HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2020 = 0.44

عنوان البحث

الحماية المعلوماتية للمحاكمة عن بعد

د. امل خلف الحباشنة[1]

[1] جامعة تبوك، المملكة العربية السعودية

HNSJ, 2022, 3(8); https://doi.org/10.53796/hnsj381

تاريخ النشر: 2022/08/01م تاريخ القبول: 2022/07/03م

المستخلص

هدفت الدراسة الى التعرف على الحماية المعلوماتية للمحاكمة عن بعد في المحاكم الأردنية والمصرية، وقد تناولت الدراسة، أسس الحماية المعلوماتية، وبيان مفهوم أمن المعلومات ووسائله، واطلعت الدراسة على صور الاعتداء على أمن المعلومات والتعرف على الإطار التشريعي للحماية المعلوماتيّة، وبيان المواجهة التشريعية لأمن المعلومات في التشريع المصري والأردني في ظل الانفتاح والانتقال السريع للمعلومة بسبب ثورة التقنية والمعرفة والاتصالات، بحيث أصبح العالم قرية صغيرة في إطار المحاكم الالكترونية او المقاضاة عن بعد.

وقد اعتمدت الدراسة على المنهجَ الوصفي التحليلي لكونه من أكثرِ المناهج استخداماً في دراسة الظواهر الاجتماعية الإنسانية وتقوم الدِّراسة على توظيف هذا المنهج لتحليل الحماية المعلوماتية للمحاكمة عن بعد، ويستخدم هذا المنهج في القياس حتى يكيف الوقائع التي ينظرها ويحدد المحكمة المختصة بنظرها،

وقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات حيث أكدت الدراسة على ضرورة جود نظام قضائي محكم في ظل الانفتاح والانتقال السريع للمعلومة بسبب ثورة التقنية والمعرفة والاتصالات في الأردن ومصر. كما أوصت الدراسة على ضرورة وجود دليل إرشادي تقني وقانوني حول صور جرائم التقنية الحديثة والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية، وضرورة تحديث هذا الدليل الإرشادي وتعميمه على المختصين بهذا المجال.

الكلمات المفتاحية: أمن المعلومات، الحماية المعلوماتية، المحاكمة عند بعد.

RESEARCH TITLE

INFORMATION PROTECTION FOR REMOTE TRIAL

Dr. Amal Khalaf Habashneh[1]

[1] **Tabouk University, KSA.**

HNSJ, 2022, 3(8); https://doi.org/10.53796/hnsj381

Published at 01/08/2022 **Accepted at 03/07/2021**

Abstract

The study aimed to identify the information protection of remote trial in the Jordanian and Egyptian courts, and the study dealt with the foundations of information protection, and the statement of the concept of information security and its means. Egyptian and Jordanian legislation in light of openness and rapid transmission of information due to the revolution of technology, knowledge and communications, so that the world has become a small village within the framework of electronic courts or litigation from afar.

The study relied on the descriptive analytical method, as it is one of the most widely used methods in the study of human social phenomena.The study is based on employing this method to analyze the informational protection of remote trial, and this method is used in measurement in order to adapt the facts that it considers and determine the competent court to consider it.

The study reached a set of results and recommendations, as the study emphasized the need for a court system in light of the openness and rapid transmission of information due to the revolution of technology, knowledge and communications in Jordan and Egypt. And the investigation and methods of dealing with digital evidence, and the need to update this guideline and circulate it to specialists in this field.

Key Words: information security, information protection, trial at a distance.

المقدمة

شكلت ثورة المعلومات والاتصالات والتقنية والتطورات المتسارعة وفي ظل التحولات العالمية التي تحكمها دوافع العولمة والتي جعلت العالم قرية صغيرة في إطار المتغيرات التي يشهدها العالم. وفي ظل ما يعرف بالإدارة العامة التي نقع في إطار الحكومات الالكترونية , لذا فالقضاء كغيره من المجالات التي تتسارع وسائل تطويره ولابد من مواكبة هذه التطورات والمستجدات والمتغيرات التي يشهدها العالم للتفاعل معها بإيجابية والتعاطي مع قضاياه من منطلق درء الضرر عن المجتمع الذي أصبح يعرف مثل هذه القضايا الخطيرة عليه.

إن النظام القضائي العربي لم يكن بمنأى عن هذه التطورات واستيعابها والتفاعل معها باعتبارها جزءًا لا يتجزأ من منظومة القضاء الذي يتطلب مواكبته والتفاعل معه، و يكون اللجوء إلى الوسائل التكنولوجية الحديثة في المعاونة القضائية بشكل أمن، مثل التحقق من صحة الجهات التي تخدم عدة جهات رسمية مثل البنوك والسفارات إلى جانب خدمة الاستعلام عن المعاملات من خلال (الرد الآلي) استفسارات المواطنين حول سير المعاملات في وزارة العدل دون الذهاب ومراجعة المحاكم (مكتب الوزارة) وكذلك بعض الخدمات في تفعيل أنظمة المحاكم الإلكترونية من خلال معرفة مواعيد جلسات المحكمة والقرارات الصادرة عن طريق رسائل التذكير مثل جلسات المحكمة وجلسات الرسائل القصيرة).

وكذلك بيان التجارب الدولية والعربية التي حظيت بنجاح كبير في تطوير المنظومة القضائية، ومن أجل ذلك تم الاطلاع على وسائل الحماية المعلوماتية للنظام القضائي الالكتروني من خلال الاطلاع على أسس الحماية المعلوماتية والإطار التشريعي للحماية المعلوماتية.

مشكلة الدراسة : تكمن مشكلة الدراسة في موضوع الحماية المعلوماتية للمحاكمة عن بعد وذلك بعد ان أصبح عالم حماية المعلومات للمحاكم ضرورة ملحة في عالم يشهد ثورة تكنولوجية تقنية معرفية اتصالاتية فأصبح من الضرورة توفير التقنيات اللازمة لغايات تطبيق المحاكمات عن بعد وتامين المعلومات السرية وذلك من قبل وزارة العدل بالتنسيق ما بين كافة الشركاء بمن فيهم مراكز الإصلاح والتأهيل ونقابة المحامين حتى تسير الإجراءات بكل امن وسلامة .

أهمية الدراسة : تبرز أهمية الدراسة في نطاقين : علمي وعملي

الأهمية العلمية : تشكل الأهمية لهذه الدراسة إضافة إلى الدراسات في مساهمة هذه الدِّراسة في توفير دراسة علمية حديثه, قد تفيد الباحثين والمختصين وتزود المكتبات ومراكز الأبحاث في بيان أهمية الحماية المعلوماتية للمحاكمة عن بعد في عالم الانفتاح والتكنولوجيا.

الأهمية العملية : تظهر الأهمية العملية لدراسة الحماية المعلوماتية للمحاكمة عن بعد من خلال بيان أسس الحماية المعلوماتية وأهمية الاطلاع على الإطار التشريعي للحماية المعلوماتيّة في كل من الأردن ومصر

أهداف الدراسة : من خلال الدراسة يمكن التعرف على الأهداف التالية :

1. التعرف على أسس الحماية المعلوماتية

2. بيان مفهوم أمن المعلومات ووسائله
3. معرفة صور الاعتداء على أمن المعلومات
4. التعرف على الإطار التشريعي للحماية المعلوماتيّة
5. بيان المواجهة التشريعية لأمن المعلومات في التشريع الاردني المصري

أسئلة الدراسة : من خلال أسئلة الدراسة يمكن الإجابة على التساؤلات التالية :

1. ما أسس الحماية المعلوماتية؟
2. ما مفهوم أمن المعلومات ووسائله؟
3. ما صور الاعتداء على أمن المعلومات؟
4. ما الإطار التشريعي للحماية المعلوماتيّة.
5. ما المواجهة التشريعية لأمن المعلومات في التشريع الأردني المصري؟

منهجية الدراسة

المنهج الوصفي التحليلي: وفي هذه الدِّراسة يستخدمُ الباحثُ المنهجَ الوصفي التحليلي لكونه من أكثرِ المناهج استخداماً في دراسة الظواهر الاجتماعية الإنسانية وتقوم الدِّراسة على توظيف هذا المنهج لتحليل الحماية المعلوماتية للمحاكمة عن بعد وذلك في ظل التطور التكنولوجي وفي ظل تزايد الأنماط الأكثر استخداما من قبل القانونيين مثل المحاميين والقضاة والباحثين في مجال القانون، فالقاضي مثلا يستخدم هذا المنهج في القياس حتى يكيف الوقائع التي ينظرها حتى يحدد المحكمة المختصة بنظرها.

مصطلحات الدراسة

أمن المعلومات: ويقصد بها حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والاختراق والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والإطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخليّة والخارجيّة، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك(دعدوع ,2016 :2).

الحماية المعلوماتية : هي مجموعة من البيانات والمعلومات التي طرأت عليها عمليّات تغيير ومُعالجة حتى تحمل معنى وأهمية، وهي العلم الباحث في مجال توفير الحماية اللازمة للمعلومات ومنع الوصول إليها وهدرها من غير ذوي الصلاحية، وحمايتها من أيّ تهديد خارجي، ويشمل هذا المصطلح الأدوات والطرق والإجراءات اللازمة الواجب توفرّها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل والخارج (الحيارى, 2016 :1).

