جامعـــة زيان عاشور بـــالجلفة

كلية الحقوق والعلوم السياسية

قســم الحقـــوق

الجرائـم الاقتصادية في الأوساط المعلوماتية

مذكرة ضمن متطلبات

نيل شهادة الماستر حقوق تخصص إدارة و مالية

إعداد الطالب:

- فكرون محمد

إشراف الأستاذ:

– الدكتور: اسعد المحاسن لحرش

لجنة المناقشة :

1- د. شلالي رضا..... رئيسا.
2- د. احمد بن الصادق..... مقررا.
3- د. لحرش اسعد المحاسن.... مناقشا.

السنة الجامعية 2017/2016

جامعة زيان عاشور بالجلفة

كلية الحقوق والعلوم السياسية

قسم الحقـــــوق

الجرائم الاقتصادية في الأوساط المعلوماتية

مذكرة ضمن متطلبات

نيل شهادة الماستر حقوق تخصص إدارة ومالية

إعداد الطالب:

– فكرون محمد

إشراف الأستاذ:

– الدكتور: اسعد المحاسن لحرش

لجنة المناقشة :

د. شلالي رضا..... رئيسا.

د. احمد بن الصادق..... مقررا.

د. لحرش اسعد المحاسن.... مناقشا.

السنة الجامعية 2017/2016

شكر العرفان

أتقدم بالشكر الجزيل إلى الدكتور الفاضل

لحرش أسعد المحاس

الذي تفضل بالإشراف على إعدادي لهذه المذكرة ولم يدخر جهدا بتوجيهاته

وإرشاداته القيمة

جزاه الله عنا كل الخير

إلى جميع أساتذة جامعة زيان عاشور بالجلفة وبالأخص أساتذة قسم الحقوق

ودون أن أنسى أعضاء اللجنة المشرفة الموقرة

وشكرا

الإهـــــداء

إلى روح من فرحت بقدومي إلى الحياة وغمرتني بفائض حبها ولم تنساني بدعائها

..... روح أمي رحمها الله

إلى روح من منحني رعايته وأفتخر بأني من صلبه وأحمل اسمه ... روح أبي رحمه

الله

إلى الزوجة الكريمة والأبناء الأحبة مخلوف .فاطمة .أيوب .شروق .إسراء

إلى إخوتي وأخواتي

إلى الأصهار جميعا

إلى كل من آزرني وساعدني في هذه المرحلة الدقيقة

الى جميع الطلبة الذين تعرفت عليهم بالجامعة .

مقدمة

مقدمـة:

يشهد العالم في الوقت الراهن ثورة تكنولوجية هائلة تتجلى أبرز مظاهرها في ثورة المعلومات والاتصالات والأجيال الجديدة للحسابات الآلية.

ولا شك في أن هذه التكنولوجيا الحديثة تقدم للدول وأجهزتها الكثير من التسهيلات والإمكانيات التي تهتم في رفع كفاءتها وتطوير قدراتها في جميع الميادين إلا ان هذا التطور التكنولوجي أدى ويؤدي في الوقت نفسه إلى تطوير وتحديث جريمة من حيث الأساليب والمضامين وبخاصة في ظل أنشطتها وممارستها الإجرامية وفي هذا الصدد تقول روي جودسون خبيرة بمركز المعلومات الوطني الامريكي ((لقد اصبحت الجريمة أكثر قوة بفضل التقنية الحديثة)) .

فالإعلام الآلي الذي ارتقى بمستوى الانسان وانتقل به الى عصر المعلوماتية والتقدم هو ذاته الذي يستخدمه بارونات الجريمة وعصابات المافيا ، فإذا كانت الاسلحة المتطورة والمعدات الحديثة من الامور

الشائعة الاستخدام في ممارسة الجريمة فان الجديد في هذا المجال هو تكثيف استخدام نظم المعلومات والاتصالات الحديثة في الانشطة الاجرامية لتمكينها من التخطيط لأنشطتها وتنفيذها .

فالمعلوماتية مثل لكل تطور جديد تحمل في طياتها جانبا مظلما تتجسد في مجال القانون الجنائي بظهور المجرم المعلوماتي أو ظاهرة الاجرام المعلوماتي بصفة عامة . اذ لم يعد مجرم القرن الأخير انسانا مقنعا فيشهر سلاحه في وجه ضحيته بل رجلا ذا باقة بيضاء فالصراع قائم بين العلم والجريمة صراع مستمر بين استخدام العلم من أجل الانسان وأمنه واستقراره وبين استخدامه ضد الانسان وزعزعة أمنه واستقراره لذلك فوسائل الاعلام لا تخلوا اسبوعيا من الاخبار المتعلقة بأمن الشبكات الحاسوبية فالحرب مستمرة بين يدي الكمبيوترات والمختصين الا ان الشبكات أو ما أحدثته من خسائر مادية عبر العالم مما أدى إلى تسليط الأضواء على جريمة الحاسوب.

فمع تزايد نسبة الجرائم الاقتصادية في الأوساط المعلوماتية وتنوع طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة اكثر مما تسببه الجرائم الأخرى ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل كبير على الاقتصاد العالمي ككل.

ما يواجهه العالم اليوم هو هجوم شرس من أشخاص أو مجموعات أو منظمات مخترقة هدفها الرئيسي الربح المادي بالإضافة إلى أهداف أخرى وذلك بالاستفادة من توسع استخدام الكمبيوتر والانترنت .

وقد أشارت توقعات بأن الجرائم الاقتصادية في الوسط المعلوماتي قد تسببت بخسائر دول مجلس التعاون الخليجي ما بين 55 مليون و 755 مليون دولار أمريكي سنويا.

كما أكد اقتصادي متخصص أن معدل نسبة الجرائم الالكترونية في العالم تصل الى 57.6 % حيث يكلف الاقتصاد العالمي ما يقارب 12.950مليار دولار سنويا، وقال أن نسبة معدل الهجمات الالكترونية في السعودية ما يقارب47.8% لعام2009.

كما كانت نسبة الهجمات للحسابات الشبكية للأفراد عام 2009 بلغت 40% واختراق المواقع بلغ 63% ورسائل الاحتيال 43%، كما كشفت السلطات الامريكية عام 2009 ان عمليات القرصنة والسرقة طالت اكثر من 130 مليون بطاقة ائتمان وبطاقة حساب مصرفية.

حيث رصد 100 تهديد الجريمة الالكترونية وأظهر تقرير نشرته سمانتك كوربوريشن تزايدا مطردا في هجمات للجريمة الالكترونية في الثانية خلال عام 2009 وفي دراسة أجرتها شركة فورتن الرائدة في تطوير الحلول المبرمجة الامنية أن ثلثي مستخدمي الأنترنت حول العالم تعرضوا لجريمة الكترونية على الاقل مرة واحدة وقد تمثلت في هجمات فيروسية وتجسسيه واحتيالية لسرقة بطاقة الائتمان أو البيانات المصرفية.

إلا أن تهديدها الحقيقي يبقى على الاقتصاد ولأهمية المعلومات يسعى المنتمون لمجتمع الأعمال بكل ما أتو من قوة من أجل الحصول عليها سواء بالطرق المشروعة أو غير المشروعة الامر الذي أدى بالبعض إلى التقرير بوجود سوقين لشراء المعلومات إحداهما شرعي والثاني يطلق عليها السوق السوداء للمعلومات الذي يرتبط بالجانب الأكبر من الجرائم التي تستهدف الانشطة الاقتصادية في العالم ويمكن أن تتحقق بالنسبة للمعلومات المالية التي تتصل بالوضع المالي والإداري وتداول رؤوس الاموال والاستمارات في المنشآت الاقتصادية سواء كانت عامة او خاصة ويمكن ان تتحقق أيضا بالنسبة للمعلومات التجارية والصناعية والتي تنقلت بالسوق والمشروعات الاستثمارية والصناعية والانتاج والتجارة والتوزيع وكذلك بالنسبة للمعلومات المخزنة في ذاكرة الحاسبات الموجودة في البنوك والمؤسسات الاقتصادية .

اهميـة الدراسة :

الدراسة تستمد اهميتها من كونها

اولا : تتعلق بموضوع اصبح يشهد اهمام الباطلين والعاملين على انقاذ القانون وذلك لخطورة الجرائم الاقتصادية في الاوساط المعلوماتية وانعكاساتها المدمرة على مجالات الاقتصاد والمال والاعمال .

ثانيا : ان هذا الموضوع لم تتناوله الا القليل من الدراسات مما يقتضي ايلائه مزيدا من الاهتمام والدراسة الأكاديمية .

الإشكالية:

وعليه فيكون طرح الإشكالية التي مفادها : **الى اي مدى يمكن اعتبار المعلوماتية موضوعا للجرائم الاقتصادية وما دور المشرع الجزائري و المشرع الدولي في مكافحة هذه الظاهرة ؟**

و يندرج تحت هذه الاشكالية التساؤلات الاتية:

. هل ينطبق وصف الجريمة التقليدية على تلك المعلوماتية و هل يمكن تطبيق اركان الجرائم التقليدية ذات الطبيعة المادية و الملموسة على تلك القيم غير المادية المتولدة عن الجرائم الاقتصادية في الاوساط المعلوماتية؟

اهداف الدراسة :

يسعى هذا البحث الى تحقيق هدفه الرئيسي المتمثل في محاولة تقديم دراسة تكشف عن اهم التحديات القانونية وذلك عبر رصد الظاهرة الاجرامية الاقتصادية في الاوساط المعلوماتية ولتقيق هذا الهدف سنحاول القاء الضوء على عدد من المفاهيم المرتبطة بهذه الظاهرة وهذا على النحو التالي:

1. التعرف على الطبيعة الاجرامية للجريمة المعلوماتية في الوسط الاقتصادي.

2- محاولة التعريف بظاهرة الجريمة الاقتصادية في الاوساط المعلوماتية وخصائصها ومميزاتها

3. التطرق الى موقف التشريعات العالمية و المحلية من جرائم المعلوماتية

4- التطرق الى صور و مراحل حدوث الجرائم الاقتصادية في الاوساط المعلوماتية.

5- الوقوف على آثار الجريمة الاقتصادية في الاوساط المعلوماتية الوقوف على آليات مكافحة هذه الجرائم دوليا واقليميا ومحليا.

6- ابراز دور المشرع الجزائري من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

أسباب اختيار الموضوع :

يعود سبب اختيارنا لهذا الموضوع لكونه حديث تزامن مع التطور التكنولوجي لوسائل الاتصال والاعلام هذا من جهة ومن جهة أخرى نظرا لكونه من الجرائم الأكثر تعقيدا خاصة في ما يخص إشكالية

الاتيان بالأدلة المؤدية إلى إدانة المتهم أو تبرئته وأن الدليل في مثل هذه الجرائم في أغلب الأحيان ذا طبيعة خاصة أي طبيعة إلكترونية وكذلك إلى التأثير الواضح لهذه الجرائم على الاقتصاد العالمي والمحلي.

الدراسات السابقة :

أهم الدراسات السابقة في مجال الإجرام المعلوماتي إلى يومنا هذا في دراسات أجنبية باعتبار أن رصيد التشريع العقابي في هذا المجال في الدول الأجنبية ثري وأسست بالمقارنة حتى التشريع الوطني في حين أن الكتابات الوطنية اقتصرت فقط في الدراسات الجامعية.

- الصعوبات :

هناك صعوبات جمة تعترض الباحث في هذا النوع من الجرائم المستحدثة وذلك راجع الى حداثة استخدام الحاسب الآلي وما يتسم به من صيغة علمية بحتة غريبة في تصورنا على رجال القانون سواء كان على المستوى النظري او المستوى التطبيقي للقوانين مما يزيد من اهمية التشريعية لدراستنا.

المنهج المتبع:

سنعالج موضوع الجرائم الاقتصادية في الاوساط المعلوماتية متبعينا منهجا يتماشى وطبيعة الموضوع والمنهج الافضل في رأينا للخوض في هذا البحث هو المنهج الوصفي التحليلي لان دراستنا ستعتمد على وصف الجرائم المعلوماتية وتحليل اهم النصوص القانونية المنظمة لها في مختلف التشريعات و لأجل هذا الغرض قسمنا موضوع المذكرة الى فصلين

كما قلنا في الاشكال القانوني الى اي مدى يمكن اعتبار الجريمة المعلوماتية جريمة اقتصادية وما دور المشرع في مكافحتها..

الاجابة على هذا السؤال تظهر من خلال فصلين كما تتطلبه الدراسة التقليدية للجرائم وبالتالي ستضم المذكرة فصلين : الفصل الاول تحت عنوان الاطار المفاهيمي للجرائم الاقتصادية في الاوساط المعلوماتية حيث يندرج ضمن هذا الفصل مبحثين : الاول يحدد مفهوم الجرائم المعلوماتية واركانها.

اما الثاني : فيتطرق الى الصور والاثار المترتبة عن هذه الجرائم .

بالنسبة للفصل الثاني ارتأينا ان نلقي الضوء على مكافحة الجرائم الاقتصادية في الاوساط المعلوماتية من خلال التطرق لاهم الاتفاقيات والمعاهدات الدولية والقانون العربي النموذجي (في المبحث الاول) ثم سلطنا الضوء على دور المشرع الجزائري من خلال قانون العقوبات وخاصة القانون 09-04- المتضمن للقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال .

الفصل الأول

الإطار المفاهيمي للجرائم الاقتصادية في الأوساط المعلوماتية

تمهيد:

شهد العالم ثورة من نوع غير مألوف اصطلح على تسميتها بثورة المعلومات كان بطلها جهاز الحاسب الالي الذي تطور دوره بحيث تعدى اجراء العمليات الحسابية المعقدة ليشمل قضايا الناس في جميع

معاملاتهم، الا انه واكب هذه الثورة آثار سلبية تجسدت في الجرائم المستحدثة التي ترتكب عن طريق الوسائل التقنية والتي يطلق عليها بجرائم المعلوماتية.

يثير هذا الاجرام المعاصر الكثير من الاشكالات وفي نواحي عديدة، اهمها صعوبة اكتشاف هذه الجرائم واثباتها، فالمجرم المعلوماتي يمكنه إحداث جرائم معلوماتية دون ان يترك خلفه أي آثار خارجية ملموسة، خصوصا وانه مجرم يتميز بالذكاء والمهارات التقنية العالية، كما انه على دراية بمجال المعلومات وانظمة برامج الحاسبات الالية.

فمن خلال دراستنا لهذا الفصل تتعرض للإطار المفاهيمي للجرائم الاقتصادية في الأوساط المعلوماتية التي قد يرتكبها المجرم مستفيدا من تكنولوجيا الاعلام والاتصال ونظم المعلومات وموظفيها في تحقيق مكاسب غير مشروعة خاصة في الميدان المالي والاقتصادي.

ونحاول في هذا الصدد أن نتعرف على الصيغة القانونية لهذه الظاهرة الاجرامية وأن نعطي لها تعريفا بحيث يذكر أهم الأركان الأساسية التي تقوم عليها، ثم نتطرق لمراحل حدوث هذه الظاهرة والصور والآثار المترتبة عليها على مستوى الفرد وعلى مستوى البنوك والجهات الحكومية وغير الحكومية والمؤسسات (الشركات).

