موقف القانون والقضاء من الجريمة الالكترونية [السيرانية] دراسة مقارنة

م. كوثر حازم سلطان

الجامعة التكنولوجية

الملخص:

الجريمة السيرانية (Cyber Crime) أي الجريمة الافتراضية الواقعة في فضاء الكتروني المنبثق من (Cyber Space) أي الفضاء التخيلي او الافتراضي، ويعد وليام فيسبون اول من استخدم هذا المصطلح في رواية له عام 1984.

ثم جاء المؤتمر العاشر للأمم المتحدة المنعقد في فيينا سنة 2000 ليؤكد هذه التسمية عن الجرائم الالكترونية التي انتشرت في الآونة الأخيرة بسبب انتشار شبكة الانترنيت وفتح مجالات عديدة للاستفادة منها والذي فرضته هذه التقنيات الحديثة والتدفق الغزير للمعلومات يمكن استخدامها لمصلحة البشرية وفي الوقت نفسه هناك اضرار حدثت خلال السنوات الأخيرة وباتت هذه الجرائم من أخطر أنواع جرائم العصر انتقل مرتكبيها بالجريمة من صورها ووسائله التقليدية الى أخرى الكترونية.

"**سبب اختيار الموضوع**": يتعلق بأهمية البحث في هذه الأنواع من الجرائم لحداثتها واختلاف طرق اثباتها وما تتمتع به من غموض.

فرضيات البحث:

يناقش البحث فرضيتين هما هل تستطيع التشريعات والمحاكم القضائية بوسائلها وإجراءاتها الورقية ان تواجه غموض وتحديات جرائم العصر وماذا سيحل بمرافق العدالة إذا انتقلت الدولة برمتها الى البيئة الالكترونية مما يشكل عبئ جديد.

خطة البحث

تبدأ خطة البحث بتحليل مفهوم الجريمة وخصائصها ثم يبين موقف الاتفاقيات الدولية والتشريعات الوطنية وأخيرا إجراءات المحاكم وما تطبقه من عقوبات بحق مرتكبي هذه الجرائم لذا ستقسم البحث الى ثلاث مباحث وكما يلي:

- **المبحث الأول: مفهوم الجريمة السيبرانية وخصائصها.**
- **المطلب الأول: مفهوم الجريمة السيبرانية.**
- **المطلب الثاني: سمات وخصائص الجريمة.**
- **المبحث الثاني: موقف الاتفاقيات والتشريعات المقارنة من الجرائمة السيبرانية.**
- **المطلب الأول: موقف الاتفاقيات والتشريعات الدولية .**
- **المطلب الثاني: موقف التشريعات العربية.**
- **المبحث الثالث: موقف القضاء من الجريمة السيبرانية.**
- **المبحث الأول: موقف القضاء الدولي المقارن.**
- **المطلب الثاني: موقف القضاء العربي.**
- **ونختم البحث بعدة توصيات توصلنا اليها من خلال دراستنا المتواضعة لهذا الموضوع.**

المبحث الأول

مفهوم الجريمة الالكترونية وخصائصها

استجابة للتطور الكبير في تقنيات الاتصالات والمعلومات والزيادة الهائلة في حجم المتعاملين معها رافق ذلك من ممارسات سلبية تصل في كثير من الأحيان الى جرائم تهدد الامن بمعناه الشامل مما اوجد بعض التحديات لمواجهة هذه الجرائم منها زيادة الحاجة ال جهات تمارس التحقيق بشكل متخصص بالإضافة الى الضغوط على الجهات القضائية والأمنية فضلاً عن الحاجة الى التكامل المعرفي بين رجال القانون والتحقيق والقضاء مع الجهات التقنية والحاسوبية.

المطلب الأول

مفهوم الجريمة الالكترونية

الجريمة لغةً هي:

من جرم جرماً أي (ذنب ذنباً) ويقال جرم نفسه وقومه وجرم عليهم وإليهم[1]. وقد ورد في القرآن الكريم لفظ الجريمة. [وَلاَ يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَى أَلاّ تَعْدِلُواْ اعْدِلُواْ هُوَ أَقْرَبُ لِلتَّقْوَى[2]] .

وانطلق فقهاء القانون من معايير لتحديد مفهوم الجريمة الالكترونية منها معيار موضوع الجريمة او وسيلتها وآخرون ركزوا على النتيجة التي تتركها وكما يلي:

❖ فهي الجرائم التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دوراً رئيسياً[3].
فهذه الجرائم تمس برامج الكومبيوتر او تحلل معلومات غير مصرح بها[4].

❖ وقد ذهب الفقيه (Rosenblatt) بتعريفه الى هذا النوع من الجرائم على انها نشاط غير مشروع ينصب على المعلومات المخزنة داخل الحاسوب وتغييرها وحذفها والسلوك هنا ذو طبيعة ذهنية[5].

فهي كل فعل او نشاط إيجابي او سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الالي او بنظام المعلومات العالمية الانترنت او الإبقاء عليه عند تحققه او التأثير عليه بأي وسيلة كانت[6].

❖ والاعتداء او السلوك الغير مشروع واللاأخلاقي وغير مصرح به[7]. يشمل البرامج والمعلومات والمعالجة الالية للبيانات.

ويتفق الفقيه (Parker) الأمريكي مع الفقيهين 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) [8].

و من اهم الانتقادات الموجهة لمعيار السلوك المادي او موضوع الجريمة هو انه غير دقيق حيث يكون التأثير على المعلومات واتلافها وإعاقة الأنظمة عن أداء وظائفها قد تتم بواسطة اشخاص مصرح او غير مصرح لهم بالدخول الى النظام المعلوماتي.

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

(سلوك اجرامي يتم بمساعدة الحاسب الالي)[10].

❖ وتتفق الدكتورة فائزة بابا خان مع هذا المفهوم الواسع للجريمة المعلوماتية وترى بأنها:

(الفعل الجديد الذي يمارس باستخدام الأجهزة التقنية الحديثة مثل الحاسب الالي والهاتف النقال او أحد ملحقاتها في تنفيذ أغراض مشبوهة[11]).

❖ فهذا النوع من الجرائم تتطلب ان تتوافر لدى فاعلها معرفة بتقنية وتكنولوجيا الحاسوب.

❖ وهذا التعريف الذي اخذت به او تبنته وزارة العدل الامريكية في تقريرها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاث.

- ويتفق الأستاذ محمد امين الشوابكة مع الأستاذ (Middet Credo) بأن الجريمة السيبرانية تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة الى الحالات المتعلقة بالولوج غير المصرح به للحاسوب الالي او بياناته لتشمل الاعتداءات المالية المادية[12].
- 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)[13].

ومما يؤخذ على هذا المعيار توسعه الكبير لمفهوم الجريمة فمن شأنه ان يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك فقد لا يعد ان يكون الحاسب الالي محلاً تقليدياً في النشاط الاجرامي.

وبعد ان 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)بأن هذه الجرائم هي عبارة عن اعتدلءلت قانونية ترتكب بواسطة المعلوماتية غرضها الأساسي تحقيق الربح المتمثل بالمال[14].فهذا التعريف ركز على النتيجة وهي تحقيق المال إضافة الى معيار الوسيلة.
- فالهدف من العبث ببرامج الكومبيوتر وإعاقة استخدامها هو ارتكاب جريمة أخرى او بث فيروس من شأنه التأثير على أدائه[15].
- وهذا المفهوم الضيق اخذ به ايضاً الفقيه (Tredmann) لأنها جرائم بداية ضد المال مرتبطة بالمعالجة الالية للمعلومات[16].

والمال هنا ينصرف مفهومه طبعاً الى الأموال المادية والمعنوية فالاعتداء او الامتناع العمدي ينشأ عن استخدام غير المشروط للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية او المعنوية[17].

- وقد يكون هدف الجريمة الإساءة لسمعة الضحية او لجسدها او عقليتها فهي (اية مخالفة ترتكب ضد افراد او جماعات بدافع جرمي ونية الإساءة لسمعة الضحية وعقليتها سواء كان ذلك بطريقة مباشرة او غير مباشرة باستخدام وسائل الاتصالات الحديثة مثل الانترنت[18].