المحاكمة عند بعد : المحاكمة عن بعد يعني القضاء الالكتروني او هو نظام قضائي معلوماتي يتم بموجبه تطبيق كافة إجراءات التقاضي عن طريق المحكمة الالكترونية بوساطة أجهزة الحاسوب المرتبطة بشبكة الانترنت

وعبر البريد الالكتروني لغرض سرعة الفصل في الدعاوى و تسهيل إجراءاتها على المتقاضين و تنفيذ الأحكام الكترونيا والحفاظ على سلامتها (الكرعاوي,2016 :265)

هيكلية الدراسة

المبحث الأول : أسس الحماية المعلوماتية

المطلب الأول : مفهوم أمن المعلومات ووسائله

المطلب الثاني: صور الاعتداء على أمن المعلومات

المبحث الثاني : الإطار التشريعي للحماية المعلوماتيّة

المطلب الأول : المواجهة التشريعية لأمن المعلومات في التشريع المصري

المطلب الثاني: المواجهة التشريعية لأمن المعلومات في التشريع الأردني

المبحث الأول : أسس الحماية المعلوماتية

بدأ علم أمن المعلومات وتطور مع بداية تقنية المعلومات وتطورها. فعندما بدأت الحاسبات الآلية باحتواء معلومات مهمة، بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها وتخزينها وتنقلها؛ فبدأ التفكير في تأمين مواقع هذه الأجهزة والمعلومات التي فيها وحمايتها، وزاد الأمر تعقيدًا ارتباط أجهزة الحاسب الآلي حول الكرة الأرضية بشبكة واحدة هي شبكة الإنترنت، واعتماد كثير من الناس عليها في أداء أعمالهم، وتنمية وزيادة تحصيلهم العلمي، وتواصلهم الاجتماعي، وإنهاء إجراءاتهم الحكومية وتنظيم المنظومة القضائية. ولكن لا تخلو الخدمات الالكترونيّة كما سبق وأوضحنا من التهديدات، لذلك كان لابد من البحث عن وسائل لضمان أمن المعلومات.

ظهرت الحاجة الماسة في الحد من هذا الجانب المظلم لابد من حماية المعلومات من منظور قضائي؛ فجميع الإجراءات القانونية التي تتم عبر النظام المعلوماتي لابد من تشديد الحماية عليها منعًا من اختراقها، فهذه المعلومات قد تكون عل درجة بالغة من الخطورة ولذلك يجب حمايتها بكل الوسائل، كذلك تعتمد المحكمة الالكترونيّة على حاسبات آلية ترتبط ببعضها عن طريق شبكات داخلية، وترتبط هذه الشبكات بالشبكة العنكبوتية عن طريق وسائل الاتصالات الحديثة، ومن خلال هذه الشبكات يجرى تداول بيانات المحكمة ومعلوماتها، وهذا دليل على خطورة هذه المعلومات، وخصوصيتها وسرية بعضها.

ولكن يترتب على حل مشاكل الاستخدامات على شبكات الاتصال الالكترونيّة تكلفة عالية جدًا بتطهير الهجمات المتعددة للفيروسات، وفق لمركز التنسيق ERT، وهو مركز مراقبة حماية شبكات الاتصال الالكترونيّة.[1]

ومن هنا يعد نظام الحمايّة المعلوماتيّة والجنائيّة لهذه البيانات أحد مقومات المحكمة الالكترونيّة، إذ يحقق

([1]) لورنس م. أوليفا، المرجع السابق، ص 17.

الثقة والفاعلية في نظام المحكمة الالكترونيّة، ويشجع المتقاضين للتعامل معها دون خوف أو تردد.

المطلب الأول : مفهوم أمن المعلومات ووسائله

عرفت اتفاقية بودابست النظام المعلوماتي بأنه "كل ألة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى، تنفيذًا لبرنامج معين، بأداء معالجة آلية للبيانات".[2]

كما ذكر أنه: "يقصد بأمن المعلومات حماية وتأمين الموارد المستخدمة كافة في معالجة المعلومات، إذ يكون تأمين الشركة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات الشركة"[3]. في حين عرف البعض أمن المعلومات أنه: "هو اختصار الطرائق والوسائل المعتمدة للسيطرة على أنواع ومصادر المعلومات كافة وحمايتها من السرقة، والتشويه، والابتزاز، والتلف، والضياع والتزوير، والاستخدام غير المرخص، وغير القانوني".[4]

2- أهمية أمن وسرية المعلومات:

وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك. فتنبع أهمية أمن المعلومات من أنها تستخدم من لدن الجميع بلا استثناء....الدول والشركات، والأفراد، كما أنها هدف للاختراق من جانب الجميع، وفي بعض الأحيان تكون المعلومات هي الفاصل بين المكسب والخسارة للشركات وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان. يذكر في هذا العصر بالذات أنه لم تعد مشكلة الناس الحصول على المعلومات، إنما أصبحت مشكلتهم هي هذا الفيض الهائل من المعلومات كيف نحمي هذه المعلومات من الأخطار التي تهددها.[5]

3- عناصر أمن المعلومات :

يتلخص هدف جميع مستخدمي الإنترنت في الحصول على المعلومات ونقلها بشكل آمن، وهناك مجموعة من التحديات التي يجب أخذها في الحسبان لضمان نقل آمن للمعلومات، [6] وأهم عناصر أمن المعلومات هي:

أ- **السريّة:** تعني منع اطلاع أي شخص غير مخوّل من الوصول إلى بيانات شخص آخر.

---

[2] د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، علي ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، النهضة العربية، القاهرة، 2000، ص 40 -41.

[3] د. حسن طاهر داود، الحاسب وامن المعلومات، مركز الدراسات و البحوث، المملكة العربية السعودية، 2000م، ص 23.

[4] د. هيثم محمد الزعبي السامرائي، د. إيمان فاضل، نظم المعلومات الإدارية، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، 2004م، ص238.

[5] د. حسن طاهر داود، الحاسب وامن المعلومات، مرجع سابق، ص30.

[6] د. نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف بالإسكندرية، 2008، ص 151.

ب- **التكامليّة وسلامة البيانات:** وتعني التكامليّة هنا المحافظة على البيانات من التعديل أو التغيير من قبل الأشخاص غير المخوّلين بالوصول لها، مثل أن يصل شخص بقصد أو بغير قصد لبيات غير مسموح له بالوصول إليها، كذلك في حال وصول فايروس إلى الحاسوب ويعدل بياناته فهذا يعد أيضاً انتهاكاً للتكامليّة وعدم توفر الحماية الكاملة للمعلومات.

ت- **توفر البيانات:** وتعني توفر البيانات كاملةً عند الحاجة إليها بحيث تكون معلومات صحيحة ودقيقة غير معدّلة أو ناقصة، مما يجعل عناصر النظام تعمل بشكلٍ صحيح.

أما عن حماية المعلومات من منظور قضائي؛ تعتمد المحكمة الالكترونيّة على حاسبات آلية ترتبط ببعضها عن طريق شبكات داخلية، وترتبط هذه الشبكات بالشبكة العنكبوتية عن طريق وسائل الاتصالات الحديثة، ومن خلال هذه الشبكات يجري تداول بيانات المحكمة ومعلوماتها، فيدل ذلك على خطورة هذه المعلومات، وخصوصيتها وسرية بعضها. ومن هنا يعد نظام الحماية المعلوماتية والجنائية لهذه البيانات أحد مقومات المحكمة الالكترونية، إذ يحقق الثقة والفاعلية في نظام المحكمة الالكترونية، ويشجع المتقاضين للتعامل معها دون خوف أو تردد. أما عن وسائل حماية أمن المعلومات، فسنواليها بالشرح كالتالي.

ثانيًا: وسائل حماية أمن المعلومات:

هناك مجموعة من مظاهر الحماية المعلوماتية التي يقوم بها التقنيين، ومن أهم هذه المظاهر ما يلي:

1- تشفير البيانات والمعلومات المتداولة في المحاكم عن بعد: هو عملية تتمثل في تحويل المعلومات المقروءة إلى إشارات غير مفهومة[7]. فبعض مستخدمي شبكة الإنترنت يبتغون أن يتمكنوا – بواسطة برنامج خاص – من تشفير معلوماتهم قبل نقلها عبر الشبكة. وهو وسيلة تأمينية تتمثل في إلزام الشركات المنتجة للبرنامج بوضع عراقيل فنية للحيلولة دون دخول المتلصصون أو القراصنة[8] إلى تلك البرامج وما تحويه بنوك المعلومات وقواعد

---

[7] GOLIARD (F), Télécommunication et règlementation françaises du cryptage, d. 1988, Chron., p.120.

La cryptographie ou chiffrement est le processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible. La loi française définit les prestations de cryptologie comme : "toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet.Article 28 de la loi 90-1170 du 29 décembre 1990 modifiée.

[8] لقد قضت المحاكم الأمريكية بمسئولية شركة، لإنها قدمت نفسها للجمهور على أنها تمارس رقابة على محتوى الخدمات التي تتولى تقديمها باستخدام برامج تقنية من نوعية خاصة، وباتباع منهج معين يقوم به أشخاص متخصصين في هذا المجال، ومع ذلك لم يقم بمنع الرسائل والمعلومات غير المشروعة وبالتالي تكون قد أخلت بالتزامها بتقنية المعلومات على الشبكة.

THOUMYRE (Lionel), Responsabilités sur le web: une histoire de la ré- glementation des réseaux numériques, disponible a l'adresse : http://www.lex-electronica.org/articles/v6-1/thoumyre.htm, N 35.P.7.-

البريد الالكتروني من أسرار[9]، لذلك يقوم التقنيون بتشفير البيانات والوثائق الموجودة على قواعد البيانات والنظام الآلي والموقع الالكتروني للمحكمة من خلال عمليات ترميزية معقدة وسرية فهم يقومون بوضع العديد من المعادلات الرياضية التي تقوم بدورها بتغيير البيانات التي تظهر للعامة والغير المخول لهم بالدخول إلى النظام الآلي أو الموقع فلا يستطيعون الاطلاع عليها أو تفسيرها والاستفادة منها حتى وإن وصلوا إليها فلن يستطيع الوصول إلى معناها الحقيقي دون فك شفرت المعادلات التي بنيت بها، إلا أنه يتم حل هذه الشفرة عند وصولها إلى وجهتها الصحيحة أي عند وصولها إلى المستلم في حالة إرسال بيانات ومعلومات لشخص ما كطرف في نزاع قضائي سواء أكان ذلك الطرف هو أحد أطراف الادعاء أو المدعى عليهم أو المحامون المعلوماتيون أو هيئة قضاة المعلوماتيين أو أحد الإداريين [10].

