جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها
كلية الشريعة والقانون بالقاهرة
جامعة الأزهر

العدد الرابع والأربعون
نوفمبر ٢٠٢٤م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية – كلية الشريعة والقانون – القاهرة – الدراسة – شارع جوهر القائد

ت: ٢٥١٠٧٦٨٧

فاكس: ٢٥١٠٧٧٣٨

https://mawq.journals.ekb.eg/

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

١٨٠٥٣ / ٢٠٢٤

الترقيم الدولي للطباعة

ISSN: 2812–4774

الترقيم الدولي الإلكتروني:

ISSN: 2812–5282

الحماية الجنائية للتوقيع الإلكتروني
في القانون الأمريكي والكويتي

Criminal Protection of Electronic Signature in US and Kuwaiti Law

إعداد

د. نايف شافي المظافره الهاجري

أستاذ القانون الجزائي المشارك

أكاديمية سعد العبدالله للعلوم الأمنية

دولة الكويت

الحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي

نايف شافي المظافره الهاجري
قسم المقررات القانونية، أكاديمية سعد العبدالله للعلوم الأمنية، دولة الكـــويت.
البريد الإلكتروني: **bo.shafi2007@gmail.com**

ملخص البحث :

عند تناول موضوع الحماية الجنائية للتوقيع الالكتروني في النظم القانونية (الأمريكي والكويتي)؛ فإن ثمة اتجاهين متعارضين في هذا الشأن، حيث يؤكد أنصار الاتجاه الأول أن التشريعات الأمريكية والكويتية قد اهتمت بهذا الجانب، وقامت بتدشين بيئة تشريعية في هذا الموضوع، خاصة أن التوقيع الإلكتروني يُعدّ حجة في مسألة الإثبات القانوني.

في حين يرى أنصار الاتجاه الثاني أن هناك قصورًا في تلك التشريعات حيال جرائم التوقيع الإلكتروني؛ لعدة أسباب، منها: حداثة هذه الجرائم، الى جانب القصور التشريعي، وضعف الخبرة الفنية في التعامل مع جرائم التوقيع الإلكتروني.

وترتيبًا على ما سبق: يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس، على النحو التالي:

ما آليات الضبط التشريعي للحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي؟

تساؤلات الدراسة:

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

١) ما أشكال الجرائم التي يرتبها التوقيع الإلكتروني للعقود عبر الوسائط الالكترونية؟

٢) كيف تعاطت التشريعات الأمريكية والكويتية مع جرائم التوقيع الإلكتروني؟

٣) كيف يمكن تفعيل آليات الضبط التشريعي لتحقيق الحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي؟

منهجية الدراسة

يعتمد الباحث في هذه الدراسة على المنهج الوصفي والمنهج المقارن.

الكلمات المفتاحية: الحماية الجنائية، التوقيع الإلكتروني، القانون الأمريكي، القانون الكويتي.

Criminal Protection of Electronic Signature in US and Kuwaiti Law

Nayef Shafi Al-Muzhafera Al-Hajri
Department Of Legal Courses, Saad Al Abdullah Academy For Security Sciences, State Of Kuwait.
E-mail: bo.shafi2007@gmail.com

Abstract:

When dealing with the issue of criminal protection for the electronic signature in the comparative legal systems (American and Kuwaiti), there are two conflicting trends in this regard, as the supporters of the first trend assert that the American and Kuwaiti legislations have paid attention to this aspect and have launched a legislative environment in this matter, especially since the electronic signature is an argument In the matter of legal proof.

While the supporters of the second trend believe that there are shortcomings in these legislations regarding electronic signature crimes for several reasons, including the novelty of these crimes in addition to the legislative shortcomings and the weak technical expertise in dealing with electronic signature crimes.

Based on the above, the researcher can formulate the research problem of the current study in the form of a main question as follows:

What are the legislative control mechanisms for the criminal protection of the electronic signature in the US and Kuwaiti law?

Study questions

The current study poses a set of the following sub-questions:

1) What are the forms of crimes committed by the electronic signature of contracts through electronic media?

2) How did the US and Kuwaiti legislation deal with electronic signature crimes?

3) How can legislative control mechanisms be activated to achieve criminal protection for electronic signatures in US and Kuwaiti law?

Study methodology

In this study, the researcher relies on the descriptive approach and the comparative approach.

Keywords: Criminal protection, Electronic signature, American law, Kuwaiti law.

مقدمـــة

لاشك أن العقود الإلكترونية تُعدّ من أبرز أنواع العقود الاستهلاكية التي تتم بين المتعاقدين عبر شبكة الإنترنت، وعلى الرغم من فاعلية هذه العقود، إلا أنها تثير العديد من الإشكاليات المرتبطة بالجرائم التي تنجم عن إبرام تلك العقود، وهو أمر يثير -بدوره- مسألة البحث حول الحماية الجنائية للعقود الإلكترونية، وإذا كانت التشريعات قد وقفت - فيما سبق- أمام فكرة التعاقد بواسطة التلكس أو الهاتف؛ فإنها -من جديد- تقف أمام مسألة استخدام نُظُم الكمبيوتر وشبكات المعلومات في التعاقد؛ فيما انتجته الحواسيب والشبكات من مخرجات، وبحث مدى حجية مستخرجات الحاسوب، والبريد الإلكتروني E-Mail، وقواعد البيانات المخزنة داخل النظم وغيرها. واستخدام وسائل تقنية المعلومات لإبرام العقود والتصرفات القانونية، وتبادل البيانات، وإجراء عمليات تتصل بالذمة المالية؛ قد أثار ويثير العديد من الإشكالات حول مدى اعتراف القانون، وتحديدًا قواعد التعاقد بهذه الآليات الجديدة للتعبير عن الإيجاب والقبول وبناء عناصر التعاقد، كما أثارت وتثير إشكالات في ميدان الإثبات بكون النظم القانونية قد حددت الأدلة المقبولة وحددت قواعد الاحتجاج بها وسلامة الاستدلال منها[١].

وفي خِضَمّ البحث في الحماية الجنائية للتعاقد الإلكتروني؛ ظهرت التجارة الإلكترونية بوصفها نمطا جديدا من أنماط التعامل التجاري في ميادين التعاقد كافة، كعقود التأمين والخدمات وغيرها. وأثارت التقنية العالية -وتحديدًا محتواها الفني والمعرفي- تحديات كبيرة في ميدان نقل التكنولوجيا والتبادل الفني والمعرفي والتزام مورد التكنولوجيا ومتلقيها، وأظهرت التقنية تحديات قانونية تستلزم التنظيم بالنسبة لعقود تقنية المعلومات، التوريد والبيع والصيانة والتطوير ورخص الاستخدام، وبالنسبة لعقود الوكالات التجارية والتوزيع، وعقود اشتراكات المعلوماتية وخدمات الاتصال، وكان - وسيبقى إلى حين - أوسع أثر لها في حقل التجارة الالكترونية والتعاقد الإلكتروني[٢].

---

(1) Under Federal Rules of Evidence, electronic evidence is admissible if it complies with traditional evidentiary principles, i.e. it must be relevant, authenticated, and not subject to exclusion on hearsay or other grounds. See Lorraine v. Markel Am. Ins. Co., Inc., 241 FRD 534 (D. Md. 2007). See also Fed. R. Evid. 902(13) (a record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person, is self-authenticating and requires no extrinsic evidence of authenticity in order to be admitted); Fed. R. Evid. 803(6) (hearsay exception for business records).

(2) Bert Swart, "Modes of International Criminal Liability", in: Antonio Cassese, The Oxford Compaion to International Criminal Justice, Oxford University Press, 2009. Bajan, Peter, (1998). New Communities , New Social Norms. Studia-Psychologica. V. 40 (4.

ويحتاج المستهلك إلى الحماية، سواء على المستوى الوطني أو الدولي، وتنبع أهمية توفير حماية المستهلك من أنه يمثل الطرف الضعيف في العملية التعاقدية، فالرغبة في الربح السريع دفعت العديد من التجار والمنتجين، ومقدمي الخدمات لاتباع أساليب غير مشروعة للإثراء السريع، باستخدام وسائل الغش والخداع المختلفة، ومن هنا تظهر أهمية التعريف بالمستهلك الذي نسعى لتوفير الحماية له، وبعد اتساع مستخدمي الإنترنت في العالم؛ بدأ يتبلور مفهوم الحماية الإلكترونية للمستهلك، والذي يعني الحفاظ على حقوق المستهلك وحمايته من الغش أو الاحتيال أو شراء بضائع مغشوشة باستخدام أدوات شبكة الإنترنت التي تستطيع الوصول إلى كل مكان، وتمارس تأثيرًا يتجاوز -أحيانًا- الأدوات التقليدية في الواقع[١].

ولقد اتجهت النظم القانونية والقضائية والفقهية -بوجه عام- الى قبول وسائل الإثبات التي توفر - من حيث طبيعتها- موثوقية في إثبات الواقعة وصلاحية للدليل محل الاحتجاج، وتحقق فوق ذلك وظيفتين، هما: إمكان حفظ المعلومات لغايات المراجعة عند التنازع، التوسط في الإثبات عن طريق جهات الموثوقية الوسيطة أو سلطات الشهادات التعاقدية، ومن هنا قَبِل نظام (سويفتSWIFT) التقني لغايات الحوالات البنكية، وكذا نظامي شيبس وشابس ونحوهما، وكذلك قَبِل التلكس لتحقيقهما هذه الطبيعة والوظائف، في حين بقي الفاكس خارج هذا الإطار ومجرد دليل ثبوت بالكتابة أو بينة مقبولة ضمن شرائط خاصة، ومن هنا -أيضًا- أثارت وتثير الرسائل الإلكترونية عبر شبكات المعلومات، كالإنترنت والرسائل المتبادلة عبر الشبكات الخاصة (الإنترانت) والبريد الإلكتروني مشكلة عدم تحقيق هذه الوظائف في ظل غياب المعايير والمواصفات والتنظيم القانوني الذي يتيح توفير الطبيعة المقبولة للبيانات وتحقيق الوظائف التي تجيز قبولها في الإثبات[٢].

والتحديد القانونيِ للرّسائل الإلكترونيةِ يثير السّؤال حول ما إذا كانت قوانين الإثبات في الولايات المتحدة الأمريكية تنظم وتحكم المعلومات المتبادلة إلكترونيًا (electronically) مثلما تنظم وتحكم المستندات والرسائل والمخاطبات الصادرة عن طريق الوسائلِ الورقيةِ

---

(1) NY GOL §5-1401 (parties to a contract that involves at least $250,000 may select New York law to govern their rights and duties under such contract, without requiring any other connection to New York).

(2) See, e.g., Naldi v. Grunberg, 80 A.D.3d 1, 11 (N.Y. App. Div. 1st Dept. 2010) (holding an email to be capable of satisfying the statute of frauds contained in New York General Obligations Law § 5-703); Newmark & Co. Real Estate Inc. v. 2615 East 17 Street Realty LLC (N.Y. App. Div. 1st Dept 2011) (holding an email to be capable of satisfying the statute of frauds contained in New York General Obligations Law § 5-701).

التّقليدية، فتعبير "رسالة إلكترونية" يَعْني المعلومات: المدخلة، المرسلَة؛ المستلمة أو المخَزنةَ بالوسائلِ الإلكترونيةِ، ويشمل ذلك -لا بشكل حصري- البيانات الإكترونية المتبادلة، بريد إلكترونيE-MAIL، برقية، تلكس. ونجد العديد من التّشريعات تنظم وتستخدم وتشير الى تعبيرات، مثل: "كِتابَة Writing"، " توقيع Signature "، " وثيقة Document "، " أصلي Original "، "نسخة مطابقة"، "نشر"، "ختم"، "سجل"، "ملف"، "طبعة"، "سجل"، "يُسلّمُ "، إلخ[١]. ومن المهم التنبه إلى أن المقصود بالرسائل الإلكترونيةِ الشكل الإلكتروني أو الرقمي، ولَيسَ الشّكلَ الورقيَ اللاحقَ، حينما يتم استخراج الرسائل الإلكترونية (طباعتها) على الورق. فإذا أخضعنا هذه الحقائق للتحليل؛ نجد أن التعاريف المستقرة بالمفاهيم القانونية والعرفية والقضائية تعرف الكِتابَة بما يفيد أنها يجب أَن تكونَ نتيجةَ فعل يد شخصٍ أو بالطّباعةِ. وتعرف الطباعة بأنها يَجِب أَن تكُونَ نتيجةَ الفعلِ بإفراغ الرسالةِ على "ورقة". من هنا لا يشمل ذلك الرسائل الإلكترونية. وتعرف التوقيع بأنه يَتضمّنُ قيام شخصٍ بفعل "التوقيع"، أي وضع الرمز الكتابي الدال على شخصيته، وهذا الفعل لا يشمل التحديد الرقمي الدال على الشخص في بيئة التجارة والأعمال الإلكترونية. كما أن مفهوم الوثيقة يتعلق بالكتابَة، "ومن هنا تكون محصورة بالوثائق الورقيةِ. وبالتالي فإن تعبير "كِتابة " لا يشمل الرسائل الإلكترونيةِ. وهذا ينطبق على التعابير الأخرى، مثل " وثيقة "، " توقيع "... إلخ. بوصفها محصورة في المظاهر المادية الورقية [٢] . وهذا قد يؤثر على مستقبل التنظيم القانوني للتجارة والأعمال الإلكترونية، بل ومستوى تطورها. أو خيار تعديل التشريعات القائمة لجهة اعتبار تعبيرات الكتابة والوثيقة والتوقيع و.... إلخ شاملة للرسائل والتواقيع الإلكترونية. ومشكلة ذلك: سعة نطاق التعديل وصعوبته، والأهم حاجته الى دراسة شاملة

---

(1) See, e.g., Ceglia v. Zuckerberg, 2013 WL 1208558, at *4-6, *16, *73 (W.D.N.Y. Mar. 26, 2013) (holding a contract with a handwritten signature, later scanned and emailed as a .pdf file, to be valid)

17 See, e.g., People v. Johnson, 31 Misc.3d 145(A) (Sup. Ct. App. Term 2011) (holding that a police officer's electronic facsimile signature was valid and admissible in court).

(2) Please refer to: U.S. EPA Electronic Signature Procedure (April 2018) https://www.epa.gov/sites/production/files/2018-4/documents/electronic_signature_procedure.pdf accessed in 3March 2023

• U.S. EPA eReporting Policy Memorandum https://www.epa.gov/sites/production/files/2016-03/documents/epa-ereporting-policy-statement-2013-09-30.pdf accessed in 3March 2023

• U.S. EPA Information Technology (IT) Architecture Standards Profile http://cfint.rtpnc.epa.gov/oito/itarchitecture/standards.cfm accessed in 3March 2023

لكافة تشريعات النظام القانوني. أو خيار إصدار تشريع خاص بمفهوم الرسائل الإلكترونية، وهي طريقة إحالة إلى سائر التشريعات الأخرى، بحيث ينص على أن مفهوم الكتابة والوثيقة والتوقيع وغيرها بأنه يشمل الرسائل والتواقيع الإلكترونية أينما وردت، وهذا الخيار يمثل ما يمكن تسميته بتشريع أوَّليّ، لا يعالج مسائل التجارة والأعمال الإلكترونية بشكل شامل، إنما أحد تحدياتها. والخيار الأخير الذي نتبناه إصدار تشريع للحماية الجنائية للتعاقد الإلكتروني ينظم مكافحة جرائم التوقيع الإلكتروني وغيرها، وهذا الخيار أو المسلك هو ما تتجه إليه مختلف النظم القانونية القائمة في تعاملها مع تلك الجرائم المرتبطة بالعقود الإلكترونية[(١)] .

مشكلة الدراسة:

عند تناول موضوع الحماية الجنائية للتوقيع الإلكتروني في النظم القانونية (الأمريكي والكويتي)؛ فإن ثمة اتجاهين متعارضين في هذا الشأن؛ حيث يؤكد أنصار الاتجاه الأول أن التشريعات الأمريكية والكويتية قد اهتمت بهذا الجانب، وقامت بتدشين بيئة تشريعية في هذا الموضوع، خاصة أن التوقيع الإلكتروني يُعدّ حجة في مسألة الإثبات القانوني.

في حين يرى أنصار الاتجاه الثاني أن هناك قصورًا في تلك التشريعات حيال جرائم التوقيع الإلكتروني؛ لعدة أسباب، منها: حداثة هذه الجرائم، الى جانب القصور التشريعي، وضعف الخبرة الفنية في التعامل مع جرائم التوقيع الإلكتروني.

وترتيبًا على ما سبق: يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس، على النحو التالي:

ما آليات الضبط التشريعي للحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي؟

تساؤلات الدراسة:

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

٤) ما أشكال الجرائم التي يرتبها التوقيع الإلكتروني للعقود عبر الوسائط الالكترونية؟

٥) كيف تعاطت التشريعات الأمريكية والكويتية مع جرائم التوقيع الإلكتروني؟

---

(1) National Institute of Standards and Technology (NIST), Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) (March 2023). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

• NIST, Security Requirements for Cryptographic Modules (FIPS 140-2) (March 2023) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

٦) كيف يمكن تفعيل آليات الضبط التشريعي لتحقيق الحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي؟

أهمية الدراسة:

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

١- حداثة موضوع الدراسة على المستوى الكويتي؛ إذ يجد الباحث ندرة في الكتابات الأكاديمية العربية التي سعت للخوض في هذا الموضوع، خاصة في الجانب المقارن مع التشريع الأمريكي.

٢- يستمد هذا الموضوع أهميته من طبيعة هذه العقود الإلكترونية ودورها؛ فهذه العقود الإلكترونية تُعدّ حديثة على المجتمع الكويتي، وتحتاج للمزيد من الإهتمام والدراسة.

٣- الوقوف على بعض الجوانب والنقاط المهمة والمؤثرة في موضوع الحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي والكويتي، وعلاقتها بخلق عوالم جديدة من التحديات أمام القضاء العربي والعالمي.

٤- تمهيد الطريق أمام إجراء عدد من الدراسات التي تناولت الموضوعات المماثلة لموضوعنا هذا بصورة علمية وشاملة، والتي تضيف المزيد من المتغيرات المؤثرة في هذه الدراسة، بما يسهم في تحقيق التراكم المعرفي والبحث.

منهجية الدراسة

يعتمد الباحث في هذه الدراسة على المناهج التالية:

١- المنهج الوصفي:

وذلك من خلال مراجعة الدراسات ذات الصلة بالموضوع، من كتب ورسائل علمية ودراسات وأبحاث ودوريات وندوات وغيرها، سواء باللغة العربية أو باللغة الانجليزية، مع السعي نحو تحديد المفاهيم الموجودة بها مع إيضاح العلاقات بين هذه المفاهيم؛ حتى يمكن الوصول إلى إطار نظري دقيق يستعين به الباحث في دراسته.

٢- المنهج المقارن:

وذلك من خلال دراسة وتحليل التشريع الكويتي والأمريكي التي تتناول الحماية الجنائية للتوقيع الإلكتروني، ويتم ذلك من خلال معالجة وتحليل المواد والنصوص القانونية في القانون الأمريكي والكويتي.

الإطار المفاهيمي

لقد عَرَّفت لجنة التجارة الدولية -التابعة للأمم المتحدة- التوقيع الإلكتروني بأنه: "مجموعة أرقام تمثل توقيعًا على رسالة معينة"، يتحقق هذا التوقيع من خلال اتباع بعض الإجراءات الحسابية المرتبطة بمفتاح رقمي خاص بالشخص المُرسِل، ومن ثمة فإنه -

بالضغط على هذه الأرقام الخاصة بمستخدم الإنترنت- يتكون التوقيع الإلكتروني، ويمكن أن يتم تحديد هذه الأرقام الخاصة من خلال اتفاقيات جماعية لمستخدمي الإنترنت في المعاملات التجارية أو من خلال عقد مبرم بين الطرفين يحدد الرقم السري الخاص بكليهما، بحيث إن اقتران الرسالة المرسلة بهذه الأرقام يستطيع الشخص أن يحدد شخصية المتعاقد الذي أرسل الرسالة، وهذا يعني إمكانية تعدد التوقيع الإلكتروني بتعدد المعاملات التي يقوم بها الشخص [١].

كما أوردت التعليمة الأوربية -المؤرخة في ١٣ ديسمبر ١٩٩٩ في المادة ٢ منه- تعريفًا للتوقيع الإلكتروني بأنه عبارة عن: "معلومات أو معطيات في شكل إلكتروني، ترتبط أو تتصل منطقيًا بمعطيات إلكترونية أخرى، وتستخدم كوسيلة لإقرارها" [٢].

ومن التعاريف التي اقترحها الفقهاء: التعريف القائل بأن التوقيع الإلكتروني هو: "اتباع مجموعة من الإجراءات أو الوسائل التقنية التي يتاح استخدامها عن طريق الرمز أو الأرقام أو الشفرات، بقصد إخراج علامة مميزة لصاحب الرسالة التي نقلت إلكترونيا" [٣].

كما هو واضح من خلال تعريفات التوقيع الإلكتروني؛ فإنه يتميز عن التوقيع التقليدي من خلال خصائصه التي نوردها فيما يلي:

- أن التوقيع الإلكتروني - وعلى العكس من التوقيع الكتابي- لا يقتصر على الإمضاء أو بصمة الأصابع، بل يشمل صورًا لا يمكن حصرها، منها: الحروف، والأرقام، والصور، والرموز، والإشارات، وحتى الأصوات؛ كل ذلك بشرط أن يكون لها طابع فردي، يسمح بتمييز الشخص صاحب التوقيع، وتحديد هويته، وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه؛ فالتوقيع الإلكتروني على رسالة ما أو وثيقة

---

(1) Pipitone, T. (2012). Cops, prosecutors botched Casey Anthony evidence. Click Orlando [online]. As of December 3, 2014: http://www.clickorlando.com/news/Cops-prosecutors-botched-Casey-Anthony-evidence/17495808 accessed in 15 Mar2023

(2) See International Law Enforcement Cooperation Report, supra note 3, at 26-27; Press Release, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges, U.S. Dep't of Justice , https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; Press Release, Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars, U.S. Dep't of Justice , https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-d accessed in 17 Mar2023

هو عبارة عن بيانات مجتزأة من الرسالة ذاتها (جزء صغير من البيانات) يجرى تشفيره[١] وإرساله مع الرسالة؛ بحيث يتم الاستيثاق من صحة صدور الرسالة من الشخص عند فك التشفير، وانطباق محتوى التوقيع على الرسالة[٢].

- أن التوقيع الإلكتروني يتميز بأنه لا يتم عبر وسيط مادي، أي دعامة ورقية، بحيث تذيل به الكتابة، كما هو الحال بالنسبة للتوقيع الكتابي، وإنما يتم كليًا أو جزئيًا عبر وسيط إلكتروني من خلال أجهزة الكمبيوتر، أو عبر الإنترنت، بحيث يكون بإمكان أطراف العقد الاتصال ببعضهم البعض والاطلاع على وثائق العقد، والتفاوض بشأن شروطه وإفراغ هذا العقد في محررات إلكترونية، وأخيرًا التوقيع عليها إلكترونيًا[٣].

---

(١) ويرتبط التوقيع الإلكتروني بالتشفير ارتباطًا عضويًا؛ فالتشفير هو عملية لتغيير البيانات، بحيث لا يمكن قراءتها إلا من قِبَل الشخص المستخدم وحده باستخدام مفتاح فك التشفير. والطريقة الشائعة للتشفير تتمثل في وجود مفتاحين: المفتاح العام، وهو معروف للعامة، ومفتاح خاص، يتوفر - فقط- لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لأي شخص يملك المفتاح العام أن يرسل الرسالة المشفرة، لكن لا يستطيع أن يفك شفرتها إلا الشخص الذي لديه المفتاح الخاص. ويجب -في هذا الصدد- عدم الخلط بين التوقيع الإلكتروني وبين تشفير الرسالة الإلكترونية، فصحيح أن كليهما يقوم على عملية حسابية يتم من خلالها تشفير مضمون التوقيع أو الرسالة، لكن هناك فرق، هو: أن تشفير الرسالة يشملها بأكملها، في حين أن التشفير في التوقيع الإلكتروني يقتصر فقط على التوقيع دون بقية الرسالة، بحيث يمكن أن يكون مرتبطًا برسالة غير مشفرة.

FBI, Internet Crime Report 2021, supra note 13, at 15-16; see, e.g., Press Release, Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators, U.S. Dep't of Justice (Mar 19, 2023), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware

(2) See International Law Enforcement Cooperation Report, supra note 3, at 1-2, 11. However, even VASPs ostensibly located outside the United States may still have obligations under the BSA if they qualify as domestic financial institutions, including by doing business wholly or in substantial part in the United States. See, e.g., 31 C.F.R. § 1010.100(f).

(3) Based, P., Security, D., Rudolf, R., & Physics, A. (1997). The list of paper based valuable documents is nearly interminable and extends from. 437, 28–30.

CISA. (n.d.). Security Tip (ST04-018) Understanding Digital Signatures. 2009. https://www.us-cert.gov/ncas/tips/ST04-018#:~:text=A digital signature—a type,%2C or a digital document).&text=Digital signatures are significantly more secure than other forms of electronic signatures

- لزوم تدخل طرف ثالث يقوم بدور الوسيط بين أطراف العقد؛ حيث استلزمت ضرورة الأمن القانوني وجوب استخدام تقنية آمنة في التوقيع الإلكتروني تسمح بالتعرف على شخصية الموقع [١]، وسوف يتم تفصيل هذه الخاصية عند معالجة حجية التوقيع الإلكتروني.

