جامعة عبد الرحمان ميرة – بجاية –

كلية الحقوق والعلوم السّياسية

قسم القانون الخاص

الإطار القانوني للجريمة الالكترونية

دراسة مقارنة

مذكرة لنيل شهادة الماستر في الحقوق

تخصص: القانون الخاص و العلوم الجنائية

من إعداد الطالبتان:

بوشعرة أمينة

موساوي سهام

تحت إشراف الأستاذة الدكتورة :

دموش حكيمة

أعضاء لجنة المناقشة :

سقلاب فريدة .....أستاذة محاضرة. أ، جامعة عبد الرحمن ميرة، بجاية.....رئيسة

دموش حكيمة.....أستاذة محاضرة. ب، جامعة عبد الرحمن ميرة، بجاية.....مشرفة

عشاش حفيظة.....أستاذة مساعدة. أ ، جامعة عبد الرحمن ميرة، بجاية.....ممتحنة

السنة الجامعية

2018/2017

بسم الله الرحمان الرحيم

(وَابْتَغِ فِيمَا آتَاكَ اللَّهُ الدَّارَ الْآخِرَةَ وَلَا تَنْسَ نَصِيبَكَ مِنَ الدُّنْيَا وَأَحْسِنْ كَمَا أَحْسَنَ اللَّهُ إِلَيْكَ وَلَا تَبْغِ الْفَسَادَ فِي الْأَرْضِ إِنَّ اللَّهَ لَا يُحِبُّ الْمُفْسِدِينَ)

صدق الله العظيم . سورة القصص الآية 77

اهداء

الحمد لله على إحسانه ، و الشكر له على توفيقه و إمتنانه ، أما بعد أترحم على روح خالي الطاهرة ، و أدعو الله أن يحشره في زمرة النبيئين و الشهداء و حسن أولئك رفيقا.

أهدي عملي إلى من أوصاني بهما ربي برا و إحسانا والديٌ . و على من أشد بهم أزري إخوني و أخواتي ، و إلى جميع أصدقائي كل باسمه ، كما أتقدم بالشكر إلى جميع الأساتذة الكرام على مدار جميع السنوات الجامعية و بالأخص الأستاذة دموش .

أمينة .

الحمد و الشكر لله عز و جل، بفضل قدرته بلغت هذه المرتبة ،أهدي هذا العمل إلى منبع الحنان و الرحمة لأمي .

إلى من أحمل اسمه بكل فخر أبي ، و إلى من يجري حبهم في عروق دمي إخوتي ، إلى أستاذي الكريم طباش عز الدين الذي لم يبخل علي بالنصائح و التوجيه ، إلى كل أصدقائي.

سهام

قائمة لأهم المختصرات

أولا : باللغة العربية

ج ر.ج.ج:الجريدة الرسمية للجمهورية الجزائرية.

د.ط : دون طبعة .

ص : صفحة.

ص ص : من صفحة إلى صفحة .

ق.ع.ج : قانون العقوبات الجزائري .

ق.إ.ج.ج : قانون الاجراءات الجزائية الجزائري .

ق.ع.ف : قانون العقوبات الفرنسي .

إلخ : إلى آخره .

ثانيا : باللغة الفرنسية .

P : page

مقدمة

كشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة لم تكتشفها عقودا من الزمن ، شهد من خلالها العالم تطورا ملحوظا في مجال تكنولوجية الإعلام و الإتصال حيث يعد الجانب الاعلام الآلي و الأنترنت حجر الزاوية في مجال التقنية الحديثة التي تهدف لخدمة البشرية في مختلف مناحي الحياة . لدرجة أنها أضحت إحدى مفردات التعامل اليومي بالنسبة للأفراد و المجتمعات على حد سواء .

شكلت في نفس الوقت قفزة حضارية نوعية في حياة الأفراد و الدول ، حيث تعتمد القطاعات المختلفة في وقتنا الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لما تتميز به من عنصري السرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها و من ثم نقلها و تبادلها بين الأفراد و الجهات الأخرى و يلعب في ذلك الكمبيوتر دور فعال من خلال غزوه لجميع الفضاءات ، و أصبح وسيلة لا يمكن الإستغناء عنها في حياتنا اليومية ، و هذا ما عبر عنه الأستاذ bart schutter بقوله "**لقد ترك الحاسب الآلي بصمات** واضحة على حياتنا الحديثة ، و يرجع إليه الفضل في تطوير عدد كبير من الأنشطة اليومية سواء من حيث المضمون أو الشكل أو الزمن أو المسافة"[1] .

على الرغم من المزايا الهائلة التي تحققت و هي بصدد التحقق كل يوم بفضل التطور العلمي على جميع الأصعدة و في شتى ميادين الحياة المعاصرة ، فإن الثورة التكنولوجية المتنامية صاحبتها جملة من الإنعكاسات السلبية و الخطيرة من جراء سوء إستخدام هذه التقنية ، حيث يستغلها البعض في مآرب غير مشروعة طبقا لمصالحهم ، فأصبح الحاسب الآلي بشكل عام و شبكة الأنترنت على وجه الخصوص أدوات أو محل ارتكاب للجريمة بمفهومها الحديث ، حيث

[1] أحمد خليفة الملط ، الجرائم المعلوماتية ، دط ، دار الفكر الجامعي مصر ، ص160.