ولذلك فتشفير بيانات المحكمة الالكترونيّة ومعلوماتها المتداولة عبر الشبكة : يعني تحويل الكلمات المكتوبة إلى أرقام أو صورة رقمية لا يمكن معرفة مضمونها، إلا عن طريق فك الشفرة ذاته[11]، وذلك بأن يكون لدى المستقبل القدرة على استعادة محتوى الرسالة، وذلك في صورتها الأصلية قبل التشفير، وذلك باستخدام عملية عكسية لعملية التشفير التي تسمى الحل[12].

2- تأمين خصوصية المعلومات: : فيقصد بخصوصية المعلومات؛ ألا تستخدم المعلومات في غير الغرض المرخص به من صاحب المعلومة، وهي تقنية المعلومات بواسطة المستخدم؛ فتوجد برامج تسمح للمستخدم أن يمنع الدخول إلى بعض المواقع. فالمستخدم يمكنه أن ينشئ لنفسه قائمة بالمواقع المحظور الدخول إليها[13]، لذا يتعين أن يكون لدى المحكمة الالكترونيّة وثيقة تسمى- وثيقة خصوصية المعلومات- وهذه الوثيقة تحدد الخطوات الواجب اتباعها للحصول على مستويات عالية من الخصوصية.

فيمتنع على المستخدمين أنفسهم الذين لهم الحق في الدخول إلى الموقع الالكتروني للمحكمة والوصول إلى المعلومات والبيانات التي تخص الدعاوي الجنائية المرفوعة وهم طرفًا فيها، أن يستخدموا هذه المعلومات في أي أغراضًا غير مرخص بها من قبل صاحب المعلومة، وعلى هذا الأثر يتعين على المحكمة الالكترونيّة أن تقوم بنشر وثيقة خاصة بخصوصية المعلومات والتي توضح فيها الجزاءات والعقوبات التي يتعرض لها من يحاول انتهاء خصوصية المعلومات لأغراضٍ غير مصرح بها ودون علم صاحب هذه المعلومات، وتُحدد هذه الوثيقة الخطوات والإجراءات التي يجب اتباعها لكي يتم الحصول على حماية وخصوصية المعلومات الواردة في الدعوى

---

[9] د. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 2002م، ص 12.

[10] أكرم فاضل سعيد، مرجع سابق، ص 17.

[11] Les problèmes posés par la législation française en matière de chiffrement by Maitre ValerieSedallian, Droit de l'Informatique et des télécoms 98/4 (10/98).

[12] د. رامي نعمان الجاغوب، "أمن وسرية المعلومات في الحكومة الإلكترونيّة "، ندوة متطلبات الحكومة الالكترونية، الإمارات، وزارة الداخلية، 2002، ص 3-4.

[13] د. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، مرجع سابق، ص 113.

الجنائية المرفوعة[14].

ويمُنع تعديل البيانات أو المعلومات الموجودة على النظام الآلي الخاص برفع الدعاوي وعلى الموقع الالكتروني للمحكمة لمن لا صلاحية له لفعل ذلك، وأيضًا التأكد من هوية المستخدم والأشخاص الذين يقومون بإرسال الأوراق والمستندات والآخرين الذين يستقبلونها[15]، وتحديد الأشخاص الذين لهم حق الدخول والولوج أثناء عملية سير الدعوى الجنائية الالكترونية، فلا يحق للأشخاص الغير مصرح لهم بالدخول إلى معرفة معلومات خاصة بالقضية أو سيرها أو الاطلاع على المستندات والأوراق المتضمنة في المحررات الالكترونيّة أو حتى حضور الجلسات دون داعي أو طلب لوجوده، ويتم التحكم في سير هذا الأمر كما هو مخطط له وكما ينبغي دون الإخلال بعملية سير القضية من خلال قيام التقنين بإرسال اسم مستخدم وكلمة سر لكل الأطراف المعنية في الدعوى الجنائية المرفوعة أمام المحكمة، فيعتبر اسم المستخدم وكلمة المرور أو كلمة السر هما الهوية الخاصة بالفرد في البيئة الالكترونيّة،[16] وكذلك الحفاظ على الكمبيوتر من الفيروسات التي قد تصيبه من المصادر مجهولة الهوية، وحفظ نسخ احتياطية من البيانات المتضمنة في النظام الآلي والنظم المساعدة والفرية له على الخوادم والسيرفرات الموجودة على الإنترنت[17]. وبتأمين تحقيق الحماية لمحتوى البيانات ضد محاولات التغيير أو التعديل أو المحو، خلال مراحل تبادل المعاملات والوثائق، مع ضمان التحقق من شخصية المرسل أو المستقبل. ومن قبيل ذلك لا يمكن الحصول على تفاصيل الدعوى إلا من قبل أطرافها، إذ تتولى الجهة القائمة على إدارة الدائرة القضائية الكترونيًا تحديد الأشخاص المصرح لهم بالدخول إلى نظام المعلومات وتسجيل الدعاوى والاطلاع عليها، كالقضاة وموظفي المحكمة والمحامين والخبراء وأطراف الدعوى، وذلك بتزويد هؤلاء باسم مستخدم وكلمة مرور خاصة بكل منهم، لكي يتمكنوا من الاطلاع على أدق التفاصيل في دعواهم، وهذا النظام يضمن منع الأشخاص غير المرخص لهم من اختراق نظام المعلومات، والاطلاع على مستندات الدعوى.

3- تطبيق أساسيات الأمن السيبراني على المحاكمة عن بعد: يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه، سواء أكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني[18]، إلى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الالكترونية.

---

[14] د. صفاء أوتاني: المحكمة الإلكترونيّة (المفهوم والتطبيق)، مرجع سابق، ص 176.

[15] القاضي حازم محمد الشرعة، التقاضي الالكتروني والمحاكم الالكترونية، مرجع سابق، ص 63.

[16] د. محمد أمين الرومي، النظام القانوني الالكتروني، مرجع سابق، ص 124.

[17] د. صفاء أوتاني، المحكمة الإلكترونيّة (المفهوم والتطبيق)، مرجع سابق، ص 177-178.

[18] الفضاء السيبراني مجال عملياتي يعتبر الميدان الخامس للحروب الحديثة بعد ميدان الحرب البرية والجوية والبحرية والفضائية، وفي تعريف أخر : "مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة" .د.صالح بن علي بن عبدالرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، المملكة العربية السعودية، هيئة الاتصالات وتقنية المعلومات، رؤية 2030، ص7.

وبعد الحديث عن وسائل حماية المعلومات، سوف نتحدث في الفرع التالي عن صور الاعتداء على أمن المعلومات.

المطلب الثاني: صور الاعتداء على أمن المعلومات

احتلّ التقدّم في مجال المعلومات والاتّصالات جانبًا كبيرًا ومُهمًّا في حياة النّاس وتعاملاتهم؛ فصار الحاسوب أساس التّعامل بين الأشخاص والشّركات والمؤسسات، وقد ازداد التوجّه لاستخدام شبكات المعلومات الالكترونيّة في الفترة الأخيرة بصِفَتها أداة اتّصال دولية في مُختلف مناحي الحياة، مُوفِّرةً بذلك الكثير من السّرعة والمسافات والجهد على الإنسان.إنّ الاستخدام الكبير لِلأنظمة التكنولوجية قاد إلى الكثير من المشاكل والمَخاطر، فبقدر ما يحققه تطور التقنيات من فوائد كبيرة في مجال الرقي والتقدم الإنساني فإنها في الوقت ذاته مهدت السبيل إلى بروز أشكالًا وأصنافًا جديدة من الجرائم لم تكن مُتداولةً سابقًا، لاسيما بعد أن تم ربط الحاسب الآلي بالشبكة العالمية للإنترنت، فقد واكب هذا التطور بروز خبراء يتمتعون بالخبرة والحرفية لتطويع هذه التقنية للقيام بأعمال إجرامية ذات طابع معاصر، حيث وجد المجرم تقنية عالية وأساليب حديثة تساعده في ارتكاب العديد من الجرائم وسُميّت هذه الجرائم بالجرائم الالكترونية، فما هي الجرائم الالكترونية؟ وما هي أنواعها؟

أولًا- تعريف الجرائم الالكترونيّة:

لقد تعددت المصطلحات المستخدمة للتعبير عن الجرائم (المعلوماتية)، ويوجد تباين بشأن هذه المصطلحات مع أنها تدل جميعها على الظاهرة الإجرامية الناشئة في بيئة نظم المعلومات والشبكات، فتعددت الاقتراحات من إساءة استخدام الكمبيوتر، والجريمة المرتقبة بالكمبيوتر، احتيال الكمبيوتر، الجريمة المعلوماتي، وغيرها، لكن كل هذه المسميات استندت على البعدين التقني والقانوني.[19]

وفي الفقه نجد مؤلفات الفقيه "ULRICH SIEBER" قد اهتمت بحصر مختلف التعريفات التي وضعت عن الجرائم المعلوماتية فهنالك معايير قانونية للتعريف وهنالك معايير تستند إلى موضوع الجريمة ونمطها والعناصر المتصلة بها أو سمات مرتكبيها.[20]

لقد تولى الفقه المقارن وعرض المشرع سواء على المستوى المحلي أو الإقليمي الحديث عن الجريمة المعلوماتية بمسميات مختلفة ضيقة وواسعة منها " يقصد بجرائم الكمبيوتر جرائم الأموال وجرائم الأشخاص وجرائم المصلحة العامة التي يقع باستعمال الكمبيوتر ويقصد بجرائم الإنترنت تلك الجرائم التي تقع عن طريق استعمال شبكة الإنترنت سواء داخل البلاد أو خارجها.[21]

كما عُرفت بأنها: "كل الجرائم التي يتم ارتكابها بوسائل تكنولوجية ويشمل بطبيعة الحال جرائم الحاسوب

---

[19] د. أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة " في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2015، ص 84 .