وللتوقيع الإلكتروني صورتان شائعتان، إحداهما التوقيع الرقمي وآخر بيومتري.

أولًا: التوقيع الرقمي Digital signature.

يطلق عليه -أيضًا- اسم التوقيع الكودي Key based signature، تقوم هذه التقنية بتزويد الوثيقة الإلكترونية بتوقيع مشفر يمكنه تحديد الشخص الذي قام بتوقيعها، والوقت الذي قام فيه بتوقيعها، ومعلومات أخرى خاصة بصاحب التوقيع.

ثم يسجل التوقيع الرقمي بشكل رسمي عند جهات تعرف بسلطات التوثيق Autorités de certification [٢]، ويتم هذا التوقيع بوجود مفتاحين: مفتاح عام، وهو معروف للكافة،ومفتاح خاص يتوفر فقط لدى الشخص الذي أنشاه. ويمكن بهذه الطريقة لأي شخص يملك المفتاح العام أن يرسل الرسائل المشفرة، لكن لا يستطيع أن يفك شفرة الرسالة إلا الشخص الذي لديه المفتاح الخاص، ويستخدم هذا النظام خاصة في التعاملات البنكية. وأوضح مثال على ذلك: بطاقة الائتمان التي تتضمن رقمًا سريًّا لا يعرفه إلا الزبون الذي يدخل بطاقته في آلة السحب، عندما يطلب الاستعلام عن حسابه، أو يبدي رغبته في صرف جزء من رصيده. ويمكن تلخيص مزايا هذا التوقيع فيما يلي:

- أنه يؤدي إلى إقرار المعلومات التي يتضمنها السند أو التي يهدف إليها صاحب التوقيع.
- يسمح بإبرام العقود عن بُعد، وذلك دون حضور المتعاقدين جسديًا في ذات المكان، الأمر الذي يساعد في ضمان وتنمية التجارة الإلكترونية.
- هو وسيلة مأمونة لتحديد هوية الشخص الذي قام بالتوقيع.

أما أكبر سلبية من سلبيات التوقيع الرقمي فتتمثل في أن احتمال تعرض الرقم السري أو الكودي للسرقة أو الضياع أو التقليد، مما يجعل صاحبه ملزمًا بِسِرِّيَّة رقمه، وفي حالة تَسَرُّب الرقم للآخرين فيعد هو المسؤول عن الآثار المترتبة على ذلك، مادام لم يراعِ قواعد الحيطة والحذر، إلا إذا قام بالإبلاغ عن سرقته أو فقدانه إلى سلطات التوثيق أو البنك[٣].

---

(1) Zhong, Y. (2013). Secure digital certificate design based on the RSA algorithm. Journal of Digital Information Management, 11(6), 423–429.

(2) Hosseini Seno, S., Budiarto, R., & Wan, T.-C. (2011). A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority. Arabian Journal for Science and Engineering, 36(2), 245–257.

(3) D. Kah. (1996). TheCodebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.

Garain, U., & Halder, B. (2008). On automatic authenticity verification of printed security documents. Proceedings - 6th Indian Conference on

ثانيًا: التوقيع البيو متري Biométric Signature

يعتمد التوقيع البيو متري على تحديد نمط خاص تتحرك به يد الشخص الموقع أثناء التوقيع؛ إذ يتم توصيل قلم إلكتروني بجهاز كمبيوتر، ويقوم الشخص بالتوقيع باستخدام هذا القلم الذي يسجل حركات يد الشخص أثناء التوقيع كَسِمَة مميزة له، آخذا في الاعتبار أن لكل شخص سلوكا معينا أثناء التوقيع [١].

ويتم التحقق من صحة هذا التوقيع عن طريق قيام نفس البرنامج الذي تم التوقيع بواسطته، بفك رموز الشفرة البيو مترية، ومقارنة المعلومات مع التوقيع المخزن، ثم إرسالها إلى برنامج كمبيوتر يعطي الإشارة فيما إن كان التوقيع صحيحًا أم لا [٢].

وفي القانون الفيدرالي الأمريكي لعام ٢٠٠٠ : وردت عدة تعريفات للتوقيع الإلكتروني علي مستوي تشريعات الولايات، ولكننا سنكتفي بذكر التعريف الوارد في القانون الفيدرالي الموحد بشأن التوقيع الإلكتروني لعام ٢٠٠٠ م؛ حيث عرَّف التوقيع الإلكتروني بأنه: "صوت أو رمز أو إشارة أو أي إجراء آخر يقع في شكل الكتروني يلحق (يتصل منطقيًا) بعقد أو سجل آخر (وثيقة)، ينفذ أو يصدر من شخص؛ بقصد التوقيع علي مستند أو سجل". وقد عرَّف هذا القانون السجل بأنه : "المعلومات الموضوعة علي وسيط ملموس، أو المخزنة في

Computer Vision, Graphics and Image Processing, ICVGIP 2008, 706–713. https://doi.org/10.1109/ICVGIP.2008.67

(١) يمكن الرجوع الى:

Sae-Bae, N., Memon, N.: 'Online signature verification on mobile devices', IEEE

Trans. Inf. Forensics Sec., 2014, 9, (6), pp. 933–947

2 Meenakshikalera, K., Sargur, S., Aihua, X.: 'Offline signature verification and

identification using distance statistics', Int. J. Pattern Recognit. Artif. Intell., 2004, 18, (7), pp. 1339–1360

3 Fuentes, M., Garcia-Salicetti, S., Dorizzi, B.: 'On-line signature verification: fusion of a hidden Markov model and a neural network via a support vector machine'. Proc. of Int. Workshop on Frontiers of Handwritten Recognition, Niagara on the Lake, Canada, August 2002, pp. 253–258

(2) Yang, L., Widjaja, B.K., Prasad, R.: 'Application of hidden Markov models for signature verification', Pattern Recognit., 1995, 28, (2), pp. 161–170

Fierrez-Aguilar, J., Nanni, L., Lopez-Peñalba, J., et al.: 'An on-line signature verification system based on fusion of local and global information'. Proc. Of Fifth IAPR Int. Conf. on Audio and Video based Biometric Person Authentication, Berlin, Heidelberg, 2005, pp. 523–532

وسيط إلكتروني أو غيره" [١]. ويلاحظ على هذا التعريف أنه ذكر وظيفتي التوقيع من حيث تحديد هوية الموقِّع وإظهار رضائه بمضمون المحرر، كما أنه لم يشترط صورة محددة للتوقيع الإلكتروني، الأمر الذي من شأنه فتح المجال أمام دخول جميع صور هذا التوقيع المعروفة حاليًا، والتي يمكن أن تستجد مستقبلاً حسب تطور تكنولوجيا المعلومات.

في قانون المعاملات الإلكترونية الكويتي لعام ٢٠١٤: عَرَّفت المادة الأولي من هذا القانون التوقيع الإلكتروني بأنه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخري مماثلة في مستند أو سجل إلكتروني أو مضاف عليها أو مرتبطة بها بالضرورة، ولها طابع يسمح بتحديد هوية الشخص الذي وقَّعها ويميزه عن غيره".

وقد عَرَّفت المادة (١) من قانون المعاملات الإلكترونية الكويتي الكتابة الإلكترونية بأنها: "كل حروف أو أرقام أو رموز أو أي علامات أخري تَثْبُت علي دعامة إلكترونية أو رقمية و ضوئية أو أيه وسيلة أخرى مشابهة، وتعطي دلالة قابلة للإدراك، ويمكن استرجاعها لاحقًا". ويتضمن نص القانون الكويتي أن الكتابة الإلكترونية لا تُدوّن علي الورق كالكتابة العادية، بل علي دعامة أخري غير مادية، سواء أكانت إلكترونية أم رقمية أم ضوئية أم غيرها، وينظر إليها، لا من حيث ارتباطها بالدعامة المستعملة في تدوينها، بل من حيث وظيفتها في إعداد الدليل علي وجود التصرف القانوني وتحديد مضمونه، بما يُمكِّن أطرافه من الرجوع إليها في حالة نشوب خلاف فيما بينهم، وهو ما يستلزم أن تعطي هذه الكتابة دلالة قابلة للإدراك، أي أن تكون مدونة بحروف أو رموز أو أي علامات أخري معروفة ومفهومة للشخص الذي يراد الاحتجاج بها عليه، وإلا تتعرض للتعديل أو التحريف، وأن تتصف بالاستمرارية والثبات؛ حتي يمكن بذلك استرجاعها لاحقًا، وحينئذ تأخذ حكم الكتابة التقليدية (الورقية)[٢].

---

(1) For more Information please refer to:
Lejtman, D.Z., Gorge, S.E.: 'On-line handwritten signature verification using wavelets and back-propagation neural networks', Sixth Int. Conf. on Document Analysis and Recognition Proc. IEEE, 2001, pp. 992–996
Huang, N.E., Shen, Z., Long, S.R.: 'A new view of nonlinear water waves: the Hilbert spectrum', Annu. Rev. Fluid Mech., 1999, 31, pp. 417–457
12 Chang, C.P., Lee, J.C., Su, Y., et al.: Using empirical mode decomposition for iris recognition', Comput. Stand. Interfaces, 2009, 31, pp. 729–739

(2) E.A.CAprioli,les lettres Recommandées Electroniques,cahiers de Droit de l' E- = terprise' mai 2011'N° 3,p.68.

= وأما القضاء الفرنسي فيبدو أنه قَبِل -ضمنًا- مبدأ التعادل الوظيفي بين الكتابة الورقية والكتابة الإلكترونية قبل صدور القانون ٢٣٠ لسنة ٢٠٠٠م، وهو ما يتضح من حكم لمحكمة النقض الفرنسية،

تقسيم البحث

المبحث الأول: الأحكام العامة لجرائم التوقيع الإلكتروني في القانون الأمريكي

المطلب الأول: البيئة التشريعية لجرائم التوقيع الإلكتروني الأمريكي.

المطلب الثاني: واقع وتطبيقات جرائم التوقيع الإلكتروني وفق القانون الأمريكي.

المبحث الثاني: الأحكام العامة لجرائم التوقيع الإلكتروني في القانون الكويتي

المطلب الأول: تعاطي المشرع الكويتي مع جرائم التوقيع الإلكتروني.

المطلب الثاني: إشكاليات جرائم التوقيع الإلكتروني في القانون الكويتي في ضوء رؤية مقترحة.

صدر بتاريخ ٢ ديسمبر ١٩٩٧م، جاء فيه: "إن الكتابة يمكن أن تُنْشَأ وتُحفَظ علي أي دعامة، بما فيها الفاكسات، طالما أن سلامتها ونسبتها إلي شخص معين كانتا محققتين أو لم ينازع فيهما".

" L' écrit peut être établi et conservé sur tout support , y compris les Télécopies, déslors que son intégrité et L'imputabilité contenu à L' auteur désigné ont été Vérifiées,ou ne sont pas contestès" .

Cass.com . fr'2dèc. 1997,D.1998, p.192,Note D.r.Martin

ومع ذلك فإنه كان يمكن للقاضي الفرنسي أن يرفض قبول الدليل الإلكتروني في الإثبات ، علي الرغم من تأكده من صحته ونسبته غلي الشص الذي وقَّع عليه؛ بحجة أنه لا يعتبر كتابة في مفهوم المادة ١٣٤١ من القانون المدني ، لكن المادة (١-١٣١٦) من هذا القانون والمضافة بالقانون ٢٣٠ لسنة ٢٠٠٠م؛ قد تغلبت علي هذه العقبة، وقررت -صراحة- أن الكتابة الإلكترونية تعادل الكتابة التقليدية.

E.A.caprioli, Le Juge et La preuve Electronique, Réflexion Sur Le projet de Loi portant Adaptation De La preuve Aux technologies de L'information et Relatif à La Signature Electronique ". www caprioli - avocats.com

المبحث الأول

الأحكام العامة لجرائم التوقيع الإلكتروني في القانون الأمريكي

مقدمة

يطبق فى الولايات المتحدة الأمريكية القوانين الخاصة بالغش فى مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لأغراض ارتكاب الغش على جرائم سرقة المعلومات. بل إن بعض الولايات الفيدرالية أصدرت قوانين أعطت- بموجبها- مفهومًا واسعًا للمال، بحيث يشمل "كل شيئ ينطوى على قيمة"، ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة، وتعاقب هذه القوانين على الاستخدام غير المسموح به بغرض ارتكاب أفعال الغش أو للاستيلاء على المال[(١)]، وعلى المستوى الفيدرالى صدر قانون الولوج المصطنع فى الحاسب الآلى فى أكتوبر

---

(١) استحدثت الولايات الأمريكية -مثل أريزونا وكاليفورنيا وكولورادو وديلا وير وفلوريدا وجورجيا وإلينوي وميتشغان وميسوري ومونتانا وأوتارا ونيومكسيكو...)- العديد من القوانين الجنائية التي تعاقب على الاستخدام غير المسموح به للحاسب الآلي بغرض الاحتيال أو الحصول على مال، والمجال -هنا- ليس متسعًا لفحص جميعها؛ ولذا نكتفي بإيراد ملاحظتين عليها.

أولهما: أن آليات التجريم -في هذه القوانين- على درجة كبيرة من الاختلاف، ويبدو ذلك من زاويتين:

(أ) أن جميع هذه القوانين إذا كانت تتمسك بضرورة توافر الغش أو سوء النية في الأفعال المعاقب عليها، إلا أن صيغتها -فى هذا الشأن- جاءت غير مطابقة، وعلى سبيل المثال: فقانون كاليفورنيا ينص على أن "يعاقب كل شخص ولج عن عمد أو سوء نية...."، مادة ٥٠٢ من قانون عقوبات كاليفورنيا الصادر سنة ١٩٧٩م، والمعدل سنة ١٩٨٢م، وقانون "ديلا وير" ينصان على: "كل من .... وكان ذلك عن تبصر أو تروٍّ مباشر أو بطريق غير مباشر". مادة ٥٥٨ والمعدلة في سنة ١٩٨٢م، وقانون فلوريدا ينص على: "كل من باشر.... عن تروٍّ وعلم وبدون إذن....." وقانون ١٩٧٨ وقانون بنسلفانيا" ينص على: "كل من ..... عمدًا وبدون إذن " قانون سنة ١٩٨٣".

(ب) أن بعض هذه القوانين مال إلى تقنين -وبشكل مختصر- الأفعال المجرمة، مقتديًا في ذلك بالنموذج الفيدرالي، ومنها قانون كاليفورنيا، الذى يعاقب "كل من ولج عمدًا في نظام أو شبكة معلوماتية، بغرض محاولة أو تنفيذ أي مؤامرة أو حيلة بغرض الحصول على نقود أو خدمات". قانون العقوبات مادة ٥٠٢/ب"، ويجرم هذا القانون أيضًا "كل من ولج -وبسوء نية- في نظام شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير، أو كل من أدخل معلومات مصطنعة؛ بغرض تحسين أو إساءة سمعة الغير، ويعاقب أخيرًا كل شخص ولج -بسوء نية- أتلف أو محا أو أضرّ بأي نظام معلوماتي أو شبكة معلوماتية أو كيان منطقي أو بيانات. وعلى النقيض تنبت بعض القوانين الأخرى المنهج التحليلي، ومنها على سبيل المثال: قانون فلوريدا، الذى احتوى على ثلاث مجموعات أساسية، إحداها: مخصصة للجرائم التي تقع على البيانات الموجودة

سنة ١٩٨٤[(١)] counterfeit access device and computer Fraud and abuse act ، الذى ولج عمدًا فى حاسب آلى بدون إذن، أو كان مسموحًا بالولوج منه، واستغل الفرصة التى سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن، وقام عمدًا عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة فى الحاسب متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية، وطالما

بالبرامج، والثانية: خاصة بالجرائم التي تقع على المعدات والتجهيزات المعلوماتية والثالثة : خاصة بجرائم المستخدمين لنظم المعلومات، ولكل مجموعة منها قواعدها الداخلية الخاصة بها، وثانيهما: تتعلق بالمنهج الأنجلو سيكسوني في التعاريف القانونية؛ حيث يلاحظ أن هذه التعاريف ليس لها أي قيمة خارج الولايات المتحدة، بل -أيضًا- خارج الولاية التي تنص عليها، وفضلًا عن ذلك فليس لها أي قيمة خارج النص الذي يحتويها؛ حيث إنها تعطى من أجل احتياجات النص.

(١) بدأت "أنفينا سيكوريتى كورب" في بادئ الأمر وكأنها شركة إنترنت نموذجية، بمكاتبها وحاسباتها وموظفيها ونظامها الأمني الحاسوبي، ولم يكن ينقصها سوى الزبائن. لكن تبين الآن أن تلك الشركة التي بدت مشروعًا فاشلًا للوهلة الأولى كانت شركة وهمية، أنشأها مكتب التحقيقات الفيدرالية الأمريكي "إف بي أي"؛ للإيقاع بشابَّيْن روسيين متهمين باختراق كمبيوترات شركات إنترنت أمريكية، واختلاس معلومات حساسة؛ فى محاولة لابتزاز المال. وتقول السلطات: إن "إليكسى ايفانوف" ٢١ عامًا و"فاسيلى جورشكوف" ٢٥ عامًا، وكلاهما من مدنية شليابنسك الروسية؛ قد ابتلعا الطعم ووقعا في فخ الإف بى أى. وفى حين رفض مكتب التحقيقات الفيدرالية الإدلاء بأية تعليقات؛ فإن وثائق قضائية -كشف عنها النقاب مؤخرًا- تبدو وكأنها رواية جاسوسية يروي فيها عملاء الـ "إف بي أي" كيف تمكنوا من الإيقاع باللِّصين عن طريق إنشاء شركة زائفة، ودعوة إيفانوف وجوشكوف لمحاولة اختراق أنظمتها الحاسوبية المحصنة، وبعد أن نجح القرصانان الروسيان في اختراق الأنظمة عن بُعْد؛ وجَّه موظفو شركة أنفيتا دعوة لهما للقدوم إلى سياتل في الولايات المتحدة لمناقشة إبرام عقد شراكة واستعراض كامل إمكانياتهما في مجال التسلل إلى أجهزة الكمبيوتر عبر الإنترنت، وبينا كان الشابان يستعرضان مهاراتهما في الشراكة الوهمية؛ استخدم الـ "إف بي أي" تقنية تصنت حاسوبية، تبسط نشاطها عبر الانترنت، وتخترق النظام الحاسوبي الخاص بالمتهمين في روسيا.

ويقول خبراء أمن الانترنت: إن القضية تعرض لمدى تطور مقدرات مكافحة جرائم الإنترنت لدى مكتب التحقيقات الفيدرالية، لكن الدفاع يشير إلى الاستفهام حول مشروعية استخدام هذه الأساليب.

راجع في ذلك:

See Public Consultation on the Review of the Electronic Transactions Act, INFOCOMM MEDIA DEV. AUTH. (https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/Consultation-Papers/2019/Public-Consultation-on-the-Review-of-the-Electronic-Transactions-Act.

أثرت هذه الأفعال على أداء وظيفته. ويمكن لهذا النص -وبطريق غير مباشر وبشروط معينة- أن يشمل النصب الذى يرتكب عن طريق الحاسب الآلي، لكن وزارة العدل الأمريكية قدمت فى أغسطس سنة ١٩٨٤[١] مشروعًا بقانون يستهدف مباشرة حالة الغش المعلوماتي، الذى يعاقب "كل من رتَّب أو صمَّم خطة ما أو حيلة؛ بغرض ارتكاب غش، أو الاستيلاء على مبلغ من النقود أو مال لا يخصه، وولج أو حاول الولوج فى حاسب آلى بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس.....". ومصطلح "المال" property وفقًا لهذا المشروع بقانون يشمل "كل الوسائل المالية والمعلومات التى تحتوى على بيانات معالجة والمكونات الإلكترونية والكيانات المنطقية وبرامج الحاسب الآلي، سواء أكانت بلغة الآلة أم بلغة مقروءة للإنسان، وكل قيمة أخرى ذات طابع مادي أو معنوي".

ومن خلال ما سبق يمكن تقسيم المبحث الأول على النحو التالي:

المطلب الأول: البيئة التشريعية لجرائم التوقيع الإلكتروني الأمريكي.

المطلب الثاني: واقع وتطبيقات جرائم التوقيع الإلكتروني وفق القانون الأمريكي.

---

(١) صدر في الولايات المتحدة الأمريكية القانون الفيدرالي بشأن الغش والعبث المعلوماتي computer fraud & abuse act في عام ١٩٨٤م، وأدخل عليه تعديلات، كان آخرها عام ١٩٩٦. ويواجه هذا القانون عدة أفعال تتصل بالدخول غير المشروع أو الحصول، متجاوزًا التصريح على معلومات تتعلق بالدفاع الوطني أو العلاقات الخارجية لا يجوز الكشف عنها. ويعاقب -أيضًا- على نقل مكونات لبرامج أو معلومات دون موافقة من صاحب الشأن في حالة ما إذا ترتب على هذا النقل خسائر لشخص أو أكثر، ويواجه القانون -أيضًا- مشكلة غش كلمات المرور بما يمكن مرتكبه من الدخول على نظام للكمبيوتر إذا كان من شأنه الإضرار بالتجارة بين الولايات بالتجارة الخارجية.

المطلب الأول

البيئة التشريعية لجرائم التوقيع الإلكتروني الأمريكي

تاريخيًا: أرجع الفقه الجنائي الأمريكي جرائم الحاسوب إلى العام ١٩٦٠[(١)]. أما جرائم الإنترنت فإنه يمكن القول بأنها بدأت مع العام ١٩٨٨م، وكانت أول الجرائم التي ترتبط -عضويًا- بالإنترنت: جرائم العدوان الفيروسي، فيما هو معروف في التاريخ القانوني بجريمة "دودة موريس المؤخرة واقعتها في ٢ نوفمبر ١٩٨٨م. ولا يزال الفقه والتشريع المقارن -في حقيقة الأمر- يستشعر الحرج في التمييز بين كل من جرائم الحاسوب وبين تلك الناجمة عن استخدام الإنترنت، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام ١٩٩٥ تبنَّي الموقف المقارن المذكور هذا، فصدر عنوان التقرير Computer crimes & other crimes related to computer

لذلك نجد أن تعريف جرائم الحاسوب -ومنها جرائم التوقيع الإلكتروني في الفقه والتشريع- يسوده اتجاه يجمع بين الجرائم التي تقع على الحاسوب ذاته، وتلك التي يكون الحاسوب وسيلة ارتكابها، فهي -لدي هذا الاتجاه- تُعرَّف بأنها: "فعل غير مشروع، يتورط نظام الحاسوب فيه، سواء أكان الحاسوب -كآلة- هو موضوع الجريمة أم كان الوسيلة إلى ارتكابها، أو مستودع الدليل المرتبطة بالجريمة". وهو تعريف مستمَد من أكثر التعريفات شعبية لجرائم الحاسوب الذي قال به الأستاذ Donn Parker؛ من حيث إن جرائم الحاسوب هي "جرائم تتطلب دراية ضرورية بالحاسوب؛ لكي يتم ارتكاب الجريمة بنجاح"[(٢)].

---

(1) (SIEBER) Dr. Ulrich – Computer crimes & other crimes related to information technology rev. inter.de droit penal 1991 p. 1033.

(2) ((the royal candian mounted police) " computer crimes is any illegal act which involves a computer systems whether the computer is an obect of crime, an instrument used to commit a crime or a respsitory of evidence related to a crime". Available online in feb. 2000 at: http://www.rcmp.com (mak d. rasch – criminal law and the internet – the internet and association. Copyright © 1996 by the computer law association, inc. p.6, donn parker of sri, is necessary for the successful commission of the offense.

الفرع الأول

تطور قوانين الجرائم الإلكترونية بالتشريع الأمريكي

لقد توسعت إدارة العدل الأمريكية في ربط الحاسوب بتقنيته، فذهبت إلى تعريف جرائم الحاسوب بأنها: "هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية الحاسوب، ويكون عرضة للتحقيق والاتهام"[(١)] كان ذلك بالطبع بتأثير من اتجاهات المشرع الأمريكي في تعديل ١٩٩٦ لقانون البنية الوطنية للمعلومات The National Infrastructure Information Act (القسم ١٠٣٠)، الذي استوحي التجريم من الربط بين الحاسوب وتقنيته ككل، فتمخّض هذا الاتجاه عن وجود ثلاثة أنواع من الجرائم التي يمكن ارتكابها عبر الحاسوب وذلك وفقاً للمنهج الأمريكي، وهي:

أولًا: الجرائم التي يكون الحاسوب هدفًا لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسوب، أو إحداث إضرار به، أو بنظام تشغيله، أو بالشبكة التي يعمل خلالها[(٢)].