أفرز عن ذلك بروز ظاهرة إجرامية جديدة في العالم الإفتراضي و تسمى بالجريمة الإلكترونية حيث قد تم تعريفها بأنها ثالث أكبر تهديد في العالم بعد الأسلحة الكيميائية و النووية ، و بالتالي تعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية و التي تختلف كثيرا عن الجريمة التقليدية في طبيعتها [2]، و مضمونها و نطاقها ، ووسائلها و حتى في خصوصية و تميز مرتكبيها ، و قد ساهمت عوامل التحضر السريع و الرغبة في تحقيق الثراء و توفر الغرض من ارتكابها في انتشارها و ارتفاع نسبة ضحاياها ، حيث أصبحت لا تقتصر على إقليم دولة واحدة ، بل تجاوزت حدود الدول ، باعتبارها جرائم مبتكرة ومستحدثة تمثل ضرب من ضروب الذكاء الإجرامي ، مما يصعب إدراجها ضمن القوانين الجنائية التقليدية ، نظرا لحداثة هذا النوع المستجد من الجرائم ، و سرعة تطوره ، حيث أصبح لا يقتصر على جريمة واحدة بل يتعدى ذلك إلى عدة جرائم، هذا ما دفع معظم التشريعات إلى تطوير بنيتها التشريعية لمواكبة هذا النوع المستجد من الجرائم وذلك بتضافر الجهود في مجال التصدي للجريمة الإلكترونية، سواء على المستوى الوطني ، أو على المستوى الدولي .

من هنا تأتي أهمية موضوع هذا البحث الذي يمكن الإستفادة منه على أرض الواقع ، حيث يتناول التصورات والرؤى المتعلقة بالجوانب الموضوعية والإجرائية للجريمة الإلكترونية في محاولة تقديم الحلول القانونية الممكنة لمكافحة هذه الجريمة في ظل النصوص التشريعية. لهذا نتساءل حول نجاعة الطرق المنتهجة من طرف مختلف التشريعات في مكافحة الجريمة الإلكترونية ؟

[2] عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون(دراسة مقارنة)، ط2، منشورات الحلبي الحقوقية ، بيروت ، 2007،ص31.

ومن خلال ذلك اتبعنا على على المنهجين التحليلي و المقارن لدراسة حيثيات موضوعنا بكل جوانبه،بذلك قسمنا بحثنا إلى قسمين نتطرق في(الفصل الأول) إلى دراسة الأحكام العامة للجريمة الإلكترونية،أما (الفصل الثاني) فيتمحور حول الآليات المعتمدة لمكافحة و قمع الجريمة المعاوماتية.

الفصل الاول

الأحكام العامة للجريمة

الالكترونية

أصبحت تقنية المعلومات من أساسيات الحياة في عصرنا الحالي، لكن بعضنا من مستخدمي هذه التقنية الحديثة استغلها في مآرب غير مشروعة طبقا لمصالحه، فأصبح الحاسب الآلي بشكل عام وشبكة الإنترنت على وجه الخصوص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث، واحترف بعض الجناة ارتكاب العديد من الجرائم بواسطة الحاسب الآلي وشبكة الإنترنت[1].

هذا مأدى بالبعض إلى التمييز بين الأفعال التي تستهدف المعلومات في نظام الكمبيوتر ذاته من خلال مرحلة المعالجة، التخزين، الاسترجاع، وبين الأفعال التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، والمصطلح الشامل لهذه الجرائم نجده في مصطلح الجريمة الإلكترونية الذي يشمل في مضمونه الجرائم التي تستهدف النظم المعلوماتية والشبكات على حد سواء[2].

تعتبر هذه الجريمة لا حدود جغرافية لها هذا ما يكسبها طابعا دوليا ،وتعد هذه السمة نقطة هامة تستحق الوقوف عندها وبحثها باستفاضة باعتبار جرائم المعلوماتية جرائم عابرة للحدود، وترجع تسميتها بالعاملين إلى مزاولة الأنشطة الإجرامية فيها على مستوى عالمي وعبر الدول حول

[1] عبد الله عبد الكر يم عبد الله ،الجرائم الإلكترونية،دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية و الأنترنت مع الإشارة إلى جهود مكافحتها محليا و عربيا ودوليا،ط1،منشورات الحلبي الحقوقية،بيروت،2007،ص.5.

[2] عائشة بن قارة مصطفى،حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن،دط،دار الجامعة الجديدة،الإسكندرية،2010،ص.34.

الحدود، نتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات[3]، فهذا النوع من الإجرام أصبح ظاهرة تؤرق العديد من دول العالم لما لها من آثار خطيرة على وضع ومكانة هذه الدول، وتعتبر من المواضيع الحديثة والخطيرة التي تشغل اهتمامات رجال القانون والفقهاء.

تجعلهم في أحيان كثيرة عاجزين عن مواجهتها وفهم طبيعتها نظرا لكونها من الجرائم السريعة التطور، لذا وجب علينا الإلمام بالأحكام العامة لهذه الجريمة بتبيان مفهومها (المبحث الأول) ثم التطرق إلى دراسة أركانها (المبحث الثاني).