[20] "ULRICH SIEBER" هو محامي متخصص في الكتابة في مجال الجرائم المعلوماتية وله مجموعة من المؤلفات ابتدأ من السبعينات، مشار إليه لدى د. أيمن عبد الله فكري، المرجع السابق، ص 92 .

[21] د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، 2010، ص 11 .

والإنترنت".[22]

كما يرى جانب من الفقه[23] تعريف الجريمة المعلوماتية (الالكترونيّة) من زاوية فنية وأخرى قانونية، فالتعريف الفني يميل إلى القول بأن الجريمة المعلوماتية هي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.

ومن الناحية القانونية عُرفت بانها " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الحاسب، أو هي الجرائم التي تلعب فيها البيانات والكمبيوتر والبرامج المعلوماتية دورًا رئيسيًا.[24]

لقد أصبح العالم أمام مجموعة من الجرائم المستخدمة ذو تكنيك متميز[25]، الأمر الذي يستوجب تدخل المشرع الدولي والمحلي بالاتفاقيات، وكذلك سن التشريعات الوطنية لمواكبة هذه الجرائم.

وهنالك تعريف وصفه خبراء منظمة التعاون والتنمية الاقتصادية (O.C.D.E) للإجرام المعلوماتي بأنه: "كل سلوك غير قانوني أو ضد الأخلاق أو غير مصرح به، والذي يتعلق بمعالجة آلية للبيانات أو بنقل هذه البيانات"[26].

وقد عرفها البعض بأنها:" تلك الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي، عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة بها " [27]

وقد اختلفت صور محاولات المشرع والقضاء في مختلف الدول للتصدي للأعمال غير المشروعة التي ترتكب عن طريق الإنترنت، فكان منها التدخل التشريعي لوضع ضوابط للإنترنت أو كان توسع من جانب القضاء في تفسير النصوص الجنائية الموجودة لتشمل هذه النصوص ما استجد من جرائم إنترنت وذلك لأن طبيعة نصوصها تسمح بذلك[28].

وبالنظر لأن هذه الجرائم ذات طبيعة خاصة بالاستناد لحداثتها وارتباطها بتكنولوجيا الحاسبات وما شابهها من أجهزة معالجة الكترونيّة، علي أساس أن الغرض من هذا الإجرام هو الاعتداء علي المكونات غير المادية للحواسيب والتي تتمثل ببرامجه وبياناته[29].

وبالنظر إلي أن الجرائم الالكترونيّة هي ظواهر إجرامية أو جرائم ذكية تحدث في بيئة الكترونية أو بيئة

---

[22] د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، دار النهضة العربية، القاهرة، 2004، ص 219.

[23] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، حقوق الطبع محفوظة للمؤلف، 2009، ص 1.

[24] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 3.

[25] د. محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ،2004،، ص 219 .

[26] د. حاتم عبد الرحمن منصور الشحات، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 2002، ص21.

[27] د. منير محمد الجنبيهي ،د. ممدوح محمد الجنبيهي، جرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2004، ص 13.

[28] د. مدحت رمضان، جرائم الاعتداء علي الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000،ص17.

[29] د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الإسكندرية، ص11.

رقمية يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، وينجم عنها ضرر لا يستهان به مع اختلاف هدف كل جرم[30].

وهناك تعريف موضوعي يستند لوقوع الجريمة علي الحاسب الآلي وهو " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلي المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[31]

فقد أظهر القبض على القرصان الشهير (Kevin Mitnice) بمعرفة المخابرات الامريكية الطريقة التي يتم فيها استخدام المعلوماتية للكشف عن الدلائل. ففي ديسمبر سنة 1994م ،أكتشف أحد الباحثين في مركز الحاسبات الآلية الموجود في San Diego – جنوب كاليفورنيا– أنه تم اختراق الحاسب الآلي الشخصي الخاص به من جهاز يقع بمدينة شيكاغو، ولكن يتم التحكم فيه عن بعد. وبعد شهر عثر على المعلومات المسروقة على موقع Well على الإنترنت، فقام المجني عليه بمراقبة الشبكة، إلا أنه يبدو أن القرصان كان يعمل من عدة مدن . وبمراجعة المكالمات التليفونية المسجلة بمعرفة شركة التليفونات عن طريق الكمبيوتر وجد أن الجاني يقوم بالبث باستخدام مودم متصل بتليفون محمول. وباختراقه المدينة (بأريال هوائي) خاص متصل بجهاز محمول أمكن لفريق البحث أن يحدد المكان الذي تصدر منه النداءات وأن يقوم بالقبض على القرصان. وعلى ذلك يتضح أن استخدام المعلوماتية في هذه الحالة كانت هي الوسيلة الوحيدة للوصول إلى المجرم.[32]

ثانيًا– أنواع الجرائم الالكترونيّة وتقسيماتها

لقد جرى تقسيم صور الاعتداء بهذا المجال من قبل فقهاء القانون عدة تقسيمات إلا أن التقسيم الأكثر اتفاقًا مع طبيعة الجرائم المتصلة بنظام معالجة المعلومات آليًا هو تقسيمها إلي جرائم سلوك ونتيجة، ومناط هذا التقسيم هو تطلب النتيجة كعنصر من عناصر النموذج القانوني للجريمة[33].

تضم الجريمة الالكترونيّة أشكالا متعددة ومتنوعة يصعب حصرها وهي بازدياد كلما زاد استخدام الحاسب الآلي وشبكة الإنترنت[34].

إن الدساتير والتشريعات الحديثة تنص جميعها علي مبدأ شرعية الجرائم والعقوبات إذ لا جريمة ولا عقوبة إلا بنص، فلابد من تحديد المشرع النشاط الجرمي وعناصره، وكان المشرعين الفرنسي والأمريكي سباقين بهذا المجال حيث تقدمت الحكومة الفرنسية بتعديل لمشروع قانون أعد لتعديل قانون حرية الاتصالات وسمي بقانون فيوننسبةلـ(François **Fillon**)وزير الاتصالات في ذلك الوقت، وقد صدر بتاريخ 30 سبتمبر1986م، حيث تم تعديله بإضافة مواد جديدة من ضمنها تعريف القائم علي تقديم خدمة الإنترنت، وبائت هذه المحاولة بالفشل بعدما

---

[30] د. علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، بدون تاريخ، ص8.

[31] Michael Alexander, Computer Crime, Ugly secret for business, Computer world, Vol. xxiv, No.11, 1990, pp.104.

[32] DARAGON (E.), OP. Cit., N 410, P. 236.

[33] د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية،1995، ص12.

[34] الباحث القانوني. عبد الصبور عبد القوي علي مصري، دار العلوم للنشر والتوزيع، أحد فروع مجموعة العلوم ثقافية، ص12.

عرض هذا المشروع علي المجلس الدستوري، حيث أكد أنه لا يجوز أن ترتب المسئولية الجنائية علي توجهات أو قرارات عامة لم توضح الأسس التي تقوم عليها، إلا أن النصوص القائمة بقيت تغطي الجرائم التي تقع بهذا الشأن[35].

إن أول تشريعات صدرت لمكافحة جرائم الكمبيوتر في الولايات المتحدة الأمريكية بعام 1978 بولاية فلوريدا وولاية أريزونا، أما علي المستوى الفيدرالي صدر أول تشريع في عام 1984[36].

وهنالك عدة تقسيمات للجرائم المعلوماتية، التقسيم الفقهي والتقسيم الأوربي والتقسيم الأمريكي، حيث اعتمد التقسيم الفقهي علي دور نظم المعلومات بارتكاب الجرائم، إذ تعد نظم المعلومات هدفا للجريمة (كما هو في حالة الدخول غير المصرح به إلي النظام أو تدمير المعطيات والملفات بزراعة الفيروسات، والاستيلاء علي البيانات المخزنة والمنقولة)، وتعد نظم المعلومات كذلك أداة لارتكاب جرائم تقليدية، كالاستيلاء علي أرقام بطاقات ائتمان وإعادة استخدامها بهدف الاستيلاء علي أموال أصحابها الأصليين، وتستخدم نظم المعلومات كذلك في جرائم القتل عن طريق التلاعب في برمجيات الأجهزة الطبية بتحويرها أو تحويلها وتكون نظم المعلومات بيئة للجريمة[37].

كما حاول العديد من الفقهاء وضع تقسيمات لهذه الجرائم ومنهم Ulrich Silber وMartin Wasik، حيث قسّم الفقيه Ulrich Silberالجرائم إلي جرائم الحاسب الآلي الاقتصادية وجرائم الحاسب الآلي التي تعتدي علي الحياة الخاصة والجرائم التي تهدد المصالح القومية أو السلامة الشخصية للأفراد[38].

أما تقسيم الفقيه Martin Wasikفاعتمد علي أنماط السلوك المختلفة من الأفعال غير المشروعة، ومنها الدخول والاستعمال غير المصرح بهما للنظام المعلوماتي، والجرائم التي يساعد الحاسب الآلي علي ارتكابها[39].

كذلك فإن للجهود الأوربية لتقسيم الجرائم المعلوماتية خطوات في سبيل تدويل القانون الجنائي وذلك بالاستناد لما اتسمت به هذه الجرائم بالدولية لمكافحتها، فكان هنالك إسهامات إقليمية ودولية في تقسيم هذه الجرائم[40] ومنها:

---

[35] د. مدحت رمضان، جرائم الاعتداء علي الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000، ص17-19.

[36] Edward M. wise, Computer Crimes and Other Crimes against Information Technology in the United States, Rev.int. dr. pen-1993, P657.

مشار إليه في كتاب د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، مرجع سابق، ص5.