وقد انتقد هذا المعيار ايضاً (لان جرائم الكومبيوتر يمكن ان تنصب على المعلومات ذاتها دون السعي لتحقيق الربح.كذلك فأن تضييق نطاقها يقود الى افلات كثير من الأشخاص مرتكبي هذا النوع من الجرائم من قبضة العدالة.

من خلال ما تقدم يمكننا ان نعرف الجريمة الالكترونية بأنها :

(كل نشاط غير مشروع يكون معرفة تكنولوجيا الحاسبات أداة لارتكابه ولملاحقته بقصد الاضرار بالأخرين او حق يحميه القانون)

والقصد هنا يتحقق بتوافر العلم لدى الجاني بأنه يقوم بأحد الأفعال التي حرضها نصوص القوانين.

المطلب الثاني

سمات وخصائص الجريمة السيرانية

اصبحت تقنية المعلومات من اساسيات الحياة في عصرنا الحالي رغم استغلال البعض لهذه التقنية لغايات غير مشروعة وذلك الى خطورة من هذا النوع من الجرائم لان الجانب التنظيمي يشملها بصورة متكاملة لتعدد صورها والتجدد فيها وتميزها عن غيرها من الجرائم التقليدية فما هي السمات المميزة لها نتناول هذه الخصائص وكما يلي:

1- الجريمة الالكترونية (عابرة للحدود) حيث ان القدرة التي تتمتع بها الحاسبات الالية في نقل وتبادل كميات كبيرة من المعلومات بين انظمة يفصل بينها الاف الاميال اسفر هذا الامر الى نتيجة مفادها ان اماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية[19].

2- الجريمة الالكترونية جريمة ناعمة لا تتطلب قدرات عنيفة لارتكابها كتبادل اطلاق النار او سفك دماء كذلك لا يوجد شعور لدى المجرم المعلوماتي بعدم اخلاقية ما يقوم به او بمساسه بمصالح او قيم يحرص المجتمع على حمايتها ولا يعتبر ما يقوم به يدخل في عداد الجرائم[20] .

3- الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم السيراني فقد يوجد الجاني في بلد ما ويستطيع الدخول الى ذاكرة الحاسب الالي الموجود في بلد آخر. ذلك يظهراكثر في البرامج الخبيثة (Viruses) حيث يتم نسخها في بلد وترسل الى دول مختلفة من العالم[21].

4- عولمة الجريمة السيرانية تثير مشاكل حول القانون الواجب التطبيق.

5- جاذبية الجريمة السيرانية : نظراً لما تمثله سوق الكومبيوتر من ثروة كبيرة فقد غدت اكثر جاذبية بأستثمار الاموال وغسلها وتوظيف الكثير منها في تطوير تقنييات واساليب تمكن الدخول الى الشبكات وسرقة المعلومات[22].

6- جريمة متطورة لا يمكن حصر اساليبها في الوقت الحاضر وان امكن حصرها الا انه لا يمكن التنبوء بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات[23] 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 او البيئة التي ترتكب فيها.

7- التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالانترنت عند الاثر المادي وانما يتعدى ذلك ليهدد نظام القيم والنظام الاخلاقي خاصة في المجتمعات المحافظة والمغلقة.

8- تعدد دوافع الجريمة السيبرانية فقد تكون سببها مجرد سداد الديون او ادمان لعب القمار او المخدرات او بيع المعلومات المختلسة[24] او مجرد الدخول وجمع معلومات دون قيود كما اشار الاستاذ ليفي مؤلف كتاب قراصنة الانظمة(Hackers)[25].

9- صعوبة اكتشافها وامكانية اثباتها لسبب عدم تخلفها لآثار ظاهرة خارجية فهي تنصب على البيانات والمعلومات المخزنة.

10-الوصول اليها واكتشاف حقيقتها تتطلب الاستعانة بخبرة فنية عالية المستوى.

11-امتناع المجني عليهم عن المطالبة بالتعويض او حتى التبليغ عنها خوفاً من الفضيحة او بسبب عدم علمهم بها الا عندما تكون انظمتهم المعلوماتية هدفاً لفعل الغش[26].

المبحث الثاني

موقف القوانين من الجريمة السيرانية

في دراسة أجريت من قبل مكتب التحقيقات الفيدرالية عام 2003 تبين بأن اكثر خسائر المؤسسات بالولايات المتحدة الامريكية* أتى من الاستيلاء عن المعلومات والتي قدرت

*سنة 2002 وصل عدد المواقع الإباحية (3433) ووصل عام 2006 الى (10656) توجد 54% من المواقع الإباحية للقاصرين في الولايات المتحدة الامريكية وعدد الجرائم الجنسية بلغ 850 الف حالة.
و عمليات سرقة الهويات 92 الف حالة بينما وصل عدد جرائم الاحتيال للحصول على الأموال نحو 207 الف عملية و145 عملية اختراق اما حجم الخسائر المادية لجرائم الحاسب الالي في المؤسسات السعودية خلال عام 1419 هـ بلغ نحو (65205) مليون ريال

خلال هذا العام خسائر تتعدى 70 مليون دولار امريكي وفي المركز الثاني نشاط تعطيل نظم المعلومات محققاً خسائر تتجاوز 65.5 مليون دولار وعند ارتفاع ارقام الجريمة المرتكبة بواسطة هذه التقنيات الامر الذي دعا رجال القانون على الصعيد الدولي والوطني الى البحث عن تعديل نصوص قانون العقوبات لمواجهة هذا الامر بشتى أنواعها او الحاجة ملحة لاستحداث قوانين خاصة باعتبارها جرائم ذات طبيعة خاصة.

و بعد ان عرفنا مفهوم الجريمة السيرانية لا بد من استعراض موقف القوانين على الصعيد الدولي والعربي.

المطلب الأول

موقف القوانين والمنظمات الدولية

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

اولاً: فعلى مستوى المنظمات الدولية

فقد لعبت الأمم المتحدة دوراً كبيراً في هذا المجال من خلال متابعتها واشرافها وحتى عقد المؤتمرات الدولية الخاصة بمنع الجرائم من هذا النوع[27] فمنذ عام 1968 شهد مؤتمر الأمم المتحدة لحقوق الانسان طرح موضوع مخاطر التكنولوجيا الحق في الخصوصية ثم المؤتمرالسابع المنعقد في ميلانو عام 1985 كلف لجنة.

الخبراء العشرين بدراسة موضوع حماية نظام المعالجة الالية والاعتداء عن الحاسوب.

اما المؤتمر الثامن المنعقد في هافانا 1990 والتي من اهم توصياته التأكيد على 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 (63/55) المؤرخة في 2000/4/12. عرفت الهاكر او المخترق

بأنه (المبرمج المتفوق جداً ولكنه يستخدم جل طاقاته في الاتجاه الغير شرعي لمحاولة اختراق أنظمة حاسوبية لغرض اثبات قدرته او التباهي او احياناً لأهداف إجرامية)*.

اما اتفاقية بودابست لعام 2001[29] فقد قسمت مادتها (48) الجرائم السيبرانية الى أربعة اقسام:

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 بالأخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات).

ج- وقد عمدت دول الاتحاد الأوربي على تأسيس جهاز الاوردجست (Eurojust) يعمل على المستوى الأوربي الاوروبول في مجال مكافح-ة جميع الجرائم التي تم انشاءه عام 2002 يمارس اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد او دولة عضو مع دولة أخرى واتخذ من لاهاي مقراً له اما انشطته فتتمركز حول معالجة المعلومات المرتبطة بالأنشطة الاجرامية.

اما 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[31].

ثانياً: الجريمة السيبرانية في التشريعات المقارنة.

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

اتبعت الولايات المتحدة الامريكية السويد حيث شرعت قانوناً خاصاً بحماية أنظمة الحاسوب عام(1976) وفي عام 1985 حدد معهد العدالة القومي خمسة أنواع رئيسية

*وقعت اتفاقية بودابست (26) دولة اعضاء وقد انضمت اربعة دول غير اعضاء وهي (كندا – اليابان – الولايات المتحدة الامريكية – جنوب افريقيا).

للجرائم المعلوماتية وهي: (جرائم الحاسب الالي الداخلية / جرائم الاستخدام غير المشروع عن بعد / جرائم التلاعب بالحساب الالي / دعم التعاملات الاجرامية وسرقة البرامج الجاهزة والمكونات المادية للحاسب.