المبحث الأول

مفهوم الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية موضوعا واسعا، فهي ظاهرة إجرامية تعاني منها المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية.

تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم،سواء في التشريع المقارن أو في التشريع الجزائري، حيث أثيرت العديد من التساؤلات حول تحديد تعريف جامع لهذه الجريمة العالمية(المطلب الأول) و تبيان خصائصها(المطلب الثاني)

المطلب الأول

تعريف الجريمة الإلكترونية

لقد تعددت واختلفت التعاريف بشأن الجريمة الإلكترونية، بإعتبارها ظاهرة جديدة مازالت قيد البحث والدراسة من طرف القانونيين والعديد من الفقهاء ،وبالمثل لايوجد تعريف محدد ومتفق عليه لهذا النوع المستحدث من الجرائم[4].

يرجع ذلك إلى خشية حصرها في مجال ضيق في ظل التطور المعلوماتي الحاصل على مستوى العالم،وعليه سوف نحاول تبيان مختلف التعاريف لهذه الجريمة سواء في التشريعات المقارنة(الفرع الأول)،وفي التشريع الجزائري(الفرع الثاني)

الفرع الأول

تعريف الجريمة الإلكترونية في التشريعات المقارنة

قبل التطرق إلى مختلف التعريفات التي جاءت لتحديد مفهوم الجريمة الإلكترونية ،لابد من الإشارة إلى تعدد التسميات بشأن هذه الجريمة، التي تبدو للوهلة الأولى أنها تختلف من حيث دلالتها ،إلا أن معظمها يشير إلى نفس الظاهرة ،فبينما استعمل البعض اسم الجرائم الإلكترونية،فقد أطلق البعض الآخر اسم جرائم الحاسوب الآلي و الأنترنت،أو الجرائم المتصلة بالكمبيوتر وجرائم

[4] باطلي غنية،الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر و التوزيع، الجزائر،2015،ص.15-16.

تكنولوجيا المعلومات، في حين هناك من وجد تسمية جرائم إساءة استخدام تكنولوجيا المعلومات أكثر دلالة ومواكبة للتطور الذي يشهده عالم الإعلام والإتصال[5].

كماانتشر اصطلاح جرائم أصحاب الياقات البيضاء إلى جرائم الهاكر و "**السيبركرايم**" أو **الجرائم السبرانية**" في المجال الأوروبي ويقصد به جرائم العالم الإفتراضي.[6]

ومما تقدم سنقوم بعرض مختلف التعريفات المقدمة للجريمة الإلكترونية في التشريعات المقارنة.

أولا:تعريف الجريمة الإلكترونية لدى بعض التشريعات العربية

اختلفت التشريعات العربية في تعريف الجريمة الالكترونية، ومع النمو المتسارع لاستخدام شبكة الانترنت ظهرت أنماط من جرائم مستنبطة عن هذا النوع من الإجرام، مما أدى إلى تنوع التعاريف بشأن هذه الجريمة المستحدثة[7].

لذا سنحاول تبيان التعريف الذي قدمه كل من المشرع السعودي(أ) و المشرع المصري(ب).

أ تعريف المشرع المصري للجريمة الإلكترونية:

تعتبر الجريمة الالكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة،نظر لكونها جريمة حديثة ، بالعودة إلى المشرع المصري نجده لم يقم بتعريف الجريمة بل ترك مسألة تعريف الجريمة الإلكترونية للفقه،و بالتالي اختلف الفقهاء في تعريفها ،

[5] عبد الله عبد الكريم،المرجع السابق،ص.-ص5-6.

[6] معتوق عبد اللطيف،الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن،مذكرة لنيل شهادة الماجستير في العلوم الجنائية،كلية الحقوق،جامعة الحاج لخضر،باتنة،2011.ص.6.

[7] عائشة بن قارة ،المرجع السابق،ص،31-32.

فهناك من عرّفها من الزاوية التقنية أو الفنية على أساس انها عمل أوامتناع يأتيه أضرار بمكونات الحاسب، وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابا[8].

فهي تنشأ عن استخدام غير مشروع لتقنية المعلوماتية، ويهدف إلى الاعتداء على الموال أو الأشياء المعنوية.

كما يعرفها البعض الآخر من الفقه على أنها نشاط غير مشروع موجه لنسخ أو تغيير أوحذف أو الوصول إلى المعلومات المخزنة داخل الحاسب،أوالجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات،إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية.

من عرفها اعتمادا على وسيلة ارتكاب الجريمة،على أساس أنهل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية لحدوث هذا النوع المستحدث من الإجرام[9].

ب تعريف المشرع السعودي للجريمة الإلكترونية

عرف المشرع السعودي الجريمة الالكترونية من خلال نظام مكافحة جرائم المعلوماتية بأنّها:

" **أي فعل يرتكب متضمنا استخدام الحاسب الآلي أوالشبكة المعلوماتية بالمخالفة لأحكام هذا النظام**"[10]

[8] العريان محمد علي،الجرائم المعلوماتية، ،دارالجامعةالجديدة،الإسكندرية،2011،ص.56.