المبحث الأول : مفهوم الجرائم المعلوماتية و أركانها

وعليه سوف نقسم هذا المبحث إلى مطلبين نتناول مفهوم الجريمة المعلوماتية في(المطلب الأول) و أركان الجريمة المعلوماتية في (المطلب الثاني).

المطلب الأول : مفهوم الجريمة المعلوماتية

إن موضوع الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول عامة ولاسيما الجزائر وتزداد أهمية تلك المسألة أمام الطابع الدولي والعالمي لشبكة الإنترنت فهذه الأخيرة تعتبر سلاح ذو حدين، يعمل بين جنبيه الظلمة والنور ويعكس وجهي الخير والشر في الإنسان، فهو وسيلة للربط و الاتصال والتقارب وتبادل المعلومات والمنافع بين بني الإنسان إلا أنه يمكن أن يكون أداة تزوير وتضليل ولب الرذيلة والتعدي على حقوق الآخرين، لذا ظهرت الحاجة الماسة في الحد من الجانب المظل.

ومن خلال هذا المطلب نستعرض تعريف الجريمة المعلوماتية (الفرع الأول) ثم خصائصها (الفرع الثاني).

الفرع الأول : التعريف بالجريمة المعلوماتية

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك على تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، و ما سيتبع ذلك من تسهيل للوصول إلى الحلول المناسبة لمواجهتها، و سوف نحاول الوصول إلى تعريف يتلاءم مع طبيعة الجريمة المعلوماتية.

أولا: تعريف الجريمة المعلوماتية على أساس وسيلة ارتكاب الجريمة:

إن أصحابها ينطلقون من أن الجريمة المعلوماتية تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، ومن ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية دورا رئيسا[1].

كما عرف الفقه الجريمة المرتكبة عبر الإنترنت بأنها :" هي نشاط إجرامي تستخدم فيه التقنية الالكترونية (الحاسوب الآلي الرقمي و شبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف"[2].

عرفها الفقيه الألماني تاديمان بأنها:" هي شكل من أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب باستخدام الحاسب الآلي"[3]، كما تعرف بأنها:" كل نشاط إجرامي يؤدي فيه نظام الحاسب

---

[1] –محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الإنترنت ،دار النهضة العربية، القاهرة، ب س، ص33.

[2] –عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الإنترنت(الجرائم الإلكترونية) ، منشورات الحلبي الحقوقية، بيروت، طبعة أولى ،2007، ص15.

[3] –عبد الفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي ،دار الفكر الجامعي الإسكندرية،2006،ص22.

الآلي دورا لإتمامه على أن يكون هذا الدور على قدر الأهمية"[1]، وفي ذات الاتجاه عرفت بأنها:" الجرائم التي يكون دور الحاسوب فيها ايجابيا أكثر منه سلبيا"[2]، كما تعرف جرائم الإنترنت: "أنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتعلقة بالكمبيوتر والانترنت في أعمال وأنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الالكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الإنترنت باستخدام النقود أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة".

إن تعريف الجريمة المعلوماتية المعتمدة على الوسيلة المستخدمة في ارتكابها، قد تعرض إلى عدة انتقادات مفادها أن تعريف الجريمة يستوجب الرجوع إلى الفعل والأساس المكون لها، ليس لمجرد أن الحاسب استخدم في جريمة يتعين أن نعتبرها من جرائم الإنترنت.

ثانيا: تعريف الجريمة المعلوماتية على أساس شخصي

يستند أنصار هذا الاتجاه إلى معيار شخصي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات[3]، ومن بين هذه التعريفات نجد تعريف في وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة المرتكبة عبر الانترنت بأنها:" أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكن من ارتكابها"، ومن قبيل هذا التعريف جاء تعريف الأستاذ "thonasèm David" لجريمة الإنترنت بأنها" لأية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".[4]

إن قصور هذا التعريف واضح إلى أن مجرد توافر المعرفة التقنية بعلم ما لا يكفي في ضوء عدم توافر العناصر الأخرى لتصنيف لجريمة ضمن الجرائم المتعلقة بذلك العلم.[5]

---

[1] –نائلة عادل فريد قورة، جرائم الحاسب الاقتصادية(دراسة نظرية تطبيقية)، دار النهضة العربية، الإسكندرية،2004،ص26.

[2] –عبد الفتاح بيومي حجازي ،المرجع السابق،ص24.

[3] –محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية ،دار الثقافة للنشر و التوزيع، الأردن،2005،ص16.

[4] –هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني و اقتراح إنشاء ألية عربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون و الكومبيوتر والإنترنت، من 1–3 ماي2000،بجامعة الإمارات العربية المتحدة ،كلية الشريعة و القانون، المجلد الثاني، الطبعة الثالثة،2004،ص407.

[5] – محمد عبيد الكعبي، المرجع السابق،ص34.

ثالثا: تعريف الجريمة على أساس موضوعها

يذهب اتجاه أخر إلى التركيز على الجانب الموضوعي باعتبار أن هذه الجريمة ليست الجريمة يستخدم الحاسب الآلي كأداة في ارتكابها فحسب بل تقع على الحاسب الآلي و في داخل نظامه[1]، يرى واضعو هذا التعريف لأن الجريمة المرتكبة ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه.[2]

ويوسع البعض من مفهوم هذه الجريمة حيث يعرفها الخبير الأمريكي "Parcker" :"كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عن خسارة تلحق بالمجني عليه فعل أو مكسب يحققه الفاعل"[3].

أما في الوقت الحاضر فقد تبين مؤتمر الأمم المتحدة لمنع الجريمة و معاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته، حيث عرف الجريمة المعلوماتية بأنها :" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي"، أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[4].

أما تلك التعريفات المتعددة والصادرة عن وجهات نظر قانونية واجتماعية وفلسفة أحيانا، ويمكن بدورنا أن نضع لها تعريف أخر، يتمثل في أن" جرائم تكنولوجيا المعلومات هي كل فعل وعمل و كل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما له دراية و معرفة بتكنولوجيا المعلومات المختلفة (تكنولوجيا التخزين، والاسترجاع وتكنولوجيا اتصالات الحديثة) ويوجه ضد المصلحة الخاصة"، وتشمل تلك الجرائم من الناحية المبدئية جميع الجرائم التي يمكن أن ترتكب فيع أو عبر وسط الكتروني ويقر لها القانون عقوبة أو تدبير.

الفرع الثاني : خصائص الجريمة المعلوماتية

تتميز جريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته كما تتميز بطابعها

---

[1] –عبد الفتاح بيومي حجازي، المرجع السابق،ص26.

[2] – أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، 2006،ص 85,86.

[3] – محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت(الجريمة المعلوماتية)، مكتبة دار الثقافة، عمان،2004،ص15.

[4] – جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة المعلوماتية)، دار البداية، عمان، 2007، ص110.

الدولي في أغلب الأحيان حيث تتخطى أثارها هذه الجريمة حدود الدولة الواحدة، ولسوف نبين هذه الخصائص التي ميزت الجريمة المعلوماتية مرتبطة بذات الإنسان و شخصيته.

أولا : صعوبة اكتشاف الجريمة المعلوماتية:

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية و مستتر في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة، مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها، و التجسس و سرقة المكالمات وغيرها من الجرائم.[1]

كما أن وسيلة تنفيذها التي تميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن الإبلاغ عنها في حال اكتشافها لخشية المجني عليهم في فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل الإثبات في مدة تقل عن الثانية الواحدة.

كما أن المجني يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرض أكثر الجهات التي تتعرض أنظمنها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى من موظفيها عما تعرض له وتكتفي عادة بإجراءات داخلية إدارية دون الإبلاغ عنها السلطات المختصة تجنبا للأضرار أو بسمعتها و مكانتها وهو الثقة في كفاءتها.

ثانيا : صعوبة إثبات الجريمة المعلوماتية :

فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن و أجهزة التحقيق و الملاحقة[2]، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يحقق في الجهات الأمنية و القضائية لدينا ، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي الذي ضد هذه الظاهرة.

---

[1] – محمد عبيد الكعبي، المرجع السابق،ص32.

[2] – محمد عبيد الكعبي، المرجع السابق،ص40.

لم تعد قادرة القوانين التقليدية على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى تطور الجريمة من خلالها، و ظهور جرائم لم تكن موجودة في السابق، وباتت القوانين القديمة عاجزة عن مواجهتها [1]، ما يشكل عائقا أساسيا أمام إثبات الجريمة الإلكترونية.

ثالثا: أسلوب ارتكاب الجريمة المعلوماتية: ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكاب وطريقتها فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال جريمة السرقة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت مع وجود مجرم يوظف خبرته و قدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغرير أو التغرير بالقاصرين كل ذلك دون الحاجة لسفك الدماء).

رابعا: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص: تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالب ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص أخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب و تحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد تكون اشتراكا سلبيا وهو الذي يترجم بصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيلها وإتمامها، وقد يكون اشتراكا ايجابيا وهو غالبا كذلك ما يتمثل في مساعدة فنية و مادية.

خامسا: خصوصية مجرمي المعلوماتية: المجرم الذي يرتكب الجريمة المعلوماتية الذي يطلق عليه المجرم ألمعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية(المجرم التقليدي).

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها –باعتبارها قاعدة عامة – فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن

---

[1] – نفس المرجع ،ص 41.

يرتكبها عادة ما يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة و القدرة على استعمال جهاز الحاسب و التعامل مع شبكة الانترنت.

سادسا: الجريمة المعلوماتية جريمة عابرة للحدود: بعد ظهور شبكات المعلومات لم يعد هناك كحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينهما ألاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في أن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة مما جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، هذه الطبيعة تتميز بها الجريمة المعلوماتية كونها جريمة عابرة الحدود خلقت العديد من المشاكل حول تحديد الدولة صاحية الاختصاص القضائي بهذه الجريمة، فهل عي الدولة التي وقع بها النشاط الإجرامي أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت الطبيعة أيضا الشكوك حول مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية و بصفة خاصة فيما يتعلق بجمع و قبول الأدلة.[1]

الحقيقة أن عملية التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر الوسائل التي تثير الإشكالات في المجال الحاسوب، وبشكل خاص الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق، وهذا بدوره عامل رئيسي في نماء دعواته تضافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بإرهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول و اختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من يد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحتها[2].

---

[1] –نائلة عادل فريد قورة ، المرجع السابق، ص 54.

[2] – جعفر حسن جاسم الطائي، المرجع السابق، ص142.

المطلب الثاني : أركان الجريمة المعلوماتية

تتخذ الجريمة المرتكبة عبر الإنترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات ننفرد بها، إلا أن ذلك لا يعني عدم وجود نشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة، حيث نسلك سبيل المقارنة بينها وبين التقليدية، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة المرتكبة عبر الإنترنت (الفرع الأول)، ثم نوضح الركن المادي (الفرع الثاني)، لننتهي إلى تحديد الركن المعنوي فيها(الفرع الثالث).

الفرع الأول : الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل و يوضح العقاب المترتب عليه وقت وقوع هذا الفعل[1]، فمبدأ الشرعية الجنائية يمنع المسائلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة و لا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هذه الفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم، غير ان السؤال المطروح هو مدى تطبيق مبدأ الشرعية على الجرائم التي ترتكب عبر الإنترنت؟

أولا: مدى انطباق النصوص القائمة على جرائم الإنترنت:

تشعب الإشكالات الناجمة عن استخدام الحواسيب الألية وشبكاتها جعل مهمة القضاء صعبة نظرا لعدم وجود نصوص كفيلة بمعالجة هذه المشكلات و التي من بينها الاستخدام غير المشروع لشبكة الإنترنت.

حاولت قوانين العقوبات مواجهة تحديات الجرائم المرتكبة عبر الإنترنت بطرق تقليدية كتلك المقررة في جرائم الأموال، إلا انه تبين قصور هذه الوسائل التقليدية عن مواجهة العديد من الفعال التي تهدد مصالح اجتماعية و التي ارتبطت بظهور و انتشار أجهزة الكمبيوتر.

تبين في بعض الأحوال أن ثمة أفعالا جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، من ذلك الاعتداء على حرمة الحياة الخاصة، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما تجميع معلومات عن الأفراد وتسجيلها في الكومبيوتر، فإنه لا يخضع للتجريم وفقا للقواعد العامة، كما أن التداخل في النظام نظام الحاسب الآلي وتغيير البيانات، فهي صور جديدة لا يعرفها قانون العقوبات قبل ظهور الكمبيوتر وشبكة الإنترنت، كل ذلك يؤكد قصور القواعد التقليدية في القانون الجنائي على مكافحة هذا النوع الجديد من الجرائم.[2]

لا يتطور القانون الجنائي دائما بنفس السرعة التي تتطور بها التكنولوجيا ولا بنفس المهارة التي يأتي بها الذهن البشري لتسخير هذه المبتكرات لاستخدامه السيئ، لذلك وكاستنتاج أولى ومنطقي نعتقد أن

---

[1] – عبد المحسن بدوي محمد أحمد، استراتيجيات و نظريات معالجة قضايا الجريمة و الانحراف في وسائل الإعلام الجماهيري، الندوة العلمية حول الإعلام و الأمن ، مركز الدراسات و البحوث، قسم الندوات و اللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الخرطوم 11–13 سنة 2005،ص5.

[2] – غانم محمد غانم، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون و الكمبيوتر و الإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، 1–3 ماي 2003، المجلد الثاني،ص625–626.

القانون الجنائي لا يكفي من حيث المبدأ في مواجهة هذا النمط من الإجرام خاصة أن النصوص قد وضعت للتطبيق وفق معايير معينة كانت سائدة أيام وضعها.[1]

ثانيا: الحاجة لتدخل المشرع لمواجهة جرائم الإنترنت

تعتبر الجريمة الواقعة من نتاج التطور التكنولوجي أنها من المستحدثات التي عجزت مواد القوانين العقابية التقليدية مواجهتها، لذلك سعت معظم دول العالم ولا سيما تلك المتقدمة قانونيا إلى سن التشريعات و القوانين لمواجهة هذه الجرائم.

تعتبر الولايات المتحدة الأمريكية من بين الدول السابقة التي جسدت تشريع مستقل بشأن جرائم الكمبيوتر بصفة عامة وجرائم الإنترنت بصفة خاصة كما تتميز الولايات المتحدة الأمريكية بوجود أكبر قدر من التشريعات تغطي مسائل جرائم الكمبيوتر والإنترنت والاتصالات.

وضعت الولايات المتحدة الأمريكية قانونا خاصا بحماية الحاسوب و الشبكات المحوسبة، وذلك عام1976، وفي عام 1985 حدد معهد العدالة القومي فيها خمسة أنواع رئيسية لهذا النوع من الجرائم و هي:

1-جرائم الحاسوب الداخلية.
2-جرائم الاستخدام غير المشروع عن بعد، شبكات المعلومات المحوسبة.
3-جرائم التلاعب بالحاسوب، أي التلاعب غير المخول وغير المشروع في الشبكات المحوسبة.
4-دعم التعاملات الإجرامية للنظم و الشبكات المحوسبة، وإسنادها من قبل الآخرين.
5- سرقة البرامج الجاهزة و المكونات المادية.