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

واعتبر قانون كاليفورنيا عام 1985 مرتكب جنحة كل من دخل عمداً الى منظومة او شبكة حواسيب عمداً.

اما ثالث دولة تسن قوانين خاصة بجرائم الحاسب الالي فهي بريطانيا حيث اقرت قانون مكافحة التزوير والتزييف عام 1981 الذي شمل في تعاريفه الخاصة أداة التزوير (وسائط التخزين الحاسوبية المتنوعة او أي أداة أخرى يتم التسجيل عليها بالطرق التقليدية او الالكترونية[32].

ونهج القانون السويسري نهج القانون الامريكي فأصدر قانون (غش واساءة استخدام الحاسوب لسنة 1984) وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الالي والانترنت حيث عدلت عام 1985 القانون الجنائي ليشمل هذه الجرائم وتحديد عقوبات لتدمير انظمة الحاسوب كما جاء بالمادة 387 خاصة اذ كانت عن عمد.

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

كما تعطي القوانين الالمانية الحق للقاضي باصدار امره بمراقبة اتصالات الحاسب الالي وتسجيلها والتعامل معها وذلك خلال مدة اقصاها ثلاثة ايام.

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الاجرامية حيث اصدرت عام 1988 القانون رقم (19-88) الذي اضاف الى قانونها العقابي جرائم الحاسب الالي مثال ذلك اضاف فقرتين (5-6) 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 اي او استخدام هذه المستندات[33].

في حين سوى المشرع الفرنسي بين الكتب الالكترونية والكتب الخطية بالقانون رقم 2000/3/13 وذهب القانون الفرنسي ابعد من ذلك حيث تم اعداد 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 والفلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الالي متى ما كانت هناك جريمة[34] وهو اتجاه القانون البلجيكي المرقم 23 لسنة 2000 في مادته (88).

المطلب الثاني

موقف القوانين العربية من الجريمة السيبرانية

نالت الجريمة الالكترونية قسطاً كبيراً من الاهتمام من قبل المشرعين العرب فمنهم من يفرد لها نصوص خاصة من خلال تعديل القوانين الجنائية واخرين أدركوا خطورة هذه الجرائم فخصص لها قانون مستقل نبين ذلك من خلال النقاط التالية:

1- 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.

فبالإضافة الى 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 الاخلال بسير نظم المعالجة الالية للمعطيات او ما يسمى بالقانون الجنائي المعلوماتي لان الأفعال التي جرمها كانت تنصب على البيانات او المعطيات بشكل أساسي.

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

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

وهناك عدة قوانين[35] أصدرها المشرع المغربي ليتصدى للجرائم الإلكترونية من القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات.

2- 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 اية وسيلة من وسائل الاتصال فعاقبت المادة (17) منه بالحبس من سنة الى 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 4/2/2005 الذي أورد تنظيماً لبعض العمليات التجارية التي يجريها المحترف عن بعد بواسطة الانترنت وفرض عقوبات جزائية على المخالف. بالإضافة الى لما تقدم من نصوص فأن قانون العقوبات عاقب كل من يقدم على سرقة وحيازة المعلومات (م283/282).

3- القانون التونسي

كان المشرع التونسي من السباقين وبادر بوضع اطار قانوني للمتدخلين في المجال الالكتروني عن طريق احكام متفرقة منها القانون رقم 42 لسنة 1993 الذي نص على ان الاتفاق يعتبر ثابت سواء وقع من الأطراف او بتبادل رسائل او برقيات وغيرها من وسائل الاتصال فهذا اقتراف صريحاً بهذه الطرق كوسيلة من وسائل الاثبات.

بعد الالفية الثانية بدأ إدراك أهمية الموضوع بتزايد مما حث المشرع التونسي الى سن قانون خاص بالتجارة الالكترونية[36] فعاقب كل من استغل ضعف او جهل شخص في إطار عمليات البيع الالكتروني بغرامة تتراوح 2000 دينار.

ومواكبة للتطور أصدر المشرع ايضاً 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 .

4- قانون الامارات العربية ودولة البحرين.

اما دولة الامارات 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 تعريفه للمعلومات بأنها (البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن ان تكون قواعد البيانات والكلام)[37].

5- القانون المصري.

ومن الملاحظ ان القانون المصري في بداية الامر لم يعالج او يتدخل بنص صريح جرائم الانترنت بل اعتمد في ذلك على قانون العقوبات لكنه انشأ في وزارة الداخلية المصرية مكتب اداري لمكافحة جرائم الحاسب الالي وشبكة المعلومات عام 2002.

فالتشريع المصري اعتمد على قانون العقوبات فيما يتعلق بجزئية السب والقذف سواء كانت بالنشر عبر الوسائل المقروءة او 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[38].

6- القانون السعودي.

ايضاً 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 او بإحدى العقوبتين كل شخص يرتكب الجرائم المعلوماتية الاتية (التصنت او الدخول الغير مشروع لتهديد شخص او بقصد اتلاف للموقع).

وتزداد العقوبة حتى تصل الى السجن أربع سنوات إذا كان الدخول هدفه الغاء بيانات خاصة او تشويش[39] الخدمة او تعطيلها.

اما انشاء موقع لمنظمات إرهابية فالعقوبة تصل الى عشر سنوات.

7- القانون الجزائري.

أستخدم المشرع الجزائري مصطلح المساس بنظم المعالجة الالية للمعطيات وذلك بالقانون رقم (15/4) في 10/نوفمبر/2004 وينصرف هذا المصطلح الى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات فقد عمد المشرع في المادة (8) من القانون أعلاه الى حماية سرية وسلامة المعلومات وعاقب بالحبس كل من يدخل عن طريق الغش المتعمد للمعالجة الالية.

وفي المادة (15) من القانون حددت بأن تكون المحاكم الجزائية مختصة بالنظر في الجرائم المتعلقة بتكنولوجيا الاعلام المرتكبة خارج الوطن عندما يكون مرتكبها اجنبياً وتستهدف مؤسسات الدولة الجزائرية[40] 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 الاعمال احد اركانها قد تم في الجزائر).

8- القانون السوداني.

انفرد المشرع السوداني عن اقرانه من المشرعين العرب بمعالجته الجريمة الالكترونية.

فأصدرا قانون خاص لجرائم المعلوماتية سنة 2007 وعاقب بالسجن مدة لا تتجاوز سنتين او بالغرامة او بالعقوبتين معاً كل من دخل موقعاً او نظام معلومات دون ان يكون مصرحاً له بالاطلاع عليها او نسخ منه وفي حالة الغاء بيانات او معلومات ملكاً للغير فتشدد العقوبة الى أربع سنوات سجن[41].

وتميز ايضاً القانون السوداني بأنشاء شرطة رقابة متخصصة بجرائم المعلوماتية وايضاً محكمة مختصة بهذا النوع من الجرائم[42].

9- القانون الأردني.

استحدث المشرع الأردني عام 2008 شعبة المتابعة والتحقيق الخاصة بالجرائم الالكترونية بقانون جرائم أنظمة المعلومات لسنة 2010[43] بالتفريق بالعقوبة إذا كان مرتكبها انسان عادي او موظف بخدمة عامة فالأول يعاقب مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر وبغرامة مالية وتضاعف العقوبة بحق كل من قام بارتكابها اثناء تأدية الوظيفة او بسببها[44].

وبهذا اتفق القانون الأردني مع القانون السوري (قانون مكافحة الجرائم الالكترونية) لسنة 2010[45].

10- القانون السوري.

والجدير بالذكر ان القانون السوري السابق الذكر اعتبر الأدلة الرقمية ادلة اثبات ما لم يثبت تزويرها اما البرامجيات فهي من الأشياء المادية التي يجوز تفتيشها وضبطها وفق قانون أصول المحاكمات الجزائرية[46].

وقد اعطى القانون السوري للضابطة العدلية القيام بالمراقبة الالكترونية بناءً على اذن من النيابة العامة او على أنابه من قاضي التحقيق[47].

11- القانون القطري.