[9] أمير فرج يوسف،الجريمة الإلكترونية و المعلوماتيةو الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر و الأنترنت الطبة الأولى ، مكتبة الوفاء القانونية،مصر،2011،ص.10.

بالتالي فالجريمة الإلكترونية بحسب هذه المادة هي عبارة عن سلوك إجرامي يستخدم فيه الحاسب الآلي أو شبكة المعلوماتية كوسيلة لحدوث هذا النوع المستجد من الجرائم كما نجد أن نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية عرف من جهة الجريمة المعلوماتية، على غرار بعض التشريعات الأخرى التي تركت مسألة تعريف هذا النوع المستحدث من الجرائم للفقه كالمشرع المصري والمشرع الجزائري،ومن جهة أخرى قام هذا النظام بتحديد أنواع الجرائم المعلوماتية والعقوبات المقررة عليها وهو مانقوم بدراسته في الفصل الثاني.

ثانيا:تعريف الجريمة الإلكترونية في بعض التشريعات الأخرى

لا يوجد مصطلح موحّد للدلالة على الجريمة الالكترونية، فقد تعددت التعاريف بشأنها، لذا نقتصر بعرض جهود كل من فرنسا والولايات المتحدة الأمريكية في مجال تعريف هذا النوع المستجد من الجرائم.

ا تعريف المشرع الفرنسي للجريمة الإلكترونية

المشرع الفرنسي بدوره لم يعرف لنا الجريمة الإلكترونية و إنما نص على تجريم بعض الأفعال المساهمة في حدوثها ضمن نصوص قانونية ، وترك مسألة تعريف الجريمة الالكترونية للفقه، لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى، ووضعوا تعريفات مختلفة ومن

[10]المادة الأولى من نظام مكافحة الجرائم الإلكترونية،عد إلى :عبد الفتاح بيومي حجازي،جرائم الكمبيوتروالأنترنت في التشريعات العربية"دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية،ط1،دار النهضة العربية،الإسكندرية،2009،ص.17.

الفقه الفرنسي يعرف الفقيه **Masse** جريمة الكمبيوتر بأنّها " **الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح**"[11].

كما يعرفها الفقيهان الفرنسيان **Vivant, Stane** بأنها: "**مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب**"[12].

يعرفها جانب آخر من الفقه على **أساس أنها ذلك النشاط الإجرامي الذي تستخدم فيه تقنية الحاسب الآلي كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود فعله.**

ونجد أن المشرع الفرنسي قام بإدراج الفصل الثالث من القانون العقوبات الفرنسي تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على الجريمة الإلكترونية ،ويظهر ذلك في تجريمه لبعض الأفعال المساهمة في حدوث الجريمة الإلكترونية، كتجريمه لفعل البقاء والدخول بطريق الغش إلى نظام المعالجة الآلية للمعطيات حيث عاقب على ذلك بعقوبة الحبس لمدة سنتين وغرامة قدرها 60000 أورو[13]، وبالتالي فالمشرع الفرنسي لم يعرف الجريمة الإلكترونية بل اكتفى بالتجريم بعض الأفعال التي تساهم في حدوث الجريمة الإلكترونية.

[11] محمد أمين أحمد الشوابكة،جرائم الحاسوب والأنترنت (الجريمة المعلوماتية) ،ط1،دار الثقافة للنشر والتوزيع،عمان،2004.ص.7.

[12] العريان محمد علي،المرجع السابق،ص،57.

[13] L'article 323-1 du code pénal ,dispose : le fait d'accéder ou se maintenir frauduleusement dant tout ou partie d'un systéme de taitement automatisé de données est puni de deux ans d'emprisonnement et de 60000 euros d'amende. »le code pénal francais,www ,legifrance.fr

ب تعريف المشرع الأمريكي للجريمة الإلكترونية

يتبنى الخبير الأمريكي Parker مفهوما واسعا للجريمة المعلوماتية، حيث يشير إلى أنّها " **كل فعل إجرامي متعمّد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.**[14]

حسب نظره، الجريمة الالكترونية أو المعلوماتية تنطوي على ست خطوات أساسية يتمّ تنفيذها آليا بواسطة برنامج أو عدّة برامج، ويمكن تحديد هذه الخطوات فيما يلي:

1- البحث عن نظام الحاسب الآلي الذي يحتوي على المعلومات أو البرامج المطلوبة.

2- الوصول إلى نقاط الضعف في النظام الذي يحتوي على هذه المعلومات او البرامج.

3- الاستفادة من هذه النقاط للدخول إلى النظام ثم التحكم فيه.

4- تنفيذ السلوك الإجرامي الذي تمّ التخطيط له وتحديده مسبقا.

5- تحويل هذا السلوك إلى ربح غير مشروع يحصل عليه الجاني أو إلى خسارة تلحق بالمجني عليه.

6- إخفاء جميع الأدلة تجنّبا لكشف الفاعل وسلوكه الإجرامي.

كما يعرفها الفقيه David Thompson بأنها "أية **جريمة يكون متطلبا لإقترافها،أن يتوفر لدى فاعلها معرفة تقنية الحاسب.**[15]

[14] محمد أمين أحمد الشوابكة،المرجع السابق،ص.7-8.

