqiata, maktabat al'iisheae alfaniyati, alqahirat, 1988m.

• alhiqbani, rayiz bin salim, maharat albahth waltahqiq fi aljarayim almaelumatiati, kuliyat almalik fahd al'amniat, alrayad, 2014.

• alhakimi, eabdalbasit muhamad sif, alnazariat aleamat liljarayim dhat alkhati aleami, risalat dukturah, baghdad, 2000m.

• hmad, hamzat eabdalkrim, jarimat 'iighraq albarid al'iiliktrunii bialrasayil alaiqtihamiat fi alqanun al'iimarati, majalat jamieat alshaariqat, alshaariqat, almujalad 16, aleadad 1, 2019m.

• diab, salah muhamad 'ahmadu, alhimayat alqanuniat lilhayaat alkhasat lileamil wadamanatuha fi zili alwasayil altiknulujiat alhadithati, dar alkutub alqanuniati- masr- 2010m.

• ridwan, hilal muhamad, buhuth wara' jadidat fi majal kashf altazyif waltazwiri, ealam alkutub, 1993m.

• ramadan, midahat ramadan, alhimayat aljinayiyat liltijarat al'iilikturuniati, dar alnahdat alearabiati, alqahirati, 2001m.

• alruwmi, muhamad 'amin, jarayim alkumbiutar wal'iintirnti, dar almatbueat aljamieiati, aliaiskandiriat, 2003m.

• alsandi, eabdalrahman bin eabdallah, al'ahkam alfiqhiat liltaeamulat al'iiliktrunia "alhasib alali washabakat almaelumati, al'iintirntu", dar alwaraqi, dar alniyrin liltibaeat walnashr waltawzie, bayrut, altabeat althaalithati, 2006m.

• alshaadhli, fatuh eabdallah, jarayim altaezir almunazamat fi almamlakat alearabiat alsaeudiati, maktabat alrushdi, alrayadi, altabeat alraabieatu, 2020ma.

• alshanawi, muhamad, jarayim alnusb almustahdatha (al'iintirniti, bitaqat aliaytimani, aldieayat altijariat alkadhibatu), dar alkutub alqanuniati, misr almahalat alkubraa, 2008m.

• alshawabkatu, muhamad 'amin, jarayim alhasub waliantirnta, aljarimat almaelumatiatu, dar althaqafat lilnashr waltawziei, eaman, alardin,2009m.

• eabdalhamid, thurwat, altawqie al'iilikturuni, maktabat aljala' aljadidati, almansurati, 2002m.
• eabdallah, fahd bin saedu, al'ahkam alshareiat walnizamiat lijarayim tazwir almuharirat alrasmiati, mudhakiratan linayl risalat almajistir, almaehad aleali lileulum al'amniat, alriyad, 1996m.
• eta allah, shima' eabd alghani muhamad, al'ahkam alhimayat aljinayiyat liltaeamulat al'iiliktruniati, dar aljamieat aljadidati, 2007m.
• eawdatu, eabdalqadir, altashrie aljinayiyu al'iislamiu mqarnaan bialqanun alwadei, ta11, muasasat alrisalati, ji1.
• alghafiri wakhrun, husayn alghafiri wamuhamad al'alfi, jarayim al'iintarnit bayn alsharieat al'iislamiat walqanuni, dar alnahdat alearabiati, 2008m.
• fath allah, mahmud rajaba, alwasit fi aljarayim almaelumatiati, dar aljamieat aljadidati, al'iiskandiriati, 2019m.
• frid, nayilat eadil muhamad, jarayim alhasib alali alaiqtisadiati, manshurat alhalabii alhuquqiati, altabeat al'uwlaa, 2005m.
• qanun aleuqubat alfaransii almueadal alsaadir 1994m.
• qanun almubadalat waltijarat al'iilikturuniat altuwnusiu raqm (1) qanun eadad (83) lisanat 2000m.
• qurat, eadil, muhadarat fi qanun aleuqubati, alqism aleama sa-103) muntadayat 'astar taymiz, bitarikh
• 2014/12/28 mi, https://www.startimes.com/f.aspx?t=36015683.
• alqahwaji, eali eabdalqadir, alhimayat aljinayiyat lilbayanat almuealijat 'ilktrwnyaan, dirasat muqadimat limutamar kuliyat alsharieat walqanun bijamieat al'iimarat alearabiat almutahidati, fi mawdue (alqanun walkumbuyutir walaintirnti), fi alfatrat min 1-3 lisanat 2000m.
• kamil, husam aldiyn, alhaqu fi aihtiram alhayat alkhasati, dar alnahdat alearabiati, alqahirati, 2013m.
• majmueat al'ahkam alqadayiyatu, almujalad alraabie waleishruna, wizarat aleadl alsueudiatu, markaz albuhuthi, 2012m.
• almawsueat alfiqhiat alkuaytiati, wizarat al'awqaf walshuwuwn al'iislamiati, alkuayti, ta3, 1984m.
• mahmud, eabdallah husayn ealay, sariqat almaelumat almukhzanat fi alhasib alaly, dar alnahdat alearabiati, alqahirati, altabeat al'uwlaa, 2001m.