ثانيًا: الجرائم التي يكون الحاسوب وسيلة لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسوب لتسهيل ارتكاب بعض الجرائم التقليدية، مثل: الاحتيال على البنوك، كما لو قام موظف بأحد البنوك باستخدام برمجية تحويل العملة لصالحه، فيودع مبالغ محولة لحسابه عوضًا عن وضعها في مسارها الصحيح، وكذلك القيام بإعداد Produce أو نقل Transfer أو حيازة Possess آلة Device، بما في ذلك الحاسوب؛ بنية استخدامها في تزوير وثائق إثبات شخصية To Falsify Identification documentation (18 US Code Sec. 1028)

ولقد توسعت بعض التشريعات في مدلول مصطلح "أدوات التزوير Forgery Devices"؛ لكي تشمل الحاسوب وملحقاته Equipment وبرمجياته Software إذا أعدت خصيصًا بغرض التزوير، مثل قانون ولاية نيوجيرسي (N.J.Stat.ANN. Sec. 2 C : 21-1) ،

---

(1) (SCALION) Robert – crime on the internet, fall 1996, p. 1. "compuer crime is any violation of the law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution" available online in feb. 2000 at :
http://wings.buffallo.edu/complaw/complawpapers/scalion.html - THOUMYRE - abuses in the cyberspace, op cit. P. 7

(2) Washington Electronic Authentication Act, ch. 250, 1996 Wash. Sess. Laws 1190 (codified at WASH. REV. CODE §§ 19.34.010–19.34.903

ومما تجدر الإشارة إليه: أن مثل هذا التقسيم السالف ليس جامعًا مانعًا للتعبير عن جرائم الحاسوب؛ إذ هناك من الجرائم التي ترتكب بواسطة الحاسوب، ومع ذلك لا يمكن إدراجها في أي من الأقسام أو الأشكال الثلاثة، مثلما هو الحال في جريمة سرقة وقت الحاسوب مثلًا، وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641 من التقنين الأمريكي كجريمة من جرائم المعلوماتية[(١)].

وربما يكون السبب في التوسع السالف عائدًا إلى أن إمكانيات الحاسوب لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات الحاسوب يقل كثيرًا عما نعلمه عن قدرات الإنترنت. فهذه الأخيرة -وإن كانت لم تأخذ حظها كما ينبغي- قد تناولها الساسة وفقهاء القانون والاقتصاد على المستوى الإقليمي والدولي بكثير من الأمل، وهي بعد في بداياتها، في حين أن مسيرة الحاسوب تبدو هادئة أو طبيعية. ومثل هذا الأمر وجد له تأثيرًا كبيرًا في الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣، حيث اعترفت الاتفاقية -في المادة الأولى منها- بمصطلح "نظام الحاسوب Computer System"، ولم تأخذ في الاعتبار مجرد مصطلح "الحاسوب Computer"، فقد حددت الاتفاقية هذا المصطلح بكونه يشمل "أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن -بإضافة برمجية إلى واحد أو أكثر منها- أن تقوم بمعالجة آلية للبيانات"[(٢)].

---

(1) (United States v Sampsonm, 6 COMP, L. SERV. REP. 879 (N.D. Cal.) ففي هذه القضية فقد اعتبرت المحكمة أن الاستخدام غير المصرح به لحاسوب في مؤسسة حكومية يشكل جريمة عدوان على أملاك الحكومة وفق ما هو Unauthorized use of computer time مقرر في القسم Sec. 641 المشار إليه – انظر كذلك فيما يتعلق بالقسم ٦٤١ المذكور :
18 U.S.C. & 641. See : United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (Theft of grand jury transcripts and information contained therein was theft of government property). Cert. denied. 404 U.S. 958 : United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of classified information supports embezzlement conviction); United States v. DiGillo, 538 F. 2d 972 (3d Cir). Cert. denied. 429 U.S. 871 (1971) (theft by photocopying government secords sufficient to support & 641 convocation) : United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of competitior's confidential bid information violates & 641).

(2) (Art. 1 Definitions : "For purposes of this convention : Computer System means any device or a group of inter – connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"

وبدون إحداث اتصال بين الحاسوب وبين الإنترنت عن طريق وسيط – حتى الآن- لا يمكن القول بوجودنا على الإنترنت. وعليه فإن مجرد القول بارتكاب جريمة حاسوب لا يعني ضرورة وجودنا على الإنترنت، إنما يكفي أن يكون الحاسوب في حالة عمل، في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الإنترنت دون أن نكون على الإنترنت Online[(١)].

ومثل هذا القول نجده في القانون الأمريكي؛ حيث يميز القسم 1030١٨ USC Sec. بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية Protected computer، فهذا الأخير يعني ذلك الحاسوب المتصل بغيره عن طريق الشبكات / الإنترنت، في حين أن إيراد مصطلح حاسوب Computer فقط يعني مجرد الحاسوب غير المتصل بأي شبكة ولو داخلية (حيث يُعد هنا أداة تخزين فقط).

لذلك يتجه بعض القانونيين إلى إحداث فصل في هذا الإطار، من حيث تعريف جرائم الإنترنت تعريفًا منفصلًا عن جرائم الحاسوب بوصفها جرائم ناجمة عن استخدام الإنترنت، وهو التعريف المبني على فهم عميق لطبيعة المشكلة من حيث ضرورة الفصل بين نوعي هذه الجرائم؛ حيث إن الإنترنت أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر الحاسوب؛ حيث إنه -كنتيجة لظهور الإنترنت- أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر الحاسوب، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم الحاسوب – الجرائم المرتبطة بالحاسوب وتفصيلاتها أيضًا ...إلخ)[(٢)]. ولعل ما انتهي إليه التطور الذي نراه سلبيًا في توصيات مؤتمر G8 (الثمانية الكبار) عام ١٩٩٨ ليدعو إلى مزيد من التأمل في هذا الشأن؛ إذ تم التوصل

---

(١)) أن مصطلح Online يثير جدلًا؛ حيث إنه -بالإنجليزية- يشير إلى وجودنا على الإنترنت، حيث إن ما يؤخذ في الاعتبار: أن النظرة إلى الإنترنت كونها خط مفتوح يلزم -لكي نصل إليها- أن نكون على هذا الخط، في حين أنه إذا كان خارجها فإن المصطلح المستخدم هو Off Line .

Roy, A., Doherty, J.F.: 'Raised cosine fiter-based empirical mode decomposition', IET Signal Process., 2011, 5, (2), pp. 121–129

(2) (KASPERSEN) Prof. Dr. Henrik W. K. – crimes related to the computer network. Threats and opportunities criminological perspective, p. 258. five issues in European criminal justice: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime proceedings of the vi European colloquium on crime and criminal policy Helsinki 10-12 December 1998, European institute or crime prevention and control, affiliated with the united nations (heuni) p. O. Box 161, fin- 00131 Helsinki Finland publication series no. 34

- Thoumyre – abuses in the cyberspace, op. cit., p. 10

إلى مصطلح High- Tech Crime أو جرائم التقنية العالية أو المتقدمة كنوع من محاولة التوسع في جرائم الحاسوب؛ لكي تشمل كافة الجرائم التي يكون الحاسوب طرفًا فيها. وهذا كله يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم الحاسوب وجرائم الإنترنت، على الرغم من الالتصاق الذي يكاد يكون طبيعيًا بينهما.

وهذا الاتجاه الذي نأخذ به يجد له أساسًا فقهيًا يسعي إلى إقامة بنيانه على النحو الذي يحقق مصلحة الإنسان قبل الآلة؛ إذ يذهب هذا الاتجاه إلى أن جرائم الإنترنت هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية[١]. وهنا يمكن تحديد بعض النقاط المهمة على النحو التالي:

النقطة الأولى: موضوع العالم الافتراضي Cyberspace، الذي هو عبارة عن العالم المرئي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلة التقنية[٢]. والذي يطلق عليه الفقه العربي تسمية "الفضاء الإلكتروني"[٣]. وهو العالم الذي ابتكر فكرته كاتب الخيال العلمي الشهير William Gibson في روايته الشهيرة The NeuRomancer، التي أصدرها عام ١٩٨٤؛ حيث وصف في هذا الكتاب فانتازيا إلكترونية Fantasy Electronic[٤] تقابل فيها مجموعة هكرة من مهرة الحاسوب، وطالما نشاطهم الاختراق، والعديد من المظاهر التي تكاد تصل -في بعض الأحيان- إلى منطق الجريمة عبر الإنترنت كما هي مقررة في التشريعات المعاصرة.

وإذا كان قانون العالم الافتراضي / الإنترنت (Cyber Law) لا يُشكّل عقبة في إطار بناء نظريته -إن أمكن تكاثف الجهود نظرياً على الأقل – فإن الحال غير ذلك فيما يتعلق بتطبيق هذه النظرية وتنفيذها، سيما في النطاق القضائي؛ ذلك أن تركيبة قانون العالم

(1)Niang, O., Thioune, A., Gueirea, M.C.E., et al.: 'Partial differential equation-based approach for empirical mode decomposition: application on image analysis', IEEE Trans. Image Process., 2012, 21, (9), pp. 3991–4001

(2) (Rehman, N.U., Mandic, D.P.: 'Filter bank property of multivariate empirical mode decomposition', IEEE Trans. Signal Process., 2011, 59, (5), pp. 2421–2426

(3) Krinidis, S., Krinidis, M., Chatzis, V.: 'Workspace for image clustering based on empirical mode decomposition', IET Image Process., 2012, 6, (6), pp. 778–785

(4) (NICHOLSON) Keith – International Computer Crime : A Global Village Under Siege – New England International & Comparative Law Annual 1996 – New England School of Law P. I. available online in 16Mar. 2023 at : http://www.nest.edu/annual/vol2/computer.htm

الافتراضي/ الإنترنت ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بُعد دولي[١] يتطابق -شكليًا- مع مفاهيم العولمة، وليس مع المفاهيم التي يعرفها القانون الدولي، في الوقت الذي يتسع مدلوله ليشمل فروع القانون الأخرى؛ ذلك أنه -من خلال مصطلح CyberLaw- هرع الفقه المقارن ليضع تفريعات جديدة لهذا المصطلح تعمل في إطاره ووفق فروع القانون المعمول بها، مثل: Cyberbehavior للدلالة على سلوكيات القانون المدني، ومصطلح CyberCrime للدلالة على سلوكيات القانون الجنائي، ومصطلح Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار قانون الإنترنت، ومصطلح Cybertribunal على المحاكمات عبر الإنترنت ... إلخ.

إن عملية إحداث ملائمة بين النظام القانوني القائم وبين الإنترنت؛ كانت قد برزت بداية حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الإنترنت بأسلوب التنظيم النفسي للإنترنت Self – regulation ، بحيث يجب ألا يكون هذا التنظيم هو الأداة الوحيدة وإنما يقبل إلى جوار التنظيم القانوني بالأداة التشريعية تواجد أدوات تنظيمية نابعة من طبيعة الإنترنت، أي التقنية المعلوماتية. وسببية رفض وحدة التنظيم الذاتي كنظام قانوني للإنترنت يكمن في أن التنظيم الذاتي ليس مقنعًا بالدرجة الكافية[٢]، بما يجعل العالم الافتراضي آمنًا بالدرجة الكافية التي تسمح بالأمن والاستقرار [٣]. على أن الأمر ليس على ذلك القدر من السهولة إذا تأملنا الاتجاه المضاد الذي يأخذ بضرورة التدخل القانوني لتنظيم العالم الافتراضي؛ حيث إنه توجد لديه صعوبات أيضًا، من حيث إن أهم صعوبة تتمثل في تحديد طبيعة النظام القانوني الذي يحكم الإنترنت، وهل تكفي النظم الأساسية في الدولة لحسم هذه الصعوبات وتذليل محتواها أم أن العالم الافتراضي قام هكذا فجأة؟ وبالتالي يمكن أن يوجد له أساس في النظم القانونية المعاصرة، إلا أن

---

(1)(TRANSNAIONAL NATURE OF CYBERSPACE, (CYBERCRIME AND CYBERPUNISHMENT< ARCHAIC LAW THERATEN GLOBAL INFORMATION p. 2 report prepared by : McConnell INTERNATIONAL http://www.mcconnellinternational.com with support from WITSA http://www.witsa.com December 2000 available online in Dec. 2000, at : http://www.mcconnellinternational.com/services/cybercrime.html

(2)(United States Government Accountability Office. (2017). COUNTERING VIOLENT EXTREMISM Actions Needed to Define Strategy and Assess Progress of Federal Efforts.

(3)(CyberCrime And Cyberpunishment , archaic law threatens global information op-cit p. 2

العقل القانوني لم يستظهر هذا الأساس بعد، وهنا فإن المسألة فقط تحتاج إلى مزيد من الوقت والتأمل والحكمة القانونية.

النقطة الثانية: ترتبط بالنتائج المترتبة في النظام القانوني الأمريكي؛ حين فصل جرائم الحاسوب Computer Crimes عن جرائم الإنترنت CyberCrime ، ومدى إمكانية قيام هذا الفصل تقنيًا. والحقيقة أنه من الصعوبة بمكان فصل جرائم الحاسوب عن جرائم الإنترنت؛ نتيجة لارتباط الإنترنت بالحاسوب ارتباطًا تقنيًا. إلا أن هذه الصعوبة سوف تتقلص كثيرًا إذا أدركنا أن تقنية الحاسوب أعم كثيرًا من تقنية الإنترنت؛ فهو – أي الحاسوب- ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية؛ إذ كما أنتجت تقنية الحاسوب الإنترنت فإن ذلك لا يعني نهاية المطاف في هذا الشأن، فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب تبرز في الأفق قريبًا، وتدليلًا على ذلك فإن دولًا -مثل كندا- تربط جرائم الانترنت بجرائم الاتصال عن بُعد Telecommunication Crime التي يمكن أن تقع بواسطة الانترنت، كما يمكن أن تقع بواسطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك.

وإذا كان حقيقيًا أن تقنية الحاسوب قد انطلقت لكي تبتكر الإنترنت؛ فإن منطقة الخلاف بين العمل السلبي الذي يكون محله الحاسوب وبين ذلك الناجم عن استخدام الانترنت تُعد أحد الصعوبات الجديدة التي تواجه فقه القانون حقيقة، فإذا تحدد هذا التعريف فإنه من السهولة التوصل إلى بحث التوجه السياسي والتشريعي في دولة ما؛ لأجل ذلك نجد أن البعض لا يمانع في إطلاق صفة "جرائم الحاسوب" Computer Crime على جرائم التوقيع الإلكتروني، إلا أنه يشترط بالضرورة أن يكون الحاسوب مرتبطًا بشبكة Connected [(١)] أو Protected Computer . ويمكن القول إجمالًا: بأن هناك اتجاهين في إطار رصد تعريف جرائم الانترنت، الاتجاه الأول بنحو منحى التعريف المضيق الذي يقوم برصيد جرائم الانترنت في ربط جرائم العالم الافتراضي -ككل- بالحاسوب؛ حيث يذهب هذا الاتجاه إلى "أن مصطلح العالم الافتراضي مرجعه استخدام الحاسوب لتسهيل ارتكاب الجرائم" [(٢)] .

---

(1) Nicholson – International computer crime op – cit P.2

(2) (KATYAL) Neal Kumar – criminal law in criminal law in Cyberspace , Georgetown University law center 2000< P.13 A revised version of This working paper is forthcoming in the university of Pennsylvania law review < Volume 149 April 2001 This paper can be downloaded without charge from

لذلك فإن الأرجح هو الاتجاه إلى التوسع في تعريف جرائم الانترنت، ومنها -بالطبع- جرائم التوقيع الإلكتروني، ومكمن التعريف الموسع هو السعي إلى بحث استقلالية لجرائم الانترنت تتنافى مع ربطها بالحاسوب وجرائمه . وبالتالي فإن التعريف الذي نقول به يجعلنا في الحقيقة نعترف مسبقًا بأن ظاهرة الانترنت ما زالت غامضة في دراسات القانون، وفى هذا الإطار رصد المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسوب Federal guidelines for searching and computers أهمية الاعتراف بأن رجال القانون بدؤوا في مواجهة مشاكل جديدة على أثر إنجاز ثورة معلومات الحاسوب والاتصالات في القرن الواحد والعشرين [1]

---

the social science research Network Electronic paper collection at Http://papers.ssrn.com/ aperitif abstract id=249030 working paper No 249030

(1) Theoumyre – abuse in the cyberspace , op-citP.8

الفرع الثاني

الأحكام الخاصة بالعقوبات في القانون الأمريكي حول التوقيع الإلكتروني

كانت بعض الولايات الأمريكية متقدمة في إصدار تشريعات تنظم الاعتراف بالتوقيع الإلكتروني في الإثبات الجنائي، مثل: كاليفورنيا، إلينوي، ميسوري. لكن السلطات الفيدرالية كانت راغبة في إطار قانوني عام ينظم مسألة التوقيع الإلكتروني على المستوى الاتحادي، بما يسهم في تنويب الاختلاف في تشريعات الولايات المختلفة، ويحقق نوعًا من الانسجام والتناغم بينها، ويدعم الثقة في المعاملات الإلكترونية. وبالفعل تم إعداد مشروع قانون حول التوقيع الإلكتروني، وافق عليه الكونجرس بمجلسيه، أصدره الرئيس الأمريكي في ٣٠ يونيه ٢٠٠٠م، على أن يسري اعتبارًا من أول أكتوبر ٢٠٠٠، فيما عدا بعض الاستثناءات[١].

ويطبق القانون على التصرفات القانونية التي ينتمي طرفاها إلى ولايات مختلفة، وعلى التصرفات القانونية التي تتم مع أطراف أجنبية، وهو يعترف بحجية المحرر الإلكتروني والتوقيع الإلكتروني في الإثبات الجنائي، ولا يطلب لذلك الحصول على شهادة توثيق تثبت موافقة أو قبول جهة أخرى على هذا التوقيع .[٢]

وبصفة عامة: فإن أحكام القانون الاتحادي تفضل وتقدم على أحكام القوانين الصادرة في الولايات حول التوقيع الإلكتروني عند تعارض أحكامها مع مبادئه، كما يسمح للولايات بأن تعتنق أحكام القانون الموحد للتجارة الإلكترونية، والذي تم إعداده من قِبل المؤتمر القومي لمندوبي لجان القانون الموحد للولايات، بديلًا عن أحكام القانون الاتحادي حول التوقيع الإلكتروني. كما يمكن للولايات تعديل المتطلبات الاتحادية والاستعاضة عنها بإجراءات خاصة ينص عليها، شريطة أن تكون متوافقة مع أحكام القانون الاتحادي، وألّا تهدف إلى تفضيل تقنية خاصة للتوقيع الإلكتروني .ومن هنا فإن تطبيق قانون ولاية "كونتا كوتا" -على سبيل المثال- ينحصر في هذا النطاق. فهذا القانون يقر بصحة التوقيع الإلكتروني الذي يتم في نطاق الإدارات المحلية، كما يسمح للوكالات الحكومية بقبول التوقيع الإلكتروني في الأوراق والمحررات أو الإجراءات الإدارية. غير أنه ليس واضحًا ما إذا كانت أحكام القانون الاتحادي تفضل على قانون الولاية في هذا الشان ، رغم عدم

---

(1) Christopher REINHART, FEDERAL and state electronic signature laws. BRUMFIELD FRY, A preliminary analysis of Patricia federal and state electronic commerce laws.

(2) See Electronic Signature Software, SOFTWARE ADVICE, www.softwareadvice.com/electronicsignature/ accessed in 16 Mar 2023

وجود تعارض بين أحكامهما. ومن هنا فإن القانون الاتحادي يحد مستقبلًا من سلطة الولاية التشريعية في مجال التوقيع الإلكتروني .

أما بالنسبة للتشريعات السارية في الولايات الأخرى فان أحكامها تتباين؛ إذ نجد أن بعض الولايات تقر أي نوع من التوقيع الإلكتروني، في حين يشترط البعض الآخر بعض إجراءات تحقيق الثقة والأمان، أما القسم الأخير فلا يقر إلا التوقيع الرقمي (والذي تستخدم الشفرة في إجرائه)، كما تختلف هذه التشريعات -فيما بينها- فيما يتعلق بالمعاملات التي يجوز استخدام التوقيع الإلكتروني في إجراءها .[1]

المبادئ الأساسية للتشريع الأمريكي حول التوقيع الإلكتروني:

تشمل أحكام التشريع الاتحادي الأمريكي -حول التوقيع الإلكتروني في مجال التجارة على المستوى الداخلي أو الخارجي- التصرفات التي تتم على مستوى الولايات أو مع الخارج. ويقصد بالتصرف: كل رابطة قانونية بين شخصين أو اكثر تتعلق بالأعمال أو الاستهلاك أو التجارة، وهي تضم عمليات: البيع، الإيجار، الترخيص، الإتجار، المبادلة الواردة على الحقوق الشخصية، بما فيها الحقوق المعنوية، وكذلك تقديم الخدمات، كما تشمل البيع أو الإيجار أو التصرفات الأخرى الواردة على حق الملكية. ويعترف التشريع الاتحادي بالحجية القانونية للمحررات الإلكترونية والتوقيع الإلكتروني، دون أن يعلق هذا الأثر على الحصول على موافقة شخص ما، أو ترخيص من جهة معينة. ووفقًا لأحكام هذا التشريع فإنه يقصد بالتوقيع الإلكتروني كل أصوات أو إشارات أو إجراءات تتم عبر وسط غير مادي، ويستخدمها أحد الأطراف في تعاقد أو محرر، بما فيها توقيع المستند. والمحرر الإلكتروني هو: كل محرر يُدوّن أو يُرسَل أو يُستقبَل أو يُحفَظ على وسائط إلكترونية .

ويقضي التشريع كذلك بأن المحررات الإلكترونية تعد مستوفية للشروط المتطلبة للحفاظ على المحرر إذا كانت تعبر بثقة عن المعلومات المدونة بها، ويمكن لذوي الشأن الوصول إلى هذه البيانات والاطلاع عليها؛ لذلك يجب أن تتم بطريقة تجعل استعادتها أو الحصول على نسخة مطابقة منها أمرًا ممكنًا. كما يمكن القيام بأعمال التوثيق والاعتراف والفحص إلكترونيًا. وتدوين اليمين أو الشهادة في شكل إلكتروني .

(1) See, e.g., The Difference Between Digital Signatures and Electronic Signatures, SIGNIX, www.signix.com/blog/different; accessed in 17 Mar 2023

ومن بين الأمور المختلفة الأخرى التي ينص عليها التشريع: الطلب إلى وزارة التجارة بأن تولي اهتمامًا بالتجارة الإلكترونية على المستوى الدولي، كما يتضمن نصوصًا خاصة بالسندات لحاملها، والحقوق القابلة للتحويل .[١]

أما بالنسبة للاستثناءات في الأحكام العقابية التي لا يشملها القانون فهي على النحو التالي:

- لا تطبق أحكام القانون الاتحادي بشأن التوقيع الإلكتروني، على العقود والمحررات الخاضعة لنصوص القانون التالية:[٢]

أ- التشريعات الخاصة بإنشاء أو تنفيذ الوصايا وقوانين الميراث وتقسيم التركات والنصوص المنظمة للتأمينات العينية .

ب- التشريعات الخاصة بالتبني، والطلاق، والحالة العائلية .

ج- نصوص القانون التجاري الموحد (فيما عدا استثناءات قليلة تضمنها المادة (٢) والتي تنظم أحكام بيع البضائع كما لا تطبق أحكام هذا التشريع على :

- أوراق المحاكم.
- الأوراق المتعلقة بإلغاء أو إنهاء المنافع العامة.
- بعض المحررات الخاصة بإثبات اتفاقات الائتمان أو الإيجار لأغراض السكن . . .
- الأوراق الخاصة بإلغاء أو إنهاء التأمين على الحياة أو التأمين الصحي، أو إلغاء الاستفادة منه.
- المحررات المتعلقة بالترخيص بإنتاج بعض الأشياء التي تحتاج إلى موافقة إدارية مسبقة.
- الوثائق الخاصة بأوراق اليانصيب، والسموم، والأشياء الخطرة .

وقد عهد التشريع المشار إليه لوزارة التجارة مهمة مراجعة هذه الاستثناءات بعد مرور ثلاث سنوات من تاريخ سريان أحكام القانون، وخوّل لإحدى الوكالات الاتحادية إمكانية استبعاد هذه الاستثناءات بشروط معينة .[٣]

---

(1) See Kennedy & Millard, supra note 43; see also Seth Rosenblatt & Jason Cipriani, Two-Factor Authentication: What You Need to Know, CNET, https://www.cnet.com/

(2) See, e.g., Aaron S. Edlin and Alan Schwartz, Optimal Penalties in Contracts, 78 Chicago-Kent L. Rev. 33 (2003); Robert Scott and George Triantis, Embedded Options and the Case Against Compensation in Contract Law . 104 Columbia Law Review ___ (2004).

(3) See David D. Friedman, Contracts in Cyberspace [online draft]; Clayton P. Gillette, Reputation and Intermediaries in Electronic Commerce, Louisiana

- لم يغفل التشريع الخاص بالتوقيع الإلكتروني مسألة إعلام المستهلك؛ فقد نص على ضرورة ترك الحرية للمستهلك في استخدام تقنيات التوقيع الإلكتروني بتوقيع المحررات، كما أوجب على أي تشريع أو لائحة أو قرار يتضمن النص على إمكانية استخدام التوقيع الإلكتروني أن يمد المستهلك بالمعلومات الضرورية، كما يجب أن تكون هذه المعلومات واضحة وصريحة في الاعتراف بحق المستهلك في رفض التعامل بالمحررات الإلكترونية. لكن لا يجوز -وفقًا لأحكام التشريع- تقرير بطلان عقود الاستهلاك؛ بسبب عدم الحصول على رضاء المتعاقد، أو الحصول على تأكيد لرضائه قبول المحرر الإلكتروني، فتوافر هذا السبب فقط غير كافٍ لتقرير بطلان العقد .