ركز هذا القانون على محل الجريمة بأن تكون أحد المواقع الإلكترونية التابعة لأجهزة الدولة او 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 او بأحدى وسائل تقنية المعلومات بغير وجه حق من الدخول الى موقع الكتروني لاحد أجهزة الدولة او مؤسساتها.

وايضاً عاقب على التصنت العمدي او التقط دون وجه حق بيانات مرسلة عبر الشبكة المعلوماتية او احدى وسائل تقنية المعلومات[48].

12- القانون العراقي.

لا يزال المشرع العراقي قيد اصدار 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 الى سحبه وتأجيله الى اشعار آخر او لأنه لم يراعي المعايير او أسس التشريع السليم.

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

1- قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.
2- قانون الاثبات العراقي رقم 107 لسنة 1979 نصت المادة 27 منه (يكون للبرقيات حجية السندات العادية اذا كان احلها المودع في مكتب الإصدار موقعاً من مرسلها).
3- قانون المطبوعات رقم (206) لسنة 1968 الذي يخص الصحف والمجلات وتستند عليه فيما ينشر على مواقع الانترنت بما فيها التواصل الاجتماعي[49].
4- قانون مكافحة الإرهاب رقم (13) لسنة 2005 فيما يخص جرائم الإرهاب الالكتروني فقد جرمت المادة الأول منه كل فعل اجرامي أوقع بالممتلكات العامة او الخاصة او اثارة الرعب والخوف بأي وسيلة كانت.
5- قانون مكافحة الإرهاب في إقليم كردستان رقم (3) لسنة 2006 حيث نصت المادة الثالثة منه في فقراتها الرابعة على ان (تعطيل وسائل الاتصالات وأنظمة الحاسوب او اختراق شبكاتها او التشويش عليها او ادخال معلومات او بيانات هي جرائم ارهابية[50].

واما المادة الرابعة / الفقرة الثانية فعاقبت بالسجن مدة لا تزيد عن خمس عشرة سنة كل من حاز اشرطة مسجلة او نظائرها او صوراً تتضمن تحريضاً او لارتكاب جرائم إرهابية بقصد النشر.

وساوى القانون في الفقرة الرابعة من المادة أعلاه بين وسائل الاعلام المرئية والالكترونية او نشر البيانات على مواقع الانترنت بغرض تهديد الإقليم.

❖ ومن الملاحظ على قانون الإرهاب العراقي رقم (13) لسنة 2005 بمادته الاولى انه عرف الإرهاب بشكل غير كامل وكان الاجدر به الاستعانة بتعريف الاتفاقية العربية لمكافحة الإرهاب والذي أنظم اليها وصادق عليها فقد شملت بالتعريف كل طبع او نشر ممرات او تسجيلات مهما كان نوعها.

*لم يكن استعمال الانترنت مسموحاً به في العراق حتى عام 1999 حتى استقبال القنوات الفضائية كان ممنوعاً وان وجد في حدود ضيقة ومراقب من قبل الحكومات.

لذلك فأن الحاجة ملحة للإسراع بسن قانون خاص بالجرائم المعلوماتية في العراق وذلك لمواكبة التقنيات الحديثة.

المبحث الثالث

موقف القضاء من الجريمة السيبرانية

تتباين الدول في مواقفها بشأن قبول الأدلة المستحصلة من أنظمة الحاسبات الالية وواجهت المحاكم صعوبة في تكييف النصوص القانونية لتجريم الأفعال التي تنص على اداوت معلوماتية ناهيك عن مشكلة القانون الواجب التطبيق نظراً لعالمية هذا النوع من الجرائم وصعوبة تحديد مكان وقوع الجريمة بالإضافة الى إمكانية او قابلية انطباق نصوص القانون التقليدية على طائفة من هذه الجرائم.

المطلب الأول

موقف القضاء المقارن

❖ **القضاء الإنكليزي**

أقام القضاء البريطاني تسوية بين الالة والشخص في مسألة قبول السند المزور في قضية R.V وCld لسنة 1981 و(قضية Moritz) لعام 1982 الخاصة بعائدات قيمة الضرائب الإضافية لأحدى الشركات فقرر: (ان الخداع يتطلب عقلاً بشرياً يمكن خداعة والتحايل عليه على الرغم من ان المادة (15) من قانون السرقة الإنكليزي لعام 1968 التي تجزم الحصول بالخديعة على مال بحوزة الغير بنية حرمانه منه بصفة مؤبدة والمادة الأولى من قانون السرقة لسنة 1978 التي تجزم الحصول بالخديعة على خدمة يمكن تفسيرها على نحو متسع يسمح بتطبيقها على خداع نظام معلوماتي او الة[51].

وفي قضية أخرى قام القضاء الإنكليزي بمقاضاة شركة (مورجان ستانلي) مرتين من قبل الموظفين العاملين بها بسبب التمييز العنصري حيث كشفت مبادئ الطب العدلي الشرعي المستخدمة في مجال جرائم الكومبيوتر عن وجود (نكات عنصرية) يتم توزيعها عبر نظام البريد الالكتروني الخاص بالشركة[52].

وقد قبل القضاء التسوية من أطراف النزاع في قضية (Merchant Bank City) حيث تم نقل 8 مليون جنيه من أحد ارصدته الى رقم حساب في سويسرا وقد تم القبض على الفاعل اثناء محاولته سحب المبلغ المذكور ولكن البنك بدل الادعاء على الفاعل قام

بدفع مبلغ مليون جنيه له بشرط عدم اعلام الاخرين عن جريمته وشريطة اعلام البنك عن الالية التي نجح من خلالها باختراق نظام الامن الخاص بحاسوب البنك الرئيسي[53].

وذهبت محكمة الاستئناف الإنكليزي بقرار صريح وواضح عام 1990 بأن: (جريمة الضرر الجنائي يمكن تطبيقها حيثما يقع الضرر على بيانات الحاسوب) [54].

ولم يهتم القضاء الإنكليزي بالاختصاص المكاني، فقد طبق القضاء حكمه على قضية لم تحدث على الأراضي البريطانية منطبقاً من عالميه هذه الجرائم.

(كما حدثت في قضية مبرمج إنكليزي يعمل بأحدى البنوك لدولة الكويت قام بالتلاعب بنظام الحاسب الالي ليقوم بأجراء خصومات من ارصدة العملاء ثم يقوم بإيداعها في الحساب الخاص به وقدم للقضاء الإنكليزي وحكم عليه بالحبس رغم ان فعلي السحب والإيداع كان في الكويت[55].

واعتبر القضاء البريطاني (الحصول على بيانات المعلوماتية بدون تصريح هي جريمة سرقة فقد قضى واعتبر القضاء البريطاني الحصول على البيانات المعلوماتية بدون تصريح هي جريمة سرقة فقد قضى بالحبس ودفع غرامة مقدارها 20,000 باوند استرليني على شخص ادعى انه طالب وقام بأفعال غير مشروعة للحصول على ايميلات مئات للطلبة[56].

❖ القضاء الأمريكي

اتجه القضاء الأمريكي الى اتجاه مغاير لنظيره البريطاني من حيث الاختصاص المكاني حيث وافق على تسليم شخص يدعى جوزيف اتهم بأعداد برامج خبيثة (Virus) عام 1990 وذلك لان ارسال هذه البرامج تم من داخل المملكة المتحدة البريطانية[57].

وبنفس السياق ايضاً قدمت الولايات المتحدة الامريكية مواطناً امريكياً للمحاكمة الجنائية نتيجة قيامه بتقديم خدمة المقامرة عن طريق الانترنت وانشاء هذا الموقع وبيعه لمواطني الولايات المتحدة الامريكية فقضت عليه المحكمة بالحبس (21) شهراً ومنعت الموقع من الاستمرار ، واعتبرت ذلك مخالفة لقانون الاتصالات السلكية لسنة 1991.

وفي قضية أخرى عرضت امام المحاكم الامريكية هي جرائم السرقة او القرصنة.

(فقد حكمت المحكمة بالسجن 3 سنوات على اخصائي كمبيوتر روسي الجنسية ومقيم في مدينة (st petersburg) هاجم نظم الكمبيوتر الخاص بـــ(Citybank) وذلك بهدف الحصول علة مبلغ قدره (10,000,000)عشرة مليون دولار امريكي وقد ضبط في لندن عام 1995[58].

