الجريمة الإلكترونية: تفعيل لآليات القانون من أجل تحقيق العدالة

Cybercrime: activating the mechanisms of law in order to achieve justice

سعاد طعبة

جامعة الجلفة (الجزائر)، toabaso@yahoo.fr

تاريخ الاستلام: 2022/08/06 تاريخ القبول: 2022/09/25 تاريخ النشر: 2022/10/08

ملخص:

مع دخول الحاسوب و الانترنت إلى مجتمعاتنا، وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم الالكترونية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم و التوعية بها ومتابعة هذا النوع من الجرائم وسن القوانين والتشريعات اللازمة لمكافحة الجرائم الإلكترونية نظراً لما تسببه من خسائر مادية ومعنوية كبيرة. حيث تعتبر الجرائم الإلكترونية من الأشكال الحديثة للإجرام، نظرا لارتباطها بالتطورات التقنية التي يعرفها العالم، والتي قوامها تكنولوجيا المعلومات والاتصالات، لذا كان لزاما أن يتصدى القانون ويضع القواعد الملائمة للاستفادة منها،حتى تحفظ الحقوق بأنواعها من كل اعتداء محتمل، لذلك كان من الواجب سن القوانين و القواعد التي تجرم كل فعل يهدف إلى المساس بالآخرين، وهذا يتطلب تدخل القضاء لتوسيع نطاق النص الجنائي ليعاقب هذا النوع من الجرائم.

كلمات مفتاحية: الجريمة الالكترونية، القانون، القضاء

Abstract:

With the entry of computers and the Internet into our societies, and in all aspects of our lives, a new type of crime called cybercrime has begun to appear, and therefore there is a need to define these crimes, raise awareness and follow up on this type of crime, and enact laws and legislation necessary to combat cybercrime due to the great material and moral losses it causes. Where cybercrime is considered one of the modern forms of crime Therefore, it was necessary to confront the law and set appropriate rules to benefit from them, in order to preserve the rights of all kinds from every possible assault. Therefore, it was necessary to enact laws and rules that criminalize every act aimed at harming others, and this requires the intervention of the judiciary to expand the scope of the criminal text to punish this type of offense crimes.

Keywords: Cyber crime, law, justice

1- مقدمة

مع تطور الانترنت وتوسع استخداماته وازدياد أعداد المستخدمين لها في العالم (حوالي 1.6 مليار مستخدم يمثلون ربع سكان العالم) أصبح الانترنت وسطاً ملائماً للتخطيط ولتنفيذ عدد من الجرائم بعيداً عن رقابة وأعين الجهات الأمنية. إذ أصبحت الجريمة الالكترونية تستخدم الوسائط الحاسوبية والشبكات وشبكات الإنترنت لارتكاب جريمة أو التخطيط لها .

حيث ساهمت التكنولوجيا منذ نشأتها بتغيير الكثير من المفاهيم التي اعتاد الناس عليها، وتباينت هذه التغييرات بين السلبية والإيجابية. ففي الوقت الذي قامت فيه التكنولوجيا على سبيل المثال بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية (Hackers Internet)، ويقومون من خلالها باقتحام خصوصية الفرد رغما عنه حيث تتنوع نشاطات أولئك القراصنة، ويقابل ذلك التنوع بنشاطات القراصنة تنوعا آخر بمدى الضرر الذي يستطيعون إلحاقه بالمستخدم، حسب النشاط الذي يقومون باستخدامه. في كثير من الأحيان تمكن المعلومات التي يحصل قراصنة الشبكة العنكبوتية عليها من القيام بعمليات احتيال باسم الضحية، كالقيام بالبيع أو الشراء أو طلب قروض مصرفية وغير ذلك من الأمور.

لقد سهلت الشبكة العنكبوتية على القراصنة مسألة سرقة الهوية من خلال توفيرها للكثير من الطرق التي تساهم بإنجاح أهدافهم بشكل كبير. فعلى سبيل المثال، تعتبر غرف الدردشة مرتعا خصبا لتنفيذ هذا النوع من السرقات، حيث يقوم القراصنة بتصميم برامج فايروسية تسمى أحصنة طروادة (Horses Trojan)،)التي تستطيع من خلال دخولها على أحد أجهزة الحاسوب، أن تتجسس على صاحبه للحصول على معلومات معينة مثل كلمات المرور التي يستخدمها، لتقوم هذه الأحصنة بعد ذلك بإعادة هذه المعلومات للقرصان، و في هذا المقال سوف يكون لنا إسهاب حول الجريمة الالكترونية ونظرة القوانين العربية منها ودور القضاء العربي .

2.تعريف الجريمة الإلكترونية:

تعرف بأنها الجرائم التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دوراً رئيسيا. فهذه الجرائم تمس برامج الكومبيوتر أو تحلل معلومات غير مصرح بها. [1]

و ذهب (Rosenblatt) بتعريفه الى هذا النوع من الجرائم على أنها نشاط غير مشروع ينصب على المعلومات المخزنة داخل الحاسوب وتغييرها وحذفها والسلوك هنا ذو طبيعة ذهنية .

فهي كل فعل او نشاط ايجابي أو سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي أو بنظام المعلومات العالمية الانترنت أو الإبقاء عليه عند تحققه أو التأثير عليه بأي وسيلة كانت.

[1]- عبد العال الدريني، **الجريمة المعلوماتية (دراسة مقارنة)**، ط1، دار، النهضة العربية، 2000، (ص14).

ويتفق (Parker)الأمريكي مع الفرنسيين (Lestance) و(Virant) بالاتجاه وضرورة بالتوسع في موضوع الجريمة فهي عندهم : (كل فعل اجرامي متعمداً أيا كانت صلته بالمعلوماتية والتي يمكن ان تكون جديرة بالعقاب) .[1]

و من أهم الانتقادات الموجهة لمعيار السلوك المادي أو موضوع الجريمة هو انه غير دقيق حيث يكون التأثير على المعلومات وإتلافها وإعاقة الأنظمة عن أداء وظائفها قد تتم بواسطة أشخاص مصرح أو غير مصرح لهم بالدخول إلى النظام المعلوماتي.