ويحظر القانون على القواعد التنظيمية الاتحادية أو الخاصة بالولايات فرض متطلبات أو شروط إضافية علاوة على تلك التي وضعها التشريع الاتحادي، كما يحظر عليها أن تعطي أفضلية لتقنية معينة في إجراء التوقيع الإلكتروني، وإذا رأت إحدى الهيئات أن هناك مبررًا جوهريًا لتلك؛ فيجب أن تراعى ألا تفرض أعباء مبالغ فيها لتوقيع المحرر إلكترونيًا كما يجب أن تكون أحكام اللائحة متوافقة مع مبادئ التشريع الاتحادي في شأن التوقيع الإلكتروني[1] .

Law Review, Vol. 63 (2002); Henry H. Perritt, Jr., Dispute Resolution in Cyberspace: Demand for New Forms of ADR, 15 Ohio St. J of Disp. Resol 675 (2000).

(1) See, for example, Specht v. Netscape Comm'cns Corp., 306 F.3d 17, 26 n.11 (2d Cir. 2002) (assessing whether clicking to download software created enforceable agreement to arbitrate, and noting that the matter of whether "the agreement is a 'written provision' despite being provided to users in a downloadable electronic form… has been settled by [the ESIGN Act]," although ultimately finding that consumers clicking "yes" in the context presented in that case did not manifest assent to license terms

المطلب الثاني

واقع وتطبيقات جرائم التوقيع الإلكتروني وفق القانون الأمريكي

لقد خوّل الكونجرس الأمريكى[١] لقطاع الخدمة السرية سلطة التحقيق فى عمليات جرائم التوقيع الإلكتروني التى تتم عبر الشبكات، والتى تعرف باسم "عمليات التحايل على وسائل الدخول للمعلومات"، وذلك بموجب البند رقم ١٨ من قانون الولايات المتحدة الأمريكية القسم ١٠٢٩، ويضم القسم المذكور تعريفًا عامًا لمصطلح وسائل الدخول للمعلومات، وهو: "أية بطاقة أو لوحة أو رقم كودى أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أى شئ آخر ذي قيمة يمكن استخدامه وسيلة من وسائل بدء نقل الأموال". ومن هنا نرى أن المصطلح يمكن أن يتسع بحيث يشمل بطاقات الائتمان وأرقام حساباتها، وكذا بطاقات الشحن الهاتفية، وأكواد الدخول على التليفونات. ويلاحظ على نص القسم ١٠٢٩ أنه قد منح قطاع الخدمة السرية سلطة ومباشرة فى مواجهة ذلك "العالم الرقمى الخفى" دون أن يشير من قريب أو بعيد لكلمة كمبيوتر[٢]. وإن كان مكتب تقييم التقنية في الولايات المتحدة الأمريكية قد عرّف الجريمة المعلوماتية -ومنها جرائم التوقيع الإلكتروني- بأنها: الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًا[٣]..

---

(١) انظر فى ذلك:

The Hacher crackdown law and Disorder on the Electronic fron – tier by Bruce sterling p.0172,1994.

(2) See, for example, the "Administrative Procedures for Filing, Signing, and Verifying" provided by the U.S. District Court for the Western District of Virginia at http://www.vawd.uscourts.gov/

(3) See, for example, the "Administrative Procedures for Filing, Signing, and Verifying" provided by the U.S. District Court for the Western District of Virginia atp://www.vawd.uscourts.gov/

الفرع الأول

أسباب جرائم التوقيع الإلكتروني في الولايات المتحدة الأمريكية

يأتي في مقدمة أسباب جرائم التوقيع الإلكتروني ما يلي:

أولا: غاية التعلـم

يشير الأستاذ "ليفي" مؤلف كتاب "قراصنة الأنظمة" HACKERS إلى أخلاقيات هؤلاء القراصنة، التي ترتكز على مبدأين أساسيين، هما: أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم، وأن جمع المعلومات يجب أن تكون غير خاضعة للقيود. ويسعي مرتكبو جرائم التوقيع الإلكتروني إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار والربح جراء العقود التي يتم تدشينها عبر الإنترنت، وتعريف الآخرين بمجالات اختصاصهم، ويدع قراصنة الأنظمة نظامًا خاصًا لمجال المعرفة الذي يجذبهم ويعلمهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة، وإن لم تكن قانونية دائمة[(١)].

ثانيًا: السعي إلى الربح عبر جرائم التوقيع الإلكتروني

لاشك أن أحد أبرز أهداف جرائم التوقيع الإلكتروني هو الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة؛ حيث أشارت إحدى الدراسات إلى:

- أن ٤٣% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال.
- ٢٣% من أجل سرقة المعلومات.
- ١٩% أفعال إتلاف.
- ١٥% سرقة وقت الآلة، أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

---

(1) See Berkson v. GoGo LLC, 97 F.Supp.3d 359 (E.D.N.Y. 2015) (establishing general principles for enforceability of internet agreements: (1) the evidence must show that the user had notice of the agreement, (2) the link to the terms is located where users are likely to see it and (3) a "user is encouraged by the design and content of the website and the agreement's webpage to examine the terms clearly available through hyperlinkage.") In this case, the court required that "the offeror must show that a reasonable person in the position of the consumer would have known what he was assenting to" and accordingly distinguished the noticeably smaller hyperlink for the contract terms from the large, colored "Sign In" button.

ثالثًا: الدوافع الشخصية وراء جرائم التوقيع الإلكتروني

إن الدافع لارتكاب جرائم التوقيع الإلكتروني يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم التوقيع الإلكتروني إلى إظهار تفوقهم ومستوي ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، يحاولون إيجاد –وغالباً ما يجدون– الوسيلة إلى تحطيمها، بل والتفوق عليها(١).

وتبدو أكثر المشاكل جسامة -لا في مجال صعوبة اكتشاف وإثبات جرائم التوقيع الإلكتروني- هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب، وهو ما يعرف بالرقم الأسودBlack No.؛ حيث لا يعلم ضحايا هذه الجرائم شيئًا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفًا لفعل الغش، أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل(٢).

---

(١) يميل القراصنة إلى التحدي، وإلى معرفة تفاصيل تكنولوجيا الكمبيوتر، ويبدو أن ولعهم بالكمبيوتر يدفعهم إلى ارتكاب الجرائم. وفي هذا الخصوص يحدثنا الدكتور Perey Black أستاذ علم النفس بجامعة نيويورك: أن القراصنة يتملكهم جميعًا شعور بالبحث عن القوة، ويؤدي ارتكابهم للجرائم -بواسطة الكمبيوتر- إلى تعويضهم عن الإحساس بالدونية.

راجع في ذلك:

CYBER CRIME op. cit. p. 25.

(٢) في إحدى الوقائع الشهيرة تعرّض بنك merchant bank city في بريطانيا لنقل ٨ مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور، ولكن البنك بدل الادعاء على الفاعل قام بدفع مبلغ مليون جنيه له، بشرط عدم إعلام الآخرين عن جريمته، وشريطة إعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيسي.

Scheuplein v. City of W. Covina, No. B206203, 2009 Cal. App. Unpub. LEXIS 7805, at *26–27 (Cal. Ct. App. 2d Dist. Sept. 29, 2009) (finding emails to be authenticated when accompanied with a declaration that the emails were retrieved from the company's computers and the printouts were accurate representations of the retrieved messages)

الفرع الثاني

تصنيف جـرائم التوقيع الإلكتروني بالقانون الأمريكي

تتعدد أنماط الجريمة في مجال التوقيع الإلكتروني، والتي يمكن تصنيفها إلى عدد من المحاور التي تشكل جميعًا انتهاكًا يستحق العقاب، وذلك على النحو التالي:

أولًا: جرائم التوقيع الإلكتروني عبر الاختراق وانتحال الهوية

في جرائم التوقيع الإلكتروني من الممكن الاختراق أو انتحال الهوية، إما ماديًا أو إلكترونيًا؛ فالاختراق المادي يسمح بالدخول في مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية. وأسلوب الاختراق الأكثر شيوعًا هو أن يقف شخص غير مسموح له بالدخول أمام البوابة المغلقة حاملًا بين ذراعية متعلقات خاصة بالحاسب الآلي كالشرائط الممغنطة desbandes، أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب، فيدخل معه في نفس الوقت؛ لذا فإنه يمكن القول بأن التواجد في صالات الحاسبات الآلية هو أمر حتمي لارتكاب هذه الجرائم[١]. وينطوي الفعل غير المشروع -عبر جرائم التوقيع الإلكتروني- على اطلاع غير مسموح به على المعلومات المختزنة في نظم المعلومات، وله صور عديدة.

١- سرقة القائمة. وهي عملية مادية بحتة، يكتفي فيها السارق بسحب القائمة من الطابعة.

٢- الإطلاع على المعلومات. والمقصود بذلك: مطالعة المعلومات التي تظهر على شاشة الحاسب الآلي.

٣- التصنت المجرد على المعلومات. ويتم ذلك عن طريق استخدام مكبر للصوت[٢] والذي يلتقط المعلومات والبيانات.

---

(١) انظر:

D. Parker, op. cit., p. 44 et s.

(٢) قبل أن يقوم Hacker باقتحام شبكة الحاسب الآلي؛ يجب عليه استخدام تسهيلات اتصال لكي يرتبط بالشبكة، وقد تكون تكاليف الاتصال القانوني مع نظام الكمبيوتر المستهدف معرفة الـ Hackers مرتفعة للغاية، وقد يكون من الممكن تعقبها؛ لذا يقوم الـ Hackers بتوظيف أساليب فنية لتجنب هاتين المشكلتين. يقوم الـ Hackers بتوظيف أساليب فينة يطلق عليها عادة الـ Phreaking، ومن تطبيقاتها ما يلي:

١- الاتصال التليفوني بواسطة النغمة:

وهو أسلوب نقلي، يمكن التلاعب -من خلاله- في شبكات الاتصالات عن طريق استعمال تردد النغمات؛ ذلك لأن النغمات يمكن استعمالها لتنشيط وتفعيل رقم تليفون غير متصل، بما يتيح القدرة

كما أن فحص الهوية يرتكز على مجموعة معلومات متوافقة، يستخدمها المستعمل ككلمة السر[١] أو أي جملة خاصة بالمستعمل، أو أي خاصية فسيولوجية، كالبصمة الرقمية، أو

لهذا الشخص استكمال هذه الخطوط غير المتصلة، كما لو كانت خطوطه الخاصة. أما الفوائد المترتبة على هذه التقنية فتشمل: تكلفة المكالمة التليفونية التي تضاف إلى فاتورة التليفون غير المتصل، علاوة على منع حدود أو متابعة أو تقصي هذه المكالمة.

٢- تلاعب Pabx : وهو أسلوب تقني يمكن للشخص -بموجبه- أن يطلب رقم تليفون pabx (وهو صندوق تحويل مُعَدّ، يحتوي على عدد من خطوط التليفون المختلفة). ويتم من خلال توصيل مكالمتهم إلكترونيًا بواحد من الخطوط في هذا الـ pabox، ثم استعمال هذا الخط للأغراض الخاصة.

٣- الاتصال الخارجي بالكمبيوتر: وبموجب هذه الوسيلة يستطيع الشخص أن يتصل برقم تليفون معين، يتيح لهم -بدوره- فرصة الوصول إلى نظام الكمبيوتر أو الوصول إلى مركز اتصالات يتيح لهم نفس المزايا الموضحة في الأسلوبين السابقين.

٤- Austpac : وهي شبكة اتصالات تشرف عليها هيئة المواصلات الرسمية التي تقدم وصلات معينة بين أنظمة الكمبيوتر؛ لأن الفواتير الخاصة باستعمال هذا النظام تعتمد على استعمال شبكة التعرف على المستعملين Network User Identieication Cnut، ويتكون هذا النظام -عادة- من سلسلة من ٩ أرقام، وهي شبيهة -من حيث المبدأ- برقم الـ PIN.

٥- الغش في بطاقات الاعتماد: هذا الأسلوب التقني يتضمن اقتباس تفاصيل بطاقات الاعتماد الخاصة بأحد المشتركين الذي يقوم -بدوره- بطلب مكالمة تليفونية لصالح الطالب، وقيد قيمة المكالمة على بطاقة الاعتماد.

٦- الاعتراض المادي: أن عملية الاعتراض المادي لخط تليفوني هي عملية بسيطة، وتؤدي إلى نفس الفوائد، مثل الاتصال بالنغمة.

٧- الوصلات غير القانونية: وهي عبارة عن تنشيط وتشغيل خدمة غير متصلة، بدون علم شركة الاتصالات، ثم استعمالها حسب رغبتك عن طريق تليفون عادي، بدون أن تتلقى الفاتورة. وهذا النوع من الاعتراض يتميز بأنه دائم ومسمر.

انظر:

Franklinclrk, investigating computer crime, Ed. CRC page 50.

(١) بعض كلمات السر يتم وضعها من خلال مدير النظام المعلوماتي، والبعض الآخر يتم استخدامه من وحي المستخدمين أنفسهم. وبصرف النظر عن ذلك فإن كلمة السر يجب أن تكون مميزة لكل حساب، ويجب تغيير وحذف الحسابات التي ليس لها كلمة سر، وينصح بتجنب استعمال كلمات السر التي يسهل الوصول إليها، مثل استعمال الأسماء الأولى والأخيرة وتاريخ الميلاد وأرقام الضمان الاجتماعي أو رقم رخصة القيادة؛ فهذه الكلمات يمكن التنبؤ بها.

كما يعرف القراصنة كلمات السر الأكثر شهرة، والتي يميل الناس إلى اختيارها؛ لذا يحظر استخدامها، مثل "كلمة سر password"، وكلمة "ادخل Enter"، و"افتح Open" و"كمبيوتر

ملامح الوجه، أو هندسة الكف أو الصوت، بالإضافة إلى أي شيء يمتلكه المستعمل كالبطاقة الممغنطة أو المفتاح المعدني.

وقد استطاع شخص أن يسرق بطاقات ائتمان ممغنطة لكل منها رقم سري يعرفه صاحبه، حيث اتصل بأصحاب هذه البطاقات مدعيًا أنه موظف بالمصرف، وأخبرهم أنه قد نما إلى علمه أن بطاقاتهم قد سرقت، وأنه بحاجة لمعرفة الرقم السري لحمايتهم وتزويدهم ببطاقات جديدة. وهكذا نجح المحتال في الحصول على الأرقام السرية لهذه البطاقات، ثم استخدامها في سرقة مبالغ من المال من الموزعات الآلية للنقود[١]. وفي حالة ثالثة أرسل فيها بعض الطلبة مذكرة لكل مستخدمي الطرفيات في جامعتهم، ذكروا فيها أن أرقام الاتصال قد تغيرت، ومنحوهم أرقامًا جديدة تتصل مباشرة بأجهزة الكمبيوتر الخاص بهم، والتي تمت برمجتها مسبقًا بشكل مطابق لأجهزة الجامعة. وهكذا كان يستخدم المستعمل الرقم السري الخاص به -بدون تردد- عبر التوقيع الإلكتروني، حيث يسجله الطلبة، ويعاودون مراسلتهم مرة ثانية طالبين منهم أن يعودوا لاستخدام رقم الاتصال القديم. ولم تكن تلك سوي لعبة استخدام الطلبة من خلال كلمات السر most de pasdse .

ثانيًا: التوقيع الإلكتروني عبر تعديل العقود بدون إذن من صاحبه.

أصبح تعديل العقود الإلكترونية تقنية سهلة وآمنة ومألوفة من تقنيات جرائم التوقيع الإلكتروني، وتتمثل في تعديل العقود قبل أو أثناء إدخالها في نظم المعلومات، أو في لحظة إخراجها من النظام المعلوماتي. ويمكن إجراء هذه التعديلات بواسطة أي شخص، والذي أسهم أو له حق الولوج في عمليات إنشاء وتشفير وتسجيل ونقل والتحقق من نقل البيانات المخصصة للإدخال في نظم المعلومات. وهناك العديد من الأمثلة التي تنطوي على تزوير أو اختلاس الوثائق واستبدال الشرائط الممغنطة[٢]، أو البطاقات المثقوبة، أو أفعال تحطيم

Computer". ويحذر هذا الاستخدام كلمات السر المرتبطة بالهوية، كما يحذر تجنب كلمات السر- ذات المقطع الكبير، أو تلك المتعلقة بمجموعة حروف أو أرقام.

راجع في ذلك:

E. Quarantiello (cybercrime) p. 94.

(١) راجع:

Burgess, Jean, (August 18, 2009), YouTube: Online Video and Participatory Culture, UK : Polity; 1 edition.

(٢) الشريط الممغنط: وهو شريط مغناطيسي يحوي المعلومات الخاصة بحامل البطاقة بعد تشفيرها بصورة إلكترونية، ويمكن قراءة هذه البيانات باستعمال النهاية الطرفية الإلكترونية الموجودة بمقار البنوك ومنافذ البيع.

إدخال البيانات، أو إحداث ثقوب إضافية في البطاقات المثقوبة، أو على العكس سد هذه الثقوب. وأخيرًا أفعال التحييد، أو إلغاء المراقبات اليدوية[١].

ومن تحليل إجراء معهد ستانفورد الدولي للأبحاث (SRI) بالولايات المتحدة شمل مائة حالة من حالات إساءة استخدام الحاسبات؛ تبين أن ٣٧.٦% منها قد ارتكب بإحداث تغيير مباشر direct modification في العقود الإلكترونية عبر تغيير التوقيعات أو تقليدها أو تعديلها، بينما وقع ٩.٥% منها فقط نتيجة تعديل وتلاعب في البرامج المستخدمة[٢].

ثالثًا: استغلال تقنية Superzapping : في التلاعب بالتوقيع الإلكتروني

يطلق مصطلح "Superzapping" على تقنية الاستخدام بأسلوب غير شرعي للبرامج الخدمية التي تؤثر على المعطيات المحفوظة في جهاز الكمبيوتر أو في ذاكرته، وهذا التأثير قد يكون بالتعديل أو الإلغاء أو النسخ أو الإدخال أو الاستعمال أو المنع. ومصطلح "Superzapping" مشتق اسمه من Superzap، وهو البرنامج الخدمي الذي يستخدم في العديد من مراكز نظم المعلومات كأداة نظام. وأي مركز نظم معلومات يسير وفقًا لخطة عمل ناجحة وفعَّالة لابد له من برنامج يلجأ إليه عند الحاجة؛ بغرض التعديل أو الكشف عن أي غموض في جهاز الكمبيوتر. وأحيانًا تتوقف أجهزة الكمبيوتر أو لا تعمل بالكفاءة المرجوة، ويصبح إصلاحها أو إعادة تشغيلها غير مفيدة، وأحيانًا أخرى يحتاج الكمبيوتر لعملية تعديل لا تسمح بها أساليب الولوج المألوفة. وفي مثل هذه الحالات فإن برامج الولوج الإجمالية تكون ضرورية؛ حيث يمكن تشبيهها -في مثل هذه الأحوال- بمفتاح يستخدم في حالات فَقْد كل المفاتيح الأخرى[٣].

Document that is being prepared with a view to submission to the European Union in Brussels.

(١) انظر في ذلك:

D. parker Op. Cit. p. 77

(2) In the US, Internet sales are currently exempt from local taxation so long as the buyer and seller reside in different states; this rule, carried over from traditional policies toward mail-order merchandising, has likely distorted locational decisions on the margin, leading retailers who would otherwise have opted for a national distribution system to concentrate their warehouse facilities in a few jurisdictions to maximize the value of the interstate tax exemption

(٣) راجع:

Nie, Norman and Erbing, Lutz (2000). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co

رابعًا: جريمة العدوان على الائتمان الرقمي من خلال توقيعات مضللة

تتخذ أشكال العدوان على الائتمان عبر جرائم التوقيع الإلكتروني أحد شكلين:

(١) الاستيلاء على أرقام كروت الائتمان؛ إذ إن لكل كارت ائتمان عنوانًا فرديًا خاصًا ID number يتميز به عن غيره، تمنحه المؤسسة المالية للمشترك لديها في هذه الخدمة، بحيث تحل محل التعامل بالأموال السائلة. وعلى الرغم من أن اتجاهًا يذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر الإنترنت إنما هي على درجة كبيرة من الصعوبة، كعملية تقنية تحتاج إلى برمجة معقدة، وبالتالي تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر الإنترنت؛ فإن حالات اختلاس هذه الأرقام عبر الإنترنت من الخطورة بمكان، وهو ما دفع المشروع الفيدرالي الأمريكي إلى عدها جريمة وفق ١٨ U.S.C. 1030(a)(1)(7) [(١)]. فقد حدث في عام ١٩٩٦م أن تم اختراق حاسوب محمول LAPTOP يحتوي على ٣١٤.٠٠٠ رقم لكروت ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا، وفي عام ١٩٩٧م قام Carlos Sadalgo Jr. (37 عامًا) باستخدام حاسوب في جامعة سان فرانسيسكو، واختلس أسماء مالكي وأرقام log-ons عدد ١٠٠.٠٠٠ كارت ائتمان، وكذلك بيانات أخرى من خلال اختراقه لمجموعة مزودي خدمات إنترنت ISPs، وقام بوضعها على اسطوانة مضغوطة CD، ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة، وحوكم سادالوجو وعوقب بالسجن ثلاثين شهرًا [(٢)].

---

(١) انظر:

- Hughes, Carole (1999). The Relationship of Use of the Internet and Loneliness among College Students. Dissertation Abstract. Vol. 60 (3 – A).

(2) The CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a « protected computer » for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency ; 2) committing fraud or extortion ; 3) transmitting destructive viruses or commands ; 4) trafficking in stolen passwords ; or 5) threatening to damage a computer system in order to extort money or other things of value. A « protected computer » is a computer 1) used exclusively by a financial institution or the United States Government ; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government ; or 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely

(٢) العدوان على التوقيع الإلكتروني ذاته: التوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان -ولا يزال- أحد اهتمامات المشرع المقارن؛ ففي إطار النظام القانوني الإنجليزي استطاع القضاء الإنجليزي في قضية Goodman V. J. Eban. Ltd تحديد الأصالة Authentication، بالإضافة إلى مناهج التوقيع الإلكتروني، على إن الأمر لم يقف عند هذا الحد، بل قامت إدارة التجارة والصناعة الإنجليزية Department of Trade and Industry في مارس ١٩٩٩م بإصدار وثيقة استشارية Consultation Document بعنوان Building Confidence in Electronic Commerce، تم هيكلتها على ضوء التوجيه الأوروبي المشار إليه أعلاه، وبناء على هذه الوثيقة أصدر البرلمان الإنجليزي قانون الاتصالات للمملكة المتحدة المؤرخ ٢٠٠٠/٥/٢٥ The UK Electronic Communications Act الذي ينص في القسم (٧) منه على تعريف للتوقيع الإلكتروني[(١)]. وأما المشرع البلجيكي فقد أصدر القانون المؤرخ ٢٠ أكتوبر ٢٠٠٠م الذي أضاف إلى القانون المدني البلجيكي المادة (٢٢٨١) مقررًا الاعتراف بالتوقيع الإلكتروني إلى جوار اعترافه بالتوقيعات التي ترد عبر الفاكس والبريد الإلكتروني والبرقيات والتلكس وبأية وسيلة أخرى[(٢)].

أما المشرع الأمريكي فقد اهتم اهتمامًا كبيرًا بموضوع التوقيع الإلكتروني؛ لكونه أداة فعالة في حركة المعاملات المدنية والتجارية، وتحديدًا كان للمشرع الولائي الأمريكي الأسبقية في هذا الإطار؛ حيث أصدر مشرع ولاية Utah في عام ١٩٩٥م أول تشريع للتوقيع الإلكتروني The digital signature act of 1995، الذي تم

---

local computer crimes, but the multistate nature of Internet transmission suggests that almost any Internet activity will amount to « interstate commerce ». see : James Garrity & Eoghan Casey. Internet Missue in the Workplace : A Lawyer's Primer, op. cit., at 14.

(1) Section 7(1) provides: In any legal proceedings:

(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and

(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data, See: Chris Reed-What is a signature?, op. cit., at 15.

(2) See generally A.M. Spence, supra, note 13; Richard Craswell, Passing on the Costs of Legal Rules:

Efficiency and Distribution in Buyer–seller Relationships. Stanford Law Review 43: 361–398 (1989).

إلغاؤه وإعادة إصدار تشريع آخر في عام ١٩٩٦م، وكان من بين الأغراض التي سعى مشرع ولاية يوتا الأمريكية بإصدار هذا التشريع هو التخفيف من حدة الاحتيال بالتزوير والنصب على التوقيعات ككل[١]. ثم تلا ذلك ولاية كاليفورنيا بقانون ٥ سبتمبر ١٩٩٥م، الذي -بعد أن اعتبر التوقيع الإلكتروني في مرتبة التوقيع المادي- قام بتعريف التوقيع الإلكتروني في القسم (٥-١٦) من كود الحكومة الولائية The Government Code بأنه "تحديد إلكتروني للهوية تم إعداده بواسطة الحاسوب ومعتمَد من قِبل مستخدمه؛ لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي، ولكن لا يشمل هذا التعريف إمكانيات التشفير"[٢]. ولتتولى بعد ذلك مظاهر الاهتمام بالتوقيع الإلكتروني من قِبل المشرع الولائي الأمريكي، مثل تشريع ولاية أويامنغ Wyoming لعام ١٩٩٥م، ثم تشريع ولاية واشنطن Washington الصادر في ٢ مارس ١٩٩٦م، الذي اعتمد على تشريع ولاية يوتا. ومما تجدر الإشارة إليه: أن تشريع واشنطن تقرر نفاذه مع الأول من شهر يناير ١٩٩٨م.