ويذكر ان اهم القضايا التي عرضت امام هذا القضاء هي قضية (الجحيم العالمي) تعامل فيها مكتب التحقيقات الفدرالية حيث تمكنوا مجموعة من الأشخاص من اختراق البيت الأبيض والشرطة الفدرالية الامريكية والجيش الأمريكي ووزارة الداخلية وبعد دراسة ملابسات القضية تبين ان المجموعة تهدف الى مجرد الاختراق أكثر من التدمير والتقاط المعلومات الحساسة.

وفي عام 2005 حكمت محكمة (بوستن) في أمريكا على شاب بالحبس 11 شهراً لقيامه بقرصنة على حساب شركة الموبايل[59].

اما بشأن حجية الدليل الرقمي امام القضاء الجنائي) فقد توصلت المحكمة العليا الامريكية في قرارها الصادر عام 1993 (بأن الدليل الرقمي من حيث إنتاجه هو دليل تتوافر فيه المصداقية لقبوله كدليل (اثبات)) [60].

وقد ظهرت الصورة الأولى للمحكمة الالكترونية في الولايات المتحدة الامريكية وذلك بتسوية منازعات التجارة الالكترونية عن طريق استخدام شبكة الانترنت (التحكم الالكتروني) واستخدام برنامج القاضي الافتراضي في آذار 1996. ويقوم القاضي الافتراضي المتخصص بالتحاور /مع أطراف النزاع الذين طلبوا الخضوع لأحكام هذا النظام عن طريق البريد الالكتروني عن ان يفصل النزاع خلال (72) ساعة[61].

❖ القضاء الفرنسي

- منذ 1977 ذهبت محكمة النقض الفرنسية بأدانة موظف يعمل في مؤسسة (Legobax) لقيامه بنسخ معلومات سرية تعود للمؤسسة من جريمة السرقة.
- و القضاء الفرنسي فرض اختصاصه على جرائم وجنح المخالفات المعلوماتية حتى لو ارتكبت الجريمة خارج الأراضي الفرنسية او أحد اركان الجريمة فقد أصدرت احدى المحاكم الفرنسية قرارها المتضمن (تطبيق القانون الفرنسي وبالتالي المحاكم الفرنسية إذا كان مركز البث او الجهاز الخادم موجوداً خارج الاقليم الفرنسي مما تظهر فيه هذه الرسائل التي يقوم الجهاز ببثها في فرنسا[62].

و نجد هنا تقارب يتقرب القضاء الفرنسي مع القضاء الأمريكي.

- اما مجلس الدولة الفرنسي فقد أشار في دراسة له صادرة حول الانترنت والشبكات الرقمية في 1998/7/2 الى الموضوعات الهامة الواجبة الحماية وقد كان في مقدمتها ضرورة حماية المعلومات الشخصية والحياة الخاصة على الشبكات والتي تعد احدى المسائل الأكثر حساسية في نظر المستخدمين وقد خلصت الدراسة في توصلها الى ان

حماية المعلومات الشخصية أصبحت مهددة إزاء مخاطر جديدة في بيئة الشبكات الرقمية[63].

لكن محكمة استئناف باريس فلها اتجاه مغاير لموقف مجلس الدولة السابق في نظرها ان الأموال المادية وحدها يمكن ان تكون موضوعاً لجريمة السرقة والمعلومات لا يمكن ان تكون محلاً للسرقة فقد قضت في احد احكامها ببراءة احد الصحافيين الذي وجهت له تهمة السرقة على اثر نشره لمعلومات تقنية تساعد القرار على فك شفرة البرامج التلفزيونية حيث اعتبرت محكمة الاستئناف بباريس ان جريمة السرقة غير قائمة ما دام فك الشفرة لا يترتب عليه نقل البرامج المحمية من حيازة المالك لها ولا من حيازة المشاهدين المستفيدين ما دامت الشركة تستمر في بث برامجها وما دام الشاهد المنخرط يستمر في استقبال البرامج التلفزيونية[64].

- فيتضح مما تقدم ان القضاء الفرنسي تقيد بمبدأ الشرعية الجنائية وما يترتب عنه من اعتماد التفسير الضيق للنص الجنائي.

ولكن بمرور الزمن نجد ملامح التغيير بدأت على اتجاه القضاء الفرنسي فقد ذهبت الغرفة الجنائية بمحكمة النقض الفرنسية تأييد ادانة مستخدم من اجل سرقة المعلومات عبر نسخها من الوثائق ما دام انه حصل على النسخ دون رضى صاحبها واخرجها بسوء نية ولا يشترط لدى الجاني نية الاضرار[65].

❖ القضاء البلجيكي

وللقضاء البلجيكي موقف فريد ومميز بهذا الشأن حيث انه يميز بين المعلومات وبين البيانات التي تتم معالجتها الكترونياً فيعتبر الأولى مجرد أفكار غير مادية ومن ثم لا سبيل لاختلاسها اما البيانات المعالجة الكترونياً فتتحدد في كيان مادي يتمثل في ذبذبات او إشارات الكترونية ممغنطة يمكن تخزينها على وسائط ونقلها فضلاً عن إمكانية تقديرها كماً فهي ليست معنوياً كالحقوق والآراء بل شيئاً له وجود مادي ويمكن قياسها[60].

وبعد ان نص القانون البلجيكي رقم 23 لسنة 2000 في مادته (88) على اعتبار البيانات الالكترونية كدليل اثبات في حالة وقوع جريمة او يمثل خطر على الأنظمة الالكترونية كما اجازت هذه المادة لقاضي التحقيق في حالة امتداد البحث الالكتروني عن ادلة الجريمة خارج نطاق بلجيكا ان يحصل على نسخة من البيانات التي يحتاجها حتى وان تم ذلك دون اذن الدولة[67].

❖ **القضاء السويسري**

سبق وان أدين هذا القضاء السيد لوزارينكو بتاريخ 2000/1/29 بالحبس لمدة (15) شهراً لقيامه بأنشطة الانترنت لأجل غسل أموال بحوالي (880) مليون دولار للفترة بين 94-97 من بينها (170) مليون تم غسلها عبر حسابات سويسرية[68].

- ويرى القضاء الكندي بأن الحل الوحيد لفرض سيطرته على هذه الجرائم بتغيير التشريعات انطلاقاً من مبدأ لا جريمة ولا عقوبة الا بنص.

فجاء على لسان القاضي (Kerr) قاضي محكمة الاستئناف الكندية في معرض تسببه عن احكامه ببراءة متهم في جريمة معلوماتية.

(ان الحل الوحيد في يد المشرع الذي عليه تغيير القانون لان المحكمة ليس لها محاولة مط القوانين القديمة).

المطلب الثاني

موقف القضاء العربي

ان محاولات تطبيق القانون على الجرائم الالكترونية وغش الحاسوب تقف امامه جملة عوائق قانونية في مقدمتها مبدأ حضر القياس في القانون الجنائي الموضوعي ومبدأ الشرعية لذلك تباين موقف القضاء العربي إزاء ذلك نوضح هذا خلال النقاط التالية:

1- القضاء اللبناني

يطبق القانون اللبناني مواد ونصوص قانون العقوبات على الجرائم الالكترونية فواجه القضاء اللبناني في عام 2000 قضية تعرض خطير للآداب والاخلاق 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 الكترونياً ذات كيان مادي تصلح محلاً للسرقة ففي سنة 2001 أصدر القاضي الجزائي حكماً ادان بموجبه احد الأشخاص لأقدامه على نقل وتقليد معلومات مخزونة على أسطوانات مرنه (Floppy Disk) تخص شركة مدعية وايضاً طبق قانون العقوبات المادة (722) [69].

- اما بالنسبة للقانون الواجب التطبيق فقد اجزم القضاء اللبناني حيث ادخل باختصاصه الجرائم الالكترونية بمجرد حصول أحد اركان الجريمة على الأراضي اللبنانية او 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 اية شركة انترنت أخرى.

- والاتجاه الحديث للقضاء اللبناني يختلف عن السابق ففي عام 2008 ادانت محكمة القضاء الجزائي اللبناني اشخاص بجرائم السرقة استناداً الى المواد (636-219) عقوبات على اعتبار انهم أقدموا على الدخول الى حسابات بعض الأشخاص في الولايات المتحدة الامريكية عن طريق الانترنت تمهيداً للاستيلاء على الأموال وبالاتفاق سابق مع القراصنة لقاء عمولة.