[15] محمد عبد الله أبوبكر سلامة،جرائم الكمبيوتر و الأنرنت،دط،منشأة المعارف الإسكندرية،2005،ص.15.

من خلال استعراض تعريفات الفقهية،يتضح لنا أن هناك إختلاف في تعريف الجريمة المعلوماتية،إلا أنه في الحقيقة تعددت التعاريف إلا أنها كلها تدل على نفس الجريمة التي نحن بصدد دراستها.

الفرع الثاني

موقف المشرع الجزائري من الجريمة الالكترونية

أدّت الحداثة التي تتميّز بها الجريمة الالكترونية، واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح موحّد للدلالة عليها، مما انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية[16]، وبالنسبة للمشرع الجزائري نجده للدلالة على الجريمة الإلكترونية اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام و الإتصال.[17]

معتبرا أن النظام المعلوماتي في حدّ ذاته وما يحتويه من مكوّنات غير مادية، محلاً للجريمة، ويمثّل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة، وبالرجوع إلى قانون العقوبات الجزائري نجده لم يعرف جرائم الانترنت بل اكتفى بالعقاب على بعض الأفعال تحت عنوان " **الجرائم الماسة بنظام المعالجة الآلية للمعطيات**"، حيث نصّت المادة 394 مكررمنه ما يلي ((يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000دج إلى 200.00دج، كل من يدخل أو يبقى عن طريق الغش في كل

[16] أشرف عبد القنديل ،المرجع السابق،ص.92.

[17] المادة الثانية من قانون رقم 09-04 المؤرخ في 5 أوت 2009،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،ج ر عدد 47،سنة 2009.

أو جزء من منظومة للمعالجة الآلية، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000دج إلى 300.000دج.))[18]

وبناء على ما سبق، نجد أن المشرع الجزائري اعتمد على عدّة معايير للدلالة على الجريمة الإلكترونية، وذلك باعتماده على معيار وسيلة الجريمة من جهة، وهو نظام الاتصالات الالكتروني، ومن جهة أخرى على معيار موضوع الجريمة ألا وهو المساس بأنظمة المعالجة الآلية للمعطيات، أما المعيار الثالث وهو قانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الإلكترونية باعتبار أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو نظام لإتصالات الإلكترونية.[19]

المطلب الثاني

خصائص الجريمة الالكترونية

تتميز الجريمة الإلكترونية بطبيعة خاصة تميّزها عن باقي الجرائم التقليدية، حيث تكون المعلومات والبرامج هي محل الاعتداء، وعليه تكون أما ظاهرة إجرامية مستحدثة ذات طبيعة

[18] قانون رقم 04-15،مؤرخ في 10نوفمبر 2004،المتضمن قانون العقوبات،ج ر عدد71،الصادرة في 10 نوفمبر 2004.

[19] نصت المادة الثانية من قانون رقم 09-04 ،المرجع السابق ،على مايلي:((يقصد في مفهوم هذا القانون بما يأتي:أ- الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية.))

خاصة[20]، فالجريمة الالكترونية إفراز ونتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع مما أعطى لونا وطابعا قانونيا خاصا وميّزها بمجموعة من الخصائص المختلفة عن الجرائم الأخرى(الفرع الأول)، كما لمرتكبيها صفات تميّزهم عن الجرائم التقليدية(الفرع الثاني).

الفرع الأول

خصوصية الجريمة الالكترونية

إن ارتباط الجرائم الالكترونية بجهاز الحاسوب وشبكة الانترنت، أضفى عليها مجموعة من الخصائص المميزة لها عن باقي الجرائم التقليدية.

أولا:جريمة عابرة للحدود

من أهم الخصائص التي تميّز الجريمة الالكترونية، أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، بسبب السرعة الهائلة في تنفيذها. يمكن أن تقع الجريمة من طرف الجاني في دولة والمجني عليه في دولة أخرى في وقت يسير جدّا.

هذه الطبيعة التي تتميّز بها الجريمة الالكترونية أدت إلى خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول القانون الواجب تطبيقه،

[20] باطلي غنية،المرجع السابق،ص.33.

بالإضافة إلى إشكاليات تتعلّق بإجراءات الملاحقة القضائية، وغيرها من المشاكل التي تثيرها الجرائم العابرة للحدود بشكل عام.[21]

ومن أهم القضايا التي أكّدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة "الإيدز"، وتتلخّص وقائعها عام 1989، حيث قام أحد الأشخاص المدعو " **جوزيف بيب**" بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل، ثمّ تظهر بعد ذلك عبارة على الشاشة يطلب الفاعل من خلالها مبلغ مالي يرسل إلى عنوان معيّن حتى يتمكن المجني عليه من الحصول على مضاد الفيروس، وفي 3 فيفري 1990، تمّ إلقاء القبض على المتهم جوزيف بيب" في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتّحدة بطلب تسليمه لها لمحاكمته أما القضاء الإنجليزي، إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية.

وتثير خاصية عالمية الحدود للجريمة الالكترونية عدّة آثار قانونية أهمها القانون الواجب التطبيق عليها، والقضاء المختص بها[22].

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

[21] باطلي غنية المرجع السابق،ص-ص.49_50.