وقد اهتمت التشريعات المقارنة بظاهرة الترويج السمعي/المرئي الفاضح، وبصفة خاصة موضوع دعارة الأطفال التي أخذت من المشرع المقارن اهتمامًا كاملًا في هذا الإطار. ففي الولايات المتحدة نشط الفقه والقضاء والتشريع في دراسة نظم القانون الأخلاقي وعملية نظمه في القانون الجنائي، على إثر الكارثة الحقيقية الممثلة في دعارة الأطفال عبر الإنترنت، وهي ظاهرة اعتبرت خطرًا على المُثُل القومية التي تقوم عليها دعائم المجتمع الأمريكي[٣]؛ لكون الإنترنت وسيلة تجعل ارتكاب مثل هذه الجرائم سهلًا، أو بمعنى أكثر دقة: تجعله من الممكن، ومن ثم توفر المناخ الملائم للحصول على ضحايا في مثل هذه النوعية من الجرائم. ومثل هذا الأمر جعل الفقه والقضاء والتشريع في الولايات المتحدة يتجه إلى الاستمرار

---

(1) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

(2) « An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature », id at 431.

(3) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for protecting kids from pornography and their applicability to other inappropriate internet content, op. cit, P.1.

في دراسة دعارة الأطفال عبر الإنترنت، وذلك بإيعاز من البيت الأبيض الأمريكي في بيانه المؤرخ ١٩٩٦/١/٢٦م الذي صدر ردًا على إلغاء القضاء الأمريكي لنصوص في قانون أخلاق الاتصالات لسنة ١٩٩٦م المعدل للقانون الصادر في ١٩٣٦[(١)].

ونتيجة لمبادرة البيت الأبيض المذكورة؛ فإنه في عام ١٩٩٨م أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي الجنسي[(٢)]، ولقد تضمن هذا القانون حث النائب العام الأمريكي على التعاون مع الأكاديمية الوطنية للعلوم/ مجلس البحوث الوطنية فيها على إعداد دراسة متكاملة لبحث مدى إمكانية تفعيل القانون الجنائي في القضايا الأخلاقية، والتي أنتجها التعامل السلبي مع تقنية المعلومات/ الإنترنت، على أن يتم وضع هذا التقرير في خلال سنتين من تاريخ صدور القانون المذكور. ولقد تم وضع التقرير في العام ٢٠٠٠م، متضمنًا الخطوات الفعالة من الوجهة العلمية من قِبل الأستاذين Herb Lin, PhD, Michele Kipke, PhD، بالتعاون مع جهات أخرى ذات علاقة. ولقد وجد التقرير أن مشكلة الدعارة المصوّرة Pornography ذات أساس من ناحيتين، الأولى: كونها تُعد داخلة في نطاق اهتمام قسم اجتماعي له دور في المجتمع، حتى وإن كان سلبيًا. أما الناحية الثانية: فيتعلق بالتحديد القضائي لمصطلح "الدعارة"، الذي يتخذ مفهومًا يتسع ليشمل الطابع المتغير فيها vary widely من نطاق اجتماعي إلى آخر Vary by community[(٣)].

كذلك يجرم القانون الأمريكي تشغيل Employ القُصَّر Minors أو دفعهم Induce إلى المشاركة في صور متحركة Visual depiction تتضمن حركة جنسية مباشرة، إذا كان التصوير قد تم باستخدام حاسوب عبر مؤسسات تجارية في الولايات أو في خارج الولايات المتحدة (١٨ US Code Sec. 2251). كذلك يحظر القانون الأمريكي استخدام الحاسوب لبيع Sell أو نقل Transfer

(1) Reno v. ACLU, US Supp. 521 U.S. 844 (1997).

(2) Protection of children from Sexual predators act of 1998 Title 9 section 901. US Code. Id at 422.

(3) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.

حق الوصايا على قاصر، مع العلم بأن هذا القاصر سوف يتم استخدامه لإعداد صور متحركة تتضمن سلوكًا جنسيًا مباشرًا (US Code Sec. 2251 (A ١٨)). كما يجرم القانون الأمريكي استخدام الحاسوب لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (US ١٨ Code Sec. 2252 & 2252 (A))[١].

(1) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

المبحث الثاني
الأحكام العامة لجرائم التوقيع الإلكتروني في القانون الكويتي

مقدمة

من القوانين من أُطلِق عليه اسم (السجل أو المستند الإلكتروني)، ومنها: قانون المعاملات الإلكترونية الكويتي الذي عرَّفه في المادة (١) بأنه: "مجموعة بيانات أو معلومات يتم إنشاؤها أو تخزينها أو استخراجها أو إرسالها أو إبلاغها أو استقبالها كليًا أو جزئيًا بوسيلة إلكترونية، على وسيط ملموس أو على أي وسيط إلكتروني آخر، وتكون قابلة للاسترجاع بشكل يمكن فهمه[(١)] . ولقد عرّف المشرع الكويتي في المادة (١٣) من قانون الإثبات "السند العادي" بقوله: "السند العادي هو الذي يشتمل على توقيع من صدر عنه، أو على خاتمه، أو بصمة إصبعه، وليست له صفة السند الرسمي". ولو دققنا في هذا النص فإننا نجد أن الأسناد العادية –وفق القانون الكويتي– تستمد قوتها من توقيع صاحب الشأن عليها بإمضائه، أو خاتمه، أو بصمته. وفي الحقيقة فإن المشرع الكويتي هنا -أيضًا- لم يكن موفقًا بإضافته كلمة "إصبعه"، والتي لا يستوي تفسيرها على غير منطوقها، ويفهم منها قصد المشرع بأن البصمة يجب أن تكون على المحرر الورقي. ولو أن المشرع اكتفى بتعبير البصمة لكان اللفظ أكثر شمولًا، وهذه صفة القاعدة القانونية[(٢)]. وهذا ما نرى أن على المشرع تفاديه بحذف "إصبعه" من نص المادة على الأقل؛ حتى يسمح للاجتهاد القضائي الكويتي -فيما إذا عرضت عليه قضية تتعلق بمحرر الكتروني يراد منه إثبات عقد الكتروني- إمكانية اعتماد أي شكل جديد من أشكال البصمة، ولا يخفى أن البصمة ما هي إلا نوع من أنواع التوقيع عمومًا[(٣)].

خصوصًا إذا علمنا أن المادة (١٦) من قانون الإثبات، والتي تعترف للرسائل العادية بحجيتها في الإثبات الجنائي إذا تحققت فيها شروط معينة، والأمر ذاته ينطبق على البرقيات، إذا كان لها أصل محفوظ في دائرة البريد، لا يمكننا تطبيقها على الرسائل

---

(١) محمود عبد الرحمن محمد، مدى حجية الوسائل الإلكترونية في إثبات المعاملات المدنية والتجارية والإدارية طبقًا لقانون المعاملات الالكترونية الكويتي، مجلة كلية القانون الكويتية العالمية، العدد١، السنة السادسة، العدد التسلسلي ٢١، جمادي الآخرة-رجب ١٤٣٩هـ-مارس ٢٠١٨م، ص. ١٦٢

(٢) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون المصري والكويتي، رسالة ماجستير غير منشورة، مصر: جامعة مدينة السادات، كلية الحقوق، ٢٠٢٠، ص. ٧٨

(٣) محمد ذعار العتيبي، النظام القانوني للعقد الإلكتروني. دراسة مقارنة بين التشريعين الكويتي والأردني، رسالة ماجستير غير منشورة، عمان، جامعة الشرق الأوسط، كلية الحقوق، ٢٠١٣، ص.١٠٣.

الإلكترونية؛ لأن حصر فهمه لها بالكتابة على الورق، واشترط التوقيع بالاسم. الأمر الذي لا يمكن معه اعتبار المحرر الإلكتروني دليلًا ينهض بمهمة الإثبات الجنائي سواء بسواء مع المحرر المكتوب في ظل النصوص الحالية، واعتباره كالرسائل التي قصدها المشرع في حكم هذه المادة. ولو أردنا اللجوء إلى المادة (١٨) من قانون الإثبات، والتي تعتبر دفاتر التجار حجة عليهم؛ بما أننا نبحث في مجال التجارة الإلكترونية، والغالب الأعم من المعاملات التي تجري فيها تكون بين التجار؛ سنصطدم -أيضًا- بالشروط التي فرضها المشرع لصحة وسلامة هذه الدفاتر؛ لتكون دليلًا صالحًا للإثبات الجنائي.

ويرى البعض [١] أن الرسائل الإلكترونية يمكن الاعتداد بها؛ كونها مبدأ ثبوت بالكتابة إذا ثبت صدورها عن الطرف المراد التمسك بها في مواجهته، وتجعل التصرف المدعى به قريب الاحتمال. ولابد من الإشارة إلى أن شكلية الكتابة اشترطها المشرع في بعض العقود، كعقود الشركات، والهبة، وبيع وإيجار السفن؛ نظرا لأهميتها، كما قد تكون باتفاق الأطراف، فالأصل أن اشتراط الكتابة -في العقود الرضائية- يكون لمجرد إثباتها، إلا أنه ليس ثمة ما يمنع المتعاقدين من اشتراط تعليق انعقاد العقد على التوقيع على المحرر المثبت له؛ إذ ليس في هذا الاتفاق ما يخالف النظام العام، وهذه الشكلية -سواء القانونية أو الاتفاقية- تقف حائلًا أمام الإثبات بالوسائل الإلكترونية، وهذا أمر منطقي يتماشى مع المبررات التي دفعت المشرع أو الأطراف إلى اشتراط الشكلية من حيث هي شريطة انعقاد. [٢] ومن ثم يمكن تقسيم المبحث الحالي على النحو التالي:

المطلب الأول: تعاطي المشرع الكويتي مع جرائم التوقيع الإلكتروني.

المطلب الثاني: إشكاليات جرائم التوقيع الإلكتروني في القانون الكويتي في ضوء رؤية مقترحة.

---

(١) - خالد فيصل الهندي، مفهوم التوقيع الإلكتروني وحمايته، رسالة ماجستير غير منشورة، الكويت: جامعة الكويت، كلية الحقوق، ٢٠٠٤، ص١١٠.

(٢) - لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، الإسكندرية، دار الفكر الجامعي ٢٠١٠، ص٢٥٤.

المطلب الأول

تعاطي المشرع الكويتي مع جرائم التوقيع الإلكتروني

في قانون المعاملات الإلكترونية الكويتي لعام ٢٠١٤م: عرَّفت المادة الأولي من هذا القانون التوقيع الإلكتروني بأنه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو اشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة، في مستند أو سجل إلكتروني، أو مضاف عليها أو مرتبطة بها بالضرورة، ولها طابع يسمح بتحديد هوية الشخص الذي وقَّعها ويميزه عن غيره "[(١)].

أولًا: مدى حجية المحررات الإلكترونية في الإثبات الكويتي.

لقد عرَّفت المادة (١) من قانون المعاملات الإلكترونية الكويتي الكتابة الإلكترونية بأنها: "كل حروف أو أرقام أو رموز أو أي علامات أخرى، تثبت على دعامة إلكترونية أو رقمية وضوئية أو أيه وسيلة أخري مشابهة، وتعطي دلالة قابلة للإدراك، ويمكن استرجاعها لاحقًا". ويتضمن نص القانون الكويتي أن الكتابة الإلكترونية لا تُدوّن علي الورق كالكتابة العادية، بل علي دعامة أخري غير مادية، سواء أكانت إلكترونية أم رقمية أم ضوئية أم غيرها، وينظر إليها، لا من حيث ارتباطها بالدعامة المستعملة في تدوينها، بل من حيث وظيفتها في إعداد الدليل علي وجود التصرف القانوني، وتحديد مضمونه، بما يُمكّن أطرافه من الرجوع إليها في حالة نشوب خلاف فيما بينهم، وهو ما يستلزم أن تعطي هذه الكتابة دلالة قابلة للإدراك، أي: أن تكون مُدوّنة بحروف أو رموز أو أي علامات أخرى معروفة ومفهومة للشخص الذي يراد الاحتجاج بها عليه، وإلا تتعرض للتعديل أو التحريف، وأن تتصف بالاستمرارية والثبات؛ حتي يمكن بذلك استرجاعها لاحقًا، وحينئذ تأخذ حكم الكتابة التقليدية.

وقد وضع المشرِّع في القوانين المنظمة للمعاملات الإلكترونية شروطًا معينة في المحرر الإلكتروني؛ حتى يمكن قبوله كدليل إثبات مثل المحرر التقليدي. ونورد -فيما يلي- النصوص القانونية التي أوردت هذه الشروط، ثم نتولى شرحها تباعًا، فقد نصت المادة (٩) من قانون المعاملات الإلكترونية الكويتي على هذه الشروط بقولها: "يشترط في المستند أو السجل الإلكتروني المنتج لآثاره القانونية أن توافر الشروط الآتية مجتمعة:[(٢)]

---

(١) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون المصري والكويتي، مرجع سابق، ص.٨٣.

(٢) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون المصري والكويتي، مرجع سابق، ص.٨٥.

أ) إمكان الاحتفاظ به بالشكل الذي تم إنشاؤه عليه، أو إرساله، أو تسليمه، أو بأي شكل يَسهُل به إثبات دقة البيانات التي وردت فيه عند الإنشاء والإرسال أو التسليم.

ب) أن تكون البيانات الواردة فيه قابلة للاحتفاظ بها وتخزينها، بحيث يمكن الرجوع إليها في أي وقت.

هـ) أن تدل البيانات الواردة فيه على هوية من ينشؤه أو يتسلمه وتاريخ ووقت الإرسال أو التسليم.

ح) أن يتم الحفظ في شكل مستند أو سجل إلكتروني طبقًا للشرائط والأسس التي تحددها الجهة المختصة التي يخضع هذا النشاط لإشرافها.

بمراجعة نص القانون الكويتي، ونصوص القوانين المقررة؛ يتبين أن المحرر الإلكتروني يمكن أن يقوم بالدور الذي يقوم به المحرر التقليدي في إثبات التصرفات القانونية (العقود) مادام يمكن قراءته، ويدل بدقة على مضمون التصرف القانوني الذي يتضمنه، ويكون كذلك إذا كان مدوّنًا على دعامة إلكترونية تضمن له الاستمرار بما يمكن الأطراف من الرجوع إليه عند الضرورة، ويوفر لهم الثقة في صح بياناته وعدم تعرضها للتعديل أو التحريف أو الزوال[١] . وكي يكتسب المحرر الإلكتروني حجية قانونية في الإثبات -وفقًا للمادة (٩) من قانون المعاملات الإلكترونية الكويتي وما يقابلها في القوانين المقارنة- يجب أن تتوافر فيه الشروط التالية:[٢]

-"(الشرط الأول) إمكان الاحتفاظ بالمحرر بالشكل الذي تم إنشاؤه عليه، أو إرساله، أو تسلمه، أو بأي شكل يسهل به إثبات دقة البيانات التي وردت فيه عند الإنشاء والإرسال أو التسليم.

ويتم حفظ المحررات الإلكترونية عن طريق تدوينها على دعامات إلكترونية (غير ورقية)، ومنها: الأقراص المدمجة، أو الأقراص المغنطة، أو الأقراص الضوئية، أو الذاكرة الإلكترونية، أو الشريط المغناطيسي، إلى غير ذلك. وتحفظ هذه الدعامات بواسطة جهات معتمدة بطريقة لا يمكن الوصول إليها إلا من ذوي الشأن.[٣]

---

(١) محمود عبد الرحمن محمد، مدى حجية الوسائل الإلكترونية في إثبات المعاملات المدنية والتجارية والإدارية طبقًا لقانون المعاملات الالكترونية الكويتي، مرجع سابق، ص.١٥٨.

(٢) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون المصري والكويتي، مرجع سابق، ص.٩٠.

(٣) حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة ، ٢٠٠٠م، ص ١١ وما بعدها، ضياء الدين مشيمش، التوقيع الإلكتروني:

- (الشرط الثاني) أن تكون البيانات الواردة في المحرر قابلة للاحتفاظ بها وتخزينها، بحيث يمكن الرجوع إليها في أي وقت.

مؤدي هذا الشرط أنه -كي يُحتَجّ بالبيانات الواردة في المحرر الإلكتروني- لا يكفي إمكانية الاحتفاظ بالمحرر ذاته، بل يجب -إلي جانب ذلك- أن تكون هذه البيانات قابلة -أيضًا- للاحتفاظ بها وتخزينها، بحيث يمكن الرجوع إليها في أي وقت، وكلما كان ذلك لزم مراجعة بنود المعاملة أو عرضها علي القضاء عند حدوث خلاف بين أطرافها، إلي غير ذلك [(١)]. وفي هذا الصدد: تجدر الإشارة إلي أن الخصائص المادية لبعض الدعامات الإلكترونية التي تستخدم لحفظ المعلومات -مثل الأقراص المغنطة- قد تعيق تحقق هذا الشرط؛ نظرًا لأنها تتميز بقدر كبير من الحساسية، مما يعرضها للتلف مع طول الوقت، نتيجة اختلاف قوة التيار الكهربائي أو الاختلاف الشديد في درجات الحرارة تنزيلها علي جهاز كمبيوتر، وينتج عن ذلك عدم إمكان الاحتفاظ بالمعلومات المحفوظة عليها في غير قليل من الأحوال لمدة طويلة. ولكن التطور في هذا المجال مستمر، وكل يوم تظهر فيه وسائل جديدة ذات سعة كبيرة ودرجة أمان وحماية فاعلة، مثل: أقراص الليزر، واسطوانات (DVD)، والفلاش ميموري، وشرائح الذاكرة وغيرها. وتجيز الفقرة الثانية من المادة (١٠) لأي شخص أن يستعين بخدمات شخص آخر مرخص له بحفظ المستندات والبيانات واسترجاعها إذا تطلب القانون حفظها[(٢)].

<u>- (الشرط الثالث) أن تدل البيانات الواردة في المحرر علي هوية من ينشئه أو يستلمه وتاريخ ووقت الإرسال أو التسلم.</u>

مقتضي هذا الشرط: أنه كي يُعوَّل على البيانات الواردة في المحرر الإلكتروني بوصفها دليلا لإثبات المعاملة محل المحرر؛ يجب أن يتبين منها هوية من أنشأ المحرر أو من يستلمه، وكذلك تاريخ ووقت إرساله أو تسلمه [(٣)] .

دراسة مقارنة ، دار صادر للمنشورات الحقوقية، بيروت، الطبعة الأولي، دون سنة نشر، ص ٧٧ وما بعدها.

(١) محمد المرسي زهرة، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، الطبعة الأولي ، ١٩٩٥م، ص ٢٩ وما بعدها، عبيدات لورنس، إثبات العقد الإلكتروني. رسالة ماجستير معهد الدراسات العربية. جامعة الدول العربية، القاهرة، ص ١٠٢ وما بعدها.

(٢) نضال سليم اسماعيل برهم، أحكام عقود التجارة الإلكترونية، رسالة ماجستير، جامعة عمان العربية، دار الثقافة، الأردن ٢٠٠٥م، ص ١٥٧ وما بعدها.

(٣)عيسى غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٦م، ص ١٢٨ وما بعدها.

- (الشرط الرابع) أن يتم الحفظ في شكل مستند أو سجل الكتروني طبقًا للشرائط والأسس التي تحددها الجهة المختصة التي يخضع هذا النشاط لإشرافها.

مؤدي هذا الشرط أنه يجب أن يحفظ المستند أو السجل وما دُوِّن فيه من معلومات أو بيانات بطريقة الكترونية، ولا يعتمد الحفظ الورقي أو الحفظ التقليدي عن طريق الكتابة؛ وذلك حتى يسهل الرجوع للمعلومات أو البيانات المحفوظة كلما كانت هناك حاجة لذلك، ويتم الحفظ الإلكتروني للمستند أو السجل في موقع ذي الشأن على شبكة الإنترنت أو في الحاسب الآلي الخاص به. ويمكن أن تنسخ صور منه على شرائط مرنة أو على أقراص مدمجة؛ بهدف الحفاظ على أمن المعلومات أو البيانات الواردة في المستند أو السجل. وكل ذلك طبقًا للشرائط والأسس التي تحددها الجهة المختصة المرخص لها بالمزاولة الخدمات الإلكترونية والتي يخضع هذا النشاط لإشرافها[١] .

ومن الجدير بالذكر: أن اللائحة التنفيذية لقانون المعاملات الإلكترونية الكويتي - الصادرة بتاريخ ٤ يناير ٢٠١٥م- قد تعرضت في الفصل الثاني منها لحفظ واسترجاع المستندات والسجلات الإلكترونية.

ثانيًا: تعاطي المشرع الكويتي مع الجرائم المرتبطة بالتوقيع الإلكتروني.

نص المشرع الكويتي على هذه الجرائم من المادة الرابعة إلى غاية المادة العاشرة، وهي تتعلق باستخدام الأنظمة المعلوماتية والمواقع للاعتداء على المراسلات أو المقدسات الدينية ورموز الدولة أو الأموال والأمن؛ حيث جاء في الفقرة الثالثة من المادة الرابعة السالفة الذكر ما يلي: "... أو التقط أو اعترض عمدًا دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات".[٢] ولقد أحسن المشرع الكويتي صنعًا عندما نص على هذا السلوك المجرم، والذي يتعلق بالتصنت أو التقاط أو اعتراض الموجات أو الترددات، خاصة تلك المتعلقة بالبث التلفزيوني المشفر، وهو ما يعرف "بإحداث التداخل"، الذى يكون الهدف منه التشويش الذي تعاني منه بعض القنوات التلفزيونية المعروفة[٣]. في حين نصت المادة التاسعة من قانون مكافحة جرائم تقنية المعلومات الكويتي على أنه: "يعاقب بالحبس مدة لا تجاوز عشر سنوات، وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار، أو بإحدى هاتين العقوبتين؛ كل من قام -عن

---

(١) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الإلكترونية بالقانون المصري والكويتي، مرجع سابق، ص٩٣.

(٢) - جاء في نهاية الفقرة: ".. فإذا أفشى ما توصل إليه؛ يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار، أو بإحدى هاتين العقوبتين".

(٣) بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي. دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، العدد٤، السنة الخامسة، العدد التسلسلي ٢٠ ربيع الأول -ربيع الثاني ١٤٣٩هـ- ديسمبر ٢٠١٧م، ص. ٣٠٠.

طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات- بغسل أموال أو بتحويل أموال غير مشروعة، أو بنقلها، أو بتمويه، أو بإخفاء مصدرها غير المشروع، أو قام باستخدامها، أو اكتسابها، أو حيازتها؛ مع علمه بأنها مستمدة من مصدر غير مشروع، أو بتحويل الموارد أو الممتلكات مع علمه بمصدرها غير المشروع؛ وذلك بقصد إضفاء الصفة المشروعة على تلك الأموال".

ظروف التشديد والتخفيف:

جاء في المادة (١١) من قانون مكافحة جرائم تقنية المعلومات الكويتي ما يلي: "لا تقل عقوبة الحبس أو الغرامة التي يحكم بها عن نصف حدها الأقصى إذا اقترنت الجريمة بأي من الظروف الآتية:[١]

- ارتكاب الجريمة من خلال عصابة منظمة.
- شغل الجاني وظيفة عامة، وارتكابه لها مستغلاً سلطته أو نفوذه.
- التغرير بالقُصَّر ومن في حكمهم من ناقصي الأهلية، أو استغلالهم.
- صدور أحكام سابقة من المحاكم الوطنية، أو الأجنبية بموجب الاتفاقيات المصادق عليها بإدانة الجاني بجرائم مماثلة".

وقد أحسن المشرع الكويتي بالنص على ظروف التشديد هذه؛ إذ إن الكثير من هذه الجرائم قد تتم وفق مخطط من طرف منظمة أو عادة ما تقع من أشخاص يشتغلون في وظيفة تسهل لهم ارتكابها. وتنص الفقرة الثانية من المادة المذكورة أعلاه على ظروف التخفيف؛ حيث أجازت للمحكمة أن تعفي من العقوبة كل من بادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة، فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق؛ تعين -للإعفاء من العقوبة- أن يكون من شأن الإبلاغ ضبط باقي الجناة في حالة تعددهم، وإن كنا نرى أنه كان من الأفضل لو كان الإعفاء من العقوبة مرتبطًا بالقبض على الجناة، وليس مرتبطًا بالعلم بالجريمة وبدء التحقيق؛ لأن هذا النوع من الجرائم يصعب إثباته ولا يتم الإبلاغ عنه عادة؛ لذا فنحن بحاجة إلى فتح المجال والترغيب، وليس العكس[٢].

---

(١) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون المصري والكويتي، مرجع سابق، ص.١٢٣.

(٢) بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي. دراسة مقارنة، مرجع سابق، ص.٣٠٩.

الأحكام الخاصة بالعقوبات:

نص المشرع الكويتي على العقوبات التكميلية في المادة الثالثة عشر؛ حيث جاء فيها: "يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجرائم أو الأموال المتحصلة منها، ويجوز الحكم بإغلاق المحل أو الموقع الذى ارتكب فيه أيّ من هذه الجرائم؛ إذا كان ارتكابها قد تم بعلم مالكها لمدة لا تزيد على سنة بحسب الأحوال، مع عدم الإخلال بحقوق الغير حسن النية، أو بحق المضرور في التعويض المناسب، ويكون الحكم بإغلاق المحل أو الموقع وجوبيًا إذا تكرر ارتكاب أي من هذه الجرائم بعلم مالكها".