[37] د. أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة "، مرجع سابق، ص134-135.

[38] SieberUlerich, The interval oval Emergence of criminal information law, Carl Heymans. Verlag K.G., 1992. P.P 327.

مشار إليه عند الدكتور أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة "، المرجع السابق، ص137.

[39] Martin Wasik, Computer Crime. Ibid.1991, p.41.

مشار إليه لدى د. أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة "، المرجع السابق، ص140،141.

[40] د. أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة "، المرجع السابق، ص134-135.

- تقسيم منظمة التعاون الاقتصادية والتنمية.
- التقسيم الخاص بالمجلس الأوربي.
- اتفاقية بودابست نوفمبر 2001 لمكافحة الجريمة المعلوماتية[41].
- التقنين الفرنسي للجريمة المعلوماتية.

ثالثًا– صور الاعتداء على نظام الإجراءات القضائية في المحاكمة عن بعد :

إن ما يهمنا بعد ما تم الحديث عن الجرائم المعلوماتية بمفهومها وتقسيماتها أن يكون مدخلًا للحديث عن هذه الجرائم التي قد تمس نظام التقاضي الالكتروني للخصومة الجنائية، والتي تعد من الصعوبات والإشكاليات التي تُثار عند تفعيل الأنظمة التي يقوم عليها التقاضي الجنائي الالكتروني، وسيثار للحديث بهذا السياق عن صور هذه الجرائم التي يتعرض لها هذا النظام، وكيف يمكن التصدي لها؟، وذلك بمكافحتها بالتشريعات ذات العلاقة، وتوفير الأمن لهذه الأنظمة ليتسنى لعملية التطوير التكنولوجي السير قُدوما لا أن يتم إعاقتها.

إن أبرز صور الاعتداء التي يمكن أن تمس نظام التقاضي الالكتروني هي **الولوج غير القانوني**، إذ يعد الجريمة الرئيسية التي تنطوي علي تهديد وتعد علي الأمن والسرية والسلامة والإتاحة للنظم والبيانات المعلوماتية، إذ تبرز الضرورة لتوفير الحماية لمصالح المنظومة، لتتحكم بنظمها دون تشويش أو عقبات، فبمجرد التدخل غير المصرح به بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي، يجب أن يعتبر غير قانوني كمبدأ عام، ويضم الولوج غير القانوني (غير المصرح به) الاختراق للنظام بأكمله أو لجزء منه، وسواء كان النظام متصل بشبكات اتصال عامة أو متصل بنفس الشبكة محلية أو إنترنت[42].

ومن صور الاعتداء التي يمكن تصور مساسها بنظام التقاضي الالكتروني هي **جريمة سرقة المال المعلوماتي**، إذ أن مصادر استخدام الحاسبات في التفاعل التجاري متعددة فالحسابات البنكية والشركات معرضة للسلب الالكتروني، عن طريق إدخال معلومات زائفة للتمويه أو عن طريق التلاعب بالبرامج لمصلحة المتحايل[43]، كذلك هنالك تكنيك السحب والدفع الالكتروني من الرصيد عن طريق الكارت الممغنط، وهي بطاقات بلاستيكية يصدرها البنك لعميله بشروط معينة ويعطى بها رقما سريا غير معروف إلا للعميل وحده، وأصبحت هذه الطريقة مستخدمة بشكل كبير في فرنسا، وقد نص المشرع الفرنسي في قانون المالية الصادر في عام 1984 علي اعتبار الكارت علي قدم المساواة في الدفع مثل الشيك والدفع النقدي[44].

وتعد المعلومات مالا معلوماتيا معنويا، فإن الغالب والمنطقي إذا حدثت سرقة فإنه لا يسرق المال المسجل

---

[41] د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، علي ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، مرجع سابق، تقسيم اعتمده الدكتور علي ضوء الاتفاقية.

[42] د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص67–72.

[43] د. هدي قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،1992، ص124.

[44] د. هدي قشقوش، المرجع السابق، ص127.

عليه المعلومات والبرامج لقيمه المادية – ثمن الشريط أو الأسطوانة– بل يسرق لما هو مسجل عليه، أي ما هو موجود بمحتواه الداخلي، أي البرامج والمعلومات[45].

وهنالك تزوير المستندات المعالجة آليا[46] أيا كان شكلها والتي تؤدي إلي حدوث ضرر للغير (وهنا تصور لوجود مثل هذا الفعل في نظام التقاضي الالكتروني).

كما يتصور وقوع جرائم تمس نظام التقاضي الالكتروني كالاعتداءات التي تقع علي البريد الالكتروني والذي يطلق عليه e–mail(فهو العنوان الالكتروني للشخص)، الذي يعين فيه اسم مستخدم الإنترنت كما ويحدد فيه الشركة المضيفة لهذا العنوان، والذي يتيح لصاحبه تبادل الرسائل الالكترونية، وهنالك العديد من الشركات المضيفة مثل (yahoo) ,hotmail , Gmail والتي تسمح للأفراد بتسجل عناوينهم الالكترونيّة مجانا[47].

إن مزايا البريد الالكتروني أدي إلي شيوع استخدامه بسبب سهولة إرسال الرسائل الالكترونيّة واستقبالها وقلة التكاليف وقصر المدة، مما أدى إلي كثرة الرسائل المقلدة والمزورة وارتكاب الكثير من الجرائم المالية من خلال البريد الالكتروني[48].

وصور الاعتداء علي البريد الالكتروني تتمثل في الجرائم التي تنص عليها قوانين العقوبات مهما اختلفت صورها لكنها تقع عن طريق استخدام البريد الالكتروني، وهنالك طائفة من الجرائم تقع علي البريد الالكتروني مثل تزوير وانتهاك سرية رسائل البريد الالكتروني[49].

وكل هذه الصور من الاعتداءات يمكن تصور وقوعها علي أنظمة تشغيل نظام التقاضي الالكتروني، حيث أنه كلما كان هنالك تطور فإنه يوازيه قوى الشد العكسي كما يقال وتدخلها بالتدمير ونشر الفيروسات والاعتداء علي سرية المعلومات الالكترونيّة وجلسات المحاكمة والبيانات المقدمة وصور اختراق عديدة يمكن لكل مجرم معلوماتي فعلها مهما كانت غايته . لكل ذلك كان لابد من وجود حماية تشريعية لأمن المعلومات وهو ما نوضحه بالمطلب التالي.

المبحث الثاني : الإطار التشريعي للحماية المعلوماتيّة

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات. وتعد المعلومة من أهم ممتلكات الإنسان التي اهتم بها، على مر العصور، فجمعها ودونها

---

[45] د. هدي قشقوش، المرجع السابق، ص62.

[46] د. هدي قشقوش، المرجع السابق، ص139.

[47] د. علي عدنان الفيل، الإجرام الالكتروني، مرجع سابق، ص18.

[48] د. علي عدنان الفيل، الإجرام الالكتروني، المرجع السابق، ص26.

[49] Eileen S. Ross, E–mail stalking: is adequate legal protection Available? J.C. 1;1,1995, p. 909.

د. نافلة عادل محمد فردي، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005، ص 44.

مشار إليها لدى الدكتور خالد ممدوح إبراهيم، مرجع سابق، ص 368.

وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتقلت إلى ورق البردي، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الحاسب الآلي والأقراص الالكترونيّة الممغنطة. لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل الحاسب الآلي على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تنف الانعكاسات السلبية التي أفرزتها هذه التقنية، نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن – تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في بيئة افتراضية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت هذه المخاطر تفاقمًا في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات، مما أفرز نوعًا جديدًا من الجرائم، لم يكن معهودًا من قبل عرفت بجرائم الحاسوب، أو الجرائم المعلوماتية.

المطلب الأول : المواجهة التشريعية لأمن المعلومات في التشريع المصري

تتمثل هذه المواجهة التشريعية في استصدار القوانين التي تُجرم كافة الأعمال التي تمس أو ذات علاقة بأمن المعلومات، والتي قد يتمكن القراصنة والمتطفلون من خلال الأدوات المختلفة للقرصنة من التلصص والاطلاع على المعلومات والبيانات الخاصة بالمحكمة الالكترونيّة والنظام الآلي الخاص بسير الدعاوي الجنائية الالكترونيّة، وتعتبر هذه التشريعات هي الحماية الجنائية التي تفعلها المحكمة الالكترونيّة لحماية بياناتها والمعلومات الموجودة عليها من خلال تجريمها لأي صورة من صور التعدي الذي قد تتعرض له[50]، ومن بين صور التعدي على معلومات والبيانات الحكمة الالكترونية، **ما يلي:**

1. التزوير المعلوماتي: ويقوم الشخص في التزوير المعلوماتي بتغيير وتعديل بعض الحقائق الموجودة في المستندات والأوراق الالكترونية، أو المحررات وسجلات الدعاوي الجنائية الموجودة على الموقع الالكتروني للمحكمة، وهناك العديد من البرامج والتطبيقات التي يتم من خلالها التزوير المعلوماتي.
2. دخول الأشخاص غير المصرح لهم إلى قواعد البيانات الخاصة بالنظام المعلوماتي للمحكمة الالكترونيّة بهدف الاطلاع على بعض المعلومات السرية أو نقل بعض الملفات أو التغيير في بعض المستندات.
3. محاولة الشخص لتدمير البيانات والمعلومات الموجودة على الموقع الالكتروني الخاص بالمحكمة أو النظام الآلي أو أحد أنظمته الفرعية، والتلاعب في البيانات الموجودة على السيرفرات الخاصة بالمحكمة [51].

إلا أنه عند النظر إلى القوانين والتشريعات الخاصة بالدول العربية نجد قصورًا واضحًا في تناول الجرائم الالكترونيّة بصفة عامة وجرائم أمن المعلومات بصفة خاصة، وقد يرجع السبب في ذلك إلى التأخر في وصول

[50] د. أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي: الحماية الجنائية للحاسب الآلي دراسة مقارنة، القاهرة: دار النهضة العربية، ط. 1، 2000، ص 3.