صدر في عام 1986 قانون أخر يعرف فيه جميع المصطلحات الضرورية لتطبيق جرائم النظم المعلوماتية و الشبكات المحوسبة، وعلى أثر ذلك قامت الولايات الأمريكية الداخلية بدورها بإصدارها تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، والتي تتماشي مع التشريعات الاتحادية المذكورة.[2]

---

[1] – محمد حماد مرهج الهيتي، التكنولوجيا الحديثة و القانون الجنائي، دار الثقافة للنشر و التوزيع، عمان، 2004، ص176.

[2] – احمد بن محمد اليماني، الحماية الجنائية للبريد الإلكتروني دراسة تأصيلية مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العدالة الجنائية، تخصص السياسة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات ، قسم العدالة الجنائية، الرياض،2010،ص99.

قام كذلك المشرع الفرنسي بسن تشريع خاص الإجرام المعلوماتي وذلك في أغسطس عام 1986، حيث تقدم النائب "جاك جودفران " باقتراح قانون تم اعتماده من البرلمان الفرنسي و صدر في 5 يناير 1988 برقم 19 تحت عنوان " الجرائم في المواد المعلوماتية"، وتم إدماجه في الفصل الثاني من قانون العقوبات و خصص له المواد 2/432 إلى 9/462 .

الجدير بالذكر أن الفصل المخصص لهذه الجرائم ألحق بالباب المخصص بالجنايات و الجنح ضد الأشخاص، أي بعد الفصل الثاني من الجرائم المخصصة بالجنايات و الجنح ضد الملكية، و قد ركزت اللجنة التشريعية على الهدف الذي توخاه اقتراح "جودفران" حماية النظام المعلوماتي ضد أي اعتداء خارجي، فقررت أن الهدف من النصوص الجديدة تجريم وردع الدخول غبر المشروع على برامج المعلوماتية.

يعتبر تدخل المشرع لوضع نصوص قانونية لتجريم الأفعال غير مشروعة الناتجة عن استعمال الإنترنت أكثر من ضروري، خاصة في ظل التطور السريع الذي يعرفه هذا النوع من الجرائم، ولقد اتخذنا المشرعين الأمريكي و الفرنسي كمثال نظرا للتطور التشريعي و لقوة القانونية التي يتمتعان بها.

غير أن الملاحظ على المستوى الدولي وجود فجوة رقمية رهيبة بين الدول، فبالنسبة للدول التي تعاني من التخلف في مجال المعلوماتي، لم تسن بعد قوانين تجرم بها الأفعال غير المشروعة عبر الإنترنت، واكتفائها بتطبيق قواعد قانون العقوبات الخاصة بها، غير أن هذه القوانين أثبتت قصورها في هذا المجال كما أسلفنا الذكر، الأمر الذي يستوجب منها التوسع في تفسير هذه النصوص لتطبيقها على الجرائم المرتكبة عبر الإنترنت.

ثالثا: التوسع في تفسير النصوص القائمة لتطبيقها على جرائم الإنترنت

ليس أمام الدول التي لم تسن بعد قوانين خاصة لتجريم مختلف الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت سوى تطبيق القوانين الجنائية القائمة بمرادها التقليدية على هذه الوقائع خوفا من إفلات الجناة من قبضة العدالة، مع بعض التفسير الموسع لهذه النصوص. [1]

فعلى الرغم من أن القصور التشريعي قد أصبح واقعا ملموسا، إلا أن هذا لا يحول دون الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الاعتداءات المختلفة على المال بحيث يمكن تطبيقها على الجرائم المستحدثة التي أوجدتها ثورة الاتصالات عن بعد، فلا محالة أن التطور قد يوسع

[1] – محمد عبيد الكعبي، المرجع السابق، ص52.

من دائرة المجالات التي تحميها نصوص التجريم والعقاب بحيث يمكن أن تدخل في إطارها عناصر أخرى طالما أمكن اعتبارها من جنسها وان المشروع يحميها بذات هذه النصوص.

يكون اتخاذ سبيل التفسير الموسع للنصوص التقليدية من اجل تطبيقها على الجرائم المرتكبة عبر الانترنت، بمنح السلطات القضائية حرية تفسير هذه النصوص حيث أن القاضي يمكنه أن يعطي تفسير أكثر مرونة للنصوص القانونية يسمح من وضع هذه الجرائم تحت طائلة التجريم والمتابعة، وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي.

فعندما تعرض قضية جزائية على القاضي فإن أول عملية يقوم بها هي تكييف الواقعة لمعرفة مدى تطابقها مع النص الذي يجرمها ، وللوصول إلى هذه الغاية يقوم القاضي باستخلاص عناصر الواقعة من النص، وقد يصادف القاضي إثناء ذلك صعوبة أو غموضا فيقوم عندئذ بتفسير النص الجنائي.[1]

لكن تطبيق هذه النصوص التقليدية بمفهومها الموسع و الخاصة ببعض الجرائم كالسرقة على سبيل المثال على الجرائم الواقعة بطريق الإنترنت من شأنه المساس بمبدأ الشرعية الجنائية، إذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله.

الفرع الثاني : الركن المادي

ينطلق مبدأ تحديد الفعل غير المشروع و إعطائه صفة الجريمة ، بتحديد الركن المادي فيه، فلا جريمة دون ركن مادي ، الذي يتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما له القانون العقاب اللازم ، وهو يتباين بتباين الجرائم المرتكبة من قبل الجاني، شريطة أن يكون له مظهر خارجي ملموس، غير أن تحديد الركن المادي في الجرائم الواقعة عبر الشبكة العالمية للإنترنت تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية و الرابطة السببية، وسوف نبين الركن المادي في هذا النطاق كالآتي:

أولا: القواعد العامة في الركن المادي للجريمة

1-السلوك الإجرامي

[1] – بارش سليمان، مبدأ الشرعية في قانون العقوبات الجزائري، دار الهدى ، عين مليلة،2006،ص18.

يعد السلوك الإجرامي أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الأفكار داخل النفس لا عقاب عليها.

يعرف السلوك الإجرامي في الجرائم التقليدية على أنه فعل الجاني الذي يحدث أثر في العلم الخارجي، وبغير هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفكاره و هواجسه الداخلية، و السلوك هو الذي يخرج النية و التفكير في الإجرام إلى حيز الوجود و اعتبار القانون، ولا يكاد يفرق بين السلوك الإيجابي (الفعل)و السلوك السلبي (الامتناع عن فعل)، مادام أن لهما نفس النتيجة.

أ-السلوك الإيجابي: يكون في صورة فعل أو قول يجرمه القانون يصدر عن الجاني و يؤدي إلى إحداث نتيجة في الجرائم ذات النتيجة و كذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية، ولا يهتم القانون بالوسيلة سواء كانت مادية أو معنوية، فإذا كان السلوك محظورا قانونا فهو يشكل جريمة، وكذلك إذا أدى إلى نتيجة منعها القانون و يدخل ضمن السلوك الإيجابي فعل السرقة، و القتل و الضرب و النصب، و شهادة الزور، و البلاغ الكاذب و التحريض على الجريمة، و الغش و التدليس و غيرها من السلوكيات. [1]

ب- السلوك السلبي: يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه أن يعمل ، ففي هذه الحالة يقوم المكلف بالحيلولة دون جسمه كله أو بعضه وبين الحركة التي يتطلبها القانون ، أو قد يتحرك باتجاه مضاد لما أمره به.

يقوم الفعل السلبي على الامتناع أو إحجام شخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، وعليه فلا يجوز للقاضي أن يمتنع عن الحم بالدعوى ولا للشاهد أن يمتنع عن الإدلاء بشهادته أمام المحكمة بواقعه يعلمها ولا للموظف أن يمتنع عن لأداء مهام وظيفته.[2]

2-النتيجة الإجرامية:

[1] - منصور رحماني ، الوجيز في القانون الجنائي العام ، دار العلوم للنسر و التوزيع ، عناية، 2006،ص94.

[2] - عبد الله سليمان ، شرح قانون العقوبات الجزائري، القسم العام ، الجزء الأول (لجريمة)، ديوان المطبوعات الجامعية ، الجزائر ، 1995،ص148.

يقصد بالنتيجة الإجرامية، الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلك الإجرامي، فالسلوك قد أحدث تغييرا حسيا ملموسا في الواقع الخارجي ، ومفهوم النتيجة كعنصر في الركن المادي للجريمة يقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج ، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى .

3-الروابطة السببية

تتمثل الرابطة السببية هي الصلة التي تربط بين الفهل والنتيجة وتثبيت أن ارتكاب الغعل هو الذي أدى على حدوث النتيجة، وأهمية رابطة السببية تؤجع إلى أن إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق رابطة السببية تلازماً مادياً بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجلني عند حد الشروع، إذ لا يعد مسؤولاً عن النتيجة التي تحققت، أما إذا كانت الجريمة غير عمدية، فإن نفي رابطة السببية يؤدي إلى انتفاء المسؤولية كلية عنها، ذلك أنه لا شروع في الجرائم غير العمدية.

ثانيا: تحديد الركن المادي في الجريمة المرتكبة عبر الإنترنت

تحديد الركن المادي في الجرائم المرتكبة عبر الإنترنت يثير جملة من الصعوبات التي تفرضها طبيعة الوسط الذي تتم فيه الجريمة المتمثل في الجانب التقني، وهذا ما يميز ركنها المادي، الذي يجب أن يتم باستخدام أجهزة الحاسب الآلي أو الشروع فيه، ومكان البداية واكتمال الركن المادي، أجزاء السلوك الإجرامي المرتكب في العالم المادي، أو العالم الافتراضي، وغيرها من التساؤلات التي تتعلق بطبيعة الجريمة.[1]

يتطلب النشاط أو السلوك المادي في جرائم الإ نترنت وجد بيئة رقمية واتصال بالإنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإ عداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها أشياء أو صور مخلة بالأداب العامة و نحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

[1] -منصور بن صالح السلمي ، المرجع السابق،ص76.

ليس كل جريمة تتلزم وجود أعمال تحضيرية، إلا أنه يصعب الفصل بين العل التحضيري والبدء في النشاط الإجرامي في جرائم الإنترنت–حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية–ففي مجال تكنولوجيا المعاومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

يتمثل النشاط المادي في الجريمة المرتكبة عبر الإنترنت في الدخول غير المشروع في نظم وقواعد معالجة البيانات، سواء ترتب عن هذا الدخول غير المشروع تلاعب بهذه البيانات أم لا، إذ أن مجرد الدخول غير الشروع لمواقع المعلومات والبرامج جريمة مرتكبة عبر الإنترنت، وقد يتخذ هذا النشاط الإجرام عدة صور كانتهاك السرية خصوصية للبيانات الشخصية و الإضرار بصاحبها و للاطلاع على المراسلات الإلكترونية والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية يعد كذلك من أهم صور الركن المادي للجريمة المرتكبة عبر الإنترنت. [1]

مجمل القول أن السلوك الإجرامي في الجريمة المرتكبة عبر الإنترنت يرتبط بالمعلومة المخزنة داخل الحاسب الآليأو انتهاك حرمة الأشخاص، و السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب الألي فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك مثلا.

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فهل تقتصر على العالم الإفتراضي، أم أن لها جزاء في العالم المدي، و هل تقتصر النتيجة على مكان واحد أو تمتد لتشمل دولا وأقاليم عدة، فعلى سبيل المثال إذ قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمرات، و هذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين.

تحديد رابطة السببية في مجال أضرار الإنترنت يعد من المسائل الصعبة والمعقدة بالنظر إلى تعقيدات صناعة الحاسوب والإنترنت، وتطور إمكانياتها وتسارع هذا التطور، إضافة إلى تعدد وتنوع أساليب الاتصال بين الأجهزة الإلكترونية تعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة

[1] – عبد الرزاق السندالي، التشريع المغربي في الجرائم المعلوماتية، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية،19–20 يونيو 2007، ص69.

المراد الحصرل عليها، كل ذلك سيؤدي حتما إلى صعوبة تحديد السبب أو الأسباب لحقيقية للإساءات المرتكبة في هذه المسؤولية.[1]

الفرع الثالث: الركن المعنوي

يعتبر الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويطلق عليه الركن الأدبي أو الشخصي و هو يعني في الحقيقة الجاني أو المجرم تحديداً فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي، من إسناد وإسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبني على المقومات، هذا على العموم في جميع الجرائم، غير أن التساؤل يثور في مجال الجرائم المرتكبة عبر الإنترنت، فهل المقومات التي تحكم الركن المعنوي في الجرائم التقليدية هي نفسها في الجرائم المرتكبة عبر الإنترنت؟

أولا: الركن المعنوي في نطاق الجريمة التقليدية

يتمثل الركن المعنوي في ظل الجرائم التقليدية في:

1-عناصر القصد الجنائي

أ- العلم

لا يتحقق القصد الجنائي إلاً إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء، فإذا كان الجاني جاهلاً بشيء من ذلك فلا يتحقق القصد الجنائي، ففي جريمة السرقة لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم أن المال المسروق ملك لغيره، ولا يتوافر القصد في جريمة التسميم إلا إذا كان الجاني يعرف أن الطعام الذي قدمه إلى المجنى عليه يحتوي على السم ، فالذي يأخذ مال غيره معتقدا لأنه ماله ، أو الذي يطعم غيره طعاما مسموما وهو يجهل ذلك، ففي كلاهما لا يتوفر القصد الجنائي، ولس كل جهل ينتفي معه القصد الجنائي، بل هناك وقائع يؤثر الجهل بها في القصد، وأخرى لا يتأثر بها القصد.

ب- الإرادة :الإرادة هي نشاط نفسي يهدف إلى تحقيق غرض معين، فإذا كان غرض الجاني تحقيق نتيجة إجرامية ، كانت الإرادة المتجهة إلى الفعل المنطوي على إحراث النتيجة هي " القصد الجنائي" و الغرض هو الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو عبارة عن الدافع إلى إشباع حاجة

[1] - منصور بن صالح السلمي، المرجع السابق، ص75-76.

معينة، و هذا الدافع له طبيعة نفسية، بخلاف الغاية التي لها طبيعة موضوعية، فإذا أراد الجاني أن يسرق المجني عليه لضائقة مالية مر بها، كانت الغاية التي يسعى لها هو الحصول على المال ، وأما الغرض فهو قتل المجني عليه لسرقته، فهذا الغرض يتصور الجاني تحقيقه بطعن المجني عليه لقتله و الاسالاء على ماله، فيوجه إرادته لهذا الغرض، أما الباعث على فعله فهو التخلص من الديون التي تثقل كاهله.[1]

2-صور القصد الجنائي

أ- القصد الجنائي العام: يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين ، بتحقيقة قد تتم الجريمة ويتوافر لها القصد الجنائي العام، ففي جريمة القتل يكون غرض الجاني إزهاق روح المجني عليه، وفي جريمة السرقة غرض الجاني حيارة المال المسروق، وفي جريمة لرشوة يكون غرض الجاني الحصول على منفعة من الراشي، وعلييه فالقصد العام أمر ضروري ومطلوب في كل الجرائم العمدية.[2]

ب- القصد الجنائي الخاص: يلتقي القصد الخاص مع القصد العام في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة، إما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر .

ثانيا: تحديد الركن المعنوي في الجريمة المرتكبة عبر الإنترنت

يكتسي تحديد الركن المعنوي بالغ الأهميه في الجريمة المرتكبة عبر الإنترنت، كما هو الحال بالنسبة للجريمة المرتكبة في العالم المادي ، حيث بموجبه يمكن تحديد مناط مسائلة الجاني ، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لايمكن أن يعاقب الشخص المرتكب للفعل.

يتلاقى القصد الجنائي بصورتيه العام والخاص في الجرائم المرتكبة عبر الإنترنت مع مثيله في الجرائم التقليديه في عدة نقاط، منها العلم والإرادة، فالمجرم يجب أن يكون عالم بأن الذي يقوم به يعتبر فعل غير مشروع، وذلك بإرادة صريحة من أجل إحداث الضرر للمجني عليه.

---

[1] – اشرف توفيق شمس الدين ، المرجع السابق، ص155.

[2] – عبد الله سليمان ، المرجع السابق ، ص261.

أما القصد الخاص فيلتقي مع القصد في الكثير من عنصره ، ويزيد في تحيد الإرادة الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى الجريمة ، وإما بنتيجة محددة يريدها، وحكمة هذا التحديد هي الرغبة في توضيح هذه الجريمة وتمييزها عن غيرها من الجرائم التي تشترك معها في بعض العناصر.

ولتبيان الفرق بين القصد الجنائي العام و القصد الجنائي الخاص، فإن القصد الجنائي العام يقوم على العلم الإرادة، كما يقوم القصد الجنائي الخاص على العلم الإرادة، غير انه يمتاز عنه بأن العلم والإرادة فيه لا يقتصران على أركان الجريمة وعناصرها، و إنما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وإذا تطلب القانون في جريمة توافر القصد الخاص فمعنى ذلك أنه يتطلب بعد ذلك انصراف العلم والإرادة إلى أركان الجريمة ، وبذلك يتوافر العام، ثم يتطلب بعد ذلك انصراف العلم والإرادة إلى وقائع لا تعد طبقا للقانون من أركان الجريمة، وبهذا الاتجاه الخاص للعلم والإرادة يقوم القصد الخاص، ولقيام الركن المعنوي في الجرائم المرتكبة عبر الإنترنت، لابد أن يعلم الجاني أنه يرتكب من خلال شبكة الإنترنت أحد الأفعال التي يتضمنها نص التجريم، وأن تتجه إرادته إلى القيم بذلك الفعل.[1]

يقوم الركن المعنوي للجريمة المرتكبة عبر الإنترنت على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون، كانتحال شخصية المزود عبر الإنترنت، وسرقة أرقام البطاقات الانتمانية، كما يجب أن تتوفر النتيجة الجرمية المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية من العمل غير المشروع الذي بيت النية على ارتكابه، وهو عالم بالآثار الضارة الناشئة عنه.

يعد تبيان مفهوم الركن المعني في الجرائم المرتكبة عبر الإنترنت من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص المادية التي يلزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة الدخول غير المشروع، لذلك فإن اتجاه القضاء المقارن في تطلب العمد بالنسبة لجريمة الدخول فقط بعد من الموضوعات المنفذة هنا.

نستنتج أنه لقيام أي جريمة يجب أن يتوافر الركن المعنوي بكل عناصره وصوره إلى جنب الأركان لأخرى، لأن الحالة النفسية للجاني بصفة عامة أو القصد بصفة خاصة هو الذي يحدد لنا مسؤولية

[1] – منصور بن صالح السلمي ، المرجع السابق ،ص78.

الفاعل من عدمها ، فمثلا لا يمكن أن نحاسب شخص مسلوب الإرادة الذي استكره على فعل أشياء معتبرة غير مشروعة في نظر القانون، بل يجب أن يكون ذا إرادة واضحة لكي تتم مسائلته.

غير أنه ورغم هذا التوافق بين جميع الجرائم في وجوب توافق الركن المعنوي فيها. إلا أن هناك استثناءات فيما يخص الجريمة المرتكبة عبر الإنترنت، وذلك في ظل الطبيعة الامادية للجريمة، والسرعة في ارتكابها، حيث لا تدع المجال لتحديد الفعل من عدمه فما بلك بتحديد القصد الجنائي فيها، بالإضافة إلى اختلاف طبيعة المجرمين، حيث ينفرد المجرمون الذين يقومون بأفعالهم غير المشروعة عبر الإنترنت عن نظرائهم في الجريمة التقليدية فيما يخص الباعث.

يتباين الركن المعنوي في الجريمة المرتكبة عبر الإنترنت بتباين الباعث الذي يدفع الجاني لارتكاب أفعاله. فكما أسلفنا الذكر، ليس كل المجرمين عبر الإنترنت لهم نية في الإجرام ، فبالرغم من أن هناك من المجرمين من يسعى لتحقيق أغراض مادية أو سياسية أو إيديولوجية، إلا انه هناك من الأفراد من يقوم بأفعاله من أجل التعلم أو لمجرد التسلية في بعض الأحيان، مما يجعل في هذه الحالة تحقق شرط القصد الجنائي منعدم ، ومنه لا يتوافر الركن المعنوي في كذا جرائم.

يعتبر الباعث الدافع النفسي لتحقيق سلوك معين بالنظر إلى غاية محددة يريدها الجاني[1]، فلباعث في الجرئم المرتكبة عبر الإنترنت يعد من الصعوبات التي تعوق الوصول إلى تحديد العقوبة لمقترف الفعل المحرم، وذلك لانعدام القصد الجنائي ، فمثلا إذا اخترق أحد القراصنة الهواة قاعدة بيانات لشركة معينة من أجل التعلم أو من أجل التسلية دون علمه أن هذا الفعل مجرم ينتقي هنا الركن المعنوي للجريمة.

غير ان الملاحظ على هذه الأفعال، وبالرغم من عدم توافر القصد الجنائي فيها، إلآ أنها تسبب أضرارا وخسائر فادحة لدى الجهة المجني عليها تفوق أضرار الجريمة التقليدية، غير أن انتفاء القصد الجنائي يعفي الجاني من المسائلة، وبالتالي يتم ضياع حقوق الجهة المجني عليها، ومنه يستحسن إيجاد سبيل للحد من هذه الصعوبة، وذلك بمسائلة الجاني على أساس الضرر الذي ألحقه بالمجني عليه أو الاكتفاء بتوفر الركن المادي والشرعي للجريمة.

---

[1] – منصور رحماني ، المرجع السابق ، ص113.

المبحث الثاني : صور واثار الجرائم الاقتصادية في الاوساط المعلوماتية

من خلال دراستنا لهذا المبحث نتعرض للجرائم التي يرتكبها المجرم مستفيدا من تكنولوجيا الاعلام والاتصال والنظم المعلوماتية وموظفها في تحقيق مكاسب غير مشروعة خاصة في الميدان المالي والاقتصادي ومن امثلة هذه الجرائم :

– تخريب المعلومات وإساءة استخدامها ، تزوير البيانات، التزييف ، الابتزاز ، تزوير العلامات التجارية، السرقة عبر الانترنت، جرائم السطو على ارقام بطاقات الائتمان والتحويل الالكتروني غير المشروع للأموال، غسيل الاموال عبر الانترنت ، تجارة المخدرات عبر الانترنت .

نحاول في هذا المبحث ان نعرض اهم صور الجرائم المعلوماتية ثم نذكر بعد ذلك المراحل التي تحدث فيها الجريمة المعلوماتية ثم نختم بذكر آثار الجريمة المعلوماتية .

المطلب الاول : صور الجرائم الاقتصادية في الأوساط المعلوماتية

صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات ، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة ، مثل البيع و الشراء ، مما أنجر عنه تطور وسائل الدفع و الوفاء و أضحت جزء لا يتجزأ من هذه المعاملات و في خضم هذا التداول المالي عبر الانترنت انتهز بعض المجرمون من أجل السطو عليها حيث ابتكرت عدة طرق من أجل ذلك على غرار السرقة و السطو و التحويل الإلكتروني غير المشروع للأموال و قرصنة أرقام البطاقات الممغنطة.

الفرع الأول: السرقة عبر الانترنت :

تعرف السرقة بأنها اختلاس شيء منقول مملوك للغير بدون رضاه بنية امتلاكه[1] وتتم سرقة المال المعلوماتي إن أمكن الوصف – عن طريق اختلاف البيانات و المعلومات و الإفادة منها باستخدام السارق للمعلومات الشخصية – مثل الاسم ' العنوان ' الأرقام الخاصة بالمجني عليهم ' و الاستخدام الغير شرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الانترنت بحيث يؤدي بالغير إلى تقديم الأموال – الإلكترونية أو المادية – إلى الجاني عن طريق التحويل البنكي.[2]

---

[1]– نايف بن محمد المرواني ' جريمة السرقة (دراسة نفسية الاجتماعية) جامعة نايف العربية للعلوم الأمنية ' الرياض الطبعة الأولى 2011 ص59.

[2]– محمد أمين أحمد الشوابكة جرائم الحاسوب و الانترنت مكتبة دار الثقافة للنشر و التوزيع عمان 2004 ص138.

تتجسد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الألى للدخول إلى شبكة الانترنت و الوصول غير المشروع إلى البنوك و المصارف و المؤسسات المالية.[1]

الفرع الثاني: جرائم السطو على أرقام بطاقات الائتمان و التحويل الالكتروني الغير مشروع للأموال

واكب استخدام البطاقات الائتمانية من خلال شبكة الانترنت ظهور الكثير من المتسللين للسطو عليها باعتبارها نقود إلكترونية، خاصة من جهة أن الاستلاء على بطاقات الائتمان أمر ليس بصعوبة كما كان، فلصوص بطاقات الائتمان مثلا يستطيعون الان سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت و من ثما بيع هذه المعلومات للآخرين[2].

تتم عملية التحويل الإلكتروني الغير مشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكومبيوتر الخاصة بالمجني عليه .

مما يسمح للجاني بالتوغل في النظام المعلوماتي و عادة ما يكون هؤلاء من العاملين على إدخال البيانات في ذاكرة الجهاز أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات 2 ' و تتم عملية التحويل الإلكتروني الغير مشروع للأموال بأحد الطرق الموالية :

أ .الاحتيال : و يتم ذلك بطريقة احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح ' فيسلم المال بطريق معلوماتي أو من خلال تصرف الجاني في المال و هو يعلم أن ليس له صفة التصرف فيه [3].

ب .الاحتيال باستخدام بطاقات الدفع الالكتروني :

يعتمد نظام بطاقات الدفع الالكتروني على عملية التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه و ذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية هيئة فيزا كارد "هيئة ماستركارد"[4] ، و تعطي بطاقة الدفع الالكتروني الحق

---

[1]– عباس أبو شامة عبد المحمود عولمة الجريمة الاقتصادية جامعة نايف العربية للعلوم الأمنية ' الرياض 2007 ص20

[2]– حسين طاهر داود ، **جرائم نظم المعلومات**، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2000 ص 73.

[3]– يونس عرب (**قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية و تجربة سلطة عمان**)

[4]– عمر الشيخ الأصم (**البطاقات الائتمانية المستخدمة الأكثر انتشارا في البلاد العربية**)، أعمال ندوة تزوير البطاقات الائتمانية 'أكاديمية نايف العربية للعلوم الأمنية ' الرياض الطبعة الأولى ' 2002 ' ص12

للعميل بالحصول على سلع و الخدمات على شبكة عن طريق تصريح كتابي أو تليفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به و تتم العملية بدخول العميل أو الزبون إلى موقع التاجر و يختار السلع المراد شراءها و يتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري[1] ، و أمام التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالحساب الغير مشروع ممكنة عبر قنوات شبكة الانترنت.

الفرع الثالث : القمار وغسيل الأموال عبر الانترنت

كثيرا ما تتداخل عملية غسيل الأموال مع القمار عبر شبكة الانترنت مما زاد من انتشار أندية القمار الافتراضية، الأمر الذي جعل مواقع الكازينوهات الافتراضية عبر الانترنت محل اشتباه و مراقبة، و من البديهي أن يأخذ المجرمون بأخر ما توصلت إليهم التقنية لخدمة أنشطتهم الاجرامية ويشمل ذلك بالطبع طرق غسيل الاموال التي استفادت من عصر التقنية فلجأت إلي الانترنت لتتوسع و تسريع أعمالها في غسيل أموالها غير المشروعة[2].

وقد ساعدت شبكة الانترنت القائمون بعمليات غسيل الاموال بين الدول و تفادى القوانين التي تضعها الدولة من أجل إعاقة هذا النشاط و كذا تشفير عملياتهم مما يعطيها قدر كبير من السرية ' و خاصة في تسهيل مرتكبي جرائم غسيل الأموال نقلها إلي أي مكان في العالم [3].

الفرع الرابع : تجارة المخدرات عبر الانترنت:

اظهر عصر الانترنت مخاوف من مواقع السوء إن صح التعبير و هو تعريف مقارب لرفيق السوء، و من تلك المواقع طبعا المواقع المنتشرة عبر الانترنت و التي لا تتعلق بترويج المخدرات و تشويق النشأ

---

[1]– محمد عبد الرسول خياط ، (عمليات تزوير البطاقات الائتمانية)، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمينة، الرياض، الطبعة الاولى ، 2012' ص41.

[2]– محمد زيدان ، محمد حمو، **(متطلبات أمن المعلومات المصرفية في بيئة الانترنت)** المؤتمر السادس لجمعيات المكتبات و المعلوماتي السعودية ' بيئة المعلومات الأمنة المفاهيم و التشريعات و التطبيقات ' 6–7 أفريل 2010 ' الرياض ص50.

[3]– خالد بن عبد الله بن معيض العبيدي ،الحماية الجنائية للتعاملات الالكترونية، في نظام المملكة العربية السعودية جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا ، قسم الجناية ، الرياض، 2009 ص50.

لاستخدامها بل تتعداه إلي تعليم كيفية زراعة و صناعة المخدرات بكافة أصنافها و أنواعها و بأبسط الوسائل المتاحة[1].

والأمر هنا لا يحتاج إلي رفاق السوء بل يمكن للمراهق الانزواء في غرفته و الدخول إلي هذه المواقع و من ثم تطبيق ما يقرأه و يؤكد هذه المخاوف احد الخبراء التربويين في بتسبيرج بالولايات المتحدة الامريكية.

الفرع الخامس: تخريب المعلومات و إساءة استخدامها [2]

يتم تخريب المعلومات بمحو الملفات أو تدمير الوسائط التي تحتويها، أما اساءة استخدام المعلومات فالمقصود بها ، الأذى الذي يتم تحقيقه باستخدام هذه المعلومات مثل عدم تمكين المستفيد من الوصول اليها واستغلالها والاضرار بمصالحه، وهذا النوع من الجرائم يمس خاصة الشركات.