لذلك اتجه فريق آخر لتحديد مفهوم الجريمة الالكترونية بمعيار الوسيلة أو أداة الجريمة فيصفها بأنها :

سلوك أجرامي يتم بمساعدة الحاسب الآلي ، وتتفق الدكتورة فائزة بابا خان مع هذا المفهوم الواسع للجريمة المعلوماتية وترى بأنها :الفعل الجديد الذي يمارس باستخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال أو أحد ملحقاتها في تنفيذ أعراض مشبوهة.

وهذا التعريف الذي أخذت به أو تبنته وزارة العدل الأمريكية في تقريرها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاث[2].

وهناك من يذهب ويوسع أكثر في مفهوم هذه الجرائم منطلقاً من الصفة العالمية للجريمة فهي (جرائم العولمة الحديثة التي انتشرت مع الهوس المجتمعي العريض بالأنترنت والوسائط الحديثة مع تطور الأجهزة لتشكل تحول الحداثة المخيف).

ومما يؤخذ على هذا المعيار توسعه الكبير لمفهوم الجريمة فمن شأنه أن يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك فقد لا يعد ان يكون الحاسب الآلي محلا تقليديا في النشاط الإجرامي. وبعد أن وسع معيار الوسيلة من مفهوم هذه الجرائم اعتمد البعض من الفقهاء معيار (النتيجة) التي تتركها الجريمة لغرض تضييق والحد من نطاق الجريمة الالكترونية.

فيرى الأستاذ (Sheldon) بان هذه الجرائم هي عبارة عن اعتدل علت قانونية ترتكب بواسطة المعلوماتية عرضها الأساسي تحقيق الربح المتمثل بالمال فهذا التعريف ركز على النتيجة وهي تحقيق المال إضافة الى معيار الوسيلة.

فالهدف من العبث ببرامج الكومبيوتر وإعاقة استخدامها هو ارتكاب جريمة أخرى أو بث فيروس من شأنه التأثير على أدائه.[3]

---

[1] -Donne Parker, **cyber crime and general prin aples** ,Cyber crime andreal world by layi the Sridhar, 19 august2008 , (p18).

[2] –كوثر حازم سلطان، **موقف القانون و القضاء من الجريمة الالكترونية(السيبرانية)**،مجلة كلية التربية الأساسية، المجلد 22، العدد 96، 2016، (ص971).

[3] – محمد علي قطب، **الجرائم المعلوماتية**، بحث مقدم الى مركز الاعلام الامني، الأردن،2008، (ص12).

وهذا المفهوم الضيق أخذ به ايضاً (Tredmann)لأنها جرائم بداية ضد المال مرتبطة بالمعالجة الآلية للمعلومات. والمال هنا ينصرف مفهومه طبعاً الى الأموال المادية و المعنوية فالاعتداء أو الامتناع العمدي ينشأ عن استخدام غير المشروط للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية .

وقد يكون هدف الجريمة الإساءة لسمعة الضحية أو لجسدها أو عقليتها فهي (اية مخالفة ترتكب ضد افراد او جماعات بدافع جرمي ونية الإساءة لسمعة الضحية وعقليتها سواء كان ذلك بطريقة مباشرة أو غير مباشرة باستخدام وسائل الاتصالات الحديثة مثل الانترنت .

ومن كل هذا نستنتج أن الجريمة الإلكترونية او السيبرانية هي فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادية أو المعنوية أو الاعتداء على خصوصية للأفراد، أو هي عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، من جهة أخرى هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القدف عبر الإنترنت .

3. أسباب ارتكاب الجريمة الإلكترونية:

إن أسباب انتشار الإجرام المعلوماتي تتأثر بلا شك بالثورة المعلوماتية، وإذا كانت الأنماط المختلفة للمجرمين المعلوماتيين تكشف لنا عن اشتراك هؤلاء عند ارتكابهم الجريمة المعلوماتية في غرض واحد؛ هو مجرد الهواية واللهو في بداية الأمر، وذلك نتيجة انبهارهم بالثورة المعلوماتية والحاسبات الآلية، فمن ناحية أخرى قد يكون رغبة هؤلاء المجرمين في تحقيق الثراء السريع يمثل أيضاً أحد أسباب انتشار الإجرام الالكتروني، وأخيراً قد تكون الأسباب الشخصية بالمجرمين هي أحد أسباب ذلك .

وعليه يمكن تلخيص أسباب انتشار الجريمة الالكترونية فيما يلي :

1.3. الولع بجمع المعلومات: هناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد من المعلومات، فيرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألا يكون عليه أي قيد؛ فالقرصان يكرس كل جهده في تعلم كيفية اختراق المواقع المحمية، وغالباً ما يكون القراصنة مجموعات الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار.

2.3.تحقيق مكاسب مالية: قد تدفع حاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة لمن يطلبها .

3.3. الدوافع الشخصية: يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توافر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى ارتكابه لجريمة معلوماتية، هذا و تتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك ،سواء كان بدافع اللهو أو الانتقام.[1]

4. خصائص الجريمة الالكترونية:

[1] – محمد أمين الرومي،**جرائم الكمبيوتر و الانترنت**، دار المطبوعات الجامعية، الاسكندرية، 2004، (ص24).

أصبحت تقنية المعلومات من أساسيات الحياة في عصرنا الحالي رغم استغلال البعض لهذه التقنية لغايات غير مشروعة وذلك إلى خطورة من هذا النوع من الجرائم لان الجانب التنظيمي يشملها بصورة متكاملة لتعدد صورها والتجدد فيها وتميزها عن غيرها من الجرائم التقليدية ومن بين خصائص الجريمة الالكترونية:[1]