وقد توسع القضاء اللبناني في تجريمه بالأفعال المرتكبة بواسطة الحاسوب والانترنت فشمل جرائم القذف والسب ايضاً 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[70].

2- القضاء العماني

فقد اقر هذا القضاء على المساواة بين الأدلة التقليدية والأدلة المتولدة من الحسابات الالية.

وطبق قانون الجزاء العماني على الجرائم المعلوماتية بعد ادرجها في المادة (276) ضمن مواد القانون رقم (72) لسنة 2001.

ففي القرار المرقم (72) المؤرخ في 2002/10/29 قررت المحكمة العليا لسلطنة عمان (ان تقدير الدليل بالصورة التي تكشف قناعة المحكمة من اطلاقات محكمة الموضوع لا تجوز اثارته امام المحكمة العليا[71].

- اما فكرة عدم جواز ان 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 ان يستمد هذا الاقتناع من مصادر يستخلصها بنفسه من التحقيق بالدعوى.
- وأكد ما سبق في قرار آخر برقم (51) في 2004/4/13 حيث جاء فيه: (كل دليل تعتمد عليه المحكمة في حكمها يجب ان يكون قد طرح شفوياً في الجلسة ويستمد القاضي إقناعه من هذه المناقشات).

3- القضاء المصري:

أثار جدلا أو تساؤل امام القضاء المصري مدى اعتبار التحويل الالكتروني للاموال من قبيل التسليم المحقق للنتيجة في جريمة الاحتيال.

فحسمت المحكمة العليا ذلك الجدل بقرار لها جاء فيه " بأن تعبير المال الوارد بالمادتين 133 عقوبات المصري الخاص بخيانة الامانة و134 عقوبات الخاص بالاحتيال يشمل النقود الكتابية وبالاستناد الى اعتبار التسليم غير متطلب له المناولة المادية وحسب ما هو مستقر في الفقه المصري والفرنسي[72].

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[73].

وان الاستيلاء عن طريق تحويلات الكترونيه 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[74].

والجدير بالذكر بان محامي المحكمة العليا في مصر الدكتور (محمد صالح العادلي) قد أطلق مصطلح الابن الغير شرعي على الجريمة الالكترونية التي جاءت نتيجة للتزاوج بين ثوره تكنولوجيا المعلومات مع العولمة او الممارسة السيئة لثوره لتكنولوجيا المعلومات[75].

وحديثا فقد استقرت محكمه النقض المصرية على اعتبار الذبذبات او الموجات الهاتفية مال منقول يمكن اختلاسه لأنه قابل للحيازة والنقل وبالتالي للسرقة[76].

فوصف المال لا تقصر ما كان جسما متحيزا قابلا للوزن طبقا للنظريات الطبيعية بل يتناول كل شيء مقوم قابل للتملك والحيازة والنقل من مكان لأخر*.

4- القضاء المغربي

في بداية الامر اتبع القضاء المغربي اتجاه القضاء المصري والفرنسي المتمسك بالشرعية الجنائية فقد أكد في غير مره على ان: " 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 وغرامه قدرها 10,000,000 درهم وذلك لارتكاب الجاني جنحه الدخول الى نظام الحاسب لشخص اخر.
- وبنفس الاتجاه اخذت المحكمة الابتدائية بالرباط بتاريخ 11|10 |2012 في قضية شركة كوماناف فيري عندما ادانت متهمين بالحبس ثلاث سنوات وثمانية أشهر لقيامها باصطناع اذونات سفر مزوره عن تغيير المعطيات المضمنة بنظام المعالجة الالية 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[77].

5- القضاء الاردني .

بصدور قانون جرائم انظمه المعلومات لسنه 2010 الاردني اصبحت الجرائم التي ترتكب داخل المملكة الأردنية يطبق هذا القانون عليها وتدخل ضمن دعاوى القضاء الاردني فقد قضى فيه أحد قراراته: " يجوز اقامه دعوى الحق العام والحق الشخصي عن المشتكي عليه امام القضاء الاردني إذا ارتكبت اي من الجرائم المنصوص عليها في هذا القانون باستخدام انظمه معلومات داخل المملكة او الحقت اضرارا بأي من مصالحها او بأحد المقيمين فيها او ترتبت اثار الجريمة فيها كليا او جزئيا إذا ارتكبت من أحد الاشخاص المقيمين فيها.

*علماً ان مصر وحدها شهدت حوالي 100 قضية شواذ جنسية واباحية ونصب واحتيال 2005.

واجاز القانون لموظفي الضابطة العدلية تفتش الاجهزة والادوات والبرامج والانظمة[78].

6- القضاء التونسي

لقد تمسك القضاء التونسي بمبدأ الشرعية والتأويل الضيق للنص الجزائي ففي قرار صادر عن محكمه التعقيب التونسية بالدعوى المرقمة 16065 بتاريخ 24 ابريل 2002 والذي تتلخص وقائعه بقيام شخص بحيازة عملة اجنبية بحكم خبراته بالانترنت وقدرته بفتح رموز سريه لبطاقات رقميه اصليه وبعد احالته الى القضاء فقرر الاخير بعدم سماع الدعوى وترك سبيله بناءا على انتقاء الركن الشرعي للجريمة وصادقته محكمة الاستئناف[79].

7- القضاء العراقي

في غياب قانون المعلومات العراقي لم يتوانى القضاء العراقي عن لعب دوره بشكل فاعل فلم يقف ذلك حائلا امام معالجته للجرائم الالكترونية حيث نجحت المحاكم العراقية في تسوية الحالات المعروضة امامها من خلال التشريعات النافذة كتطبيق قانون العقوبات رقم 111 لسنه 1969 المعدل[80].

او قانون المطبوعات رقم 206 لسنه 1968 الذي يخص الصحف والمجلات

اما بخصوص العقوبات التي تفرضها المحاكم فهي " التعويض " لانها محاكم براءة تنظر في الدعاوى المدنية او الحبس مده لا تقل عن 5 سنوات في حاله وجود جنحه.

وقد اجاز قانون المحكمة الجنائية العراقية لسنة 2005 للمحكمة ان تستعمل الوسائل الالكترونية للتوصيل السمعي او البصري كالبريد الالكتروني وما الى ذلك من الوسائل الالكترونية الاخرى.

ومن هنا يظهر ضرورة انشاء محكمة متخصصة في هذا النوع من الجرائم وتوفير كادر متدرب وذو كفاءة عالية للتعامل مع هكذا جرائم[81].

الخاتمة

وجدنا من خلال بحثنا المتواضع هذا ان معدلات الجريمة الالكترونية على المستوى العالمي في تزايد مستمر ففي بريطانيا وحدها عام 2007 هناك جريمة الكترونيه تقع كل 10 ثواني اي ما يعادل 3 مليون جريمة بالسنة او 8 الالف جرمه باليوم وأكبر نسبه تعود لجرائم التحرش الجنسي 850 ألف حاله وهنالك 92 ألف حاله لسرقه الهوية اي الحصول معلومات شخصيه حول مستخدمي الانترنت و145 ألف حاله لاختراق

الحواسيب بهدف سرقه المعلومات و207 ألف حاله للحصول على الاموال خلال الاحتيال على ارقام البطاقات الائتمانية.

وبعد الاطلاع ودراسة القواعد القانونية المتعلقة بالمعاملات والجرائم الالكترونية اكتشفنا بوجود نقص وخاصة على المستوى الجزائي فرغم ان القانون وفي إطار سعيه الى حماية الحقوق من الاعتداءات على نظام المعالجة المعلوماتية والالكترونية وتجريم العديد منها وتخصيص عقوبات ماليه وبدنيه إلا انها لا تكفي بل لابد من تدخل المشرع بتعديلات كبيره لمواجهة هذه التحديات لهذا النوع من الجرائم المتطورة

والمحتمل ان تنتشر في البيئة العربية كبيرا باعتبار ان الجاهزية التقنية والتشريعية والادائية لمواجهتها ليست بالمستوى المطلوب رغم انها من اهم وأخطر جرائم العصر.