- almakawi, muhamad mahmud, aljawanib al'akhlaqiat waliajtimaeiat walmihniat lilhimayat min aljarayim almaelumatiati, almaktabat aleasriat lilnashri, masr, 2010.
- mashri, eabd alhalim, darurat tajrim aliaetida' ealaa albarid al'iilikturuni, majalat aleulum alqanuniati, 2016m.
- nizam altaeamulat al'iilikturuniat lisanat 2007m bialmamlakat alearabiat alsueudiati, alsaadir bialmarsum almalakii raqm mi/18 bitarikh 8/3/1428hi.
- alnizam aljazayiyi lijarayim altazwir lisanat 1435hi bialmamlakat alearabiat alsueudiati, alsaadir bialmarsum almalakii raqm ma/11 watarikh 18/2/1435hi.
- nizam mukafahat jarayim almaelumatiat lisanat 2007ma, bialmamlakat alearabiat alsueudiati, alsaadir bialmarsum almalakii raqm mi/17 bitarikh 8/3/1428hi.
- yusif, 'amir faraj, altawqie al'iilikturuniu, dar almatbueat aljamieiati, al'iiskandiriati, 2008m.

فهـــــرس الموضوعـــــات

المقدمة: ١٣٦٩

أهمية وأسباب اختيار البحث: ١٣٦٩

هدف البحث: ١٣٧١

مشكلة البحث: ١٣٧١

منهج البحث: ١٣٧٢

تقسيم البحث: ١٣٧٢

مبحث تمهيدي: الأحكام العامة لجرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقا للنظام السعودي ١٣٧٣

المطلب الأول: مفهوم جرائم الاعتداء المتعمد ١٣٧٣

المطلب الثاني: مفهوم نظم المعلومات الإلكترونية ١٣٧٥

المبحث الأول: جرائم الاعتداء على نظم المعلومات الإلكترونية ١٣٧٧

المطلب الأول: جريمة سرقة المعلومات: ١٣٧٨

المطلب الثاني: جريمة تدمير المواقع وتشويهها: ١٣٨٥

المطلب الثالث: جريمة انتهاك سرية البيانات الإلكترونية والاستيلاء عليها: ١٣٩٠

المبحث الثاني: جريمة تزوير المستندات الإلكترونية وجريمة الاعتداء على التوقيع والبريد الإلكتروني.. ١٣٩٧

المطلب الأول: جريمة تزوير المستندات الإلكترونية: ١٣٩٨

المطلب الثاني: جريمة الاعتداء على التوقيع الإلكتروني: ١٤٠٤

المطلب الثالث: جريمة الاعتداء على البريد الإلكتروني: ١٤٠٩

الفرع الأول: جريمة انتهاك سرية رسائل البريد الإلكتروني: ١٤١٠

الفرع الثاني: جريمة تضخم البريد الإلكتروني SPAM: ١٤١٢

الخاتمة: ١٤١٦

أولاً: النتائج: ١٤١٦

ثانياً: التوصيات: ١٤١٨

فهرس المصادر والمراجع: ١٤٢٠

REFERENCES: ١٤٢٦

فهـــــرس الموضوعـــــات ١٤٣٠