في هذه الحالة يتكلم المشرع الكويتي عن إمكانية فرض بعض العقوبات التكميلية، والمتمثلة في المصادرة والإغلاق. وما يمكن أن نلاحظه هنا: هو أن المشرع الكويتي جعل الحكم بهذه العقوبات جوازيًّا، وهو أمر لا يستقيم مع خطورة هذه الجرائم؛ فالأموال والوسائل التي استعملت في ارتكاب هذه الجرائم يجب أن تصادَر، والمواقع والمؤسسات الضالعة فيها يجب أن تُغلَق إذا لم نقل في كل الجرائم، فعلى الأقل أخطرها مثل الإرهابية والإباحية والماسّة برموز الدين والدولة. ثم إن المشرع الكويتي لم ينتبه إلى عقوبة تكميلية مهمة جدًا هي نشر الحكم؛ لأنه يسهم في تعريف الناس بهؤلاء المجرمين وهذه المؤسسات أو المواقع.

ثالثًا: أحكام الجانب الإجرائي لقانون مكافحة جرائم تقنية المعلومات الكويتي.

ما يؤخذ على المشرع الكويتي أنه لم يتطرق بالتفصيل للجهاز الخاص بمتابعة هذا النوع من الجرائم المرتبطة بالتوقيع الإلكتروني، إلا ما ورد في المادة الخامسة عشرة، والتي جاء فيها: "للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص ضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون ،وتحرير المخالفات عنها، وإحالتها إلى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهيلات اللازمة لهؤلاء الموظفين".

كما نتمنى أن ينص المشرع الكويتي على جهاز أو هيئة وليس مجرد الإشارة إلى موظفين؛ لأن هذا النوع من الجرائم ذو طبيعة خاصة، يتطلب وجود ضبطية أو جهازخاص وموظفين ماهرين يتمتعون بكفاءة عالية في مجال تكنولوجيا الإعلام والاتصال وتقنية المعلومات. ومن المهام الموكلة للهيئة نذكر ما يلي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من جرائم التوقيع الإلكتروني ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من جرائم التوقيع الإلكتروني ومكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة جرائم التوقيع الإلكتروني من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.
- تجميع وتسجيل وحفظ المعطيات الرقمية، وتحديد مصدرها ومسارها؛ من أجل استعمالها في الإجراءات القضائية.

المطلب الثاني

إشكاليات التوقيع الإلكتروني في القانون الكويتي في ضوء رؤية مقترحة

لم ينص المشرع الكويتي على الجانب الإجرائي للجرائم المرتبطة بالتوقيع الإلكتروني بالشكل اللازم، فهذه الجرائم تتطلب وجود إجراءات خاصة؛ نظرًا لكونها تقع في عالم افتراضي، وهو ما يخلق العديد من الصعوبات من الناحية التطبيقية، ويجعل الإجراءات العادية عاجزة عن إثبات هذه الجرائم والوصول إلى المجرمين.

أولًا: مشكلات القانون الكويتي تجاه الجرائم الإلكترونية.

يمكن تحديد أبرز أوجه الإشكاليات التشريعية بالكويت تجاه الجرائم المستحدثة -ومنها التوقيع الإلكتروني- على النحو التالي:

١. هناك مشكلة خاصة بالحسابات Account الإلكترونية بالكويت؛ ذلك أن كل حساب لا يستخدم اسمه الحقيقي هو حساب وهمي، من حيث مجهولية من يديره، ولكن يجب التفرقة بين ما يسمى بالحساب الكاذب Bot -والذي يدار عن طريق الكمبيوتر- والحساب باسم مستعار، والذي يسمى عاميًا الحساب الوهمي، وقد اكتسبت فكرة الوهمية من صعوبة الكشف عن بيانات من يديره؛ كونها غير موجودة بحوزة دولة الكويت، وهي موجودة في الولايات المتحدة الأمريكية. ولعل السبب الرئيس في هذه المشكلة: هو عدم تجريم فكرة الحساب الوهمي أولًا، و عدم النجاح في حجب الحساب ثانيًا؛ حيث من الجدير بالذكر أن آلية حجب أو إغلاق الحسابات الوهمية يتمثل في حصر عدد المحاولات المبذولة لطلب الاغلاق؛ حيث إن من يقف خلف تلك الحسابات يعاودون غالبًا في كل عملية إغلاق ناجحة لفتح حساب جديد؛ بسبب طبيعة وسهولة وسرعة إنشاء الحساب في الوسط الإلكتروني، إلا أن العامل الأساس من الإغلاق أو الحجب هو هدم كمية المتابعين لدى ذلك الحساب، والتي لا يمكن الحصول على كم متابعين فعليين، وبالتالي يقل التفاعل مع الحساب، وبالتالي تأثيره، وهذا هو الفيصل في إرباك أجندة تلك الحسابات، وبطبيعة الحال تقليل الضرر على المجتمع أو التأثير عليه.

٢. غياب الوعي المجتمعي عن خطورة هذه الظاهرة، وضمان المجرمين في عدم قدرة الدولة للحصول على البيانات؛ يدفع الكثير لإنشائها والتربح منها، في ظل غياب التشريع عنها. كما أنه من المهم الانتباه إلى أن غياب التشريع الخاص بطلب المعلومات من الدولة الحاضنة، وسرعة التعامل معها؛ هو -كذلك- من الأمور التي تسبب استمرار المشكلة تتطلب من الجهة القضائية -النيابة العامة- تفعيل دورها الأساسي في طلبات المساعدة القضائية بعد إتمام اتفاقية التعاون القضائي وتسريع عمليات طلبات الإفصاح عن البيانات؛ كونها

هي الممثل الذي تعتمد عليه وزارة العدل الامريكية في الرد، وهي القناة الأساسية المعتبرة لأيّ طلبات تخص الكشف عن هوية من يقف وراء الحساب الوهمي.

٣. لا تمتلك الكويت أيّ تشريع أو آلية واضحة للتعامل مع الأصول الافتراضية، وهي كل أصل افتراضي موجود في الشبكة المعلوماتية ويعود لشخص معين يتم التنازع عليه، مثل العملات الرقمية، وأشهرها Bitcion، ولا شك أن السبب الرئيس هو عدم وجود لجنة وطنية تضم كل الجهات المعنية لدراسة هذه الأمور، والخروج بلائحة وتشريع واضح. ومن أهم الأسباب: عدم وجود نصوص تشريعية خاصة بحفظ البيانات، الى جانب عدم تفعيل دور مركز الأمن السيبراني، وكذلك عدم جاهزية شركات الاتصالات لحفظ البيانات لمدة تزيد عن ٦ شهور.

ثانيًا: التفتيش الإلكتروني وحفظ المعطيات والترصد.

لقد اتضح أن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقًا للاتفاقيات الدولية ذات الصلة، ووفقًا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

هذا، وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على التفتيش الإلكتروني؛ حيث جاء في ٢٦ منها: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى: [١]

أ – تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب بيئة أو وسيط تخزين معلومات تقنية معلومات، والذى قد تكون معلومات التقنية مخزنة فيه أو عليه.

تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش، أو الوصول إلى تقنية معلومات معينة أو جزء منها، بما يتوافق مع الفقرة (١ – أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في

---

(١) ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الإلكترونية بالقانون المصري والكويتي، مرجع سابق، ص.١٤٥.

إقليمها، وكانت هذه المعلومات قابلة للوصول قانونًا أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

ومن هنا ندعو المشرع الكويتي لتنظيم مسألة التفتيش الإلكتروني؛ كونه من بين الإجراءات المهمة في إثبات هذا النوع من الجرائم.

ويجب -في كل الأحوال- على السلطة التي تقوم بالتفتيش والحجز والسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.[١]

إذا استحال إجراء الحجز لأسباب تقنية؛ يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".[٢]

ثالثًا: الترصد الالكتروني وحتمية التعاون الدولي في ضوء التجربة الأمريكية.

من بين الإجراءات المهمة التي لم ينص عليها قانون مكافحة جرائم تقنية المعلومات الكويتي: إجراء مراقبة الاتصالات الإلكترونية، أو ما يعرف بالترصد الإلكتروني؛ ذلك أنه -مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات- يمكن لمقتضيات

---

(١) - هذا، وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على مسألة ضبط المعلومات المخزنة حسب نص المادة ٢٧، التي جاء فيها أنه: "١ – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (١) من المادة السادسة والعشرين من هذه الاتفاقية.. هذه الإجراءات تشمل صلاحيات:

أ – ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

ج- الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

٢- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أيّ شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة؛ لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين ٢ و ١ من المادة السادسة والعشرين من هذه الاتفاقية".

(٢) - يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك... انظر المادة الثامنة من القانون رقم ٠٤/٠٩.

حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي هذا تم وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

ويمكن القيام بعمليات المراقبة الإلكترونية في الحالات الآتية:

أ – للوقاية من الأفعال الموصوفة بجرائم العقود الإلكترونية أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفير معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج – لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

وعلى مستوى المشرع القطري؛ فقد حرص القانون على وضع النظام القانوني الملائم لحماية التوقيع الإلكتروني، فجعله حجة في الإثبات في حالة توافر الشروط التي تنظمها المادة (٢٨) من القانون رقم (١٦) لسنة ٢٠١٠م، بإصدار قانون المعاملات والتجارة الإلكترونيةP حيث كان المشرع معنيًا ببيان الآثار القانونية للتوقيع الإلكتروني، وكذا المسؤولية القانونية المترتبة على كل أطراف العلاقة التجارية، وذلك في المواد (٢٩)، (٣٠)، (٣١)، (٣٢)، (٣٣)، (٣٤)، كما اهتمت المواد من (٣٥) وحتى (٤٤) من ذات القانون بتنظيم خدمة التصديق على التوقيع الإلكتروني. واستكمالًا من المشرع القطري في تنظيم وحماية التجارة الإلكترونية؛ فقد وضع النصوص القانونية الكفيلة بحماية التوقيع الإلكتروني وتجريم القرصنة، حيث نص في المادة (١٠) من القانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية: "يعاقب بالحبس مدة لا تجاوز عشر سنوات، وبالغرامة التي لا تزيد على (٢٠٠,٠٠٠) ريال؛ كل من زور محررًا إلكترونيًا رسميًا أو استعمله مع علمه بذلك، كما أنه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد

على (١٠٠,٠٠٠) مائة ألف ريال، أو بإحدى هاتين العقوبتين؛ إذا وقّع بالتزوير على محرر إلكتروني غير رسمي واستعمله مع علمه بتزويره[١].

نشير إلى أن الاتفاقية العربية خصصت العديد من المواد لتنظيم مسألة التعاون الدولي؛ نظرًا لأهميتها، وقد حثت جميع الدول الأطراف على تبادل المساعدة فيما بينها بأقصى مدى يمكن لغايات التحقيقات، أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم المرتبطة بالتوقيع الإلكتروني.[٢]

---

(١) نصت المادة (١١) من ذات القانون على أنه: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (١٠٠,٠٠٠) مائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل من ارتكب فعلًا من الأفعال التالية: استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي، تُمكِّن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات من الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو التوقيع عليه بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة.

(٢) - الفصل الرابع من الاتفاقية.

الخاتمة العامة

من خلال ما سبق يمكن القول بأن التجارة الإلكترونية في العصر الحديث واجهت صعوبات من حيث اعتراف القوانين التقليدية بقانونية إبرام العقود بهذه الوسيلة الإلكترونية؛ لذلك كان على المشرع الكويتي العمل من أجل سن مزيد من القوانين الملائمة للتعاقد بالطرق الإلكترونية، والاعتراف بقانونية الإثبات وصحة وقانونية التوقيعات الإلكترونية؛ ذلك أنه لمّا كان إبرام العقد يتم على الشبكة العالمية فإن أول ما يثير الاهتمام -في هذا المجال- هو حجية هذه المحررات والعقود التي لا تتضمن أي توقيع مادي عليها. وقد استخدمت بعض الحلول المتوافقة مع طبيعة التجارة الإلكترونية، حيث تم استخدام التواقيع التناظرية أو الرموز الرقمية، غير أنه لا تعرف النظم القانونية القائمة التواقيع الإلكترونية. وقد تضمنت القواعد النموذجية للتجارة الإلكترونية التي وضعتها اليونسترال، وفي بعض الدول المتقدمة؛ قواعد تقضي بالمساواة بالقيمة بين التعاقدات التقليدية والإلكترونية، وحجية التواقيع الإلكترونية، وأجاز بعضها عمليات التشفير التي تكفل حماية التوقيع من الالتقاط أثناء عبوره شبكة الإنترنت. ويعد العقد Click Wrap Contract الأكثر شيوعًا للعقد الإلكتروني، وهو مصمم لبيئة النشاط على الخط، كما في حالة الإنترنت، وذلك بوجود وثيقة العقد مطبوعة على الموقع متضمنة الحقوق والالتزامات لطرفيه، منتهية بمكان متروك لطباعة عبارة القبول، أو الضغط على إحدى العبارتين: "أقبل" أو "لا أقبل"، بحيث يُستخدَم العقد الإلكتروني لكافة التصرفات محل الاتفاقات على الشبكة، وبشكل رئيس إنزال البرامج أو الملفات على الشبكة والدخول إلى خدمات الموقع، وتحديدًا التي تتطلب اشتراكًا خاصًا في بعض الأحيان، أو مقابلا ماليا، أو لغايات الحصول على خدمة، وكذلك لإبرام التصرفات القانونية على الخط، كالبيع والشراء والاستئجار وطلب القرض والحوالة المصرفية وإبرام بوالص التامين وغيرها.

وتثير جرائم التوقيع الإلكتروني بعض المشكلات المتعلقة بعدم اطلاع بعض المستخدمين على الشروط فعليًا وعدم معرفتهم بقواعد الإثبات القائمة لهذه الشروط المخزنة داخل النظم، كشروط نموذجية تثبت عناصر والتزامات التعاقد بسبب عدم التوقيع عليها، وعدم ثبوت حجيتها لشخص بعينه، وثبوت عدم مناقشتها بين الأطراف. كل ذلك وغيره استوجب تدخلًا تشريعيًا لتنظيم آلية إبرام العقد وشروط حجيته وموثوقيته، سواء أكان التدخل من قِبل دول العالم أم من قِبل الدول العربية، الأمر الذي يسرّع في انتشار التجارة الإلكترونية، بما فيها من فوائد من حيث الاستغناء عن المستندات الورقية وسرعة في الإنجاز، وغيرها من الفوائد.

خلاصة القول: إن على المشرع الكويتي حثّ الخطى سريعًا لتغطية الفراغ التشريعي الحاصل في مجال الحماية الجنائية للتعاقد الإلكتروني ومشكلات التوقيع الإلكتروني، وتنظيم وسائل الحماية للمتعاملين في التجارة الإلكترونية، ويأتي على راسها التوقيع الإلكتروني.

نتائج الدراسة

يمكن تحديد أبرز نتائج الدراسة الحالية على النحو التالي:

أولًا: يرتّب العقد الإلكتروني -كغيره من العقود- التزامات على عاتق كل متعاقد في مواجهة الآخر، وتثير هذه الالتزامات مسألتين، الأولى: تتعلق بكيفية تنفيذ طرفي العقد لالتزاماتهما، والثانية: بكيفية الالتزام بالوفاء.

ثانيًا: تنقسم العقود الإلكترونية من حيث كيفية تنفيذها إلى نوعين، منها: ما يُبرَم عبر الإنترنت وينفذ خارجها، حيث يشمل هذا النوع العقود التي يكون محلها الأشياء المادية التي يقتضي تسليمها في بيئة مادية، والنوع الآخر من هذه العقود: ما يبرَم ويُنفَّذ عبر شبكات الاتصال ذاتها، حيث يشمل العقود التي يكون محلها الأشياء غير المادية وتقديم الخدمات، ومنها: عقود الاشتراك في الإنترنت، وعقود الاشتراك في بنوك المعلومات، وعقود الإعلانات، وغيرها.

ثالثا: يتميز الدفع الالكتروني بأنه من بين وسائل الوفاء التي تتم عن بُعد، ويكون ذلك بإعطاء أمر الدفع عبر شبكة الإنترنت وفقًا لمعطيات الكترونية تسمح بالاتصال المباشر بين طرفي العقد، وبهذه الصفة يعتبر الدفع الالكتروني وسيلة فعالة لتنفيذ الالتزام بالوفاء في العقود الإلكترونية التي تقتضي تباعد أطراف العقد، أي يغيب التقاؤهم المادي على مائدة مفاوضات واحدة.

رابعًا: يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون مُعدّة ومحفوظة في ظروف تضمن سلامتها. ولقد أسس المشرع -من خلال هذا النص- مبدأ التعادل الوظيفي بين الكتابة في الشكل الإلكتروني والكتابة على الدعامة الورقية، غير أنه لم يأخذ به على إطلاقه، بل قيده بشرطين، هما: إمكانية التأكد من هوية الشخص الذي صدرت عنه هذه الكتابة، وأن تكون مُعدّة ومحفوظة في ظروف تضمن سلامتها.

خامسًا: أبدت التشريعات التي اعترفت بالتوقيع الإلكتروني في إثبات التصرفات القانونية -ومنها التشريع الأمريكي والكويتي- مجموعة من الضوابط الصارمة، وتدخلت الدولة في هذا الخصوص بإنشاء هيئة عامة يناط بها مهمة التوثيق، بما يؤدي إلى نوع

من التنظيم الرسمي لاستخدام الإنترنت في المعاملات التجارية وإبرام العقود بصفة عامة، وبالتالي إضفاء نوع من الثقة على التعامل الذي يتم عبر شبكة الإنترنت.

توصيات الدراسة:

يمكن في ختام الدراسة تقديم بعض التوصيات للمشرع الكويتي، وذلك على النحو التالي:

المحور الأول: توصيات لمكافحة الجرائم المستحدثة في دولة الكويت.

أولًا: أهمية تجريم الحساب الوهمي ومن يديره بأشد العقوبات الرادعة، الى جانب تجريم من يتعامل مع الحساب الوهمي، مع أهمية إبرام اتفاقيات تعاون مع الشركات الحاضنة للحساب الوهمي.

ثانيًا: أهمية إبرام معاهدة المساعدة القضائية المتبادلة MLAT مع الولايات المتحدة الأمريكية، مع تجريم كل من يقوم بمعاونة الحساب الوهمي ودعمه، سواء ماديًّا من خلال عمل إعلانات تجارية في حسابه، أو تزويده بالمعلومات.

ثالثًا: أهمية تغليظ العقوبات الرادعة على الحساب الوهمي ومن يقوم بتزويده بالمعلومات، وحذف بعض من المسميات المطروحة بالقانون رقم ٦٣ لسنة ٢٠١٥؛ لتتناسب مع طبيعة الجرائم المرتكبة في الوسط الكويتي، وبالأخص تلك التي تتعلق بالمساس بالكرامة؛ فهي مفهوم مطاطي غير واضح، يمكن إدراج أي جملة من خلاله، ويمكن الطرح بمفهوم السب والقذف، أو الاكتفاء بمفهوم مصدر الإساءة الصريحة، ويمكن حذف ما ورد في المادة ٣: "أو بما يُعدّ مساسًا بكرامة الأشخاص، أو خادشًا للشرف والاعتبار أو السمعة"، كما ورد في المادة ٦، والتي أشارت لقانون المطبوعات **بالمادة ٢١ : بند ١ : تحقير أو ازدراء دستور الدولة**، وما ورد في المادة ٦ التي أشارت لقانون المطبوعات **بالمادة ٢١ : بند ٧ : المساس بكرامة الأشخاص. ويذكر في هذا الصدد** أو المادة ٨ من القانون القطري، تنص على أنه: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على ١٠٠,٠٠٠ مائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل من تَعدَّى على أيّ من المبادئ أو القيم الاجتماعية، أو نشر أخبارًا أو صورًا أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تَعدّى على الغير بالسب أو القذف عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. **حيث** قامت الولايات المتحدة الأمريكية بإنشاء محفظة إلكترونية تخص وكالة التحقيق الفدرالية لتحويل الأموال المضبوطة من العملات الرقمية.

رابعًا: أهمية انضمام الكويت لاتفاقية بودابست، والتي تُعدّ من أهم الاتفاقيات الجماعية التي اهتمت بالجرائم الالكترونية وسبل التصدي الجماعي لها، والتي قسمتّ إجراءات

جمع الأدلة لمرحلتين، الأولى: تتمثل في الإجراءات المهدة لجمع الأدلة Kوهي نوع من المراقبة والمتابعة لاستخدام تقنية الاتصالات (الحاسب الآلي والإنترنت)، ويتولى القيام بهذه الإجراءات مقدمو خدمات الحاسب الآلي والإنترنت بتكليف من السلطة المختصة، ومباشرة هذه الاجراءات تعتبر من إجراءات التحري الأولي، ولا تعد تحريكًا للدعوى الجنائية الإلكترونية. ومن هنا نؤكد على ضرورة تمكين السلطات المختصة من التحقق من مضمون البيانات؛ للاستفادة من ذلك في أغراض التحري الجنائي، سواء أكان ذلك عن طريق التفتيش أم بالمعلومات والتقارير التي توفرها شركات تزويد الخدمة. أما إجراءات جمع الأدلة وفقًا لاتفاقية بودابست -والتي ندعو دولة الكويت للانضمام إليها- فإن إجراءات جمع الأدلة تتمثل في إصدار أمر بتقديم بيانات محددة، ويعني إلزام أي جهة بتقديم أي بيانات (سواء أكانت تلك البيانات تتعلق بالبيانات نفسها أم بخط سير البيانات).

ويلاحظ الباحث أن اتفاقية بودابست كأنما قسمتّ التحري الجنائي كذلك إلى: تحري أوَّليّ، وتحري ابتدائي، وهو يلي مرحلة فتح الدعوى الجنائية والسير في إجراءاتها، وتسبقه مرحلة التحري الأوَّليّ؛ فقد أوردت المادة (١٦) من اتفاقية بودبست عبارة (علمًا بأن هذه الإجراءات لا تُعدّ تحريكًا للدعوى الجنائية) باعتبار أن الإجراءات الأوَّلية لا يعتبر تحريكًا للدعوى الجنائية المعلوماتية وفقًا لاتفاقية بودابست.

خامسًا: تعديل قواعد الإثبات لكفالة جمع الأدلة الإلكترونية وحفظها، والتأكد من صحتها، واستخدامها في الإجراءات الجنائية. إلى جانب سن تشريعات جديدة أو تعزيز التشريعات القائمة لإتاحة الاعتراف بمقبولية الأدلة الإلكترونية وتحديد نطاقها.

سادسًا: ضرورة إضافة بعض النصوص القانونية اللازمة لإدراج الشركات الخاصة، مثل شركات مزودي خدمة الإنترنت ISP، وإلزامها -قانونًا- بالتعاون بالإفصاح عن البيانات المطلوبة وفق القانون، إلى جانب إضافة نصوص قانونية تنظم الإجراءات الإلكترونية والإثبات الإلكتروني للأصول الافتراضية.

سابعًا: أهمية الالتفات إلى مفهوم الأدلة الرقمية أو الدليل الإلكتروني داخل الأجهزة المستخدمة في ارتكاب الواقعة، مع الحاجة إلى تجريم حفظ البيانات دون وجه حق أو تسريبها أو بيعها، وكذلك تدعيم مفهوم حفظ البيانات وأسس تخزينها والاحتفاظ بها، وإلزام كافة الشركات الموجودة في الدولة.

ثامنًا: لتحسين أداء الإدارة القائمة على مكافحة الجرائم الإلكترونية؛ يجب تبني التطوير الثلاثي المتكامل، وهو ما يرتبط جانبه الأول بتدريب وتطوير القائمين على العمل بالإدارة، من خلال أحدث الوسائل والتطبيقات التقنية المعاصرة، أما الجانب الثاني فيتعلق

بتطبيقات التكنولوجيا الرقمية والأجهزة والمعدات وتوافرها بالإدارة، ويرتبط البعد الأخير بتوفير بنية تشريعية وقانونية للتعاطي مع تلك الجرائم المستحدثة.

المحور الثاني: توصيات لمكافحة جرائم التوقيع الإلكتروني في دولة الكويت.

أولًا: ضرورة تقنين قواعد جديدة لمكافحة جرائم العقود الإلكترونية؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم، ولاسيما فيما يتعلق بالإثبات في الدعاوى الجنائية الناشئة عن هذه الجرائم، كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

ثانيًا: إعادة النظر في صياغة نصوص القانون المدني الكويتي وقانون التجارة، بما يسمح للمتعاقدين عن بُعْد باستخدام الوسائط الإلكترونية وإعطاء هذه التعاقدات الإلكترونية نفس الحجية القانونية للوسائط المادية أو التقليدية. وهنا يجب التأكيد على ضرورة حث القضاء على التحرر من أَسْر المفاهيم التقليدية، ومحاولة التحرك في النصوص بالطريقة التي يمكن لها أن تساهم في إيجاد الحلول للمشكلات الحديثة الناشئة عن دخول العالم في عصر الإلكتروني، حيث يجب أن يكون للقضاء دوره بممارسة حقه في الاجتهاد القضائي لحل الإشكاليات المستحدثة، من خلال التوسع في تفسير النصوص التقليدية، وعدم الانتظار لحين تدخل المشرع في تعديل النصوص الحالية أو إضافة تشريعات جديدة إليها.