- الجريمة الالكترونية (عابرة للحدود) حيث ان القدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مفادها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية.
- الجريمة الالكترونية جريمة ناعمة لا تتطلب قدرات عنيفة لارتكابها كتبادل اطلاق النار أو سفك دماء كذلك لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقية ما يقوم به او بمساسه بمصالح أو قيم يحره المجتمع على حمايتها ولا يعتبر ما يقوم به يدخل في عداد الجرائم .
- الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم السيبراني فقد يوجد الجاني في بلد ما ويستطيع الدخول الى ذاكرة الحاسب الآلي الموجود في بلد آخر. ذلك يظهر اكثر في البرامج الخبيثة (Viruses) حيث يتم نسخها في بلد وترسل إلى دول مختلفة من العالم.
- عولمة الجريمة السيرانية تثير مشاكل حول القانون الواجب التطبيق.
- جريمة متطورة لا يمكن حصر أساليبها في الوقت الحاضر وان امكن حصرها الا أنه لا يمكن التنبوء بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا ويؤدي ذلك الى اختلاف محل الجريمة بحسب الزاوية التي ينظر اليها والدور الذي يلعبه هذا الحاسب ذاته فهو لا يعد ان يكون دور الضحية او دور المحيط أو البيئة التي ترتكب فيها.
- التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالانترنت عند الاثر المادي وانما يتعدى ذلك ليهدد نظام القيم والنظام خاصة في المجتمعات المحافظة والمغلقة.
- جاذبية الجريمة السبرانية : نظرا لما تمثله سوق الكومبيوتر من ثروة كبيرة فقد غدت اكثر جاذبية باستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات واساليب تمكن الدخول إلى الشبكات و سرقة المعلومات.
- تعدد دوافع الجريمة السيبرانية فقد تكون سببها مجرد سداد الديون او آدمان لعب القمار أو المخدرات أو بيع المعلومات المختلسة او مجرد الدخول وجمع معلومات دون قيود كما أشار الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة(Hackers) .
- صعوبة اكتشافها وإمكانية إثباتها لسبب عدم تخلفها لآثار ظاهرة خارجية فهي تنصب على البيانات والمعلومات المخزنة .
- الوصول إليها واكتشاف حقيقتها تتطلب الاستعانة بخبرة فنية عالية المستوى.

[1] – خالد ممدوح ابرهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، ط2009،1،(ص88).

- امتناع المجني عليهم عن المطالبة بالتعويض أو حتى التبليغ عنها خوفا من الفضيحة أو بسبب عدم علمهم بها الا عندما تكون انظمتهم المعلوماتية هدفا لفعل الغش .

5. موقف القوانين من الجريمة الالكترونية :

في دراسة أجريت من قبل مكتب التحقيقات الفيدرالية عام 2003 تبين بأن أكثر خسائر المؤسسات بالولايات المتحدة الأمريكية أتى من الاستيلاء عن المعلومات والتي قدرت خلال هذا العام خسائر تتعدى 70 مليون دولار أمريكي وفي المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز 65.5 مليون دولار وعند ارتفاع ارقام الجريمة المرتكبة بواسطة هذه التقنيات الأمر الذي دعا رجال القانون على الصعيد الدولي والوطني إلى البحث عن تعديل نصوص قانون العقوبات لمواجهة هذا الأمر بشتى أنواعها او الحاجة الملحة لاستحداث قوانين خاصة باعتبارها جرائم ذات طبيعة خاصة.

1.5.موقف القوانين و المنظمات الدولية:

نظراً للتطور السريع لتقنيات الإعلام والاتصال وتنوع شبكات الربط وتوسيع ميادين استعمال هذه التقنيات ثقافياً واقتصادياً وإدارياً استغل البعض هذه التقنية لغايات غير مشروعة مما دفع العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التي تهدد كل مستخدمي الانترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجرائم.

1.1.5. الجريمة الالكترونية في التشريعات المقارنة:

على صعيد التشريعات المقارنة فتعتبر **السويد** أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت حيث صدر قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها.

اتبعت **الولايات المتحدة الأمريكية** قانون السويد حيث شرعت قانوناً خاصاً بحماية أنظمة الحاسوب عام(1976) وفي عام 1985 حدد معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي: (جرائم الحاسب الآلي الداخلية / جرائم الاستخدام غير المشروع عن بعد / جرائم التلاعب بالحساب الآلي / دعم التعاملات الإجرامية وسرقة البرامج الجاهزة والمكونات المادية للحاسب).

أما القانون رقم 1213 لسنة 1985 فقد عرف جميع المصطلحات الضرورية لتطبيق القانون عن الجرائم المعلوماتية ووضعت المتطلبات الدستورية اللازمة لتطبيقه وقامت الولايات الداخلية بإصدار تشريعاتها خاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية (تكساس) لجرائم الحاسب الآلي.[1]

واعتبر **قانون كاليفورنيا** عام 1985 مرتكب جنحة كل من دخل عمدا إلى منظومة أو شبكة حواسيب عمدا.

[1] –كوثر حازم سلطان ، مرجع سابق، (ص977).

أما ثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي فهي **بريطانيا** حيث أقرت قانون مكافحة التزوير والتزييف عام 1981 الذي شمل في تعاريفه الخاصة أداة التزوير (وسائط التخزين الحاسوبية المتنوعة و أي أداة أخرى يتم التسجيل عليها بالطرق التقليدية أو الالكترونية.

ونهج **القانون السويسري** نهج القانون الأمريكي فأصدر قانون (غش وإساءة استخدام الحاسوب لسنة 1984) وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت عام 1985 القانون الجنائي ليشمل هذه الجرائم وتحديد عقوبات لتدمير أنظمة الحاسوب كما جاء بالمادة 387 خاصة إذ كانت عن عمد.

و عاقب **المشرع الالماني** في المادة (303) من قانون العقوبات المعدلة قانون الثاني لمكافحة الجريمة الاقتصادية لعام 1986 كل من (محا او أبطل وجعل غير نافع او احدث تغيير في البيانات بصورة غير مشروعة) بالحبس لمدة لا تزيد على عامين أو الغرامة وشدد العقوبة لتصل إلى خمس سنوات أو الغرامة هذه الأفعال على بيانات بموجب السلطات الإدارية .

كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

وكانت **فرنسا** من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت عام 1988 القانون رقم (88-19) الذي أضاف إلى قانونها العقابي جرائم الحاسب الآلي مثال ذلك أضاف فقرتين (6-5) للمادة (462) القانون الجنائي الفرنسي لعام 1988 التي حرمت وحرم المشرع الفرنسي بالقانون لسنة 1994 المعدل بالقانون 1998 مجرد التواصل مع نظام الحاسوب البقاء معه تزوير المستندات المعالجة .