وفي ختام دراستنا توصلنا الى عده توصيات منها:

1- ضرورة ايجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجه الجريمة الالكترونية والعمل على التوفيق بين التشريعات التي تناولتها من خلال الاتفاقيات الدولية لمعرفه مصادر المواقع العلمية فيما فيها التواصل الاجتماعي.
2- ادخال تعديلات على وسائل البحث والتحقيق لاسيما وان هذا النوع من الجرائم لا تترك اثارا بعد ارتكابها ومن المهم جدا تقليص او اهمال الاجراءات الروتينية الكثيرة والتي تتطلب وقت طويل.
3- الاسراع بسن قوانين متكاملة خاصة لطبيعة الجريمة الالكترونية المتطورة او تعديل القوانين الجنائية ليتم ادخال هذه الجرائم في إطار قانوني ويتم تجريم كل ما يشملها عن عمليا احتيال ونصب وملكيه فكريه واختراق اجهزه الاخرين
4- وضع استراتيجية كاملة تشارك فيه جميع الاجهزة ذات العلاقة وبحث سيل تطوير هذه الاجهزة ماديا وبشريا لسعف الجهات التحقيقية في انجاز عملها على هذا الصعيد
5- انشاء مكتب رئيسي في وزاره الداخلية لمكافحه الجرائم الالكترونية على غرار المكتب المركزي للجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات الفرنسي لسنه 2000
6- وجدنا بان المشرع السوداني هو السباق لإنشاء شرطه ومحكمه خاصة بهذا النوع من الجرائم ذات كادر وضيفي وقضائي يتدرب على اعلى المستويات وايضاً المشرع التونسي بادر بوضع اطار قانوني للمتدخلين في المجال الالكتروني كالقانون رقم 442 لسنة 1993.

7- الاهتمام بالأدلة الرقمية واعتبارها ادله اثبات واعطائها الحجية القاطعة
8- تهيئه رقابة على شبكات الانترنت لحذف الافكار التي لا تتفق مع المفاهيم اللاأخلاقية للدول
9- اجراء دورات تدريبيه منتظمة للقضاة واعضاء الشرطة وتحديث رجال الادعاء العام وحتى المحامين تختص بالتعامل مع أجهزة الحاسوب .
10-ضرورة اعاده النظر في قانون اصول المحاكمات الجزائية وقانون الاثبات لاختلاف وسائل اثبات هذه الجرائم عن الجرائم العادية.
11-استقطاب خريجي كليات الحاسوب من قبل وزارة العدل وتعميم اسلوب المحاكم الالكترونية في عموم العراق لتسيير الاجراءات والابتعاد عن الوسائل الورقية.
12-تعديل قانون الارهاب رقم 13 لسنه 2005 يتضمن مواد تعالج الجرائم الالكترونية كما فعل قانون الارهاب الخاص بإقليم كردستان المرقم (3) لسنة 2006.

الهوامش

(1) انظر المعجم الوجيز لابن منظور / مجمع اللغة العربية / القاهرة / 1452
(2) المائدة. الآية 7.
(3) انظر تقرير مكتب التقييم الفني في الولايات المتحدة مشار اليه عند عبد الاله احمد الهلالي / التزام الشاهد بالأعلام في الجرائم المعلوماتية (دراسة مقارنة) /ط1/دار النهضة العربية /سنة 2000/ ص14
(4) د. عبد العال الديرني / الجريمة المعلوماتية اسبابها وخصائصها / مقالة منشورة في 13 يناير 2013 /ص2.
(5) TGL Paris 1ch.correctionelle 16 Dec.1997,minister publique C.Glovanisky , dis,Enligne.en Dec.2000,a:http://www.Legalis.net.
وايضاً عبد القادر المولي/الجريمة المعلوماتية /الطبعة الثانية/دار الثقافة للنشر والتوزيع/2010/ص48.

(6) د.سومية العكور/الجرائم المستخدمة في ظل المتغيرات والتحولات الاقليمية والدولة ورقة عمل مقدمة للمتلقى العلمي للفترة 2-4-/2014 /ص3.
(7) تعريف مجموعة خبراء منظمة التعاون الاقتصادي والتنمية لعام 1983.
(8) Donn Parker –cyber crime and general prin aples 19 August 2008/Page .18 Cyber crime andreal world society by lati the Sridhar.
(9) محمد امين الشوابكة / جرائم الحاسوب والانترنت / الطبعة الاولى / 2009 / ص8.
(10) د. فائزة بابا خان / مقالة مشروع قانون الجريمة المعلوماتية العراقية / العدل نيوز / منشور في 2012/12/22 /ص1.

(11) Tom Foreter ,Essential problems to Hig-Tech society first Mitpres edition , Cambridge-massachusetts,1989-p.104

(12) محمد امين الشوابكة /جرائم الحاسوب /دار الثقافة للتوزيع والنشر /ط1/2009/ص8.

(13) د.آمال حسن / جرائم المعلوماتية / مقال منشور في 2014/2/1/ ص3.

(14) محمد علي قطب / الجرائم المعلوماتية / بحث مقدم الى مركز الاعلام الامني / الاردن/ 2008 /ص12.

(15) هذا التعريف ورد في قانون الكيان الصهيوني رقم (5755) لسنة 1995 في شأن جرائم الحاسوب.

(16) د.سومية عكور / ورقة عمل للملتقى العلمي للجرائم المستحدثة / الاردن وعمان / 2014 /ص4.

(17) د.سومية عكور / ورقة عمل للملتقى العلمي للجرائم المستحدثة / الاردن وعمان / 2014 /ص4.

(18) انظر القاضي مهدي عبود هادي / قاضي محكمة الاعلام والنشر في العراق / مقال منشور في 2013/9/6 /ص1.

(19) www.gahtan.com.cyber law fnegclopedia.

(20) cyber law and information technology by telwant singh addl.Distt and sessiens Judge .Delhi.

(21) خالد ممدوح ابراهيم/الجرائم المعلوماتية / دار الفكر الجامعي/ط1/2009/ص88.

(22) د. عبد العال الديري /الجريمة المعلوماتية / المصدر السابق /ص3.

(23) محمد حماد مرهج البهيتي / التكنولوجيا الحديثة والقانون الجنائي / دار الثقافة للنشر والتوزيع / عمان 2004/ص165.

(24) في واقعة حدثت في المانيا حيث استولى مبرمج يعمل في احدى الشركات على (22) شريطاً ممغنطاً تحوي معلومات هامة بخصوص عملاء وانتاج هذه الشركة وهدد ببيعها للشركات المنافسة مقابل فدية 200,000 دولار

(25) Steven levy :Hackers (Heroes of the computer revolution) 1984 /p104.

(26) Frades informatiques introductionsfrauduleuses de donnee's et intrusions,note sous crime.10 avril 2013,n''(2-85618) Qpc et Versailles.

Dr.Francillon,Les crimes informatiques et de eutres crimes dans le domaine de letechnologie in foretique en france int pen,1990,vd,P293.

(27) محمود احمد كبانة / جرائم الحاسوب وابعادها الدولية / دار الثقافة للنشر والتوزيع / ط1/2009/ص155.

(28) مصطفى محمد موسى / التحقيق في الجرائم الالكترونية / مطابع الشرطة / الطبعة الأولى/القاهرة /ط1/ص15.

(29) د. هلالي عبد الله احمد الجوانب الاجرائية والموضوعية لجرائم المعلوماتية في ضوء اتفاقية بودابست / دار النهضة العربية / القاهرة 2003 ص7 وما بعدها.

(30) Myriam Quememea. Cyebrerininellt's droit penel opp.econonieca September P.208.

(31) حسين بن سعيد بن سيف الظاهري / الجهود الدولية في مواجهة جرائم الانترنت /ورقة اعتماد مقدمة للاتحاد العربي للتحكيم الالكتروني لعام 2007 / ص2.

(32) و لعل التعريف الذي وصفته لجنة تدقيق الحسابات والذي ارتكزت عليه لجنة اوديت البريطانية بشأن غش الحاسوب فهي كل سلوك احتيالي وخداعي مرتبط بالكومبيوتر .