[51] د. صفاء أوتاني: المحكمة الإلكترونيّة (المفهوم والتطبيق)، مرجع سابق، ص 178–179.

التكنولوجيات الحديثة إلى مؤسسات الدولة، وتأخر دخول الإنترنت إلى الكثير من الدول العربية، مما ولد صعوبة لدى المحاكم في الفصل في القضايا الخاصة بالجرائم الالكترونيّة وجرائم الإنترنت، وكذلك تخبط لدى المحامين في إعدادهم للدعاوي الخاصة بهذا الأمر والمرافعات الخاصة بها لأنهم لم يعتادوا على هذه النوعية من الجرائم، على العكس من الدول المتقدمة التي أدركت الأمر سريعًا واستصدرت القوانين والتشريعات الخاصة بحماية المعلومات والأمن المعلوماتي وتُجرم الجرائم الالكترونيّة والمعلوماتية. ولكن في السنوات الأخيرة وبعد انتشار التكنولوجيا في كافة مناحي الحياة والتعاملات اليومية قد قامت بعض الدول العربية باستحداث قوانين خاصة بتكنولوجيا الاتصالات والأمن المعلوماتي والجرائم الالكترونيّة، سواء أكانت هذه القوانين قد صدرت أو قوانين مؤقتة، ومن بين هذه الدول العربية التي أدركت الأمر مبكرًا وبدأت باتخاذ التدابير والإجراءات التشريعية اللازمة للحد من انتشار الجرائم الالكترونية؛ هم مصر والأردن، وسوف استعرض مجموعة من القوانين التي صدرت في هاتين الدولتين والتي تبين مدى اهتمامهم بأمن المعلومات ومحاولتهم المتواصلة في مواكبة التحديثات التي تتم على القوانين والتشريعات في الدول المتقدمة.

من خلال ذلك تم الاطلاع على مجموعة من الإحكام والأنظمة التي تتعلق بمفهوم المواجهة التشريعية لأمن المعلومات في التشريع المصري والي من أبرزها:

1. إن القانون المصري للاتصالات رقم (10) لسنة (2003) في المادة رقم (73) قد نصت على أنه في حالة قيام أي شخص أثناء تأدية عمله بإخفاء أو تغيير أو إعاقة وتحوير لأية رسالة اتصالات أو قد قام عمدًا بامتناعه عن إرسالها سيوقع عليه عقوبة جنائية بالحبس والغرامة، كما تضمن القانون القواعد العامة التي يجب اتباعها في حالة وقوع خطأ أو تحريف في الإبلاغ بالرسالة الالكترونيّة إلى المرسل إليه سواء أكان ذلك بسببه أو بسبب أحد من العاملين أو التابعين له، تحمله المسئولية في حالة انتهاك سرية الأوراق والدعاوي الجنائية الخاصة بالقضية وكذلك المستندات والمراسلات والاتصالات الالكترونيّة التي تتم أثناء عملية سير القضية [52].

2. قد منح المُشرع المصري في قانون التجارة السندات أو المحررات الالكترونيّة التي يتم استصدارها بالطرق الالكترونيّة المختلفة ما بين الفاكس والتليكس والميكروفيلم وأية وسيلة الكترونية أخرى بأن لها نفس الصفة والقوة القانونية الممنوحة للسندات أو المحررات الورقية، إلا أن هناك شرط للاعتراف بهذه السندات الالكترونيّة وهو أن يتم إصدار قرار من وزير العدل يحدد فيه القواعد والضوابط الخاصة بهذه السندات أو المحررات الالكترونيّة وتوافر شرط الاستعجال، وإذا لم يتوافر شرط الاستعجال فلا يكون لهذه السندات أو المحررات الالكترونيّة الحجية القانونية الممنوحة للسندات أو المحررات الورقية [53]. وعرفت المادة (1) من قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنلوجيا المعلومات المصري رقم (15) لسنة 2004 [54].

[52] القاضي . حازم محمد الشرعة: التقاضي الالكتروني والمحاكم الالكترونية، مرجع سابق، ص 40.

[53] عصمت عبد المجيد بكر: مجلة التشريع والقضاء، بغداد: دار الكتب والوثائق، ع (2)، 2013، ص 51.

[54] عصمت عبد المجيد بكر، مرجع سابق، ص51.

3. لقد حرص مجلس أوربا للتصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 والمتعلقة بالإجرام المعلوماتي أو الجرائم المعلوماتية، وذلك إيمانًا من الدول الأعضاء الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمنة والتقارب والعولمة المستمرة للشبكات المعلوماتية.[55]

4. قد وقعت مصر على اتفاقية بودابست[56] لمكافحة جرائم الإنترنت لعام (2001)، والتي تعمل على محاربة وردع الأفعال والتصرفات التي تعتبر ضد خصوصية وسلامة نظم الحاسبات، والشبكات، وبيانات الحاسب فتعمل هذه الاتفاقية على ردع سوء استخدام التكنولوجيا والاتصالات الحديثة، وذلك من خلال تبنيها للسلطات الكافية لمكافحة هذه الجرائم، وقد أدرك المجلس الأوروبي والدول الموقعة على الاتفاقية أن هناك حاجة لتحقيق التوازن بين تطبيق وتنفيذ القانون واحترام الحقوق الأساسية للإنسان من جهة أخرى؛ والذي قد تناولته اتفاقية المجلس الأوروبي لحماية حقوق الإنسان وحرياته الأساسية لعام (1950)، والعهد الدولي للأمم المتحدة الخاص بالحقوق المدنية والسياسية لعام (1966)، وغيرها من الاتفاقيات الخاصة بحقوق الإنسان والتي تؤكد جملاً وتفصيلاً حق أي شخص في حرية الرأي دون تدخل، والحق في الحصول على المعلومات والبحث عنها ونقلها، ولكن مع احترام الخصوصية والحق في حماية البيانات الشخصية كما جاءت في اتفاقية المجلس الأوروبي لعام (1981) والتي تتعلق بالمعالجة الآلية للبيانات الشخصية.فقد غطت اتفاقية بودابست لمكافحة جرائم الإنترنت لعام (2001) ثلاث أشكال من جرائم الكمبيوتر، وهم كالتالي: الجرائم التقنية الاقتصادية، وجرائم الملكية الفكرية الخاصة بالمواد الرقمية والالكترونية، جرائم المحتوى الضار أو غير القانوني.

وصدر بعد انضمام مصر لهذه الاتفاقية عدة قوانين منها قانون الجرائم الالكترونيّة المصري رقم 63 لسنة 2015، ثم قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018[57]، الذي جرم جملة من الأفعال غير المشروعة ونص على عقوبة رادعة تكفل حماية تقنية المعلومات من أي عبث .

فقد خصص المشرع المصري الباب الثالث للجرائم الالكترونيّة والعقوبات المقررة لها وتضمنالفصل الأول– الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، وجريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها، وجريمة الدخول غير المشروع، وجريمة تجاوز حدود الحق في الدخول، وجريمة الاعتراض

---

[55] د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2006، ص 29. .

[56]بتاريخ 20 نيسان 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية – سايبر كرايم CYBERCRIME – (pc–cy) بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الإلكترونيّة – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات واطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الإنترنت لجهة التباحث وإبداء الرأي. وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ومجلس أوروبا ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام.

[57] قانون الجرائم الإلكترونيّة المصري رقم 63 لسنة 2015، ثم قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الجريدة الرسمية العدد (32) مكرر (ج) في 14 أغسطس سنة 2018 .

غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وجريمة الاعتداء على البريد الالكتروني أو المواقع أو الحسابات الخاصة، وجريمة الاعتداء على تصميم موقع، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وجريمة الاعتداء على سلامة الشبكة المعلوماتية، والبرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات.

أما الفصل الثاني فهو عن الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات، وجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الالكتروني، والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الالكتروني.

يعد هذا القانون من أعظم وأفضل ما أنجزه مجلس النواب خلال أدوار الانعقاد الثلاثة الماضية، لأنه جاء في توقيته المناسب، بعدما ازدادت الجرائم الالكترونيّة بشكل بشع، وتعرض المجتمع لأخطار فادحة من مجموعات تخصصت في إيذاء خلق الله، مستغلين الشبكة العنكبوتية في هذا الشأن. ولذلك كان لزامًا على الدولة المصرية أن تواجه كل هذه الأخطار الإجرامية.

المطلب الثاني: المواجهة التشريعية لأمن المعلومات في التشريع الأردني

وفي إطار المواجهة التشريعية لأمن المعلومات في التشريع الأردني فقد اصدر القانون الأردني عام (2010) قانون جرائم أنظمة المعلومات المؤقت رقم (30)، وقد نص هذا القانون على تجريم الأفعال والتصرفات التي تهدف إلى تخريب أو انتهاك نظم ووسائط الشبكات المعلوماتية، فقد فصل قانون جرائم أنظمة المعلومات في الأردن طبيعة الجرائم الالكترونية، وقد حدد لكلاً منها عقوبة تتناسب مع طبيعة هذه الجريمة، ومن بين هذه الجرائم التي وردت في القانون:

1. ورد في المادة (6) من قانون الجرائم المتعلقة ببطاقات الائتمان، والبيانات والمعلومات الخاصة بالمعاملات البنكية والمالية الالكترونيّة لشخصًا ما، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن سنة وغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار.
2. ورد في المواد (3–5) من قانون الجرائم المتعلقة بالدخول إلى أحد المواقع الالكترونيّة دون امتلاك الصلاحية أو الأذن لذلك، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر، أو غرامة لا تقل عن مائة دينار ولا تزيد عن مائتي دينار، ومن قام عن قصد بالتنصت أو قراءة بعض النصوص الالكترونيّة والرسائل والتي ليس له الحق في الوصول إليها وذلك من خلال البرامج الالكترونيّة أو غيرها من الوسائل الالكترونية، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن شهر ولا تزيد عن سنة، أو غرامة لا تقل عن مائتي دينار ولا تزيد عن ألف دينار.
3. ورد في المادة (8) من قانون الجرائم المتعلقة بنشر الأعمال الإباحية أو يشارك فيها أو تتعلق بالاستغلال الجنسي لمن هم أقل من ثمانية عشر عامًا، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن ثلاثة شهور وغرامة لا تقل عن ثلاثمائة دينار ولا تزيد عن خمسة آلاف دينار.