في حين سوى المشرع الفرنسي بين الكتب الالكترونية و الكتب الخطية بالقانون رقم 13/3/2000، وذهب القانون الفرنسي ابعد من ذلك حيث تم إعداد مكتب مركزي لمكافحة الجرائم المرتبطة بالمعلومات في وزارة الداخلية لتفتيش وضبط المستندات الالكترونية .وحرم المشرع الفرنسي بالقانون لسنة 1994 المعدل بالقانون لسنة 1998 مجرد التوصل لنظام الحاسوب البقاء معه .

وذهب القانون **الهولندي والفنلندي** لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي متى ما كانت هناك جريمة وهو اتجاه القانون البلجيكي المرقم 23 لسنة 2000 في مادته (88).[1]

2.1.5. الجريمة الالكترونية على مستوى المنظمات الدولية:

فقد لعبت **الأمم المتحدة** دوراً كبيراً في هذا المجال من خلال متابعتها و إشرافها وحتى عقد المؤتمرات الدولية الخاصة بمنع الجرائم من هذا النوع فمنذ عام 1968 شهد مؤتمر الأمم المتحدة لحقوق الإنسان طرح موضوع مخاطر التكنولوجيا الحق في الخصوصية ثم المؤتمر السابع المنعقد في ميلانو عام 1985 كلف لجنة. الخبراء العشرين بدراسة موضوع حماية نظام المعالجة الآلية والاعتداء عن الحاسوب .أما المؤتمر الثامن المنعقد في هافانا 1990 والتي من أهم توصياته التأكيد على

[1] -نفس المرجع، (ص 978).

ضرورة والاستفادة من التطورات العليمة والتكنولوجيا في مواجهة الجريمة المعلوماتية وتحديث ونصت اتفاقية (Trips) لعام 1994 المتعلقة بحماية المعلومات القوانين وقد عقدت هذه اتفاقية الأمم المتحدة سنة 2001 لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) المؤرخة في 12/4/2000، عرفت الهاكر أو المخترق بأنه (**المبرمج المتفوق جدا ولكنه يستخدم جل طاقاته في الاتجاه الغير شرعي لمحاولة اختراق أنظمة حاسوبية لعرض اثبات قدرته أو التباهي أو أحيانا لأهداف إجرامية**)".[1]

أما اتفاقية بودابست[2] لعام 2001 فقد قسمت مادتها الجرائم الالكترونية إلى أربعة أقسام :

أ- جرائم تستهدف عناصر السرية والسلامة مثل الدخول الغير القانوني (تدمير -المعطيات).

ب- الجرائم المرتبطة بالكومبيوتر مثل (التزوير المرتبط بالكومبيوتر، الاحتيال المرتبط بالكومبيوتر).

ت- الجرائم المرتبطة بالمحتوى (الجرائم المتعلقة بالأفعال الإباحية اللاأخلاقية).

ث- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات).

وقد عمدت دول الاتحاد الأوربي على تأسيس جهاز الاوردجست (Eurojust) يعمل على المستوى الأوربي الاوروبول في مجال مكافحة جميع الجرائم ، تم إنشاءه عام 2002 يمارس اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد أو دولة عضو مع دولة أخرى واتخذ من لاهاي مقراً له، أما أنشطته فتتمركز حول معالجة المعلومات المرتبطة بالأنشطة الإجرامية.

أما على مستوى **جامعة الدول العربية** فقد اعتمدت القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات في دورته التاسعة عشر بالقرار رقم 495 لسنة 2003 وقد تضمن المادة (27) منه معالجة الجرائم المعلوماتية.

2.5.موقف القوانين العربية من الجريمة الالكترونية:

نالت الجريمة الالكترونية قسطا كبيرا من الاهتمام من قبل المشرعين العرب ، فمنهم من يفرد لها نصوص خاصة من خلال تعديل القوانين الجنائية وآخرين أدركوا خطورة هذه الجرائم فخصص لها قانون مستقل بذاته، وفي هذا الصدد نبين ذلك من خلال القوانين التالية :

1.2.5. القانون الجزائري:

استخدم المشرع الجزائري مصطلح المساس بنظم المعالجة الآلية للمعطيات وذلك بالقانون رقم (4/15) في 10/نوفمبر/2004 وينصرف هذا المصطلح إلى المعلومات و النظام الذي يحتوي عليها بما في ذلك شبكات المعلومات فقد عمد المشرع في السادة) من القانون أعلاه إلى حماية سرية وسلامة المعلومات وعاقب بالحبس كل من يدخل عن طريق الغش المتعمد للمعالجة الآلية. وفي المادة (15) من القانون حددت بأن تكون المحاكم الجزائية مختصة بالنظر في الجرائم

[1]-هلالي عبد الله أحمد، **الجوانب الاجرائية و الموضوعية لجرائم المعلوماتية في ضوء اتفاقية بودابست**، دار النهضة العربية، القاهرة، 2003، (ص ص 8/7).

[2] - وقعت اتفاقية بودباست (26) دولة أعضاء و قد انضمت أربعة دول غير أعضاء وهي (كندا-اليابان-الولايات المتحدة-جنوب افريقيا).

المتعلقة بتكنولوجيا الإعلام المرتكبة خارج الوطن عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية (4) وهنا المشرع الجزائري قد أكد المادة (586) من قانون العقوبات الجزائري الذي نص على (تعد الجريمة مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال احد أركانها قد تم في الجزائر).