[22] عائشة بن قارة مصطفى ،المرجع السابق،ص.45.

ثانيا:صعوبة اثبات واكتشاف الجريمة الإلكترونية

تعتبر الجريمة الالكترونية جريمة مستحدثة، تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي.[23]

على اعتبار هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الالكترونية للبيانات سواء كان في تجميعها أو في إدخالها إلى الحاسوب المرتبط بشبكة المعلومات، ولغرض الحصول على معلومات معيّنة، وقد ترتكب هذه الجرائم في معالجة الكلمات أو النصوص، وتمكن المستخدم من تحرير الوثائق والنصوص على الحاسوب مع إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة.

جميع تلك العمليات هي وثيقة الصّلة بالجريمة محلّ البحث، وعليه لابد من استيعابها، وقد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء، وعليه فالطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن أن ترتكب فيه، ومن جانب آخر المحل الذي يقع عليه الاعتداء، فالتطور السريع في مجال المعلوماتية، قد يفسح المجال لاقتناء وسائل الكترونية تمكن للمتجاوزين من استخدامها في ارتكاب الجرائم المختلفة، لأن الإجرام المعلوماتي يتعلّق بكل سلوك غير مشروع فيما يتعلّق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها.[24]

فتتخذ الجريمة المستحدثة طبيعة خاصة من حيث تكييفها القانوني، وتخضع لقواعد غير القواعد التقليدية، كونها تتم في بيئة غير تقليدية، حيث تقع خارج الإطار المادي الملموس لتقوم

[23] عفيفي كامل ،جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية و دور الشرطة و القانون"دراسة مقارنة"،دط،منشورات الحلبي الحقوقية،الإسكندرية،2007،ص.270.

[24] محمود أحمد عبابنة،المرجع السابق،ص.36.

أركانها في بيئة الحاسوب والانترنت، ويطلق عليها البيئة الرقمية, مما يصعّب كشفها وإثباتها نظرا لعدم ترك الجاني آثارا مرئية أو ملموسة في أغلب الأحيان،وعادة ما يتم اكتشاف هذه الجريمة بمحض الصدفة.[25]

حيث يصعب إيجاد دليل مادي يدين مرتكب الجريمة، كون أمر طمس الدليل ومحوه كلّيا من قبل الفاعل أمر في غاية السهولة وفي زمن قصير جدّا، ومن ثمّ يتعذّر إن لم يكن مستحيلا ملاحقة وكشف شخصيته.

خاصة في حالة تفتيش الشبكات، كما قد تكون البيانات المراد البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة وهنا تثار مسألة مدى مشروعية إجباره على فكّ الشفرة، كما يصعب أيضا ملاحقة مرتكبي الجرائم الالكترونية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة بالاتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه.[26]

ثالثا :جريمة ناعمة مغرية للمجرمين

إذا كانت الجرائم التقليدية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها، فإنّ جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية، وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في

[25] قد أشار توم فوريستر في كتابه"مجتمع التقنية العالية"،إلى أنه حسب اعتقاد الخبراء فإن 15% فقط من جرائم الإحتيال المعلوماتي هي التي يعلن عنها من قبل الشركات،و أن العديد من الجرائم تمر بدون الكشف عنها ونادرا ماتتم محاكمة الحالات التي يتم الكشف عنها نظرا لصعوبة إثباتها،أنظر إلى:عائشة بن قارة مصطفى،المرجع السابق،ص.46.

[26] بعرة سعيدة،الجريمة الإلكترونية في التشريع الجزائري"دراسة مقارنة"،مذكرة مكملة لنيل شهادة الماستر في العلوم الجنائية،جامعة محمد خيضر ،بسكرة،2015،ص.35-36.

توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل على جهاز الكمبيوتر.

تتطلب الجرائم التقليدية استخدام الأدوات والوسائل المادية والعنف غالبا كما هو الحال في جرائم المخدرات والإرهاب، والسطو المسلح، إلا أن الجرائم المعلوماتية تمتاز بأنها جرائم ناعمة لا تتطلب العنف على الإطلاق.

إنّ كل ما يحتاجه المجرم المعلوماتي، هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، ويحتاج كذيلك إلى وجود شبكة المعلومات الدولية،بالإضافة إلى الإرادة في تحقيق الغرض الإجرامي وكل ذلك دون عنف.[27]

رابعا :قلة الإبلاغ عن الجريمة المعلوماتية

غالبا في الجرائم الالكترونية، المجني عليه يحجم عن طلب مساعدة السلطات المختصّة في إثبات الجريمة والكشف عنها، حتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرّة، وضياع ثقة المساهمين، في الحالة التي يكون فيها المجني عليه عادة بنكا أو مؤسسة مالية(شخصا معنويا) يهمّه المحافظة على سمعته وثقة عملائه، أكثر من اهتمامه بالكشف عن الجريمة ومرتكبيها، لذلك يفضل المجني عليه تقديم ترضية سريعة لعميله، وينهي الأمر داخليا.

[27] خليفة محمد،الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن،دط،دار الجامعة الجديدة،الإسكندرية،ص.36-37.