الفرع السادس: تزوير البيانات

وهي اوسع الجرائم انتشارا ، وتتم بإدخال بيانات مغلوطة الى قواعد البيانات او بتعديل البيانات الموجودة عمدا ، بهدف ارتكاب جريمة وبالاعتماد على وسائل لا تترك اي اثر للتعديل او للقائم به.

الفرع السابع : التزييف :

حيث يتم تزيف الوثائق، والأمثلة على ذلك كثيرة منها تزيف الشبكات المصرفية والاسهم والسندات.

الفرع الثامن : تزوير العلامات التجارية

بعض الشركات المنتجة لشرائح المعالجات المركزية يتم تزوير علاماتها التجارية على شرائح ذات أداء منخفض ، ليتم بيعها على أنها أداء أعلى و بأسعار مرتفعة ، مما يلحق ضرار بالمستفيد و بمصالح الشركة التي يتم تزوير علاماتها ، و يكون الدافع من ارتكاب هذه الجريمة السعي وراء الربح و البحث عن التفوق في المنافسة.

---

[1]– محمد صالح الألفي ' (أنماط جرائم الانترنت) 'ص11 http//www-eastlaws.com

[2] – حسين طاهر داود ' جرائم نظم المعلومات ' أكاديمية نايف العربية للعلوم الأمنية ' الرياض ' الطبعة الأولى ' 2000 ص 23

المطلب الثاني: المراحل التي يتم فيها حدوث الجريمة المعلوماتية وآثارها

الفرع 1 : يكون حدوث الجريمة المعلوماتية في احدى 3 مراحل هي:

أولا : مرحلة إدخال البيانات

حيث يقوم المجرم بتغيير و تزوير ، مثلا يتسلل إلكترونيا إلى البيانات المتعلقة بفاتورة الهاتف و يقوم بحذف الكثير من المكالمات قبل طباعتها وارسالها .

ثانيا : مرحلة تشغيل البيانات

يقوم المجرم بتغيير وتعديل البرامج التي تشغل البيانات للوصول لنتائج معينة وغير شرعية ، مثلا يستخدم المجرم برنامج لتقريب الأرقام المتعلقة بالمعلومات البنكية على حساب أحد الأشخاص ،أو تجميع الفروق بين الأرقام المقربة والأرقام الفعلية وإضافتها لحساب آخر لنفس العميل ،بحيث تشكل على مدى سنوات مبلغا ضخما

ثالثا : مرحلة إخراج المعلومات

مثل : سرقة البيانات الإلكترونية، أو إفشاء معلومات متعلقة بإحدى الشركات .

الفرع الثاني : آثار المترتبة على الجرائم الاقتصادية في الاوساط المعلوماتية

سنعرض الآثار على الناحية المالية والاقتصادية

إن تزايد وتيرة الجرائم المعلوماتية وتنوع طرقها ، يلحق خسائر فادحة أكثر مما تسبه الجرائم التقليدية ليس فقط على مستوى الأفراد بل تتعداه إلى مستوى المنظمات والبنوك والمؤسسات والجهات الحكومية وغير الحكومية، وهذا يؤثر سلبا على عالم المال والاقتصاد.

– اولا : على مستولى الفرد

لقد أصبحت أكثر التعاملات والأعمال التي يقم بها الفرد تنجز عن طريقة شبكة المعلوماتية.

إن الجرائم المعلوماتية التي يتعرض لها الفرد وتؤثر على الجانب المادي لديه، من أهمها :

– سرقة الهوية الشخصية.

– سرقة بطاقة الائتمان الخاصة به.

– الابتزاز والتهديد.

– عمليات الاحتيال.

– تحويل أو نقل حسابه المصرفي.

– نقل ملكية الأسهم.

– زيادة الفواتير بتحويل فواتير الجاني للضحية.

– ثانيا : على مستوى البنوك والمؤسسات والجهات الحكومية وغير الحكومية

لقد أتاحت تكنولوجيا الاتصال والمعلومات قنوات اتصال جديدة للناس سهلت التواصل والتفاعل مع تقدمه هذه المؤسسات والهيئات من الخدمات وعروض دون التنقل إليها.

أ– على مستوى البنوك [1]:

– السطو الالكتروني.

– العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها.

– نقل ملكية الأسهم.

ب– بالنسبة للشركات

[1]– منى شاكر فراح ، تأثير الجريمة الإلكترونية على النواحي الاقتصادية ، متاح على الموقع faculty.mu.edu.sa . تاريخ الاطلاع : 17/05/2014

– الاطلاع على معلومات سرية لصفقة أو مناقصة أو أصول تسويقية خاصة و الاستفادة منها.

– سرقة الأموال وتحويل حسابات مصرفية خاصة بالشركة.

– الغش في المعاملات الالكترونية كالتغيير في المبيعات.

– التهديد والابتزاز.

– اختراق الموقع الالكتروني الخاص بالشركة.

ج– بالنسبة للجهات و الاجهزة الحكومية:

– تعطيل أنظمة قطاعات حكومية و حيوية .

– سرقة الأموال .

– تعطيل الأنترنت بالكامل .

د– بالنسبة للجهات والأجهزة الحكومية :

– تعطيل أنظمة قطاعات حكومية و حيوية .

– سرقة الأموال .

– تعطيل الأنترنت بالكامل.

الفصل الثاني

مكافحة الجرائم الاقتصادية في الاوساط المعلوماتية

تمهيد:

فرض الاجرام المعلوماتي نفسه كظاهرة سلبية على المجتمعات بعد التطور المعلوماتي الذي وصلت اليه هذه الأخيرة ، فبدأ التأثير السلبي لهذا الاجرام واضحا مهددا للأفراد والجماعات والاموال والحكومات على حد سواء ، ولتدارك هذا الخطر بدت عملية المكافحة لجريمة المعلوماتية ضرورة حتمية يجب التصدي لها.

خاصة وقد وجدت الدول نفسها عاجزة عن أداء واجبها الدستوري و القانوني لحماية الأفراد وتحقيق هذا النوع الجديد من الإجرام بسبب الفراغ القانوني لمكافحته وذلك بتعديل قوانين عقوباتها القائمة وإصدار قوانين عقابية جديدة تتصدى لمكافحة أنواع الإجرام المعلوماتي الجديد . خاصة تلك الرائدة في مجال التطور المعلوماتي كفرنسا وأمريكا والمملكة المتحدة ....إلخ، ومدى إخضاع هذه القوانين إلى مبدأ الشرعية. كما أن خطورة هذه الجريمة وعجز الدول منفردة في مكافحتها جعلها توحد جهودها .

فعقدت اتفاقيات ومؤتمرات تأثرت بها القوانين الداخلية الى حد كبير وهذا ما سنحاول التعرض له في هذا الفصل .

المبحث الأول: الجرائم المعلوماتية المعاقب عليها في الاتفاقيات الدولية

أمام الصعوبات الكبيرة التي واجهتها الدول في مكافحة الجريمة المعلوماتية عبر قوانينها الداخلية وفي مواجهة أصعب خاصية لها كونها جريمة متعدية الحدود، وجدت الدول نفسها مضطرة لنجاح المكافحة ومن أهم الاتفاقيات الدولية التي تناولت الإجرام المعلوماتي، اتفاقية بودابست المنبثقة عن اتفاقيات المجلس الأوروبي كذلك المعاهدات والقوانين الخاصة بحماية الملكية الفكرية والاتفاقية العربية المجسدة في إطار القانون النموذجي لمكافحة الجريمة المعلوماتية في المطالب الآتية:

المطلب الأول : اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية تكافح جرائم الانترنت '' Internet Crimes **"** وتبلور التعاون و التضامن الدولي في محاربتها و محاولة الحد منها بعد ان وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص و الممتلكات.

لقد جادت بودابست لمكافحة جرائم الانترنت في العديد من الدول التي لا تستطيع بمفردها مواجهة تلك الجرائم، نظرا لكون تلك الجرائم هي من الجرائم عابرة الحدود التي لا يقف امامها اي عائق جغرافي، فتلك الدول تفضل الانضمام الى المعاهدات الدولية تبرم في المجال نظرا لكبر حجم الأضرار عن طريق

الانترنت لأن العديد من الدول حتى المتقدمة منها لا تستطيع مواجهة تلك الاخطار بمفردها دون تعاون وتضامن دولي ليتم نحاج اي مجهودات تبذل في مكافحة الجرائم التي ترتكب عبر الانترنت ،ان التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليم احترام حقوق الانسان مثل الحقوق المكية الفكرية للإنسان [1]

وفي اطار التصدي اكثر لمكافحة الجريمة المعلوماتية عقد المجلس الاوروبي في 11ديسمبر 1995 مؤتمر وزراء الدول الأعضاء لبحث مشاكل لصياغة اتفاقيات لمكافحة الجريمة المعلوماتية بعقد اتفاقية بودابست في 23 نوفمبر 2001 ، ولقد بينت المذكرة التفسيرية لهذه الاتفاقية ان تحديد الجرائم المعلوماتية فيها هدفه تحسين واصلاح وسائل منع وقمع الجريمة المعلوماتية من خلال تحديد معيار بالحد الادنى المشترك، الذي يسمح باعتبار بعض 1التصرفات من قبل الجرائم المعلوماتية ، وانه بالإمكان ان يتم استعمال هذه القائمة في القوانين الداخلية ، كما انه يأخذ في الاعتبار الممارسات غير المشروعة الاكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد.

الفرع الاول :تصنيف الجريمة المعلوماتية حسب اتفاقية بودابست

حددت الاتفاقية (اتفاقية بودابست) الجرائم المعلوماتية وصنفتها في خمسة عناوين في القسم الاول من الاتفاقية.

العنوان الاول : ويضم جوهر جرائم الحاسب الآلي ، او الجرائم المعلوماتية ، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإباحة البيانات والنظم .

العنوان الثاني : ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي ، التي تمس بعض المصالح القانونية تحميها قوانين العقوبات وتضم ايضا قوانين الغش المعلوماتي والتزوير المعلوماتي.

العنوان الثالث : ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى ، وهي التي تخص الانتاج والنشر غير المشرع للمواد الإباحية الطفولية عبر النظم المعلوماتية ، في المادة التاسعة من الاتفاقية

العنوان الرابع : ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة العاشرة من الاتفاقية .

---

[1] – جعفر حسن جاسم الطائي ، المرجع السابق ص 277–288

العنوان الخامس: وهو يشمل على احكام اضافية بخصوص الشروع والاشتراك وايضا الجزاءات والاجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الاشخاص المعنوية[1]

الفرع الثاني : الشروط ووصف الجريمة المعلوماتية حسب اتفاقية بودابست

وقد اوجبت اتفاقية بودابست مجموعة من الشروط حتى تأخذ الافعال السابقة وصف هذه الجريمة وده الشروط هي :

أ . ان ترتكب الجرائم المذكورة في الجريمة دون وجه حق.

ب . ان ترتكب الجرائم المذكورة بطريقة عمدية من اجل اقرار المسؤولية الجنائية . ولدراسة المكافحة الموضوعية للجريمة المعلوماتية في اتفاقية بودابست ارتأيت دراسة اهم المواد التي جاءت لمكافحة هذه الجريمة كالتالي مع التعليق عليها :

الجرائم الوارد العناوين من 1 الى 4 قد نصت عليها المواد من 2 الى 10من اتفاقية بودابست وهي :

المادة الثانية : جريمة الولوج او الدخول غير القانوني التي تنص على انه " يجب على كل طرف ان يتبنى الإجراءات التشريعية او اي إجراءات اخرى انها ضرورية من اجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي للولوج العمدي لكل او جزء من جهاز الحاسوب دون حق ، كما يكمن ان ترتكب الجريمة من خلال انتهاك اجراءات الأمن بنية الحصول على بيانات الحاسب ،او اية نية اجرامية اخرى وان ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر فيدخل بالتالي في عداد هذه الجرائم كل من الافعال : القرصنة والسطو والدخول الغير مشروع في النظام المعلوماتي[2]

المادة الثالثة : تنص على جريمة الاعتراض غير القانوني الهدف منها حماية الحق في احترام نقل البيانات والاتصالات ، والتسجيل التقليدي للمحادثات التليفونية بين الاشخاص وهذه الحقوق كانت مكفولة سابقا بنص المادة 8 من الاتفاقية الاوروبية لحقوق الانسان .

---

[1] – طارق ابراهيم الدسوقي عطية ، المرجع السابق ص 302

[2] –خالد ابراهيم ممدوح ، الجرائم المعلوماتية ، دار الفكر الجامعي ، بدون بلد ، الطبعة الاولى ، 2009 ص 277

المادة الرابعة: تنص على أشكال الاعتداء على سلامة البيانات ونصها كالاتي " يجب على كل طرف أن يتبنى الإجراءات التشريعية ، وأية إجراءات أخرى يرى أنها ضرورية للتجريم تبعا لقانونه الداخلي إذا تحدث ذلك عمدا ودون حق، أي إضرار أو محو أو تعطيل أو إتلاف أو طمس لبيانات الحاسب ".

المادة الخامسة: تنص هذه المادة على جريمة الاعتداء على سلامة النظام كالتالي: " يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للتجريم في قانونه الداخلي: " الإعاقة الخطيرة إذا تم ذلك عمدا ودون حق لوظيفة نظام الحاسب عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية " .

هدف هذه المادة هو تجرم الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية، بما في ذلك نظم الاتصال باستخدام أو التأثير على بيانات الحاسب والمصالح القانونية المحمية بنص هذه المادة هي مصلحة مشغلي ومستخدمي نظام الحاسب الآلي، أو نظام الاتصالات في عمل هذه الأجهزة بدقة وقد شمل نص هذه المادة على كل من افعال الإدخال أو النقل أو الإضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية وهذه المصطلحات كلها يمكن اختصارها تجريم فعل الإعاقة الذي يضمها كلها والتي يجب أن تكون جسيمة وبدون وجه حق حتى تعتبر فعلا مجرما ومعاقب عليه[1]

المادة السادسة: تنص المادة 6 من اتفاقية بودابست على جريمة إساءة استخدام أجهزة الحاسب. اعتبر نص هذه المادة أن ارتكاب مجموعة من الأفعال عمدا التي ترتبط ببعض الأجهزة، أو بيانات الولوج أو الدخول من حيث إساءة استخدامها وبغرض ارتكاب جريمة والتي حددها في كل من الأفعال التالية: إنتاج أو بيع أو الحصول من أجل الاستخدام أو استيراد أو نشر أو أي أشكال أخرى للوضع تحت التصرف:

أ. جهاز يحتوي على برنامج معلوماتي بشكل أساسي لغرض ارتكاب الجرائم المنصوص عليها في المواد 2 و 5 السابقة الذكر.

ب. كلمة المرور أو شفرة الدخول أو أية بيانات أخرى مماثلة تسمح بالولوج إلى كل أز إلى جزء من نظام الحاسب. بنية استخدامها لغرض ارتكاب جريمة من الجرائم المنصوص عليها في المواد 2 الى 5، وقد اشترطت المادة أن ينطبق التجريم على الأجهزة المصممة أساسا من أجل ارتكاب

[1]– هدى حامد قشقوش، **جرائم الحواسب الالكترونية في التشريع** المقارن، دار النهضة العربية، القاهرة ، 1992، ص 106 وما بعدها.