فقد عالج الأمر: 97-10 المتعلق بحماية حق المؤلف والحقوق المجاورة الملغي بالأمر 03-05 مسألة التعدي على المصنفات المعلوماتية إذ أدرج هذه الأخيرة بموجب المادة 4/1 ضمن المصنفات المحمية قانوناً.[1]

ثم صدر القانون 15-04 المؤرخ في: 10-11-2004 المعدل والمتمم لقانون العقوبات ، أدرج فيه المشرع قسماً كاملاً متعلقاً بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما صدر قانوناً يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نص على أحكام إجرائية تتعلق بكيفيات التحقيق في هذه الجرائم، وأدرج عقوبات تسلط على كل من يعرقل حسن سير التحقيقات القضائية في هذا المجال.[2]

2.2.5.القانون التونسي :

كان المشرع التونسي من السباقين وبادر بوضع إطار قانوني للمتدخلين في المجال الالكتروني عن طريق أحكام متفرقة منها القانون رقم 42 لسنة 1993 الذي نص على أن الاتفاق يعتبر ثابت سواء وقع من الأطراف أو بتبادل رسائل أو برقيات وغيرها من وسائل الاتصال فهذا اقترافاً صريحاً بهذه الطرق كوسيلة من وسائل الإثبات.

بعد الألفية الثانية بدأ إدراك أهمية الموضوع بتزايد مما حث المشرع التونسي إلى سن قانون خاص بالتجارة الالكترونية فعاقب كل من استغل ضعف أو جهل شخص في إطار عمليات البيع الالكتروني بغرامة تتراوح 2000 دينار.

ومواكبة للتطور أصدر المشرع أيضا القانون عدد 57 لسنة 2000 الذي اعترف به المشرع بالوثيقة الالكترونية كحجة رسمية متى ما تم تدعيم الوثيقة الالكترونية بإمضاء الكتروني.

ثم القانون رقم 101 لسنة 2002 والمتعلق بقانون المالية لسنة 2003 المتعلق بإيداع التصاريح والقائمات والكشوفات على حوامل ممغنطة.[3]

3.2.5. القانون المغربي :

أقدم المشرع المغربي منذ التسعين من القرن الماضي الى سن قوانين خاصة لمحاربة الجريمة المعلوماتية والانخراط في معاهدات دولية لتعزيز التعاون الدولي في هذا المجال .

---

[1] – القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004.

[2] – القانون رقم: 09-04) المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخة في 16غشت.

[3] – لطفي بن كريم، **التجربة التونسية في مجال المعاملات المدنية و التجارية الالكترونية** ،منتديات ستار تايمز2012/02/26،(ص9)،

فبالإضافة إلى القانون رقم 24096 لعام 1996 المتعلق بالبريد والمواصلات، وخاصة ما يتعلق منها بمخالفات المساس بالاتصالات السلكية واللاسلكية والقانون رقم 703 لعام 2003 (الفصل 3-6-7) من القانون الجنائي المتعلق بجرائم الإخلال بسير نظم المعالجة الآلية للمعطيات، أو ما يسمى بالقانون الجنائي المعلوماتي لان الأفعال التي جرمها كانت تنصب على البيانات أو المعطيات بشكل أساسي.

أما الفقرة 7 من القانون رقم 3-3 المتعلق بمكافحة الإرهاب فأنها أدرجت الجرائم المتعلقة باختراق نظم المعالجة الآلية للمعطيات ضمن لائحة الجرائم الإرهابية.

- وسمح المشرع المغربي في قانون المسطرة الجنائية بالتقاط المكالمات الهاتفية والاتصالات، إضافة لذلك فقد جرم العمليات الجمركية الناتجة عبر إدخال بيانات مزورة في النظام المعلوماتي للجمارك بالمادة 281 من قانون الجمارك لسنة 2000، حيث نصت على: (كل عمل او محاولة تعتبر تنجز بطرق معلوماتية أو الكترونية ترمي إلى إتلاف واحد أو أكثر من المعلومات المخزنة في النظم المعلوماتية للإدارة.

وهناك عدة قوانين أصدرها المشرع المغربي ليتصدى للجرائم الإلكترونية من القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات[1] .

4.2.5.القانون اللبناني:

وبنفس الاتجاه أولى المشرع اللبناني اهتمام كبير بتحريم الجريمة الالكترونية فالقانون رقم 140 لسنة 1997 المعدل بالقانون 158 لعام 1999 نص على سرية المخابرات التي تجري بواسطة أية وسيلة من وسائل الاتصال فعاقبت المادة (17) منه بالحبس من سنة إلى ثلاث سنوات وبالغرافة 100 ليرة لبنانية كل من أخل بهذا القانون .

وقانون رقم 431 لسنة 2002 المتعلق بتنظيم قطاع خدمات الاتصال.

- ثم أصدر قانون خاص لحماية المستهلك رقم 659 في 2005/2/4 الذي أورد تنظيماً لبعض العمليات التجارية التي يجريها المحترف عن بعد بواسطة الانترنت وفرض عقوبات جزائية على المخالف، بالإضافة لما تقدم من نصوص فإن قانون العقوبات عاقب كل من يقدم على سرقة وحيازة المعلومات(282م/283).

5.2.5.قانون الإمارات العربية ودولة البحرين:

أما دولة الإمارات العربية فقد أصدرت هي الأخرى قانوناً على غرار القانون التونسي السابق الذكر برقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية بالقانون الاتحادي رقم (2) لسنة 2006.

واشترك القانون البحريني رقم 83 لسنة 2002 مع القانون السابق الذكر تعريفة للمعلومات بأنها (البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعد البيانات والكلام).

6.2.5.القانون المصري:

[1] – كوثر حازم سلطان ، مرجع سابق، (ص 979).

من الملاحظ أن القانون المصري في بداية الأمر لم يعالج أو يتدخل بنص صريح حول جرائم الانترنت بل اعتمد في ذلك على قانون العقوبات لكنه انشأ في وزارة الداخلية المصرية مكتب إداري لمكافحة جرائم الحاسب الآلي وشبكة المعلومات عام 2002.

فالتشريع المصري اعتمد على قانون العقوبات فيما يتعلق بجزئية السب والقذف سواء كانت بالنشر عبر الوسائل المقروءة أو الالكترونية كذلك اعتمد على قانون حقوق الملكية رقم (82) لسنة 2002.

وبعد ذلك أصدر القانون رقم (10) لسنة 2003 الخاص بقانون تنظيم الاتصالات،ثم عقبه قانون رقم (15) لسنة 2004 الخاص بالتوقيع الالكتروني.[1]

7.2.5.القانون السعودي:

المشرع السعودي لم ينص صراحة على الجرائم الالكترونية عندما أصدر نظامي المعاملات الالكترونية سنة 2007 لكن بصدور المرسوم رقم 17 في 1430/3/8، تضمن نظام مكافحة جرائم المعلوماتية وحدد عقوبات لمرتكبيها.