من قام باستخدام الإنترنت في إعداد أو حفظ أو نشر وعرض والترويج لأنشطة وأعمال إباحية بهدف التأثير على من هم دون الثمانية عشر عامًا أو ممن يعانون نفسيًا أو ذهنيًا لكي يقوم بارتكاب جريمة، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن سنتين وغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار.

من قام باستخدام الإنترنت واستغلال من هم دون الثمانية عشر عامًا أو ممن يعانون نفسيًا أو ذهنيًا في أعمال الدعارة أو الإباحية، يُعاقب القانون على هذه الجريمة بالحبس الأشغال الشاقة المؤقتة وغرامة لا تقل عن خمسة آلاف دينار ولا تزيد عن خمسة عشر ألف دينار.

1. ورد في المادة (9) من قانون الجرائم المتعلقة بنشر وترويج أعمال الدعارة، ويُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن ستة أشهر وغرامة لا تقل عن ثلاثمئة دينار ولا تزيد عن خمسة آلاف دينار.
2. ورد في المادة (10) من قانون الجرائم المتعلقة بالأعمال الإرهابية سواء أكان ذلك دعمًا لأعمال الجماعات الإرهابية، والترويج لأفكارهم أو التنظيم للقيام بأعمال إرهابية أو تمويلهم، يُعاقب القانون على هذه الجريمة بالحبس الأشغال الشاقة المؤقتة.
3. ورد في المادة (11) من قانون الجرائم المتعلقة بالدخول إلى المواقع التي تضم وثائق ومستندات أو بيانات ومعلومات تمس الأمن القومي أو العلاقات الخارجية أو السلامة العامة أو اقتصاد الدولة بهدف الاطلاع وليس مصرحًا للجمهور العادي الاطلاع عليها، يُعاقب القانون على هذه الجريمة بالحبس لمدة لا تقل عن أربعة أشهر وغرامة لا تقل عن خمسمائة دينار ولا تزيد عن خمسة ألاف دينار [58].

أما إذا كان هدف الشخص نقل هذه البيانات والمعلومات او تعديل أو تغيير أو تدميرها، يُعاقب القانون على هذه الجريمة بالحبس الأشغال الشاقة المؤقتة وغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار. وحل محل قانون جرائم أنظمة المعلومات المؤقت رقم 3 لسنة2010 قانون الجرائم الالكترونيّة رقم 27 لسنة 2015.[59]

ونص هذا القانون علي مجموعة من الجرائم:

- م3 – الدخول علي الشبكة المعلوماتية أو نظام معلوماتي دون تصريح
- م4 – يعاقب كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع علي بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف

[58] WIPO المنظمة العالمية للملكية الفكرية، الأردن، قانون جرائم أنظمة المعلومات (مؤقت) رقم 30 لعام 2010، 2010، ص. 2–5، تم الاسترداد من:

http://www.wipo.int/edocs/lexdocs/laws/ar/jo/jo063ar.pdf

[59] قانون الجرائم الإلكترونيّة رقم 27 لسنة 2015، المنشور في الجريدة الرسمية عدد رقم 5343 الصفحة 5631 ويعمل به من تاريخ نشره بالجريدة الرسمية (2015/6/1).

أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح.

- م5 – جريمة التقاط أو اعتراض أو التصنت أو إعاقة أو تحوير أو شطب محتويات علي ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات.
- م6 – جريمة من حصل قصدًا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام علي بيانات أو معلومات تتعلق ببطاقة الانتخاب أو البيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية.
- م7 – الجرائم سالفة الذكر إذا وقعت علي نظام معلومات أو موقع الكتروني أو شبكة معلوماتية تتعلق بتحويل أموال أو تقديم خدمات الدفع أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك و الشركات المالية.
- م9 – الجرائم المتعلقة بنشر أو إرسال عن طريق نظام المعلومات أو الشبكة المعلوماتية أعمال إباحية.
- م10– جرائم الترويج للعارة عن طريق استخدام الشبكة المعلوماتية أو نظام المعلومات.
- م11– جرائم الذم والقدح والتحقير عن طريق الشبكة المعلوماتية .
- م12– الجرائم المتعلقة بالأمن الوطني والمعاملات الخارجية أو السلامة العامة أو الاقتصاد الوطني عن طريق الدخول لمعلومات غير مصرح بها.

وقد أحيل من الحكومة لمجلس النواب مشروع القانون المعدل لقانون الجرائم الالكترونيّة وأُدرج علي جدول أعمال الدورة الاستثنائية وذلك بالاستناد للأسباب الموجبة بأن التطور التكنولوجي المتسارع في وسائل الاتصالات وما نجم عنه من اتساع نطاق استخدام الشبكة المعلوماتية سواء في وسائل التواصل الاجتماعي أو تطبيقات برامج الأجهزة الذكية، لمعاقبة كل من يسئ استخدام تلك الوسائل، إلا أنه لم يلق قبولا من الشعب الذي ضغط بدوره علي النواب، ولم يخرج لحيز الوجود حتي بداية عام 2019.

كما أن للحماية المعلوماتية أوجه أخرى غير المنصوص عليها في قانون الجرائم الالكترونيّة رقم 27 لسنة 2015، ومنها ما ورد بنص المادة 158 من قانون أصول المحاكمات الجزائية رقم 9لسنة 1961 وتعديلاته بالقانون رقم 96 لسنة 2018 حيث ورد بالفقرة الثالثة أن الأدوات المستخدمة في التقنية الحديثة من أشرطة وأقراص مدمجة تخضع لإجراءات الحماية المقررة للحفاظ على سريتها وخصوصية الشاهد أو النزيل .

إضافة لما ورد بنظام استعمال الوسائل التقنية الحديثة رقم 96 لسنة 2018م، حيث ذكرت المادة (9/ب) بأن الوزارة تقدم التسهيلات اللازمة لاستخدام وسائل التقنية الحديثة وتتخذ كل ما يلزم لحمايتها وصيانتها وإدامة عملها وحفظ ما تم تسجيله عليها من معلومات .

كذلك ورد في المادة (10/ب) من ذات النظام بخضوع الأدوات المستخدمة لإجراءات الحماية المقررة كما

هو وارد بنص المادة 158 السابق الإشارة اليها .

كما لا يفوتنا أن نذكر، أن قانون المعاملات الالكترونيّة رقم 15 لسنة 2015، ضمن حماية المعلومات الالكترونيّة من خلال نص المادة (4/ب/3) حيث ألزم كل وزارة أو مؤسسة رسمية عامة أو بلدية عند إجراء أي من معاملات الكترونيًا، أن تحدد الأحكام والإجراءات المتعلقة بأمن سجلاتها ومعاملاتها الالكترونيّة وحمايتها وسريتها وسلامتها بموجب تعليمات تصدر لهذه الغاية، إلا أنه فعليًا تم النص في القانون والنظام المختص على هذا الأمر إلا أن هذه النصوص لم تفعل من خلال تعليمات ولوائح وآليات تبين كيفية توفير الحماية والسرية للمعلومات والمعاملات الالكترونية.

وتبدو أهمية إصدار دليل إرشادي تقني وقانوني حول صور جرائم التقنية الحديثة والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية، وضرورة تحديث هذا الدليل الإرشادي وتعميمه على المختصين بهذا المجال[60].

وبهذه الإجراءات نكون قد وضعنا القواعد الأساسية لحماية البيانات وتجريم الأفعال التي تقع على سرية البيانات.

الخاتمة والنتائج والتوصيات

اولا: الخاتمة

شكَّلت خاتمة الدِّراسة حصيلة النتائج التي تمثل الإجابة عن أسئلة الدِّراسة بالإضافة إلى تقديم مجموعة من التوصيات, حيث تناولت الدِّراسة الحماية المعلوماتية للمحاكمة عن بعد, وتناولت الدراسة مفهوم أمن المعلومات ووسائله, وصور الاعتداء على أمن المعلومات والإطار التشريعي للحماية المعلوماتيّة في التشريع المصري والأردني

كذلك بينت الدراسة الضرورة الى وجود نظام قضائي محكم في ظل الانفتاح والانتقال السريع للمعلومة بسبب ثورة التقنية والمعرفة والاتصالات فأصبح موضوع الحماية المعلوماتية للمحاكمة عن بعد ضرورة ملحة لتوفير التقنيات اللازمة لغايات تطبيق المحاكمات عن بعد وتامين المعلومات السرية وذلك من قبل المؤسسات والمحاكم باشراف وزارة العدل بالتنسيق ما بين كافة الشركاء بمن فيهم مراكز الإصلاح والتأهيل ونقابة المحامين حتى تسير الإجراءات بكل امن وسلامة .

كذلك خلصت الدراسة الى أهمية تطبيق كافة إجراءات التقاضي عن طريق المحكمة الالكترونية بوساطة أجهزة الحاسوب المرتبطة بشبكة الانترنت وعبر البريد الالكتروني لغرض سرعة الفصل في الدعاوى و تسهيل إجراءاتها على المتقاضين وهذا يحتاج الى دقة للحفاظ على أمن هذه المعلومات والأجهزة التي تعالجها وتخزينها وتنقلها؛ وتنظيم المنظومة القضائية. وحماية الخدمات الالكترونيّة من التهديدات، لذلك كان لابد من البحث عن

[60] د. محمد محمود عمري، الإثبات الجزائي الالكتروني في الجرائم المعلوماتية، دراسة مقارنة، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الاستراتيجية، العدد 2، سنة 2016، ص 330.