كما أن للمجني عليه دور مثير للريبة، قد يشارك بطريقة غير مباشرة في ارتكاب السلوك الإجرامي، ذلك في حالة التي يكون فيها مثلا المجني عليها إمرأة، ثمّ التحرش بها وابتزازها عبر موقع التواصل الاجتماعي Facebook، فتضطر الضّحية للرضوخ لطلبات المجني خشية من تشويه سمعتها[28].

لكن هناك حالات ضئيلة أين يتم الإبلاغ فيها عن الجرائم الالكترونية نسبة إلى شخصية المجني التي تلعب دور مهم في عملية الإبلاغ.[29]

الفرع الثاني

صفات المجرم المعلوماتي

لاشك أن الشخص الذي يرتكب الفعل غير مشروع و يعتدي فيه على حق من حقوق الغير بالمعنى الواسع،يعد في نظر القانون مجرما و يتعرض للعقاب إذا ما اقترف جريمته وتكون العقوبة هدفها تحقيق الردع العام أوالخاص أما الجريمة الإلكترونية، تتطلب مقدرة ذهنية .

[28] شهدت الجزائر في السنوات الأخيرة تضاعف مخيف للجرائم الإلكترونية،التي باتت تهدد كيان المجتمع،حيث تقول زهرة فاسي أستاذة في علم الإجتماع أن أكثر عرضة لهذا النوع من الجرائم هن النساء الاتي لايبلغن عن الفاعل خوفا من الفضيحة ،مشيرة أن العديد من الفتيات رضخن للإبتزاز وسلمن مبالغ مالية ضخمة مقابل عدم نشر صورهن على سبيل المثال ومنهم من هربت من بيوت الأهل خوفا من الفضيحة،أنظر إلى مقال صحفي،بإسم خديجة بودومي،الجزائر،www.dw .com

[29] باطلي غنية ،المرجع السابق،ص.35.

لدى الجاني، فلابد أن يكون الجاني ذو كفاءة عالية في مجال التقنية، يحتاج إلى جهاز حاسوب موصول بالشبكة العنكبوتية إلى جانب درايته بمختلف الأنظمة المستعملة في هذا المجال، ويمكن حصر هذه الصفات في عدّة جوانب.[30]

أولا:**سمات شخصية المجرم المعلوماتي**

يختلف مجرم المعلوماتي كثيرا عن المجرم في الجرائم التقليدية،ذلك أن له سمات خاصة تميزه عن غيره إلا أن هذه الصفات تقترب في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء

فكلاهما قد يكونوا من ذوي المناصب الرفيعة المستوى ويتمتعون بالاحترام والثقة والقدرة على التكيف الاجتماعي، بالإضافة إلى ذلك يمتلك هذا المجرم المعلوماتي المعرفة على كافة الظروف التي تحيط بالجريمة وتنفيذها، وإمكانية نجاحها، فيتمتع هذا الأخير بقدر لا يستهان من المهارة بتقنيات الحاسوب والانترنت[31]، فيعتبر إجرام الانترنت إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، مجرم الانترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ثمّ نيل مبتغاه.

كما يتصف مجرمو الانترنت بالخوف من كشف جرائمهم، فتساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي الانترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يُعرَّض

[30] عائشة بن قارة مصطفى،المرجع السابق،ص.41.

[31] خليفة محمد،المرجع السابق،ص.33.

المجرم إلى اكتشاف أمره هو ان يطرأ في أثناء تنفيذه لجريمته عوامل غير متوقّعة لا يمكن التنبؤ بها.[32]

نجد ان أغلب الجرائم التي ترتكب مكوّنة من مجموعة أشخاص يحدد لكل شخص دور معيّن، ويتم العمل فيها لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمن فيها متخصص في الجانب التقني من المشروع الإجرامي، وشخص آخر من المحيط الخارجي لتغطية التلاعب ولتحويل المكاسب إليه.[33]

ثانيا : الدافع إلى ارتكاب الجريمة

تتباين دوافع ارتكاب الجريمة الإلكترونية تبعا لطبيعة المجرم ومدى خبرته في مجال الحاسب الآلي،ومما لاشك فيه أن وراء كل فعل سواء كان يحمل في طياته جانب الخير أم الشر إلا وخلفه دافع أو غرض أو غاية من ذلك،وبالنسبة لجرائم الكمبيوتر و الأنترنت دوافع عديدة تحرك الجناة لإرتكاب أفعال الإعتداء الغير المشروعة،و بالتالي نتطرق إلى بعض الدوافع كآتي:

1 السعي إلى تحقيق الكسب المالي:

يعد هذا الدافع من بين أهم الدوافع تحريكا للجناة لإقتراف جرائم الإلكترونية،ذلك أن خصائص هذه الجرائم،وحجم الربح الكبير الممكن تحقيقه من بعضها،لاسيما غش الحاسوب أو الإحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع.

[32] محمد خليفة، المرجع السابق،ص.35.

[33] عائشة بن قارة مصطفى،المرجع السابق،ص.41.