فعاقبت المادة الثالثة بالسجن مدة لا تزيد على سنة وبغرامة مالية لا تزيد على 500 ألف ريال سعودي أو بإحدى العقوبتين كل شخص يرتكب الجرائم المعلوماتية الآتية (التصنت أو الدخول الغير مشروع لتهديد شخص أو بقصد إتلاف للموقع). وتزداد العقوبة حتى تصل إلى السجن أربع سنوات إذا كان الدخول هدفه إلغاء بيانات خاصة أو تشويش الخدمة أو تعطيلها.

أما إنشاء موقع لمنظمات إرهابية فالعقوبة تصل إلى عشر سنوات.[2]

8.2.5. القانون السوداني:

انفرد المشرع السوداني عن أقرانه من المشرعين العرب بمعالجته الجريمة الالكترونية، فأصدر قانون خاص لجرائم المعلوماتية سنة 2007، وعاقب بالسجن مدة لا تتجاوز سنتين او بالغرامة او بالعقوبتين معا كل من دخل موقعا أو نظام معلومات دون أن يكون مصرحا له بالاطلاع عليها او نسخ منه وفي حالة إلغاء بيانات أو معلومات ملكا للغير فتشدد العقوبة إلى أربع سنوات سجن.

وتميز أيضا القانون السوداني بإنشاء شرطة رقابة متخصصة بجرائم المعلوماتية و أيضا محكمة مختصة بهذا النوع من الجرائم.[3]

9.2.5. القانون الأردني:

[1] –محمد ابو العلا عقيدة،**التحقيق وجمع الادلة في مجال الجرائم الالكترونية**، مقال مقدم لمنتدى المنصورة،2007/6/25، (ص12).

[2] –المواد (10–3)من القانون السعودي.

[3] – المواد(8–4)من القانون السوداني.

استحدث المشرع الأردني عام 2008 شعبة المتابعة والتحقيق الخاصة بالجرائم الالكترونية بقانون جرائم أنظمة المعلومات لسنة 2010، بالتفريق بالعقوبة إذا كان مرتكبها إنسان عادي أو موظف بخدمة عامة، فالأول يعاقب مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر وبغرامة مالية وتضاعف العقوبة بحق كل من قام بارتكابها أثناء تأدية الوظيفة أو بسببها.

10.2.5. القانون السوري:

اعتبر القانون السوري الأدلة الرقمية أدلة إثبات ما لم يثبت تزويرها، أما البرامجيات فهي من الأشياء المادية التي يجوز تفتيشها وضبطها وفق قانون أصول المحاكمات الجزائية. وقد أعطى القانون السوري للضابطة العدلية القيام بالمراقبة الالكترونية بناء على إذن من النيابة العامة أو على أنابه من قاضي التحقيق .[1]

11.2.5.القانون القطري:

ركز هذا القانون على محل الجريمة بأن تكون أحد المواقع الإلكترونية التابعة لأجهزة الدولة أو مؤسساتها، فجاءت المادة (2) من قانون قطر رقم (14) لسنة 2014 قانون مكافحة الجرائم الالكترونية بأن يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبالغرامة لا تزيد على (500,000) خمسمائة ألف ريال كل من تمكن عن طريق الشبكة المعلوماتية أو بأحدى وسائل تقنية المعلومات بغير وجه حق من الدخول إلى موقع الكتروني لأحد أجهزة الدولة أو مؤسساتها. وأيضا عاقب على التصنت العمدي أو التقط دون وجه حق بيانات مرسلة عبر الشبكة المعلوماتية أو أحدى وسائل تقنية المعلومات

12.2.5.القانون العراقي:

لا يزال المشرع العراقي قيد إصدار قانون خاص ينظم الجريمة المعلوماتية وذلك للظروف الراهنة التي يمر بها العراق فقد عطل هذا القانون الذي يضم (33) مادة بمجلس النواب للضغوط من قبل نقابات حزبية ضاغطة من اضطر الحكومة إلى سحبه و تأجيله إلى إشعار آخر أو لأنه لم يراعي معايير التشريع السليم.

لكن هذا لا يعني عدم خضوع الجريمة الالكترونية للقانون بل يطبق عليها القوانين الآتية:

– قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.

– قانون الإثبات العراقي رقم 107 لسنة 1979 نصت المادة 27 منه (يكون للبرقيات حجية السندات العادية إذا كان أحلها المودع في مكتب الإصدار موقعاً من مرسلها)

– قانون المطبوعات رقم (206) لسنة 1968 الذي يخص الصحف والمجلات وتستند عليه فيما ينشر على مواقع الانترنت بما فيها التواصل الاجتماعي.

– قانون مكافحة الإرهاب رقم (13) لسنة 2005 فيما يخص جرائم الإرهاب الالكتروني فقد جرمت السادة الأول منه كل فعل اجرامي أوقع بالممتلكات العامة أو الخاصة أو إثارة الرعب والخوف بأي وسيلة كانت.

[1] – المادة (27) من قانون مكافحة الجرائم لالكترونية السوري لسنة 2010.

– قانون مكافحة الإرهاب في إقليم كردستان رقم (3) لسنة 2006 حيث نصت المادة الثالثة منه في فقراتها الرابعة على أن (تعطيل وسائل الاتصالات وأنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها او إدخال معلومات او بيانات هي جرائم أرهابية .

– أما المادة الرابعة / الفقرة الثانية فعاقبت بالسجن مدة لا تزيد عن خمس عشرة سنة كل من حاز أشرطة مسجلة أو نظائرها او صوراً تتضمن تحريضاً أو لارتكاب جرائم إرهابية يقصد النشر.