جريمة كما اشترط أن ترتكب الأفعال السابقة عمدا وبدون وجه حق وهذا تجنبا لخطر العقاب المبالغ فيه.

المادة السابعة: نصت على جريمة التزوير المعلوماتي لخطورة هذه الجريمة وسهولة ارتكابها حيث جاءت هذه المادة بغرض إنشاء جريمة في قوانين موازية لجريمة تزوير المستندات الورقية، وهي تنص على أنه " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم وفقا لقانونه الداخلي نية الغش أو نية إجرامية مشابهة من أجل تقرير غير مصرح به لبيانات المسجلة، بطريقة من المصالح القانونية المحمية، والأمن والثقة في البيانات المخزنة، عمليات الإدخال والإتلاف والمحو أو الطمس تشكل أعمالا مماثلة لجريمة التزوير محور صحيح.[1]

المادة الثامنة: وتخص جريمة الغش المعلوماتي تنص هذه المادة على أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم: التسبب عمدا أو دون حق في إحداث ضرر مالي للغير عن طريق:

أ الإدخال، الإتلاف، المحور أو الطمس، لبيانات الحاسوب.

ب كل شكل للاعتداء على وظيفة الحاسب بنية الغش أو أية نية إجرامية مشابهة من أجل الحصول دون حق على منفعة اقتصادية له أو لغيره، مضمون هذه المادة يتلخص في مكافحة الجرائم التي تتم من خلال تلاعبات بمداخلات النظام، وتغذيته ببيانات غير صحيحة بالتلاعب

المطلب الثاني: الجرائم المعلوماتية في القانون العربي النموذجي.

أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في هذا النطاق مما حذا بهذه الدول الى المحاولة لإيجاد سبل تشريعية اجرائية ناجعة لمواجهة هذا النوع من الجرائم المستجدة[2].

نجد من تلك الجهود القرار الصادر عن قرار وزراء العرب الخاص بإصدار القانون الجزائي الموحد ، كقانون عربي نموذجي.

---

[1]– طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 323.

[2] / محمد علي العريان ، **الجرائم المعلوماتية** ، دار الجامعة الحديدة ، الاسكندرية ،2004 ص 33

وقد جرم القانون العربي النموذجي لمكافحة الجريمة المعلوماتية ، مجموعة من الافعال مرتبطة بإساءة تقنية المعلومات والتي اعتبرها جرائم مستحدثة يجب التصدي لها ومكافحة خطورتها الكبيرة على الافراد والمجتمع وبين هذه الجرائم سنحاول بالدراسة مجموعة منها كما يلي :

الفرع الأول : جريمة غسيل الاموال عبر الوسائط الالكترونية

تنص المادة التاسعة عشر من القانون العربي النموذجي لمكافحة الجريمة المعلوماتية، على انه " كل من قام بتحويل الاموال غير المشروعة او نقلها او تمويه المصدر غير لها او اخفائه او قام باستخدام او حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع او بتحويل المواد او الممتلكات مع العلم بمصدرها غير المشروع وذلك عن طريق استخدام نظام الحاسب الإلكتروني او شبكة المعلومات الدولية بقصد اضفاء الصفة المشروعة على تلك الأموال وتترك العقوبة وفقا لتقدير كل دولة .

ولتجريم سلوك غسيل الاموال بمفهومها السابق يجب ان تتوفر الآتي :

اولا الركن المادي : والمتمثل في صور السلوك الاجرامي حتى تقوم هذه الجريمة وهي :

أ- **تحويل الاموال او نقلها :** ويقصد به جميع العمليات المصرفية التي يتم تحويل الأموال بمقتضاها والعمليات غير المصرفية التي تتم بوسائل الكترونية بسيطة أو معقدة كالتحويل البرقي للنقود، والتحويل من حساب الى حساب عن طريق شبكة الانترنت، كما يتم تحويل الأموال عن طريق تغيير شكلها كأن تشتري مجوهرات أو سبائك ذهب بالعملة المحلية ثم يعاد بيعها، وأيضا عن طريق بطاقات الائتمان المزورة أو التحويل عن طريق تحويل العملة الوطنية إلى عملة أجنبية عندما لا توجد قيود تشريعية على عمليات التحويل.

ب- **إخفاء وتمويه حقيقة الأموال:** ويقصد بها السلوك إبعاد الأموال عن مصدرها الإجرامي المستمد منه بإتباع أساليب بالغة التعقيد من التحولات المالية، بهدف إخفاء مصدرها غير المشروع.

ج- **اكتساب أو حيازة أو استخدام الأموال المتحصلة من الجريمة:** ويقصد بهذا السلوك أن مجرد اكتساب أو حيازة أو استخدام الأموال مع علم الفاعل بأن تلك الأموال متحصلة من جريمة من الجرائم يعد ذلك السلوك مجرما ويعاقب عليه.

د- **محل السلوك الاجرامي:** تتفق معظم التشريعات في كافة الدول " كالتشريع المصري في القانون رقم 80 الصادر في ماي 2002 والمتعلق بكافة غسل الأموال والتشريع التونسي في القانون رقم 75 الصادر سنة 2003 والتشريع السويسري الصادر في أفريل 1998" [1].

وقد نص المشرع العربي في القانون النموذجي على محل الجريمة غسل الأموال الالكترونية بأنه "الأموال غير المشرعة" حيث جاءت هذه العبارة عامة حتى يمكنها احتواء كل المصطلحات والمفردات الخاصة بالأموال سواء كانت منقولة أم غير منقولة ما دامت أنها محل لغسل الأموال.

هـ- **النتيجة الإجرامية:** تنص المادة التاسعة عشر من القانون النموذجي العربي في شأن جريمة غسل الأموال الالكترونية على النتيجة الإجرامي هو إخفاء المال وتمويه وتغيير حقيقته وطبيعته على النحو الذي يتم الحصول عليه من الجريمة الأصلية.

ثانيا: الركن المعنوي: فحسب نص المادة التاسعة عشر من القانون العربي النموذجي العربي شأن مكافحة الجريمة المعلوماتية تعتبر جريمة غسل الأموال في صورتها الالكترونية من الجرائم العمدية التي تقوم القصد الجنائي العام بعنصريه العلم والإرادة بالإضافة إلى القصد الجنائي الخاص.

فالقصد الجنائي العام معناه علم الجاني بأنه يمارس نشاطا غير مشروع وهو غسل الأموال المتحصلة من جريمة وانصراف نيته. إلى إتيان هذا الفعل وقبول النتائج المترتبة عليه أي العلم والإرادة، أما القصد الخاص يقصد به أن تتجه نية الفاعل من جريمة غسل الأموال إلى إخفاء المال أو طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته والحيلولة دون اكتشاف ذلك، أو عرقلة الوصول إلى شخص من ارتكاب الجريمة المتحصل منها على المال[2].

ولقد نصت المادة التاسعة عشر من القانون العربي النموذجي على وجوب توفر القصد الجنائي الخاص في جريمة غسل الأموال الالكترونية، بارتكابه الجريمة المنظمة عن طريق استخدام نظام الحاسب الالكتروني أو شبكة المعلومات الدولية بقصد إخفاء الصفة المشروعة تلك الأموال، بإضفاء صفة المشروعية عليها ما هو الاّ قصد جنائي خاص يتمثل في إظهار المال المغسول بمظهر المال المشروع، مع العلم أنه متحصل من مصدر غير مشروع، وتأخذ جريمة غسل الأموال الالكترونية صورا عديدة لارتكابها من هذه الصور على سبيل المثال.

---

[1]- عبد الله عبد الكريم عبد الله، المرجع السابق، ص 277.

[2]- عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، المرجع السابق ص 119.

أ- **استخدام بطاقة الائتمان:** لشراء مجوهرات أو أشياء ثمينة كلوحات فنية باهظة الثمن، يتم سداد الفاتورة الخاصة بها لاحقا بالنقود المتحصل عليها من جرائم الاتجار بالمخدرات.

ب- **أعمال الصيرفة الالكترونية** : تتلخص في عملية امتلاك مصرف وإدارته بمساعدة الاخرين بحيث يمكن لأي شخص شراء مصرف وادارة اعمال الصيرفة الالكترونية (سويفت Swift) وهي خدمة خاصة بنقل الاموال وتقديم خدمات مالية الى الوسطاء وتجار السندات وشركات المقاصة والاسواق المالية الكبرى، وسهولة اعمال الصيرفة الالكترونية ساعد على انتشار جريمة غسل الاموال الالكترونية لسيطرة عصابات الجريمة المنظمة على المصارف ، وبالتالي اصبح لديها حرية واسعة في غسل كميات كبيرة من غسيل الموال ليس لنفسها فقط بل وحتى للمنظمات الاجرامية الاخرى[1]

الفرع الثاني: جريمة اختراق النظم المعلوماتية

تنص المادة الثالثة على أنه "كل من توصل بطريقة التحايل لاختراق نظم المعالجة الآلية للبيانات يعاقب بالحبس والغرامة (تترك العقوبة لتقدير كل دولة)، وإذا نتج عن هذا الفعل محو أو تعديل للبيانات المخزنة بالحاسب أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غيرها من الأساليب المعلوماتية، تكون العقوبة بالحبس والغرامة المالية " وتترك العقوبة لتقدير كل دولة.

وحسب نص المادة تتحقق جريمة اختراق النظم المعلوماتية بارتكاب:

أ- كل من جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي بأي وسيلة تقنية كانتهاك كلمة السر الحقيقية أو عن طريق استخدام برنامج أو شفرة خاصة ، ويتحقق هذا الدخول متى دخل الجاني إلى النظام المعلوماتي كله أو جزء منه دون وجه حق، أي دون موافقة صاحب النظام أو من له حق السيطرة عليه، أما فعل البقاء غير المشروع داخل النظام المعالجة الآلية للمعطيات فقد كان الهدف من تجريمه هو تجريم البقاء غير المشروع داخل النظام المعلوماتي لمن كان دخوله إلى هذا النظام بطريق الصدفة ودون قصد جنائي ومع ذلك يبقى داخل النظام وتنصرف إرادته لذلك[2]

ب- حسب نص المادة الثالثة من القانون النموذجي العربي لمكافحة الجريمة المعلوماتية فقد عاقب المشرع على فعل إعاقة تشغيل نظم معالجة البيانات بفعلي التعطيل بأي وسيلة كانت كسبب

---

[1]- إيهاب فوزي السقا، **جرائم التزوير في المحررات الالكترونية**، دار الجامعة الجديدة، الإسكندرية، 2008، ص 42.

[2]- عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت** ، المرجع السابق ،ص 325 .

التسريب للفيروسات، ومثالها استخدام "القنبلة المنطقية" أو استخدام فيروس "حصان طروادة" التي مفادها "القنبلة المنطقية" أنها عبارة عن برنامج أو جزء منه ينفذ في لحظة محددة أو كل فترة زمنية منتظمة في شبكة المعلوماتية من أجل تسهيل تنفيذ عمل غير مشروع، أما برنامج حصان طروادة فهو برنامج يقوم بتغيير محسوس في برنامج والمعطيات، كذلك هناك فيروس "الدودة" وهو عبارة عن برنامج يتميز بقدرة فائقة على تعطيل وإيقاف نظام الحاسب، وهذه الفيروسات تقوم بإفساد البرامج والمعطيات المعلوماتية

ج- أما المحور المذكور في المادة الثالثة من القانون النموذجي العربي فيقصد به ذلك السلوك الإجرامي بإزالة جزء من المعطيات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة.

د- التعديل ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتم التلاعب في المعطيات عن طريق استبدالها أو التلاعب في البرنامج أو إمداده بمعطيات مغايرة تؤدي إلى نتائج غير التي صمم لها البرنامج.

وجريمة اختراق النظم المعلوماتية هي جريمة عمدية في كل صور السلوك الإجرامي التي رأيناها سابقا وصورة الركن المعنوي فيها هو القصد الجنائي العام بركنيه العلم والإرادة أي باتجاه إرادة الجاني إلى فعل الاختراق أو البقاء غير المشروع أي اتجاه إرادته إلى أفعال الدخول والإدخال والمحو والتعديل....التي هي صور السلوك الاجرامي في هذه الجريمة واتجاه ارادته اليها مع العلم بأن نشاطه وسلوكه هذا غير مشروع [1].

وقد عاقب المشرع العربي في القانون النموذجي على الشروع في الجرائم السابقة المشار لها وبنص العقوبة المقررة لها في حالة الجريمة التامة في المادة 24 منه.

الفرع الثالث : جريمة التزوير المعلوماتي

نصت المادة الرابعة من القانون النموذجي العربي الموحد بشأن مكافح على انه (كل من زور المستندات المعالجة آليا او البيانات المخزنة في ذاكرة الحاسوب او شريط اسطوانة ممغنطة او غيرها من الوسائط وتترك العقوبة وفقا لكل دولة) كما نصت الفقرة الثانية من المادة الرابعة من

[1] – عبد القادر القهوجي **الحماية الجنائية لبرامج الحاسب الآلي** ، دار الجامعة الحديث ، الاسكندرية ، 2006 ص 30

نفس القانون على انه " كل من استخدم المستندات المزورة آليا مع علمه بتزويرها يعاقب بنفس عقوبة التزوير فإن كان المستخدم هو نفسه مرتكب فعل التزوير يعاقب وفقا للقواعد العامة المعمول بها في هذا الشأن". فالتزوير في صورته التقليدية هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييرا من شأنه أن يرتب ضررا للغير وبنية استعمال هذا المجرم فيما أعده له.

أما التزوير المعلوماتي فهو "تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها[1].

فيتغير الحقيقة في النظام الآلي في المعالجة المعلوماتية يتم بتغيير البيانات أو المعلومات أو صنفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة في ذاكرة الحاسب أو كانت تمثل جزءا من برنامج التشغيل أو برنامج التطبيق شرط أن تطبق هذه البيانات على دعامة مكتوبة أو مسجلة بحيث يكون لها كيان مادي يمكن إدراكه.

الفرع الرابع: السرقة المعلوماتية

نص المشرع العربي في المادة الرابعة عشر على سرقة المعلومات بتجريم كل من عمليات نسخ ونشر لمصنفات الفكرية أو الأدبية، أو الأبحاث العلمية، أو ما في حكمها إذا ما ارتكب دون وجه حق، بعقوبة الحبس الذي يترك تقديرها وفقا لقانون كل دولة، ودون الاختلال بنصوص الخاصة بالملكية الفكرية لكل بلد.

أما المادة 11 من القانون النموذجي العربي فهي تعاقب على الاستيلاء على نقود الغير أو ماله إذا تم بطريق بطاقات الائتمان حيث تنص "كل من استخدم بطاقة ائتمان للسحب الالكتروني من الرصيد خارج حدود رصيده الفعلي أو قان باستخدام بطاقة مسروقة أو تحصل عليها بأي وسيلة يعاقب ويترك العقوبة لتقدير كل دولة ".