وسائل لضمان أمن المعلومات وحمايتها من منظور قضائي؛ فجميع الإجراءات القانونية التي تتم عبر النظام المعلوماتي لابد من تشديد الحماية عليها منعًا من اختراقها، فهذه المعلومات قد تكون عل درجة بالغة من الخطورة ولذلك يجب حمايتها بكل الوسائل،

كذلك أبرزت الدراسة مجموعة من مظاهر الحماية المعلوماتية والتي تتمثل في تشفير البيانات والمعلومات المتداولة في المحكمة الالكترونية من خلال تحويل المعلومات المقروءة إلى إشارات غير مفهومة, وتأمين خصوصية المعلومات اي عدم استخدام المعلومات في غير الغرض المرخص به من صاحب المعلومة، وتطبيق أساسيات الأمن السيبراني على المحاكمة الالكترونية الذي يشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال مع التطبيقات الخاصة بالحكومة الالكترونية.

ثانيا :نتائج الدراسة

1- أكدت الدراسة على وجود نظام قضائي محكم في ظل الانفتاح والانتقال السريع للمعلومة بسبب ثورة التقنية والمعرفة والاتصالات في الاردن ومصر .
2- بينت الدراسة أهمية موضوع الحماية المعلوماتية للمحاكمة عن بعد لما له من ضرورة ملحة لتوفير التقنيات اللازمة لغايات تطبيق المحاكمات عن بعد وتامين المعلومات السرية وذلك من قبل المؤسسات والمحاكم
3- أكدت الدراسة على ضرورة تعزيز الإجراءات القانونية التي تتم عبر النظام المعلوماتي وتشديد الحماية عليها منعًا من اختراقها، لما لهذه المعلومات من اهمية بالغة من الخطورة ولذلك يجب حمايتها بكل الوسائل،
4- بينت الدراسة أهمية تشفير البيانات والمعلومات المتداولة في المحكمة الالكترونية وذلك من خلال تحويل المعلومات المقروءة إلى إشارات غير مفهومة,وتأمين خصوصية المعلومات اي عدم استخدام المعلومات في غير الغرض المرخص به من صاحب المعلومة
5- التأكيد على إصدار تعليمات ولوائح وآليات تبين كيفية توفير الحماية والسرية للمعلومات والمعاملات الالكترونية من خلال الأحكام والإجراءات المتعلقة بأمن سجلاتها ومعاملاتها الالكترونيّة وحمايتها وسريتها وسلامتها بموجب تعليمات تصدر لهذه الغاية

ثالثا : التوصيات : أوصت الدراسة بناء على نتائجها على ما يلي :

1- أوصت الدراسة بأن على القائمين بالسلك القضائي ضرورة وجود نظام قضائي محكم في كل من الأردن ومصر وخاصة في ظل الانفتاح والانتقال السريع للمعلومة بسبب ثورة التقنية والمعرفة والاتصالات في العالم.
2- من الضروري للحفاظ على سرية المعلومة لا بد من تشفير البيانات والمعلومات المتداولة في المحكمة الالكترونية وذلك من خلال تحويل المعلومات المقروءة إلى إشارات غير مفهومة,وتأمين خصوصيات المعلومات والبيانات بكل سلامة وسرية .

3- من الضروري وجود دليل إرشادي تقني وقانوني حول صور جرائم التقنية الحديثة والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية، وضرورة تحديث هذا الدليل الإرشادي وتعميمه على المختصين بهذا المجال

4- اوصت الدراسة على ضرورة إصدار تعليمات ولوائح وآليات تبين كيفية توفير الحماية والسرية للمعلومات والمعاملات الالكترونية من خلال الأحكام والإجراءات المتعلقة بأمن سجلاتها ومعاملاتها الالكترونيّة وحمايتها وسريتها وسلامتها بموجب تعليمات تصدر لهذه الغاية

5- أوصت الدراسة على ضرورة تعزيز الإجراءات القانونية التي تتم عبر النظام المعلوماتي وتشديد الحماية عليها منعًا من اختراقها، لما لهذه المعلومات من اهمية بالغة من الخطورة ولذلك يجب حمايتها بكل الوسائل،

المراجع

اولا: المراجع العربية

أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي: الحماية الجنائية للحاسب الآلي دراسة مقارنة، القاهرة: دار النهضة العربية، ط. 1، 2000،

أكرم فاضل سعيد، حماية قواعد البيانات من مخاطر التنازل عنها والمنافسة غير المشروعة الواقعة عليها، جامعة النهرين، كلية الحقوق قسم القانون الخاص، 2014.

أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة " في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2015.

جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 2002.

جميل عبد الباقي الصغير، الحماية الجنائية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية، 1999.

حاتم عبد الرحمن منصور الشحات، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 2002.

حسن طاهر داود، الحاسب وامن المعلومات، مركز الدراسات و البحوث، المملكة العربية السعودية، 2000م.

الحياري , إيمان(2016). أمن وحماية المعلومات, موقع موضوع ,2, اذار , الاردن.

دعدوع , شهيرة (2016). مفهوم أمن المعلومات, موقع موضوع ,23, اب , الاردن.

رامي نعمان الجاغوب، "أمن وسرية المعلومات في الحكومة الإلكترونيّة "، ندوة متطلبات الحكومة الالكترونية، الإمارات، وزارة الداخلية، 2002.

صالح بن علي بن عبدالرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، المملكة العربية السعودية، هيئة الاتصالات وتقنية المعلومات، رؤية 2030.

صفاء أوتاني – المحكمة الإلكترونية(المفهوم والتطبيق) – بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية

والقانونية – المجلد 28 – العدد الأول، 2012.

عبد الصبور عبد القوي علي مصري، دار العلوم للنشر والتوزيع، أحد فروع مجموعة العلوم ثقافية.

عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، حقوق الطبع محفوظة للمؤلف، 2009.

عصمت عبد المجيد بكر: مجلة التشريع والقضاء، بغداد: دار الكتب والوثائق، ع (2)، 2013.

عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشأة المعارف، الإسكندرية.

علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، بدون تاريخ.

علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، منشورات زين الحقوقية، 2011.

عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية،1995..

عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، دار النهضة العربية، القاهرة، 2004،

غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، 2010.

القاضي . حاتم جعفر، دور التقاضي الإلكتروني في دعم وتطوير العدالة " قراءة في الواقع الحالي والنتائج المتوقعة " مؤتمر المناخ القضائي الداعم للاستثمار، الإسكندرية فبراير 2015.

قانون الجرائم الإلكترونيّة المصري رقم 63 لسنة 2015، ثم قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الجريدة الرسمية العدد (32) مكرر (ج) في 14 أغسطس سنة 2018 .

قانون الجرائم الإلكترونيّة رقم 27 لسنة 2015، المنشور في الجريدة الرسمية عدد رقم 5343 الصفحة 5631 ويعمل به من تاريخ نشره بالجريدة الرسمية (2015/6/1).

الكرعاوي، نصيف جاسم محمد , الكعبي، هادي حسين عبد علي (2016). مفهوم التقاضي عن بعد و مستلزماته, مجلة المحقق الحلي للعلوم القانونية و السياسية, جامعة بابل كلية القانون المجلد 8، العدد 1, 31 . اذار , العراق.

محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2006.

محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ،2004،،

محمد محمود عمري، الإثبات الجزائي الالكتروني في الجرائم المعلوماتية، دراسة مقارنة، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الاستراتيجية، العدد 2، سنة 2016.

مدحت رمضان، جرائم الاعتداء علي الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.

مدحت رمضان، جرائم الاعتداء علي الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.

مشار إليه في كتاب د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت.

المنظمة العالمية للملكية الفكرية، الأردن، قانون جرائم أنظمة المعلومات (مؤقت) رقم 30 لعام 2010، 2010،

منير محمد الجنبيهي ،د. ممدوح محمد الجنبيهي، جرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2004.

نافلة عادل محمد فردي، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005.

نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف بالإسكندرية، 2008.

هدي قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،1992.

هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، علي ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، النهضة العربية، القاهرة، 2000،.

هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، علي ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، مرجع سابق، تقسيم اعتمده الدكتور علي ضوء الاتفاقية.

هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2006، ص 29.

.

هيثم محمد الزعبي السامرائي، د. إيمان فاضل، نظم المعلومات الإدارية، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، 2004.

ثانيا :المراجع الاجتبية

Eileen S. Ross, E-mail stalking: is adequate legal protection Available? J.C. 1;1,1995, p. 909.

GOLIARD (F), Télécommunication et règlementation françaises du cryptage, d. 1988, Chron., p.120.

OP. Cit., N 410, P. 236.DARAGON (E.)

Edward M. wise, Computer Crimes and Other Crimes against Information Technology in the United States, Rev.int. dr. pen-1993, P657.

Les problèmes posés par la législation française en matière de chiffrement by Maitre ValerieSedallian, Droit de l'Informatique et des télécoms 98/4 (10/98).

Martin Wasik, Computer Crime. Ibid.1991, p.41.

Michael Alexander, Computer Crime, Ugly secret for business, Computer world, Vol. xxiv, No.11, 1990, pp.104.

SieberUlerich, The interval oval Emergence of criminal information law, Carl Heymans. Verlag K.G., 1992. P.P 327.http://www.wipo.int/edocs/lexdocs/laws/ar/jo/jo063ar.pdf

numériques, disponible a l'adresse : http://www.lex-electronica.org/articles/v6-1/thoumyre.htm, N 35.P.7.-

THOUMYRE (Lionel), Responsabilités sur le web: une histoire de la ré-glementation des réseaux