وساوي القانون في الفقرة الرابعة من السادة أعلاه بين وسائل الإعلام المرئية والالكترونية أو نشر البيانات على مواقع الانترنت بغرض تهديد الإقليم. [1]

6. موقف القضاء العربي من الجريمة الالكترونية:

إن محاولات تطبيق القانون على الجرائم الالكترونية وغش الحاسوب تقف أمامه جملة عوائق قانونية في مقدمتها مبدأ حضر القياسي في القانون الجنائي الموضوعي ومبدأ الشرعية لذلك تباين موقف القضاء العربي منه ، ونذكر من أمثلة ذلك مايلي:

1.6. القضاء اللبناني:[2]

يطبق القانون اللبناني مواد ونصوص قانون العقوبات على الجرائم الالكترونية فواجه القضاء اللبناني في عام 2000 قضية تعرض خطير للآداب والأخلاق العامة حصلت بواسطة شبكة الانترنت حيث تمكن حكم قاضي التحقيق في بيروت بالحبس والغرامة على شخص لبناني قام ببث صور ومشاهد الإباحية عبر الانترنت عرضه للالتقاط من ملايين المشتركين فهنا طبق القضاء اللبناني المادة 531-533 من قانون العقوبات اللبناني. وذهب القضاء اللبناني الى القول بأن المعلومات المعالجة الكترونيا ذات كيان مادي تصلح محلا للسرقة ففي سنة 2001 أصدر القاضي الجزائي حكماً لدان بموجبه أحد الأشخاص لأقدامه على نقل وتقليد معلومات مخزونة على أسطوانات مرنه (Floppy Disk) تخص شركة مدعيه وايضا طبق قانون العقوبات المادة (722).

أما بالنسبة للقانون الواجب التطبيق فقد اجزم القضاء اللبناني حيث ادخل باختصاصه الجرائم الالكترونية بمجرد حصون أحد أركان الجريمة على الأراضي اللبنانية أو أحد الأفعال المكونة لأركانها. ففي قضية حصلت عام 2003 حصل ادعاء النيابة العامة الاستئنافية في بيروت سنداً ضد أحد الأشخاص وحكموا عليه لاستعماله خدمات الانترنت لشركة (ISP)للوصول الى احد المواقع على الشبكة (Day Lebanon) وهو موقع مسجل في نيويورك بنشر اخباراً ومعلومات تتعلق باللواط ومتعاطيه في لبنان. وقد برأت المحكمة الشركة لان لا علاقة لها بالموقع المذكور بل ان المتهم دخل عبر الشركة للموقع وكان بإمكانه الدخول ايضاً عبر أية شركة انترنت أخرى.

[1] –كوثر حازم سلطان،مرجع سابق، (ص 983).

[2] – القاضي فوزي خميس، الجرائم المعلوماتية في ضوء القضاء اللبناني، بحث منشور بتاريخ 2008/2/23،(ص ص 7-9)

والاتجاه الحديث للقضاء اللبناني يختلف عن السابق ففي عام 2008 ادانت محكمة القضاء الجزائي اللبناني أشخاص بجرائم السرقة استنادا إلى المواد (636-219) عقوبات على اعتبار أنهم أقدموا على الدخول إلى حسابات بعض الأشخاص في الولايات المتحدة الأمريكية عن طريق الانترنت تمهيدا للاستيلاء على الأموال وبالاتفاق سابق مع القراصنة لقاء عمولة وقد توسع القضاء اللبناني في تجريمه بالأفعال المرتكبة بواسطة الحاسوب والانترنت فشمل جرائم القذف والسب أيضاً كما جاء ذلك في الدعوى القضائية ضد رئيسه مكتب مكافحة الجرائم المعلوماتية في لبنان بتاريخ 15-5-2014 عند تعرضها لاعتداءات من عنف كلامي وتحقير وإهانة.

2.6. لقضاء العماني:

فقد اقر هذا القضاء على المساواة بين الأدلة التقليدية والأدلة المتولدة من الحسابات الآلية . وطبق قانون الجزاء العماني على الجرائم المعلوماتية بعد إدراجها في المادة (276) ضمن مواد القانون رقم (72) لسنة 2001.

فني القرار المرقم (72) المؤرخ في 29/10/2012 قررت المحكمة العليا لسلطنة عمان (ان تقدير الدليل بالصورة التي تكشف قناعة المحكمة من اطلاقات محكمة الموضوع لا تجوز إثارته أمام المحكمة العليا

اما فكرة عدم جواز أن يقضي القاضي بالجرائم المعلوماتية بناء على رأي الغير فهي مما يتقيد به القاضي الجزائي ايضاً في تكوين اقتناعه عدم التعويل على رأي الغير بل يجب أن يستمد هذا الاقتناع من مصادر يستخلصها بنفسه من التحقيق بالدعوى.

وأكد ما سبق في قرار آخر برقم (51) في 13/4/2004 حيث جاء فيه: (**كل دليل تعتمد عليه المحكمة في حكمها يجب أن يكون قد طرح شفويا في الجلسة ويستمد القاضي إقناعه من هذه المناقشات**)[1].

3.6. القضاء المصري:

آثار جدلا أو تساؤل أمام القضاء المصري مدى اعتبار التحويل الالكتروني للأموال من قبيل التسليم المحقق النتيجة في جريمة الاحتيال. فحسمت المحكمة العليا ذلك الجدل بقرار لها جاء فيه " بأن تعبير المال الوارد بالمادتين 133 عقوبات المصري الخاص بخيانة الأمانة و134 عقوبات الخاص بالاحتيال يشمل النقود الكتابية و بالاستناد إلى اعتبار التسليم غير متطلب له المناولة المادية وحسب ماهومستقر في الفقه المصري و الفرنسي.[2]

وفي قرارين آخرين قررت المحكمة بان الدفع التي يتم عن طريق القيد الكتابي يعادل تسليم النقود وسند لوجود ومكان لتطبيق نص ماده الاحتيال على بعض صور جرائم غش الحاسوب واعتبار النتيجة محققه.

وان الاستيلاء عن طريق تحويلات الكترونية تجري بين الحسابات من غش الحاسوب متحققا لا يتعارض مع القانون المصري لان التسليم في جرائم النصب يحققه وضع الشيء تحت تصرف الجاني بحيث يتمكن من حيازته بغير عائق ،ولو لم يستول عليه استيلاء ماديا.

---

[1] -كوثر حازم سلطان، مرجع سابق، (ص 990).