هذا ولم يصل المشرع العربي في القانون النموذجي لمكافحة الجريمة المعلوماتية الاهتمام بنص على مكافحة الجرائم الخاصة بالاعتداء على حرمة الحياة الخاصة لما لهذه الأفعال من آثار وخيمة على حياة الأشخاص وأمرهم ، وبالتالي على المجتمع الدولي ككل لذلك النص على تجريم أفعال التنصت على المراسلات الالكترونية وذلك في المادة الثامنة من هذا القانون.

---

[1]– فوزية عبد الستار ، **قانون العقوبات (القسم الخاص)**، دار النهضة العربية، بدون بلد، 1988، ص 244.

أما المادة 19 فقد جرم فيها مجموعة من الأفعال التي تمس العقوبات القانونية والآداب العامة وهذه الأفعال المجرمة هي:

أ- أفعال الاعتداء على القيم الدينية كالإساءة إلى إحدى المقدسات والشعائر المقررة في الأديان الأخرى والإساءة إلى إحدى المقدسات و الشعائر الإسلامية.

ب- وسب أحد الأديان السماوية المعترف بها (كالمسيحية والإسلام واليهودية).

هذا وقد نصت في المادة 17 على مكافحة جرائم العرض والاتجار بالبشر من خلال نظام الحاسب الآلي لخطورة هذه الجرائم[1].

غير أن الملاحظ في هذه المحاولات على المستوى العربي هو اعتمادها على علاج نقص التشريعات والانظمة الخاصة بموضع جرائم الانترنت. كما شملت هذه المحاولات العديد من تعليمات أمن المنشآت الحاسوبية ، والأجهزة والبرامج وبعض القواعد العامة المنظمة لارتباط المنشأة الحكومية بالشبكة العالمية.

المبحث الثاني: الجهود التشريعية للحد من الجريمة المعلوماتية

[1]- عبد الفتاح بيومي حجازي ، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، المرجع السابق ، ص 678 .

دأبت المجتمعات والدول عبر حقب زمنية مختلفة في سن تشريعات وقوانين من أجل مواجهة كل من تسول له نفسه خرق الآداب العامة بأعمال غير مشروعة، ومن ذلك الجرائم المعلوماتية، إذ رقم قلتها إلاّ أنها تعتبر محاولات هامة في هذا المجال، وتتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات والمنظمات العالمية، بالإضافة إلى المنظمات الإقليمية، والتي تعتبر كإطار دولي يوازي عالمية الجريمة المعلوماتية.

تعتبر الجهود الدولية، دعامة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية ،فهي تعتبر بمثابة قوانين استرشادية بالنسبة لها، فهناك الكثير من الدول التي اتخذت سبيل تطوير قوانينها وفي هذا الإطار نستعرض تجربة المشرع الجزائري من أجل مكافحة ومواجهة الجريمة المعلوماتية.

المطلب الأول: تطور الحماية الجنائية المستوى الدولي

إن الطابع الدولي للجريمة المعلوماتية نطاقه لا يعني كونها من الجرائم الدولية التي يتناولها القانون الدولي الجنائي، فهي جرائم داخلية وإن كانت عالمية ، وهو ما جعل كل دولة تقف بمفردها عاجزة عن التصدي لها.

وسنبين الجهود الدولية في مواجهة الجريمة المعلوماتية أولا ثم نتطرق إلى الجهود الداخلية ثانيا.

الفرع الأول: الأمم المتحدة

بدأ اهتمام الولايات المتحدة الأمريكية بمكافحة الجريمة المعلوماتية في 1966 في أول قضية HANCOCKE USTATE تعرض لموضوع إساءة استخدام الحاسبات الآلية وتتلخص وقائع هذه القضية في اتفاق مبرمج لحاسبات آلية بإحدى الشركات بالاتفاق مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 59 برنامجا ملكا للشركة التي يعمل بها والتي هي ذات أهمية كبيرة وتسليمها للشركة الأخرى مقابل تلقيه 5 ملايين دولار وأثناء التسليم، تم القبض على المتهم وقدم للمحاكمة بتهمة السرقة[1]

تسعى الأمم المتحدة من خلال هيئتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة وكانت الانطلاقة في المؤتمر السابع المنعقد بميلانو 1985 والذي أكدت على

[1]– نائلة عادل قورة، المرجع السابق، ص 147.

الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الظاهرة، وقد أشارت إلى مسألة الخصوصية واختراقها بالاطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي وضرورة اعتماد ضمانات لحماية سريتها.

كما أكدت اللجنة على ضرورة تشجيع التشريعات الحديثة التي تتناول هذه الجرائم بصفتها نمط من أنماط الجريمة المنظمة، وفي سنة 1990 انعقد مؤتمر هافانا لعام 1990 أرست توصياته على مجموعة من المبادئ التالية:

1- تحديد القوانين الجنائية الوطنية.
2- تطوير أمن الحاسب الآلي والتدابير المنعية.
3- اعتماد إجراءات تمنع كافة الموظفين والوكالات المسؤولة لمنع الجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
4- تلقين آداب الكمبيوتر كجزء من مفردات الاتصال والمعلومات.
5- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم[1].

تزايد الجرائم المرتكبة عبر الانترنت وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا إجرامية لسنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى الدور الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية[2]

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل أيام 17- 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة الجريمة بما في ذلك الجريمة الحاسوبية، حيث

---

[1]- هلالي عبد الله أحمد، **الجوانب الموضوعية والاجرائية للجريمة المعلوماتية على ضوء اتفاقية بودابست الموقعة في 2001/11/23** دار النهضة العربية، القاهرة، ص 62 .

[2]- اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض اجرامية، رقم (55/63)، الصادرة عن هيئة الامم المتحدة، الجلسة العامة 81، ديسمبر 2000.

احتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[1].

دأبت منظمة الأمم المتحدة وذلك استمرارا لتلك الجهود المبذولة لمكافحة جرائم الانترنت على عقد مؤتمرات، فلم تكن المؤشرات السابقة الذكر الأولى ولن تكون الأخيرة، حيث عمدت اللجنة الاقتصادية والاجتماعية لغربي آسيا التابعة للمجلس الاقتصادي والاجتماعي وذلك تحت غطاء منظمة الأمم المتحدة على عقد ورشة عمل حول التشريعات السيبيرانية وتطبيقها في منظمة الاسكوا عام 2008.

بالإضافة إلى تلك المؤتمرات التي عقدتها أطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقدة بفينا في أكتوبر 2010، حيث بين المؤتمر فهرس الأمثلة المعلقة بتسليم المجرمين وتبادل المساعدة القانونية وأشكال أخرى من التعاون الدولي في المسائل القانونية، استنادا إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[2].

تبقى هيئة الأمم المتحدة الإطار الأمثل لمكافحة هذا النوع من الإجرام، وسوف تبقى تبذل مجهودا أكثر مادام هناك مجرمين يجوبون الفضاء السيبيراني .

الفرع الثاني: القوانين المقارنة

من هاته القوانين القانون الفرنسي، حيث كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي من فرنسا من طرف وزير العدل سنة 1995، عندما تقدم بمشروع قانون عقوبات جديدة أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان: الجرائم في المادة المعلوماتية كان يتكون من 8 مواد من 1/307 إلى 8/307 لكن هذه المحاولة لم يكتب لها النجاح إلاّ في 1986/08/05 عندما تقدم النائب "Jacquet Godfrain " ونواب آخرون إلى الجمعيات الوطنية باقتراح مشروع قانون عن الغش المعلوماتي، قد حاولوا تعديل بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية

---

[1]– مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الاخيرة، في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12–19 افريل 2010، رقم 213/09 A/Confi.

[2]– مؤتمر هيئة الأطراف في اتفاقية الامم المتحدة لمكافحة الجريمة المعلوماتية عبر الوطنية، المنعقد بفيينا في 18–22 أكتوبر 2010 رقم: CTOC/Cop/2010/ crp 5

كالسرقة وخيانة الأمانة والتزوير و الإتلاف و الإخفاء وذلك لتشمل العدوان على المال المعلوماتي، وبعد مناقشات طويلة استمرت عاما ونص العام أسفرت على صدور قانون يختلف تماما عن المشروع الذي قدم ويتشابه إلى حد كبير مع المشروع الذي قدمه وزير العدل في 1985. وقد تضمن النص على الجرائم التالية:

1- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو جزء منه وتشديد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل هذا النظام وإفساد وظيفته.
2- إدخال معطيات في النظام أو محو أو تعطيل المعطيات الموجودة فيه عمدا وبدون مراعاة حقوق الغير.
3- كل فعل من شأنه أن يعرقل أو يفسد عمدا بدون مراعاة حقوق الغير أداء النظام لوظيفته.
4- تزوير مستندات المعالجة آليا أيا كان شكلها واستعمال هذه المستندات.
5- الشروع في ارتكاب الجرائم السابقة.
6- الاتفاق الجنائي على ارتكاب الجرائم السابقة.

أما المحطة السابقة من محطات التجريم المعلوماتي فكانت عام 1994 بعد تعديل قانون العقوبات الفرنسي وقد استخدم هذا التعديل مصطلح: الغش المعلوماتي، كما طور في جريمة التزوير المعلوماتي إلى جريمة تزوير المستندات المعلوماتية[1]. قد أوكل هذا القانون إلى النيابة العامة سلطة التحقيق بما في ذلك طلب عمل التحريات وسماع الأقوال والشهود[2].

وكما أقر التعديل على مسؤولية الشخص المعنوي بعدما كان الفقه والقضاء الفرنسي منقسما بشأنها.

وبعد عشر سنوات من هذا التعديل جاء تعديل آخر لقانون العقوبات الفرنسي سنة 2004 أضاف بموجبه المشرع جريمة أخرى هي جريمة التعامل في وسائل المكتب يمكن ان ترتكب بها جريمة، أي الوسائل التي تصلح لأن ترتكب بها جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات أو الإعاقة وإفساد الأنظمة المعالجة الآلية للمعطيات[3].

---

[1]- محمد سامي الشوا، المرجع السابق ص 200.

[2]- جعفر حسن سالم الطائي، المرجع السابق، ص 162 .

[3]- عبد القادر القهواجي، المرجع السابق ، ص 69.

في كندا فهي تطبق قوانين متخصصة ومفصلة للتعامل مع الجرائم، حيث عدلت في (1985) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم خاصة بجرائم الحاسب الآلي والإنترنت كما شمل القانون الجديد أيضا تحديد للعقوبات المطبقة على المخالفات الحاسوبية وجرائم التدمير وجرائم الدخول غير المشرع على المعاملات الالكترونية، كما وضح القانون صلاحيات جهات التحقيق، كما جاء في قانون المنافسة الذي يخول لمأمور القبض القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي والتعامل معها وضبطها.

أما في الدنمارك فقد انتهت لهذا الأمر أيضا فقد سنت أول قانون خاص بها في مجال مكافحة جرائم الانترنت والحاسب الآلي (1985)، وقد شمل القانون العقوبات المحددة على ما يرتكب من جرائم مثل الدخول غير المشروع إلى الحاسب الآلي أو تزوير البيانات سواء كان هذا التزوير بالحذف أو بالإضافة أو بالتعديل[1].

أما هولندا فقد قامت هي الاخرى بتعديل القوانين الخاصة بها للتواؤم مع تلك الجرائم الحديثة ليكون في إمكانها التعامل مع محاولة السيطرة عليها، فقد قامت بتعديل القوانين الخاصة بها، ونصت في تلك القوانين على أنه من حق القاضي أن يصدر أوامره بالتصنت على شبكات الحاسب الآلي

متى ما كانت هناك جريمة خطيرة، ومتى كان التصنت على قدر من الأهمية للكشف عن تلك الجريمة.

أما فنلندا فهي الأخرى تم تعديل القوانين الخاصة بها وأصبح للقاضي الحق في إصدار أوامره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها ألاّ أن القانون قد أعطى ذلك المحقق بشرط ألاّ في مدة أقصاها ثلاثة أيام.

أما في اليابان فقد قامت هي الأخرى بسن القوانين الخاصة بها لتستوعب المستجدات الإجرامية المتمثلة في جرائم الانترنت والحاسب الآلي وقد نصت تلك على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما لتعاون مع جهات التحقيق وإنشاء كلمة سر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته كما أقرت في قانون خاص سنته عام (1990)، شرعية التصنت على شبكات الحاسب الآلي فقط إذا ما كان ذلك في مجال البحث عن الأدلة الخاص بإحدى الجرائم الالكترونية.

---

[1]– جعفر حسن جاسم الطائي، المرجع السابق، ص 230 .

قامت دولة المجر هي الأخرى بدورها تماشيا مع الوضع الجديد، بسن القوانين خاصة بها لتجرم الجرائم الالكترونية وقد نصت تلك القوانين التي سنتها على كيفية التعامل مع مثل هذا النوع من الجرائم، وأيضا كيفية التعامل مع المتهمين بارتكاب الجرائم، وهي الإجراءات التي تسهل على عمل الجهات المنوطة بها مواجهة مثل تلك الجرائم والقبض على المتهمين بارتكابها[1].

كذلك دولة بولندا قامت بسن قوانين خاصة بها فتلك القوانين التي سنتها تنص على أن للمتهم بارتكاب الجرائم الحق في عدم طبع أي سجلات خاصة بالحاسب الآلي وإنشاء كلمة السر المستخدمة أو حتى الأكواد الخاصة بالبرامج، كما أنها تنص على حقوق اخرى بالنسبة لشهود في تلك الجرائم فهي تعطي الشاهد الحق في الامتناع عن طرح المعلومات المسترجعة من الحاسب الآلي متى ذلك قد يؤدي إلى إدانته أو إدانة أي من أقاربه، بل إن تلك القوانين تذهب الى مدى أبعد من ذلك فتلك القوانين تنص على أنه لا يقابل ذلك أي اجراء قسري قد يتخذ وتكون من نتائجه إدانة بالمتهم[2].

المطلب الثاني: مكافحة الجريمة المرتكبة عبر الانترنت في قانون العقوبات وقانون الوقاية من جرائم تكنولوجيا الاعلام و الاتصال

الفرع الاول : مكافحة الجريمة المرتكبة عبر الانترنت في قانون العقوبات

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما والإجرام عبر الانترنت خصوصا بموجب القانون 04-15[3]. المتضمن تعديل قانون العقوبات، الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي:

أولا: جريمة التوصل أو الدخول غير المصرح به: تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط[4]، وهو ما أشارت إليه المادة 394 مكرر من قانون العقوبات بنصها على:

---

[1]- منير محمد الجنيهي، ممدوح محمد الجنيهي المرجع السابق، ص 106.

[2]- منير محمد الجنيهي، محمد الجنيهي المرجع السابق، ص 107.

[3]- قانون 04-15مؤرخ في 10-11-2004 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 الصادر في 10-11-2004.

[4]- أنظر في محاضرة ألقيت من طرف بورزام أحمد، وكيل الجمهورية لدى باتنة، تحت عنوان الجرائم المعلوماتية، المجلس القضائي بباتنة يوم 20 جوان 2006، ص14.

" يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب عن ذلك حذف او تغيير لمعطيات المنظومة او ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة " اورد المشرع طرفين لتشدد عقوبة الدخول غير المشروع الى المنظمات المعلوماتية اوله حذف او تغيير المعطيات، والطرف الثاني هو تخريب نظام اشتغال المنظومة وقد اشار المشرع في المادة المذكورة اعلاه على تجريم فعل الشروع في جريمة الدخول غير المصرح به، ذلك بقوله او يحاول ذلك .

ثانيا : جريمة التزوير المعلوماتي: النشاط الاجرامي في هذه ينحصر في افعال الادخال والمحو والتعديل، ولا يشترط اجتماعها معا حتى يتوافر النشاط الاجرامي فيها إذ يتوفر الركن المادي لجريمة بمجرد القيام بفعل واحد على حدا، لكن القاسم المشترك في هذه الافعال جميعا هو انطواؤها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة او محو او تعديل آخر قائمة[1]

ولقد اكد المشرع على معاقبة هذه الجرائم في المادة 394 مكرر 1 بنصها:

" يعاقب بالحبس و الغرامة كل من أدخل بطريق الغش معطيات نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ".

ثالثا: جريمة الاستيلاء على المعطيات: تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي، وهي ما أقرته المادة 394 مكرر 2 بنصها على:

" كل من يقوم عمدا أو بطريق الغش1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو مرسلة أو معالجة عن طريق منظومة معلوماتية2- حيازة أو إنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ".

رابعا: جريمة إتلاف وتدمير المعطيات : تطرق المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات والتي تنص على:

---

[1] – خثير مسعود ، **الحماية الجنائية لبرامج الكومبيوتر (اساليب وثغرات)** دار الهدى ، عين مليلة، الجزائر،2010 ص 123

" يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تضمنها "

خامسا: جريمة الاحتيال المعلوماتي : تطرقت إليه فحوى 394 مكرر

2/ 1 من خلال نصها على: "يعاقب بالحبس والغرامة كل من قام بطريق الغش بتصميم أو بحث أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة مرسلة عن طريق منظومة معلوماتية ..." أي أن يهدف مرتكبها إلى جني فوائد مالية جراء ذلك [1].

سادسا: أنشطة الانترنت المجسدة لجرائم المحتوى الضار و التصريف غير القانوني: نصت المواد القسم السابع مكرر من ق . ع وخاصة المادة 394 مكرر 2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي تطرأ على المعطيات الآلية بهدف المنافسة غير المشروعة، الجوسسة ، الإرهاب، التحريض على الفسق، جمع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر 6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[2].

تمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي:

عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة 394 مكرر 6 والمتمثلة في:

المصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل وأماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت الذي ترتكب فيه هذه الجرائم بشرط عام مالكه أو المشرع ظروفا تشدد بها لعقوبة الجريمة وهي:

– حالة الدخول والبقاء غير المشروع إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام.

– إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات للقانون العام.

---

[1]– المواد 394 مكرر 2و394 مكرر 1/2 من قانون 04–15 المؤرخ في 2004/11/10.

[2]–أنظر المواد 394 مكرر 2 و 394 مكرر 6 من قانون 04–15 المؤرخ في 2004/11/10 .

أكد المشرع الجزائري أيضا بموجب المادة 394 مكرر5 [1]. على تجريم الاشتراكات (سواء شخص طبيعي او معنوي) في مجموعة او اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية – بعقوبة الجريمة – وكان التحضير مجسدا بفعل او عدة افعال مادية[2]. اي بمعنى آخر فان المشرع استثنى العقاب الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد .

كما نصت المادة 394 مكرر4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب احدى الجرائم الواردة في الفصل السابع مكرر بغرامة تساوي 5 مرات الحد الاقصى للغرامة المحددة للشخص الطبيعي[3]. غير أن المسؤولية الجزائية للشخص المعنوي ستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة، والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر 7 من قانون العقوبات.

نص المشرع الجزائري على حماية الأشخاص من التعدي على حياتهم الخاصة وذلك من خلال المادة 303 مكرر، حيث عددت هذه المادة الحالات التي يتم فيها المساس بحرمة الحياة الخاصة وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية أو صور في مكان خاص بغير إذن صاحبها أو رضاه.

نخلص إلى أن المشرع الجزائري رغم تداركه من خلال قانون 15–04 والمتضمن تعديل قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

الفرع الثاني : مكافحة الجريمة المرتكبة عبر الانترنت قانون الوقاية من جرائم تكنولوجيات الإعلام والاتصال :

---

[1] – تنص المادة على انه " كل من شارك في مجموعة او اكثر من جرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل او عدة افعال الافعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها "

[2] – بورزام احمد، المرجع سابق ص 15

[3] – قارة امال ، الحماية الجزائية للمعلومات في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع ، الجزائر ، الطبعة الثانية ، 2007 ص 130

سنتطرق فيما يلي إلى أسباب صدور القانون رقم 09-04 مؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ثم إلى مضمون هذا القانون باختصار.

أولا: أسباب صدور قانون مكافحة الجرائم المعلوماتية:

دفع القصور الذي عرفه القانون رقم04-15 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف انواع الاعتداءات الماسة و بأنظمة المعالجة الآلية للمعطيات ، بالمشرع الجزائري الى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال و خاصة الجرائم الناشئة عن استخدام غير المشروع لشبكة الانترنت خاصة في ظل الثورة التي تعرفها في مجال استخدام الانترنت، وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة من خلال وضع إطار قانوني أكثر ملائمة مع خصوصي الجريمة المرتكبة عبر الانترنت[1].

كما تمكن أهمية هذا القانون في كونه يجمع بين القواعد الإجرامية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة هذه والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها.

ثانيا: مضمون قانون مكافحة الجرائم المعلوماتية:

يحتوي قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على ستة فصول نلخصها فيما يلي:

الفصل الأول: نص على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد من المفهوم مصطلح التقنية الواردة وكذا مجال تطبيق أحكامها.

الفصل الثاني: حيث جسد أحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية. حيث نص القانون على أربع حالات يسمح فيها للسلطات الأمنية لممارسة الرقابة المراسلات والاتصالات الالكترونية، منها الوقاية من الأفعال الموصوفة

[1]- القانون رقم 09-04 المؤرخ في 2009/2/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريمة الرسمية عدد 47 لسنة 2009.

بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حالات في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة او الدفاع اوطني او النظام العام ، ولمقتضيات التحريات والتحقيقات القضائية ما عنده يصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية، وفي اطار تنفيذ الطلبات المساعدة القضائية الدولية المتبادلة

الفصل الثالث : تضمن القواعد الاجرائية ، الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، وذلك وفقا لمعايير العالمية المعمول بها في هذا الشأن ومع مراعاة ما تضمنه قانون الاجراءات الجزائية من مبادئ عامة وعلى هذا الاساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد الى المنظومة المعلوماتية او جزء منها ، وكذا المعطيات المعلوماتية المخزنة فيها مع امكانية الى مساعدة السلطات الاجنبية المختصة من اجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد اجنبي ، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعطيات المعلوماتية المخزنة في الكشف عن الجرائم او مرتكبيها[1]

الفصل الرابع :تطرق الى التزامات المتعاملين في مجال الاتصالات الالكترونية وذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الالكترونية لا سيما التزام حفظ المعطيات المتعلقة بحرمة السير والتي من شأنها المساعدة في كشف الجرائم ومرتكبيها، يهدف هذا القانون الى اعطاء مقدمي الخدمات دور ايجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبيها . حيث الزم هذا القانون مقدمي الخدمات الانترنت على التدخل الفوري لسحب المحتويات التي تم بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة او غير مباشرة مخالفتها للقانون ، وتخزينها او جعل الدخول اليها غير ممكن ، اضافة الى وضع ترتيبات تقنية تسمح بحصر امكانية الدخول الى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة واخطار المشتركين لديهم وجودها.

الفصل الخامس: أشار الى الهيئة الوطنية للوقاية من الاجرام المتصل بتكنولوجيات الاعلام والاتصال ومكافحته، اذا نص القانون على انشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم

---

[1] – فشار عطاالله " **مواجهة الجريمة المعلوماتية في التشريع الجزائري** " الملتقى المغربي حول القانون والمعلوماتية ، اكاديمية الدراسات العليا ليبيا اكتوبر 2009، ص 35

المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، وقد تم الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة[1]

يعتبر القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها نطاقا واسعا في مجال مكافحة الجرائم المرتكبة عبر الانترنت، حيث جاء كجريمة للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عاما .

[1] -المواد 13و 14 من قانون 09-04 المؤرخ في 2009/02/05

خاتمة

الخاتمة :

من خلال دراستنا لجرائم المعلوماتية فإنه يتبين لنا انها من اكثر الجرائم خطورة، ويرجع ذلك الى ما تتصف به هذه الجرائم عن الجرائم التقليدية من اختلاف، أضف على ذلك التحديات التي فرضتها على الجهات الخاصة بوضع القوانين ونفاذها.

فجرائم المعلوماتية مشكلة من المشكلات التي أفرزتها المعلوماتية، فهذه الثورة على قدر ما قدمته من تسهيلات للأفراد و المجتمعات على حد سواء فإنها قد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التقنية والعلمية المعقدة.

تميزت جرائم المعلوماتية عن الجرائم التقليدية بعدة خصائص، فقد تعددت التعريفات واختلفت في وصف هذه الظاهرة الاجرامية المستحدثة، كذلك تميزها بطابعها العابر للحدود، بالإضافة الى ضعف القائمين على مكافحتها نظرا الى تطورها التسارع في ارتكابها، وبالتالي فان هذه الخصائص كان لها الدور الكبير في إبراز النشاط الاجرامي لهذه الجرائم المستحدثة وإيضاح الاختلاف الجوهري لها عن الخصائص العادية للجرائم التقليدية.

إن السمات التي انفرد بها المجرم المعلوماتي أضفت التميز لجرائم المعلوماتية، فهو يعتبر من الاشخاص الذين يتمتعون بنسب عالية الذكاء والمهارة والمعرفة فهو يرتكب جرائمه في هدوء دون أن يلفت الانتباه، كما أن كثرة القطاعات المستخدمة للأنترنت امكنته من الاعتداء على اكثر من قطاع واحد عبر مختلف أنحاء العالم وذلك من خلال الضغط على زر واحد، وهذا ما ليس باستطاعة المجرم التقليدي فعله.

وتعد اهم خصوصية تتمتع بها جرائم المعلوماتية هي عدم امكانية تطبيق أحكام الجرائم التقليدية عليها وسبب ذلك هو صعوبة تصنيفها فهي تتسم بالتشعب وعدم امكانية حصرها:

كل هذه الخصوصيات التي تتميز بها جرائم المعلوماتية جعلت مختلف الدول و الهيئات الدولية تدرك مدى خطورة هذه الظاهرة الاجرامية والتحديات التي تفرضها عليها مما ادى الى وضع أطر قانونية من خلالها يمكن وضع طرق فعالة لمكافحتها، و قد تمثلت هذه الجهود بالخصوص في اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية دون اغفال جهود المعاهدات والقوانين، بالإضافة الى هذه الجهود هناك جهود تبذل على المستوى العربي كالقانون العربي النموذجي، وعلى المستوى العالمي كجهود الامم المتحدة والقوانين المقارنة، أما بالنسبة الى المشرع الجزائري فنجده قد واكب ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الإنترنت في نواحي حياة المواطن الجزائري، فبدى الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال سعت لسده في بادئ الأمر بتعديل قانون العقوبات و ذلك بالقانون 04-15، لكن محدوديته دفعت بالمشرع الجزائري الى إصدار قانون خاص -09

04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومحاولتها بالإضافة الى قوانين الملكية الفكرية.

الى ان المشرع الجزائري يبقى بعيدا كل البعد عن التطور القانوني على مستوى العالمي من جهة، وتطور اساليب ارتكاب الجرائم المعلوماتية.

إزاء هذا فإننا نقترح ما يلي :

1- إصدار تشريعات جديدة أو تعديل التشريعات الجزائية القائمة لمواجهة الجرائم المعلوماتية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.

2- اعتماد الدقة والوضوح والحبكة القانونية عند تحديد انماط السلوك الاجرامي والابتعاد عن التعبيرات الغامضة أو المطاطية التي تحمل اكثر من معنى.

3-عدم الاقتصار عند التجريم او العقاب على انماط السلوك المحظور حاليا بل يجب مراعات الابعاد المستقبلية لان تكنولوجيا المعلومات و الحواسيب في تطور سريع بل يكاد يكون مذهل.

قائمة المراجع

قائمة المراجع

أولا: النصوص القانونية

- النصوص القانونية والمراسيم الوطنية الجزائرية

* القانون رقم 09-04- المؤرخ في 14 شعبان عام هـ 1430 الموافق لـ 5 اوت 2009 المتضمن :

القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها . والذي دخل حيز النفاذ بموجب الجريدة الرسمية العدد 47 الصادرة بتاريخ 16 اوت 2009

* المرسوم الرئاسي 07-375 المؤرخ في 21 ذي القعدة عام 1428 هـ الموافق لـ 1 ديسمبر 2007 المنشور في الجريدة الرسمية المؤرخة في 9 ديسمبر 2007 العدد 77 . المتعلقة بالمصادقة على اتفاقية دولية ثنائية بين الجمهورية الجزائرية والحكومة الفرنسية والمالق بالتعاون في مجال الامن ومكافحة الاجرام المنظم الموقع عليها بالجزائر في 25 اكتوبر 2003 .

ثانيا: الكتب العلمية

* احسن بوسقيعة الوجيز في القانون الجنائي الخاص / الجزء الثاني: جرائم الموظفين- جرائم الاعمال- جرائم التزوير دار هومة للنشر الجزائر طبعة 2004

...../ الجزء الاول: الجرائم ضد الاشخاص والجرائم ضد الاموال دار هومة للنشر الجزائر طبعة 2008 .

ثالثا : الكتب العلمية المتخصصة

* جميل عبد الباقي الصغير : القانون الجنائي والتكنولوجيا الحديثة (الكتاب الاول: الجرائم الناشئة عن استخدام الحاسب الآلي) الطبعة الاولى دار النهضة العربية طبعة 1992 القاهرة مصر .

* محمد امين الرومي: جرائم الكومبيوتر والأنترنت دار المطبوعات الجامعية الطبعة 2004 الاسكندرية (مصر).

رابعا : المذكرات والرسائل

* دردور نسيم: ماجستير شعبة القانون الجنائي / جرائم المعلوماتية على ضوء القانون الجزائري والمقارن – تحت اشراف الاستاذ الدكتور طاشور عبد الحفيظ (جامعة منتوري قسنطينة) كلية الحقوق سنة 2013/2012

*بن عيسى بن علية: جهود وآليات مكافحة ظاهرة غسيل الاموال في الجزائر (جامعة الجزائر) 2010.

خامسا: المقالات العلمية

* طاشور عبد الحفيظ : شبكة الانترنت الرهانات التكنولوجية والاشكالات القانونية

اعمال المؤتمر التاسع لاتحاد العربي للمكتبات والمعلومات – دمشق ايام :من21 الى 26 اكتوبر 1998.

الفهرس

الفهرس