(33) TGL Paris 1ch.correctionelle 16 Dec.1997,prerioul refrence , publique C.Glovanisky p.160

كما اشار قانون الاتصالات السمعية والبصرية الفرنسي الصادر في 1986/9/30 في مادته الاولى الى مصطلح المعلومات عند تعريفه الاتصال عن بعد بأنها كل تعامل وكل ارسال او استقبال للمعاملات والاشارات او الخطوط المكتوبة والصور للمزيد / انظر عبد الله حسن علي محمود /الجريمة المعلوماتية المصدر السابق /ص150.

(34) د. عبد العال الديري / الجريمة المعلوماتية / المصدر السابق /ص3و هو اتجاه القانون البلجيكي المرقم 23 لسنة 2000 في مادته (88).

(35) من هذه القوانين القانون رقم 2/18 في 23 فبراير /2009. والقانون 2/14 الصادر في 2006/2/20 والقانون رقم (5053) المتعلق بالتبادل الالكتروني للمعطيات القانونية الصادر في 2007/10/6.

(36) لطفي بن كريم / التجربة التونسية في مجال تنظيم المعاملات المدنية والتجارية الالكترونية / بحث منشور لمنتديات ستار تايمز في 2012/2/26 /ص80.

(37) لطفي بن كريم / التجربة التونسية في مجال المعاملات المدنية والتجارية الالكترونية المدنية والتجارية الالكترونية / المصدر السابق /ص9.

(38) محمد ابو العلا عقيدة / التحقيق وجمع الادلة في مجال الجرائم الالكترونية / مقالة مقدمة لمنتدى المنصورة / بتاريخ 2007/6/25 /ص12.

(39) انظر المواد (3–10) من القانون السعودي اعلاه.

(40) جميل وعبد الباقي الصغير / الجوانب الاجرائية للجرائم المتعلقة بالانترنت / دار الفكر العربي / القاهرة / سنة 2001/ص73.

(41) انظر المواد (4–8) من القانون السابق الذكر.

(42) المادة 28–29–30 من القانون السابق الذكر.

(43) القانون الاردني السابق هو قانون المعاملات الالكترونية عاقب في المادة (38) بالحبس ثلاث اشهر او بغرامة لكل من نسخ او غير او حذف المعلومات المخزنة.

(44) انظر المادة 3–7–16 من القانون اعلاه.

(45) انظر المادة(27) من قانون مكافحة الجرائم الالكترونية السوري لسنة 2010.

(46) م34 من القانون اعلاه.

(47) المادة (34) من قانون مكافحة الجرائم الالكترونية القطري لسنة 2010.

(48) المادة (4) من قانون مكافحة الجرائم الالكترونية القطري لسنة 2014.

(49) المادة 27 عاقبت بالحبس او الغاء اجازة الطبع اذا شكل المنشور خطر للمصلحة العامة.

(50) و كانت الفقرة الثالثة منه تنص على الابتزاز المالي وبأية وسيلة كانت.

(51) د.يونس عرب/ بحث جرائم الكمبيوتر والانترنت / ورشة عمل لتطوير التشريعات في مجال مكافحة الجرائم الالكترونية/ سلطنة عمان / 2006/2/24/ص40.www.monamallanswer.24937

(52) د.يونس عرب / الجرائم الالكترونية / المصدر السابق / ص13.

(53) د.عبد العال / الجريمة الالكترونية بين التشريع والقضاء / بحث مقدم الى المركز العربي لابحاث القضاء الالكتروني بتاريخ 20132/3/1 /ص5.

(54) خالد عرب مصطفى / جرائم الحاسوب / المصدر السابق /ص73.

(55) محمد جمال مرهج البهيتي / التكنولوجيا الحديثة والقانون الجنائي /دار الثقافة للنشر والتوزيع / عمان/2004/ص165.

(56) .Dr.Mike Mc Guire (Home office science) October 2013.p.5

(57) the Hacker crack down law and disorder on the electronic frontier by bruce.

(58) the Hacker crack down law and disorder /1994/P.159

(59) World information technology and services allionce (witsa) statement on the council of europe droft convention on cyber-crime.

(60) حكم المحكمة العليا الامريكية في قضية داو بورت ضد شركة ميريل للصناعات الدوائية عام 1993 مشار اليه في بحث/ طارق محمد الجميلي / الدليل الرقمي في مجال الاثبات الجنائي/ منتديات ستار تايمز في2012/2/26 /ص20.

(61) طبق هذا النظام في الصين والبرازيل /صفاء اوتاتي / المحكمة الالكترونية / مجلة جامعة دمشق للعلوم الاقتصادي / عدد 20122 /ص12 .

(62) شيماء عبد الغني / الحماية الجنائية للتعاملات الالكترونية / الدار الجامعية الجديدة / مصر/2007/ص376

(63) الشحات ابراهيم المنصور / الجرائم الالكترونية / دار الفكر الجامعي / الطبعة 1 /ص25 .

(64) د. سومية عكور / الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية / المصدر السابق /ص18.

(65) TGl paris 1 ch. Correctionelle 16 Dec 1997 , ministere publique C.Glovanisky dis .Enligne en .Dec 2000,a:http:p.11.

(66) اتجاه محكمة بانفرس / بلجيكا / عندما قضت بأن برامج عمليات الانتاج الخاصة بالشركة تعتبر من عناصر ذمتها المالية وليست مجرد تعليمات ذهنية وهي قابلة للنقل ولها قيمة اقتصادية تصلح ان تكون محلاً للسرقة مشار اليه عند د.سومية عكور /الجرائم المستحدثة /المصدر السابق /ص18.

(67) Meunier : Laloidu 28 Nov.2000 relative a la criminalite informatique . Rev Dr. pe crime 2002,P.611.

(68) المحامي د. يونس عرب / الجرائم الالكترونية / ورقة عمل مقدمة لورشة عمل تطوير التشريعات في مجال مكافحة الجريمة الالكترونية /عمان /ص8 .

وفي قضية اخرى ادين بيتر كير تشينكوف الذي قام بعمليات غسل اموال تقدر ب1140 مليون دولار امريكي .

(69) القاضي فوزي خميس / الجرائم المعلوماتية في ضوء القضاء /بحث منشور بتاريخ 2008/2/23 /ص7.

وفي قضية اخرى صدرت عام 2005 حيث حكمت بالحبس على مرتكبي جرائم بيع اشرطة كاسيت واشرطة مقلدة وترويج برامج كمبيوتر غير شرعية.

(70) القاضي فوزي خميس / جرائم المعلوماتية في ضوء القضاء اللبناني / المصدر السابق /ص9.

(71) راشد بن محمد البلوشي / ورقة عمل مقدمة للمؤتمر الدولي لمكافحة الاجرام السبيري / فرنسا 2008.

(72) ابو بكر سليمان / جرائم الحاسوب واساليب مواجهتها / مجلة الامن والحياة / العدد 21 /لسنة 19 / 1421 هـ /ص38 .

(73) المحامي د. يونس عرب / بحث مقدم لورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية /ص29.

(74) المحامي د. يونس عرب / بحث مقدم لورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية /ص29.

(75) ورد في بحث للدكتور ابو بكر سليمان / جرائم الحاسوب / المصدر السابق /ص1.
علماً ان مصر وحدها شهدت حوالي 100 قضية شذوذ جنسية واباحية ونصب واحتيال 2005.

(76) رقم القرار 69/1155 ق بتاريخ 2000/1/2 والقرار رقم 2591 – ق في 1998/3/4 منشور لدى زين العابدين عواد كاظم / بحث منشور في مجلة المثنى /العدد السادس. ص102.

(77) حكم المحكمة الابتدائية بالدار البيضاء / صادر بتاريخ 2008/1/3 بالدعوى المرقمة 8/293 منشور لدى سومية عكور / الجرائم المستحدثة في ظل المتغيرات/ المصدر السابق /ص20.

(78) أنظر المواد (16–12) من قانون جرائم أنظمة المعلومات لسنة 2010 الأردني.

(79) د.لطفي عبد كريم / التجربة التونسية في مجال تنظيم المعاملات / المصدر السابق / ص20.

(80) القاضي مهدي عبود هادي / مقالة حول قانون الجرائم المعلوماتية / نشر في 2013/9/6.

(81) د.فائزة بابا خان / جريمة الانترنت / بحث منشور في مجلة العدل نيوز في 2012/12/22.