ثالثًا: يتعين تدريب وتحديث رجال الادعاء العام -أو النيابة العامة- والقضاء بدولة الكويت بشأن التعامل مع أجهزة الحاسوب والإنترنت.

رابعًا: ينبغي أن تنص التشريعات الكويتية -مثلا- على اعتبار أن الانترنت يعد وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية، مع الأخذ بعين الاعتبار أن الإنترنت أوسع انتشارًا من سائر وسائل النشر والعلانية الأخرى.

خامسًا: يلزم تعديل قوانين ونظم الإجراءات الجزائية بالقدر الذي يسمح ببيان الأحكام اللازم اتباعها حال التفتيش على الحاسبات، وعند ضبط المعلومات التي تحتويه؛ حتى يستمد الدليل مشروعيته.

سادسًا: ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق، بضبط البريد الإلكتروني وأيّ تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل؛ والكشف عن الحقيقة.

سابعًا: ضرورة النص صراحة في القوانين المنظمة للإثبات الجنائي بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات.

ثامنًا: ضرورة سَنّ التشريعات الخاصة بمكافحة جرائم التوقيع الإلكتروني، وذلك بإدخال كافة صور السلوك الضار والخطر على المجتمع التي يستخدم فيها الإنترنت .

تاسعًا: يجب الإستفادة من بعض التشريعات العربية الحديثة، وتحديدًا التشريع القطري؛ حيث قام المشرع القطري في القانون رقم ١٤ لسنة ٢٠١٤ بالاهتمام DVD بتنظيم الإجراءات الإلكترونية، فوضع ضوابط للأدلة الإلكترونية وتنظيم التفتيش الإلكتروني والتدابير، وذلك كله في المواد ١٤ الى ١٩ من القانون المذكور، وكذلك وضع التزامات على مزودي الخدمة في المادة ٢١ من القانون ذاته، حيث ألزمهم بتزويد الجهات المختصة أو جهات التحقيق بجمع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناء على أمر النيابة العامة؛ وذلك لتسهيل الكشف عن هوية الجاني في جرائم التوقيع الإلكتروني.

قائمة المراجع

أ- المراجع العربية:

أولًا: الكتب.

١. د أحمد أبو الروس، القصد الجنائي والمساهمة والمسؤولية الجزائيّة والشروع والدفاع الشرعي وعلاقة السببية، القاهرة: المكتب الجامعي الحديث، دون سنة نشر.

٢. أحمد أبو الوفا، الوسيط في القانون الجنائي، القاهرة، دار النهضة العربية، الطبعة الرابعة، ٢٠٠٤م.

٣. د. أحمد زين العيدروس، مبادئ قانون الإجراءات الجزائيّة، مطبعة المسكي، القاهرة ٢٠٠٢م.

٤. أحمد عبد الكريم سلامة: القانون الدولي الخاص النوعي، (الإلكتروني – السياحي – البيئي) دار النهضة العربية، ٢٠٠٢ م.

٥. أحمد عبد الدائم، شرح القانون المدني –نظرية الالتزام، ج١، مصادر الالتزام، منشورات جامعة الكويت ٢٠٠٣م.

٦. أحمد حشمت أبو شية، نظرية مصادر الالتزام، مكتبة عبدالله وهبة، مصر، ط٣، ١٩٨٩م.

٧. أسامه أحمد بدر: حماية المستهلك في التعاقد الإلكتروني، دار الجامعة الجديدة ٢٠٠٥م.

٨. أسامة عبدالعليم الشيخ، مجلس العقد وأثره في عقود التجارة الإلكترونية. دراسة مقارنة في الفقه الإسلامي والقانون الوضعي، قسم الشريعة، جامعة أم القرى ٢٠٠٧م.

٩. د. أسامة أبو الحسن مجاهد: خصوصية التعاقد عبر الإنترنت، دار النهضة العربية، عام ٢٠٠٠م.

١٠. بشار المومني، مشكلات التعاقد عبر الإنترنت، دار الكتاب الحديث، إربد – الأردن، دون طبعة، ٢٠٠٤م.

١١. بسام ملحم الطروانة، مبادئ القانون التجاري، دار المسيرة، عمان، ٢٠١٠م.

١٢. حازم نعيم، المسؤولية في العمليات المصرفية الإلكترونية، عمان، الأردن، دار وائل للنشر ٢٠٠٣م.

١٣. حسام الدين كامل، مصادر الالتزام، القاهرة، دار النهضة العربية ١٩٨٤م.

١٤. حسن محمد بودي، التعاقد عبر الإنترنت، دار الكتب القانونية، مصر، دون طبعة ٢٠٠٩م.

١٥. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة ٢٠٠٠م.

١٦. حمدي عبد الرحمن: الوسيط في النظرية العامة للالتزامات (الكتاب الأول) (المصادر الإرادية للالتزام والإرادة المنفردة)، القاهرة، دار النهضة العربية ١٩٩٩م.

١٧. رمضان أبو السعود: مصادر الالتزام، القاهرة، دار النهضة العربية ٢٠٠٣م.

١٨. سامح التهامي، التعاقد عبر الإنترنت، القاهرة، دار الكتب القانونية ٢٠٠٨م.

١٩. سمير عبد السميع الأودن : العقد الإلكتروني، منشأة المعارف، ٢٠٠٥م.

٢٠. شفيق طعمة، التقنين المدني الكويتي، المكتبة القانونية، الكويت، ط٣، ١٩٩٧م.

٢١. ضياء الدين مشيمش، التوقيع الإلكتروني: دراسة مقارنة، دار صادر للمنشورات الحقوقية، بيروت الطبعة الأولي، دون سنة نشر.

٢٢. طاهر حسن الغالبي، صالح مهدي العامري، المسؤولية الاجتماعية وأخلاقيات الأعمال (الأعمال والمجتمع)، عمان، دار وائل للنشر ٢٠٠٥م.

٢٣. عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، عمان، دار الشقافة، ١٩٩٧م.

٢٤. عبد الرازق السنهوري، الوسيط في شرح القانون المدني نظرية الالتزام، الإسكندرية، منشأة المعارف ٢٠٠٤م.

٢٥. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، الإسكندرية، دار الفكر الجامعي، ٢٠٠٤م.

٢٦. عبد المنعم الصده، أصول القانون، دار الفكر العربي، القاهرة ١٩٩٧م.

٢٧. علاء محمد نصيرات، حجية التوقيع الإلكتروني: دراسة مقارنة، دار الثقافة، الأردن ٢٠٠٥م.

٢٨. عدنان إبراهيم السرحان شرح القانون المدني: مصادر الحقوق الشخصية – الالتزامات، دار الثقافة، عمان، ط١، الإصدار الثالث ٢٠٠٨م.

٢٩. عدنان السرحان، شرح القانون المدني مصادر الحقوق الشخصية، عمان، دار الثقافة ٢٠٠٨م.

٣٠. د عماد الحداد : التجارة الإلكترونية ، القاهرة، مكتبة الأسرة ٢٠٠٥م.

٣١. لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية ٢٠١٠م.

٣٢. محمد أبو زهرة، الملكية ونظرية العقد في الشريعة الإسلامية، دار الفكر العربي ١٩٩٧م.

٣٣. محمد الرومي، النظام القانوني للتحكيم الإلكتروني، الاسكندرية، دار الفكر الجامعي ٢٠٠٦م.

٣٤. د. محمد أمين الرومي، جرائم الحاسوب و الإنترنيت، دار المطبوعات الجامعية، الإسكندرية ٢٠١٦م.

٣٥. محمد حسين منصور: المسئولية الإلكترونية، القاهرة، دار الجامعة الجديدة ٢٠٠٣م.

٣٦. محمد حسن قاسم: التعاقد عن بُعد "قراءة تحليلية في التجربة الفرنسية، مع إشارة لقواعد القانون الأوربي "، دار الجامعة الجديدة للنشر والتوزيع ٢٠٠٥ م.

٣٧. د. محمد صادق اسماعيل، جرائم شبكات التواصل الاجتماعي والإنترنت، المنامة، مركز معلومات المرأة والطفل، ٢٠١٣م.

٣٨. محمود عبد الرحيم، التراضي في تكوين العقد عبر الإنترنت – دراسة مقارنة، دار الثقافة، عمان ٢٠٠٩م.

٣٩. مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الإنترنت، دار الكتب القانونية، مصر ٢٠١١م.

٤٠. منير محمد الجنيبي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، دون سنة نشر.

٤١. فاروق الأباصيري : عقد الاشتراك في قواعد المعلومات الإلكترونية، دراسة تطبيقية لعقود الإنترنت، دار النهضة العربية ٢٠٠٣م.

٤٢. محمد نوري الشمري، عبد الفتاح زهير، الصيرفة الإلكترونية، دار وائل للنشر، الأردن ٢٠٠٨م.

٤٣. محمد المرسي زهرة، الحاسوب والقانون، مؤسسة الكويت للتقدم العلمي، الكويت، الطبعة الأولي ١٩٩٥ م.

٤٤. محمود السيد خيال، التعاقد عن طريق التليفزيون، القاهرة، بدون ناشر ٢٠٠٠م.

٤٥. مدحت عبد الحليم رمضان : الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، دار النهضة العربية ٢٠٠١ م.

٤٦. مصطفى الجمال: شرح أحكام القانون المدني (مصادر الالتزام)، القاهرة، دار النهضة العربية ١٩٩١م.

٤٧. ممدوح محمد خيري هاشم : مشكلات البيع الإلكتروني عن طريق الإنترنت في القانون المدني، دراسة مقارنة، دار النهضة العربية ، ٢٠٠٠م.

٤٨. د. معوض عبد التواب، الوسيط فى أحكام النقض الجزائيّة ، مطبعة أطلس، منشأة المعارف الإسكندرية ٢٠٠٥ م.

٤٩. نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة والنشر والتوزيع، عمان، الأردن، الطبعة الأولى ٢٠٠٥م.

٥٠. د.هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية.

٥١. د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني فى التشريع المقارن، القاهرة، دار النهضة العربية ١٩٩٢م.

٥٢. د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة العربية ٢٠٠٦م.

٥٣. وحيد الدين سوار، شرح القانون المدني، مصادر الالتزام، مؤسسة الحلبوني، دمشق ١٩٨٩م.

٥٤. يونس عرب، حجية الإثبات بالمستخرجات الإلكترونية في القضايا المصرفية، عمان، مجلة البنوك، مايو ٢٠١٤م.

ثانيًا: الرسائل العلمية.

١. أحمد السيد طه كردى، إطار مقترح لحماية حقوق المستهلك من مخاطر التجارة الإلكترونية، رسالة ماجستير غير منشورة، مصر: جامعة بنها، كلية التجارة ٢٠١١م.

٢. جلال عايد الشورة، وسائل الدفع الإلكتروني، دار الثقافة للنشر والتوزيع، رسالة ماجستير منشورة، الطبعة الأولى، عمان، الأردن ٢٠٠٨م.

٣. خالد فيصل الهندي، مفهوم التوقيع الإلكتروني وحمايته، رسالة ماجستير غير منشورة، الكويت: جامعة الكويت، كلية الحقوق ٢٠٠٤م.

٤. عمر خالد زريقات، عقد البيع عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.

٥. رشيدة الإدريسي، إبرام العقد الإلكتروني، رسالة ماجستير غير منشورة، جامعة الكويت، كلية الحقوق ٢٠٠٥م.

٦. عيسى غسان عبد الله الربضي، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس ٢٠٠٦ م.

٧. عبيدات لورنس، إثبات العقد الإلكتروني. رسالة ماجستير معهد الدراسات العربية. جامعة الدول العربية، القاهرة.

٨. محمد ذعار العتيبي، النظام القانوني للعقد الإلكتروني. دراسة مقارنة بين التشريعين الكويتي والأردني، رسالة ماجستير غير منشورة، عمان، جامعة الشرق الأوسط، كلية الحقوق ٢٠١٣م.

٩. ناصر زيدان الذايدي، العوامل المؤثرة في ولاء المستهلك للمنتجات الغذائية الوطنية في دولة الكويت، رسالة ماجستير غير منشورة، عمان، جامعة عمان العربية للدراسات العليا ٢٠٠٩م.

١٠. ناصر مشعل ناصر الجليدان الشمري، مدى حجية العقود الإلكترونية في الإثبات. دراسة مقارنة لشروط العقود الاستهلاكية في التعاملات الالكترونية بالقانون

المصري والكويتي، رسالة ماجستير غير منشورة، مصر: جامعة مدينة السادات، كلية الحقوق ٢٠٢٠م.

١١. نضال سليم اسماعيل برهم، أحكام عقود التجارة الإلكترونية، رسالة ماجستير، جامعة عمان العربية، الأردن ٢٠٠٥ م.

١٢. نوال شعباني، التزام المتدخل بضمان سلامة المستهلك في ضوء قانون حماية المستهلك وقمع الغش، رسالة ماجستير غير منشورة، الجزائر، جامعة مولود معمري، كلية الحقوق والعلوم السياسية ٢٠١٢م.

ثالثًا: الدوريات.

١. المغازي أبو عرابي وفياض القضاة، حجية التوقيع الإلكتروني: دراسة في التشريع الأردني، مجلة جامعة دمشق للعلوم القانونية والاقتصادية، المجلد ٢٠ العدد الأول ٢٠٠٣م.

٢. آلاء يعقوب يوسف، الحماية القانونية للمستهلك في عقود التجارة الإلكترونية، بحث منشور في مجلة كلية الحقوق، جامعة النهرين، المجلد الثامن، العدد الرابع عشر ٢٠٠٥م.

٣. أيمن مساعدة – علاء خصاونة، خيار المستهلك في البيوع المنزلية وبيوع المسافة، مجلة الشريعة والقانون، العدد ٤٦، الأردن ٢٠١١م.

٤. بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي. دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، العدد٤، السنة الخامسة، العدد التسلسلي ٢٠، ربيع الأول –ربيع الثاني ١٤٣٩هـ- ديسمبر ٢٠١٧م.

٥. حاتم عبد الباري، حجية المحررات الإلكترونية في الإثبات، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية، مصر، المجلد السابع والأربعون، العدد الثالث ٢٠٠٤ م.

٦. حسن محمد، وسائل الإثبات الإلكترونية، مجلة الحقوق، جامعة الكويت، العددان ١ – ٢، السنة ٦٨، ٢٠٠٩م.

٧. رامي علوان، التعبير عن الإرادة عن طريق الإنترنت وإثبات التعاقد الالكتروني، مجلة الحقوق، الكويت: جامعة الكويت، العدد٤، السنة ٢٦، ٢٠٠٢م.

٨. عادل حامد أبو عزة، العقود الإلكترونية، خصائصها والقانون الواجب التطبيق عليها، مجلة الجزيرة، جمعية الحاسبات السعودية، العدد ١٥٨، ١٨، ربيع أول ١٤٢٧هـ - ١٦ إبريل ٢٠٠٦م ٠

٩. عبد الحليم بوقرين، الحماية الجنائية لشخص الرسول صلى الله عليه وسلم، مجلة الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط/ الجزائر، العدد ٠٨، ٢٠١٥م.

١٠. محمد بودالي، التوقيع الإلكتروني، مجلة الإدارة، العدد رقم ٢، لسنة ٢٠٠٣م.

١١. محمود عبد الرحمن محمد، مدى حجية الوسائل الإلكترونية في إثبات المعاملات المدنية والتجارية والإدارية طبقًا لقانون المعاملات الالكترونية الكويتي، مجلة كلية القانون الكويتية العالمية، العدد١، السنة السادسة، العدد التسلسلي ٢١، جمادي الآخرة- رجب ١٤٣٩هـ- مارس ٢٠١٨م.

١٢. منصور الصرايرة، الإطار القانوني للعقد المبرم عبر وسائل الاتصال الالكترونية دراسة في التشريع الأردني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٥، العدد٢، ٢٠٢٠م.

المراجع الأجنبية

1) Bert Swart, "Modes of International Criminal Liability", in: Antonio Cassese, The Oxford Compaion to International Criminal Justice, Oxford University Press, 2009. Bajan, Peter, (1998). New Communities , New Social Norms. Studia-Psychologica. V. 40 (4.

2) NY GOL §5-1401 (parties to a contract that involves at least $250,000 may select New York law to govern their rights and duties under such contract, without requiring any other connection to New York).

3) Naldi v. Grunberg, 80 A.D.3d 1, 11 (N.Y. App. Div. 1st Dept. 2010) (holding an email to be capable of satisfying the statute of frauds contained in New York General Obligations Law § 5-703); Newmark & Co. Real Estate Inc. v. 2615 East 17 Street Realty LLC (N.Y. App. Div. 1st Dept 2011) (holding an email to be capable of satisfying the statute of frauds contained in New York General Obligations Law § 5-701).

4) Ceglia v. Zuckerberg, 2013 WL 1208558, at *4-6, *16, *73 (W.D.N.Y. Mar. 26, 2013)

5) U.S. EPA Electronic Signature Procedure (April 2018) https://www.epa.gov/sites/production/files/2018-4/documents/electronic_signature_procedure.pdf accessed in 3March 2023

6) National Institute of Standards and Technology (NIST), Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) .
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
7) Electronic Signatures in Global and National Commerce Act (ESIGN Act), Public Law 106-229 (June 30, 2000
8) Homeland Security Presidential Directive 12 (HSPD-12) – Policy for a Common Identification Standard for Federal Employees and Contractors (August 2005)
9) Hook, C., Kempf, J., Scharfenberg, G.: 'A novel digitizing pen for the analysis of pen pressure and inclination in handwriting biometrics'. ECCV Workshop BioAW, 2004, 3087, pp. 283–294
10) OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors
11) U.S. EPA Code of Federal Regulations. Title 40. Part 3. Cross-Media Electronic Reporting (CROMERR) https://www.ecfr.gov/cgi-bin/text-idx?SID=0245de321adebd80c389f68ae30e1415&mc=true&node=pt40.1.3 accessed in 4 March 2023
12) Digital Signature – A subset of electronic signature technology. Digital signatures encrypt documents with digital codes to verify the user's identity and support authentication, data integrity and signer non-repudiation. Electronic signature technologies must comply with FIPS 180-4 Hash
https://csrc.nist.gov/publications/detail/fips/186/4/final(https://csrc.nist.gov/publications/detail/fips/180/4/final)) Digital Signature standards and FIPS 186-4 (
13) See John D. McGregor, Form over Substance, 6 J. OBJECT TECH. 9, 10 (2007); Steven Bragg, Substance over Form Definition, ACCOUNTINGTOOLS, www.accountingtools.com/articles/what-issubstance- accessed in 3March 2023
14) SIMONA CAVALLINI, FABIO BISOGNI, DORIANO GALLOZZI, CLAUDIO COZZA & CLAUDIA AGLIETTI, STUDY ON THE SUPPLY SIDE OF EU E-SIGNATURE MARKET: FINAL STUDY REPORT 83 (2013),
Hartini Saripan, Electronic Signature Legislative Models: The Reappraisal of the 'Unfortunate' Divergence, 3 MLJA 20 (2009) (describing, inter alia, that Utah, Washington, Missouri, Germany, Italy, Russia, and India as the first jurisdictions to craft electronic

signature legislation; these jurisdictions, modeled from the Utah statute, crafted prescriptive models of electronic signature laws that mandated uses of just one technology and set out an elaborate legal framework for rights and liabilities associated with electronic signaturetransactions); UNCITRAL, MODEL LAW ON ELECTRONIC SIGNATURES WITH GUIDE TO ENACTMENT, at 7, U.N .

15) Sales No. E.02.V.8 (2001); Stephen E. Blythe, Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security, 11 RICH. J.L. & TECH., Winter 2005, at 1, 2.

16) Thomas J. Smedinghoff, The Legal Challenges of Implementing Electronic Transactions, 41 UNIF. COM. CODE L.J. 3, 9 (2008); UNCITRAL, PROMOTING CONFIDENCE IN ELECTRONIC COMMERCE: LEGAL ISSUES ON INTERNATIONAL USE OF ELECTRONIC AUTHENTICATION AND SIGNATURE METHODS, at 69, U.N. Sales No. E.09.V.4 (2009)

17) For further details, see R. Jason Richards, The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis, 17 J. MARSHALL J. COMPUT. & INFO. L. 873, 874–75 (2019)

18) Renard Francois, Comment, Fair Warning: Preemption and Navigating the Bermuda Triangle of ESign, UETA, and State Digital Signature Laws, 19 J. MARSHALL J. COMPUT. & INFO. L. 401, 418 (2001) (critiquing E-sign's preemption provision as failing to provide clarity and stating that "[a] business has to make several educated guesses as to the meaning of [a state law's effect on section 7002(a)(1) of E-sign]"); Manuel Alba, Order Out of Chaos: Technology, Intermediation, Trust, and Reliability as the Basis for the Recognition of Legal Effects in Electronic Transactions, 47 CREIGHTON L. REV. 387 (2014).

19) See, for example, American Boat Co., Inc. v. Unknown Sunken Barge, 418 F.3d 910, 914 (8th Cir. 2005) (holding that the same presumption of delivery applicable to paper communications should apply to email); Kennell v. Gates, 215 F.3d 825, 829 (8th Cir.2000) (absent evidence to the contrary, emails properly dispatched via a generally reliable method are presumed delivered and received

20) Harry Thurlow writes an interesting article which offers insight to the EU perspective and how it lags behind the technology developments in Electronic Contracts in the United States and the

European Union: Varying Approaches to the Elimination of Paper and Pen, Vol. 5.3 Electronic Journal of Comparative Law, November 2001
21) Wooldridge & Jennings, 'Intelligent Agents: Theory and Practice', Knowledge Engineering Review Vol. 10 No. 2, June 1995, (Cambridge University Press: 2015)
22) Reception Theory - Upon reception of acceptance by the offeror, even if he has not yet read it. It is the receipt of the acceptance in the Internet access provider's mailbox, which is taken into consideration, and not the "check mail" function in the individual mailbox of the offeror's computer
23) Hussain, S. A. (2010). CHALLENGES OF GLOBALIZATION: HOW BANGLADESH CAN ADAPT ADAPT ITSELF ITSELF ITSELF TO RE TO RE TO REAP THE BEST BENEFITS IN THE 21 AP THE BEST BENEFITS IN THE 21STSTSTST CENTURY. International Journal of Sciences: Basic and Applied Research (IJSBAR), 3–4. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=
24) Rashid, H., Ahamed, A., & Rahman, S. (2020). A Critical Study on the Transnational Organized Crime along the Bangladesh-Myanmar Border. International Journal of Sciences: Basic and Applied Research (IJSBAR), 52(02), 203–210.
25) United States Government Accountability Office. (2017). COUNTERING VIOLENT EXTREMISM Actions Needed to Define Strategy and Assess Progress of Federal Efforts
26) :BIPSS. (2010). Transnational Security: Threats Facing Bangladesh (08). Author. Retrieved from https://www.google.com/url?sa=
27) Richard totta and antong hardcastle, computer related crime in information technology the law edited by chris Edwards and Nigel savage Macmillan publisher 2016, Runyon ،Consumer Behavior, Charle Merrill ،Publishing Company, 2017
28) Casey Anthony detectives overlooked Google search for "fool-proof" suffocation methods, sheriff says. CBS News
29) Delport, W., Khn, M., & Olivier, M. S. (2011). Isolating a cloud instance for a digital forensic investigation. In H. S. Venter, M. Coetzee, and M. Loock (Eds.), Proceedings of the 2011 Information Security for South Africa (ISSA 2011) Conference. Johannesburg, South Africa: ISSA
30) Graham, W. R., Jr. (2000). Uncovering and eliminating child pornography rings on the Internet: Issues regarding and avenues

facilitating law enforcement's access to Wonderland. Law Review of Michigan State University-Detroit College of Law, 457.
31) Hollywood, J. S., Boon, J. E., Jr., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015). High-priority information technology needs for law enforcement, Santa Monica, Calif., RAND Corporation, RR-737-NIJ. As of March 15, 2015:
32) http://www.rand.org/pubs/research_
33) Mellott ،Fundamentals of Consumer Behavior, Pern Well Book, Tulsa, 2013Nie, Norman and Erbing, Lutz. Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co, 2018
34) Jackson, B. A., Russo, J., Hollywood, J. S., Woods, D., Silberglitt, R., Drake, G. B., Shaffer, J. S., Zaydman, M., & Chow, B. G. (2015).
35) Fostering innovation in community and institutional corrections: Identifying high-priority technology and other needs for the U.S. corrections sector,
36) Santa Monica, Calif., RAND Corporation, RR-820-NIJ. As of March 15, 2015:
37) http://www.rand.org/pubs/research_
38) Latonero, M. (2011). Human trafficking online: The role of social networking sites and online classifieds. Los Angeles: USC Annenberg School of Communication. Available at Social Science Research Network. As of March 15, 2015:
39) http://ssrn.com/abstract=2045851 accessed in 12 Mar2023
40) Morse, D. (2014, May 6). Philip Welsh's simple life hampers search for his killer. Washington Post [online]. As of March 15, 2023:
41) Pipitone, T. (2012). Cops, prosecutors botched Casey Anthony evidence. Click Orlando [online]. As of December 3, 2014:
42) International Law Enforcement Cooperation Report, supra note 3, at 26-27; Press Release, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges, U.S. Dep't of Justice ,
https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html;
43) FBI, Internet Crime Report 2021, supra note 13, at 15-16; see, e.g., Press Release, Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators, U.S. Dep't of Justice (Mar 19, 2023),
https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware

44) International Law Enforcement Cooperation Report, supra note 3, at 1-2, 11. However, even VASPs ostensibly located outside the United States may still have obligations under the BSA if they qualify as domestic financial institutions, including by doing business wholly or in substantial part in the United States. See, e.g., 31 C.F.R. § 1010.100(f).
45) Based, P., Security, D., Rudolf, R., & Physics, A. (1997). The list of paper based valuable documents is nearly interminable and extends from. 437, 28–30.
46) CISA. (n.d.). Security Tip (ST04-018) Understanding Digital Signatures. 2009. https://www.us-cert.gov/ncas/tips/ST04-018#:~:text=A digital signature—a type,%2C or a digital document).&text=Digital signatures are significantly more secure than other forms of electronic signatures
47) Zhong, Y. (2013). Secure digital certificate design based on the RSA algorithm. Journal of Digital Information Management, 11(6), 423–429.
48) Hosseini Seno, S., Budiarto, R., & Wan, T.-C. (2011). A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority. Arabian Journal for Science and Engineering, 36(2), 245–257.
49) D. Kah. (1996). TheCodebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.
50) Garain, U., & Halder, B. (2008). On automatic authenticity verification of printed security documents. Proceedings - 6th Indian Conference on Computer Vision, Graphics and Image Processing, ICVGIP 2008, 706–713. https://doi.org/10.1109/ICVGIP.2008.67
51) Sae-Bae, N., Memon, N.: 'Online signature verification on mobile devices', IEEE
52) Fuentes, M., Garcia-Salicetti, S., Dorizzi, B.: 'On-line signature verification: fusion of a hidden Markov model and a neural network via a support vector machine'. Proc. of Int. Workshop on Frontiers of Handwritten Recognition, Niagara on the Lake, Canada, August 2002, pp. 253–258
53) Yang, L., Widjaja, B.K., Prasad, R.: 'Application of hidden Markov models for signature verification', Pattern Recognit., 1995, 28, (2), pp. 161–170
54) Fierrez-Aguilar, J., Nanni, L., Lopez-Peñalba, J., et al.: 'An on-line signature verification system based on fusion of local and global information'. Proc. Of Fifth IAPR Int. Conf. on Audio and Video based

Biometric Person Authentication, Berlin, Heidelberg, 2005, pp. 523–532
55) Lejtman, D.Z., Gorge, S.E.: 'On-line handwritten signature verification using wavelets and back-propagation neural networks', Sixth Int. Conf. on Document Analysis and Recognition Proc. IEEE, 2001, pp. 992–996
56) Huang, N.E., Shen, Z., Long, S.R.: 'A new view of nonlinear water waves: the Hilbert spectrum', Annu. Rev. Fluid Mech., 1999, 31, pp. 417–457
57) Chang, C.P., Lee, J.C., Su, Y., et al.: Using empirical mode decomposition for iris recognition', Comput. Stand. Interfaces, 2009, 31, pp. 729–739
58) E.A.CAprioli,les lettres Recommandées Electroniques,cahiers de Droit de l' E- = terprise' mai 2011'N°3,p.68.
59) See Public Consultation on the Review of the Electronic Transactions Act, INFOCOMM MEDIA DEV. AUTH. (https://www.imda.gov.sg/regulations-and-licensing/Regulations/consultations/
60) (SIEBER) Dr. Ulrich – Computer crimes & other crimes related to information technology rev. inter.de droit penal 1991 p. 1033.
61) ((SCALION) Robert – crime on the internet, fall 1996, p. 1. "compuer crime is any violation of the law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution" available online in feb. 2000 at : http://wings.buffallo.edu/complaw/complawpapers/scalion.html - THOUMYRE - abuses in the cyberspace, op cit. P. 7
62) Washington Electronic Authentication Act, ch. 250, 1996 Wash. Sess. Laws 1190 (codified at WASH. REV. CODE §§ 19.34.010–19.34.903
63) (United States v Sampsonm, 6 COMP, L. SERV. REP. 879 (N.D. Cal.)
64) U.S.C. & 641. See : United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (Theft of grand jury transcripts and information contained therein was theft of government property). Cert. denied. 404 U.S. 958 : United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of classified information supports embezzlement conviction); United States v. DiGillo, 538 F. 2d 972 (3d Cir). Cert. denied. 429 U.S. 871 (1971) (theft by photocopying government secords sufficient to support & 641 convocation) : United States v.

MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of competitior's confidential bid information violates & 641).
65) Art. 1 Definitions : "For purposes of this convention : Computer System means any device or a group of inter – connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"
66) Roy, A., Doherty, J.F.: 'Raised cosine fiter-based empirical mode decomposition', IET Signal Process., 2011, 5, (2), pp. 121–129
67) (KASPERSEN) Prof. Dr. Henrik W. K. – crimes related to the computer network. Threats and opportunities criminological perspective, p. 258. five issues in European criminal justice: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime proccedings of the vi European colloquium on crime and criminal policy Helsinki 10-12 December 1998, European institute or crime prevention and control, affiliated with the united nations (heuni) p. O. Box 161, fin- 00131 Helsinki Finland publication series no. 34
68) Niang, O., Thioune, A., Gueirea, M.C.E., et al.: 'Partial differential equation-based approach for empirical mode decomposition: application on image analysis', IEEE Trans. Image Process., 2012, 21, (9), pp. 3991–4001
69) Rehman, N.U., Mandic, D.P.: 'Filter bank property of multivariate empirical mode decomposition', IEEE Trans. Signal Process., 2011, 59, (5), pp. 2421–2426
70) Krinidis, S., Krinidis, M., Chatzis, V.: 'Workspace for image clustering based on empirical mode decomposition', IET Image Process., 2012, 6, (6), pp. 778–785
71) (NICHOLSON) Keith – International Computer Crime : A Global Village Under Siege – New England International & Comparative Law Annual 1996 – New England School of Law P. I. available online in 16Mar. 2023 at http://www.nest.edu/annual/vol2/computer.htm
72) United States Government Accountability Office. (2017). COUNTERING VIOLENT EXTREMISM Actions Needed to Define Strategy and Assess Progress of Federal Efforts.
73) (KATYAL) Neal Kumar – criminal law in criminal law in Cyberspace , Georgetown University law center 2000< P.13 A revised version of This working paper is forthcoming in the university of Pennsylvania law review < Volume 149 April 2001 This paper can be downloaded without charge from the social science research Network

Electronic paper collection at Http://papers.ssrn.com/ aperitif abstract id=249030 working paper No 249030

74) Christopher REINHART, FEDERAL and state electronic signature laws. BRUMFIELD FRY, A preliminary analysis of Patricia federal and state electronic commerce laws.

75) See Kennedy & Millard, supra note 43; see also Seth Rosenblatt & Jason Cipriani, Two-Factor Authentication: What You Need to Know, CNET, https://www.cnet.com/

76) See, e.g., Aaron S. Edlin and Alan Schwartz, Optimal Penalties in Contracts, 78 Chicago-Kent L. Rev. 33 (2003); Robert Scott and George Triantis, Embedded Options and the Case Against Compensation in Contract Law . 104 Columbia Law Review ___ (2004).

77) See David D. Friedman, Contracts in Cyberspace [online draft]; Clayton P. Gillette, Reputation and Intermediaries in Electronic Commerce, Louisiana Law Review, Vol. 63 (2002); Henry H. Perritt, Jr., Dispute Resolution in Cyberspace: Demand for New Forms of ADR, 15 Ohio St. J of Disp. Resol 675 (2000).

78) See, for example, Specht v. Netscape Comm'cns Corp., 306 F.3d 17, 26 n.11 (2d Cir. 2002) (assessing whether clicking to download software created enforceable agreement to arbitrate, and noting that the matter of whether "the agreement is a 'written provision' despite being provided to users in a downloadable electronic form… has been settled by [the ESIGN Act]," although ultimately finding that consumers clicking "yes" in the context presented in that case did not manifest assent to license terms

79) The Hacher crackdown law and Disorder on the Electronic fron – tier by Bruce sterling p.0172,1994.

80) See, for example, the "Administrative Procedures for Filing, Signing, and Verifying" provided by the U.S. District Court for the Western District of Virginia at http://www.vawd.uscourts.gov/

81) See, for example, the "Administrative Procedures for Filing, Signing, and Verifying" provided by the U.S. District Court for the Western District of Virginia atp://www.vawd.uscourts.gov/

82) See Berkson v. GoGo LLC, 97 F.Supp.3d 359 (E.D.N.Y. 2015) (establishing general principles for enforceability of internet agreements: (1) the evidence must show that the user had notice of the agreement, (2) the link to the terms is located where users are likely to see it and (3) a "user is encouraged by the design and content of the website and the agreement's webpage to examine the terms clearly

available through hyperlinkage.") In this case, the court required that "the offeror must show that a reasonable person in the position of the consumer would have known what he was assenting to" and accordingly distinguished the noticeably smaller hyperlink for the contract terms from the large, colored "Sign In" button.

83) G. Delmare, securité informatique Ressource informatique no. 1. Juill 1984.

84) Specht v. Netscape Communications Corp., 306 F.3d 17, 25 (2d Cir. 2002) citing Windsor Mills, 25 Cal App. 3d at 992 (2001) quoting Restatement (Second) of Contracts §19 (1981). See also, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004) (holding that provisions disclosed solely through browse-wrap agreements are typically enforced if the website user had actual and constructive knowledge of the site's terms and conditions, and has manifested assent to them).

85) United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008) (admitting emails based on the email addresses contained in the "to" and "from" fields, and other identifiable material such as the subject matter, signatures, and other personal and professional references).

86) Scheuplein v. City of W. Covina, No. B206203, 2009 Cal. App. Unpub. LEXIS 7805, at *26–27 (Cal. Ct. App. 2d Dist. Sept. 29, 2009) (finding emails to be authenticated when accompanied with a declaration that the emails were retrieved from the company's computers and the printouts were accurate representations of the retrieved messages)

87) Nie, Norman and Erbing, Lutz (2000). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co

88) Hughes, Carole (1999). The Relationship of Use of the Internet and Loneliness among College Students. Dissertation Abstract . Vol. 60 (3 – A).

89) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

90) « An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature », id at 431.

91) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for protecting kids from pornography and their applicability to other inappropriate internet content, op. cit, P.1.
92) Reno v. ACLU, US Supp. 521 U.S. 844 (1997).
93) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.
94) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

References:

1: alkutub

• d 'ahmad 'abu alruwsu, alqasd aljinayiyu walmusahamat walmaswuwliat aljzayyt walshurue waldifae alshareiu waealaqat alsababiati, alqahirat: almaktab aljamieia alhaditha, dun sanat nashara.

• 'ahmad 'abu alwafa, alwasit fi alqanun aljanayiy, alqahirata, dar alnahdat alearabiati, altabeat alraabieati, 2004m.

• da. 'ahmad zayn aleaydrus, mabadi qanun al'iijra'at aljzayyt, matbaeat almiski, alqahirat 2002m.

• 'ahmad eabd alkarim salamat: alqanun alduwliu alkhasu alnaweii, (al'iilikturuniu - alsiyahiu - albiyiy) dar alnahdat alearabiati, 2002 mi.

• 'ahmad eabd aldaayimi, sharh alqanun almadanii -nzariat aliailtizami, ja1, masadir aliailtizami, manshurat jamieat alkuayt 2003m.

• 'ahmad hashamat 'abu shiat, nazariat masadir alialtizami, maktabat eabdallah wahbata, masr, ta3, 1989m.

• 'asamah 'ahmad badar: himayat almustahlik fi altaeaqud al'iilikturunii, dar aljamieat aljadidat 2005m.

• 'usamat eabdalealim alshaykha, majlis aleaqd wa'atharuh fi euqud altijarat al'iiliktruniati. dirasat muqaranat fi alfiqh al'iislamii walqanun alwadei, qism alsharieati, jamieat 'umi alquraa 2007m.

• du. 'usamat 'abu alhasan mujahidi: khususiat altaeaqud eabr al'iintirnti, dar alnahdat alearabiati, eam 2000m.

• bashar almumani, mushkilat altaeaqud eabr al'iintirnti, dar alkitaab alhadithi, 'iirbid - al'urdunu, dun tabeati, 2004m.

• bsaam milhim altirwanati, mabadi alqanun altijari, dar almasirati, eaman, 2010m.

• hazim naeimi, almaswuwliat fi aleamaliaat almasrifiat al'iilikturuniati, eaman, al'urdun, dar wayil lilnashr 2003m.

• husam aldiyn kaml, masadir alialtizami, alqahirata, dar alnahdat alearabiat 1984m.

• hasan muhamad budi, altaeaqud eabr al'iintirnti, dar alkutub alqanuniati, masr, dun tabeat 2009m.

• hasan eabd albasit jamiei, 'iithbat altasarufat alqanuniat alati yatimu 'iibramuha ean tariq al'iintirnti, dar alnahdat alearabiati, alqahirat 2000m.
• hamdi eabd alrahman: alwasit fi alnazariat aleamat lilailtizamat (alkitab al'awala) (almasadir al'iiradiat lilailtizam wal'iiradat almunfarida), alqahirata, dar alnahdat alearabiat 1999m.
• ramadan 'abu alsaeudi: masadir alialtizami, alqahirata, dar alnahdat alearabiat 2003m.
• samih altahami, altaeaqud eabr al'iintirnti, alqahirata, dar alkutub alqanuniat 2008m.
• smir eabd alsamie al'uwdun : aleuqd al'iilikturuni, munsha'at almaearifi, 2005m.
• shfiq tiemati, altiqnin almadaniu alkuaytiu, almaktabat alqanuniat, alkuayti, ta3, 1997m.
• dya' aldiyn mishimish, altawqie al'iiliktruniu: dirasat muqaranati, dar sadir lilmanshurat alhuquqiati, bayrut altabeat al'awli, dun sanat nashira.
• tahir hasan alghalibi, salih mahdii aleamiri, almaswuwliat aliajtimaeiat wa'akhlaqiaat al'aemal (al'aemal walmujtamaei), eaman, dar wayil lilnashr 2005m.
• eabaas aleabudii, altaeaqud ean tariq wasayil aliatisal alfawrii wahujyatiha fi al'iithbat almadanii, eaman, dar alshaqafati, 1997m.
• eabd alraaziq alsanhuri, alwasit fi sharh alqanun almadanii nazariat alialtizami, al'iiskandiriati, munsha'at almaearif 2004m.
• eabd alfataah biumi hijazi, altawqie al'iilikturuniu fi alnuzum alqanuniat almuqaranatu, al'iiskandiriatu, dar alfikr aljamieii, 2004m.
• eabd almuneim alsaduhi, 'usul alqanuni, dar alfikr alearabii, alqahirat 1997mi.
• eala' muhamad nusayratu, hajiat altawqie al'iilikturunii: dirasat muqaranati, dar althaqafati, al'urduni 2005m.
• eadnan 'iibrahim alsarhan sharh alqanun almadani: masadir alhuquq alshakhsiat - alailtizamati, dar althaqafati, eaman, ta1, al'iisdar althaalith 2008m.
• eadnan alsarhan, sharh alqanun almadanii masadir alhuquq alshakhsiati, eaman, dar althaqafat 2008m.

• d eimad alhadaad : altijarat al'iilikturuniat , alqahiratu, maktabat al'usrat 2005m.
• lzahir bn saeidi, alnizam alqanuniu lieuqud altijarat al'iiliktiruniati, dar alfikr aljamieii, al'iiskandariat 2010m.
• muhamad 'abu zahrata, almalakiat wanazariat aleaqd fi alsharieat al'iislamiati, dar alfikr alearabii 1997m.
• muhamad alruwmi, alnizam alqanuniu liltahkim al'iilikturuniu, aliaskandiriati, dar alfikr aljamieii 2006mi.
• d. muhamad 'amin alruwmi, jarayim alhasub w al'iintirnit, dar almatbueat aljamieiati, al'iiskandariat 2016m.
• muhamad husayn mansur: almasyuwliat al'iiliktiruniatu, alqahirati, dar aljamieat aljadidat 2003m.
• muhamad hasan qasima: altaeaqud ean bued "qara'at tahliliat fi altajribat alfaransiati, mae 'iisharat liqawaeid alqanun al'uwrubiyi ", dar aljamieat aljadidat lilnashr waltawzie 2005 m.
• d. muhamad sadiq asmaeil, jarayim shabakat altawasul aliajtimaeii wal'iintirniti, almanamati, markaz maelumat almar'at waltifla, 2013m.
• mahmud eabd alrahimi, altaradi fi takwin aleaqd eabr al'iintirnit - dirasat muqaranati, dar althaqafati, eamaan 2009m.
• mustafaa musaa aleajarimatu, altanzim alqanuniu liltaeaqud eabr shabakat al'iintirnti, dar alkutub alqanuniati, misr 2011m.
• manir muhamad aljinibi, altabieat alqanuniat lileaqd al'iilikturunii, dar alfikr aljamieii, al'iiskandiriata, dun sanat nashira.
• faruq al'abasiri : eaqd aliashtirak fi qawaeid almaelumat al'iilikturuniati, dirasat tatbiqiat lieuqud al'iintirnta, dar alnahdat alearabiat 2003m.
• muhamad nuri alshamri, eabd alfataah zuhayr, alsayrafat al'iiliktiruniatu, dar wayil lilnashri, al'urduni 2008m.
• muhamad almursi zahratu, alhasub walqanuni, muasasat alkuayt liltaqadum alealamii, alkuayt, altabeat al'awalii 1995 mi.
• mahmud alsayid khayal, altaeaqud ean tariq altilifizyun, alqahirati, bidun nashir 2000m.
• mdahat eabd alhalim ramadan : alhimayat aljinayiyat liltijarat al'iilikturuniat - dirasat muqaranati, dar alnahdat alearabiat 2001 mi.

• mustafaa aljamal: sharh 'ahkiam alqanun almadanii (masadir aliailtizami), alqahirata, dar alnahdat alearabiat 1991m.
• mamduh muhamad khayri hashim : mushkilat albaye al'iiliktrunii ean tariq al'iintirnit fi alqanun almadanii, dirasat muqaranati, dar alnahdat alearabiat , 2000m.
• d. mueawad eabd altawabi, alwasit faa 'ahkam alnaqd aljzayyt , matbaeat 'atlas, munsha'at almaearif al'iiskandariat 2005 mi.
• nidal 'iismaeil birahmi, 'ahkam euqud altijarat al'iiliktruniati, dar althaqafat walnashr waltawziei, eaman, al'urduni, altabeat al'uwlaa 2005m.
• da.hudaa hamid qashqush: alhimayat aljinayiyat liltijarat al'iilikturuniat eabr al'iintirnti, dar alnahdat alearabiati.
• d. hudaa hamid qashqush, jarayim alhasib al'iilikturunii faa altashrie almuqarani, alqahirata, dar alnahdat alearabiat 1992m.
• d. halali eabd allaah 'ahmadu, taftish nuzam alhasib alali wadamanat almutaham almaelumati, alqahirata, dar alnahdat alearabiat 2006m.
• whid aldiyn swar, sharh alqanun almadani, masadir alailtizami, muasasat alhalbuni, dimashq 1989m.
• yunis earab, hajiat al'iithbat bialmustakhrajat al'iilikturuniat fi alqadaya almasrifiati, eaman, majalat albunuka, mayu 2014m.

2: alrasayil aleilmia

• 'ahmad alsayid tah kardaa, 'iitar muqtarah lihimayat huquq almustahlik min makhatir altijarat al'iiliktruniati, risalat majistir ghayr manshurtin, masri: jamieatan binha, klit altijarat 2011m.
• jalal eayid alshuwrat, wasayil aldafe al'iiliktrunii, dar althaqafat lilnashr waltawziei, risalat majistir manshurat, altabeat al'uwlaa, eaman, al'urdun 2008m.
• khalid faysal alhindi, mafhum altawqie al'iiliktrunii wahimayatuhi, risalat majistir ghayr manshuratin, alkuayt: jamieat alkuayti, kuliyat alhuquq 2004m.
• eumar khalid zarayqat, eaqid albaye eabr al'iintirnti, risalat dukturah, kuliyat alhuquqi, jamieat eayn shams.
• rashidat al'iidrisi, 'iibram aleuqd al'iilikturuni, risalat majistir ghayr manshuratin, jamieat alkuayti, kuliyat alhuquq 2005m.

• eisaa ghasaan eabd allah alrabidi, alqawaeid alkhasat bialtawqie al'iiliktruni, risalat dukturah, kuliyat alhuquqi, jamieat eayn shams 2006 mi.
• eabidat lurinsi, 'iithbat aleaqd al'iiliktruni. risalat majistir maehad aldirasat alearabiati. jamieat alduwal alearabiati, alqahirati.
• muhamad dhaear aleutaybi, alnizam alqanuniu lileaqd al'iiliktrunii. dirasat muqaranat bayn altashrieayn alkuaytii wal'urduniy, risalat majistir ghayr manshuratin, eaman, jamieat alsharq al'awsat, kuliyat alhuquq 2013m.
• nasir zaydan aldhaaydy, aleawamil almuathirat fi wala' almustahlik lilmuntajat alghidhayiyat alwataniat fi dawlat alkuayt, risalat majistir ghayr manshuratin, eaman, jamieat eaman alearabiat lildirasat aleulya 2009m.
• nasir misheal nasir aljalidan alshamriu, madaa hajiat aleuqud al'iiliktruniat fi al'iithbati. dirasat muqaranat lishurut aleuqud alaistihlakiat fi altaeamulat alalkitruniat bialqanun almisrii walkuayti, risalat majistir ghayr manshurtin, masr: jamieat madinat alsaadat, kuliyat alhuquq 2020m.
• nidal salim asmaeil birahmi, 'ahkam euqud altijarat al'iiliktiruniati, risalat majistir, jamieat eamaan alearabiat, al'urduni 2005 ma.
• nawal shaebani, ailtizam almutadakhil bidaman salamat almustahlik fi daw' qanun himayat almustahlik waqame alghash, risalat majistir ghayr manshurtin, aljazayar, jamieat mawlud maemari, kuliyat alhuquq waleulum alsiyasiat 2012m.

3: aldawryat

• almaghazi 'abu earabi wafayaad alqudaati, hijiat altawqie al'iiliktrunii: dirasat fi altashrie al'urduniy, majalat jamieat dimashq lileulum alqanuniat walaiqtisadiati, almujalad 20 aleadad al'awal 2003m.
• ala' yaequb yusif, alhimayat alqanuniat lilmustahlik fi euqud altijarat al'iiliktruniati, bahath manshur fi majalat kuliyat alhuquqi, jamieat alnahrayni, almujalad althaamina, aleadad alraabie eashar 2005m.
• 'ayman musaeidat - eala' khasawinat, khiar almustahlik fi albuyue almanziliat wabuyue almasafati, majalat alsharieat walqanuni, aleadad 46, al'urdun 2011m.

• buqrin eabd alhalim, qanun mukafahat jarayim taqniat almaelumat alkuaytii. dirasat muqaranati, majalat kuliyat alqanun alkuaytiat alealamiati, aleadadu4, alsanat alkhamisata, aleadad altasalsulia 20, rabie al'awal -rbie althaani 1439hi- disambir 2017m.
• hatum eabd albari, hijiat almuharirat al'iiliktruniat fi al'iithbati, almajalat aljinayiyat alqawmiatu, almarkaz alqawmiu lilbuhuth alaijtimaeiati, masr, almujalad alsaabie wal'arbaewn, aleadad althaalith 2004 ma.
• hasan muhamadu, wasayil al'iithbat al'iiliktruniati, majalat alhuquqi, jamieat alkuayti, aleuddan 1 - 2, alsanat 68, 2009m.
• rami eulwan, altaebir ean al'iiradat ean tariq al'iintirnit wa'iithbat altaeaqud alalkitruni, majalat alhuquqi, alkuaytu: jamieat alkuayt, aleudadu4, alsanat 26, 2002m.
• eadil hamid 'abu eazati, aleuqud al'iiliktruniati, khasayisuha walqanun alwajib altatbiq ealayha, majalat aljazirati, jameiat alhasibat alsueudiati, aleadad 158, 18, rabie 'awal 1427h - 16 'iibril 2006m 0
• eabd alhalim buqrin, alhimayat aljinayiyat lishakhs alrasul salaa allah ealayh wasalama, majalat alhuquq waleulum alsiyasiati, jamieat eamaar thalijayi al'aghwati/ aljazayr, aleadad 08, 2015m.
• muhamad budali, altawqie al'iilikturuni, majalat al'iidarati, aleadad raqm 2, lisanat 2003m.
• mahmud eabd alrahman muhamad, madaa hajiat alwasayil al'iiliktruniat fi 'iithbat almueamalat almadaniat waltijariat wal'iidariat tbqan liqanun almueamalat alalkutruniat alkuayti, majalat kuliyat alqanun alkuaytiat alealamiati, aleadadu1, alsanat alsaadisati, aleadad altasalsulia 21, jamadi alakhrt- rajab 1439hi- maris 2018m.
• mansur alsarayrt, al'iitar alqanunia lileaqd almubram eabr wasayil alaitisal alalkitruniat dirasatan fi altashrie al'urduniy, majalat jamieat dimashq lileulum alaiqtisadiat walqanuniati, almujalad 25, aleudadu2, 2020m.

فهـــرس الموضوعـــات

الموضـــــوع الصفحة