[2] – ابو بكر سليمان،**جرائم الحاسوب و أساليب مواجهتها**،مجلة الامن و الحياة، العدد2019،21، (ص 38).

وحديثا فقد استقرت محكمة النقض المصرية على اعتبار الذبذبات او الموجات الهاتفية مال منقول يمكن اختلاسه لأنه قابل للحمارة والنقل وبالتالي للسرقة.

4.6. القضاء المغربي:

في بداية الأمر اتبع القضاء المغربي اتجاه القضاء المصري والفرنسي المتمسك بالشرعية الجنائية فقد أكد في غير مره على أن: " الاموال المادية وحدها يمكن ان تكون موضوعا لجريمة السرقة وان المعلومات لا يمكن ان تكون محلا للسرقة ".

وفي عام 2006 فرض القضاء سيطرته على هذا انواع من الجرائم .فقد اصدرت المحكمة الابتدائية بالدار البيضاء قرارها بعدد 364 بتاريخ 17 ابريل 2006 وادنت شخص بالحبس 6 أشهر وغرامة قدرها 10,000,000 درهم وذلك لارتكاب الجاني جنحة الدخول الى نظام الحاسب لشخص آخر. وبنفس الاتجاه اخذت المحكمة الابتدائية بالرباط بتاريخ 11|10 |2012 في قضية شركة كوماناف فيري عندما أدانت متهمين بالحبس ثلاث سنوات وثمانية أشهر لقيامها باصطناع أذونات سفر مزورة عن تغيير المعطيات المضمنة بنظام المعالجة الآلية الخاص بالشركة.

والجدير بالذكر ان المشرع المغربي قد عاقب مستعمل هذه الوثائق المزورة بنفس العقوبة المقررة لمزورها واعتبرت ذلك مساساً خطيرا بالثقة في الائتمان بالسوق المالية بالمغرب. بل اعتبرت ان استعمال الحاسوب ظرفا مشددا للعقوبة وفي هذه الجرائم .[1]

5.6. القضاء الأردني:

بصدور قانون جرائم انظمه المعلومات لسنة 2010 الأردني أصبحت الجرائم التي ترتكب داخل المملكة الأردنية يطبق هذا القانون عليها وتدخل ضمن دعاوى القضاء الاردني فقد قضى فيه أحد قراراته: " يجوز أقامة دعوى الحق العام والحق الشخصي عن المشتكي عليه امام القضاء الاردني إذا ارتكيت أي من الجرائم المنصوص عليها في هذا القانون باستخدام انظمه معلومات داخل المملكة أو الحقت أضرارا بأي من مصالحها او بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها كليا أو جزئيا إذا ارتكبت من أحد الاشخاص المقيمين فيها[2].

7. الخاتمة:

في الوقت الذي قامت فيه التكنولوجيا بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية من خلال موضوع الجرائم الإلكترونية، حيث نجد أن الأجهزة القضائية وأساتذة القانون ما زالوا عاجزين عن الخروج بتصور واضح عن قانون للجريمة الالكترونية ، وذلك لصعوبة ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة

[1] -كوثر حازم سلطان، مرجع سابق، ص (991).

[2] – المواد (12-16) من قانون جرائم أنظمة المعلومات لسنة 2010 الأردني

لتشريعاته والقانون لا يعاقب على فعل سرقة المعلومات الإلكترونية لكونها غير مادية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وانما يصعب الأمر في حالة وقوع اعتداء على العنصر المعنوي في النظام المعلوماتي كالبرامج و المعلومات المخزنة.

وبعد الاطلاع و دراسة القواعد القانونية المتعلقة بالمعاملات و الجرائم الالكترونية وجدنا نقص وخاصة على المستوى الجزائي فرغم أن القانون و في إطار سعيه إلى حماية الحقوق من الاعتداءات وتجريم العديد منها وتخصيص عقوبات مالية وبدنية، إلا أنها لا تكفي بل لابد من تدخل المشرع بتعديلات كبيرة لمواجهة هذه التحديات لهذا النوع من الجرائم المتطورة.

8. قائمة المراجع:

1- أبو بكر سليمان،**جرائم الحاسوب و أساليب مواجهتها**،مجلة الأمن و الحياة، العدد2019،21.

2- محمد علي قطب، **الجرائم المعلوماتية**، بحث مقدم إلى مركز الإعلام الأمني، الأردن،2008.

3- محمد أمين الرومي،**جرائم الكمبيوتر و الانترنت**، دار المطبوعات الجامعية، الإسكندرية، 2004.

4- خالد ممدوح ابرهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، ط1، 2009.

5- كوثر حازم سلطان، **موقف القانون و القضاء من الجريمة الالكترونية(السيبرانية)**،مجلة كلية التربية الأساسية، المجلد 22، العدد 96، 2016.

6- هلالي عبد الله أحمد، **الجوانب الإجرائية و الموضوعية لجرائم المعلوماتية في ضوء اتفاقية بودابست**، دار النهضة العربية، القاهرة، 2003.

7- لطفي بن كريم، **التجربة التونسية في مجال المعاملات المدنية و التجارية الالكترونية** ،منتديات ستار تايمز2012/02/26.

8- محمد ابو العلا عقيدة،**التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، مقال مقدم لمنتدى المنصورة،2007/6/25.

9- القاضي فوزي خميس، **الجرائم المعلوماتية في ضوء القضاء اللبناني**، بحث منشور بتاريخ 2008/2/23.

10- عبد العال الدريني، **الجريمة المعلوماتية (دراسة مقارنة)**، ط1، دار، النهضة العربية، 2000.

11-Donne Parker, **cyber crime and general prin aples** ,Cyber crime andreal world by layi the Sridhar, 19 august2008 , (p18).

القوانين و المواد :

1- القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004.

2- القانون رقم: 09-04) المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخة في 16غشت.

3- المواد (10-3)من القانون السعودي.

4- المواد(8-4)من القانون السوداني.

5- المادة (27) من قانون مكافحة الجرائم لالكترونية السوري لسنة 2010.

6- المواد (16-12) من قانون جرائم أنظمة المعلومات لسنة 2010 الأردني.