إذا ما انتقلنا للدراسات الحديثة ،فسنجد أن هذا الدافع يعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية،وفي مقدمة هذه الدراسات و التقارير الإحصائية ،نجد التقارير الصادرة عن مركز احتيال المعلومات الوطني للولايات المتحدة الأمريكية.[34]

2 الانتقام من رب العمل وإلحاق الضرربه:

لقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق الأعمال الأخرى،يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل و المشكلات المالية،هذه الأمور قد تدفع إلى النزعة إلى تحقيق الربح،لكنها في حالات عديدة،مثلت قوة حركة لبعض العاملين لارتكاب جرائم الإلكترونية،باعثا لانتقام من المنشأة أو رب العمل.

3 الرغبة في قهر النظام و التفوق على تعقيد الوسائل التقنية:

يرى البعض أن الدافع إلى ارتكاب الجرائم الإلكترونية،يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح،ومع أن الدراسات لاتظهر هذه الحقيقة ،إذ يظهرفي قهر النظام نسبة معتبرة من جرائم الحاسوب،كما هو الحال بالنسبة إلى مايعرف أنشطة الهاكر،حيث يميل مرتكبو هذه الجرائم إلى تفوقهم و مستوى ارتقاء براعتهم،لدرجة أنه ازاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون ايجاد سبل لتحطيمها،ويتزايد شيوع هذا الدافع

[34] جعفر حسن الطائي،جرائم تكنولوجيا المعلومات،رواية جديدة للجريمة الحديثة،ط1،جامعة عمر المختار،2007،ص.168

لدى صغار السن،الذين لديهم شغف المغامر،محاولين بذلك كسر حواجز أمن أنظمة الحواسيب و شبكات المعلوماتية،و لإظهار تفوقهم على وسائل التقنية.[35]

ثالثا : أنماط مجرمي المعلوماتية

يمكن تصنيف مرتكبي الجرائم الالكترونية على أساس أغراض الاعتداء إلى الفئات التالية:

1الفئة الأولى:تضم هذه الفئة نوعين من المتطفلين،الهاكر والكراكز

أ **الهاكر:**الهاكر هم الأشخاص الشغوفين و الذين لديهم ميل لفهم و استعمال التقنية والبرامج ،ويصنف على أنهم الأشخاص الذين يدخولون إلى المواقع المعلوماتية بدون استخدام العنف،حيث يعرف الأستاذ"**VIVANT**" الهاكر بأنه "كل شخص يدخل إلى النظام لإرضاء رغبته بدون تخريب للمعطيات الموجودة داخل النظام"،وهناك من يطلق على الهواة أو "**HACKER**" بصغار نوابغ المعلوماتية".

وتستعمل هذه الطائفة أجهزة خاصة بهم،وغالبا مايرتكبون هذه الجرائم بمحض الصدفة فيصلون إلى نظام معلوماتية سواء خاصة بالوزارات أو الشركات التجارية ،وعليه فإن الدافع الإجرامي لديهم غير موجود عند اتصالهم.[36]

[35] جعفر حسن جاسم الطائي،المرجع السابق،ص-ص 168-169.

[36] نذكر على سبيل المثال عصابة 414 من أمريكا نسب إليها 60 فعلا،أنظر إلى باطلي غنية،المرجع السابق،ص.38.

ولا يمكن تصنيفهم من بين الطوائف الإجرامية لأن نادرا ماتكون غير شريفة ،بل تميل إلى المغامرة و الإكتشاف و يمكن لهؤلاء أن تتطور أعمالهم و تتغير شخصيتهم ليدخلوا في نطاق ال CRACKERS.

ب الكراكز:تعرف هذه الطائفة بالمجرمين البالغين ،الذين يتمتعون بالمهارات والمعارف الفنية في مجال الأنظمة الإلكترونية ،و تدل الإعتداءات التي يقترفها أفراد هذه الطائفة إلى جانب كبير من الخطورة الإجرامية[37]،على أساس أن الهاكر و من يقم بتحريف و تحويل التقنيات المطورة من طرف الهاكر لأغراض مادية ويطلق عليهم ب SPIDERS لأنهم يعملون في الخفاء ،ولا يتركون آثار مادية لأفعالهم [38]لذلك فهم أشد خطورة،إذا ماتم تبادل تقنياتهم فيما بينهم و شكلوا ما يعرف بالجماعات أو الفرق المتخصصة.[39]

2الفئة الثانية:تشمل فئة المحترفين ،التي تعد أخطر من بين مجرمي التقنية العالية،تتميز هذه الطائفة بالتقنية العالية و المهارات التقنية،وبالتنظيم و التخطيط للأنشطة التي ترتكب من قبل أفرادها ،حيث تهدف اعتداءاتهم من جهة إلى تحقيق الكسب المادي لهم[40]،أو لجهات التي كفلتهم و سخرتهم لإرتكاب هذا النوع المستحدث من الجرائم ،ومن جهة أخرى قد تهدف إلى تحقيق

---

[37] محمد طارق عبد الرؤوف الخن ،المرجع السابق،ص.186.

[38] باطلي غنية ،المرجع السابق،ص،39.

[39] نذكر على سبيل المثال ،ماحدث أثناء محادثات السلام في كامب ديفيد الثانية بين الفلسطين و الإحتلال الإسرائيلي تحت رعاية الولايات المتحدة الأمريكية ،فقد أرسل القراصنة فيروسا جديد غير معروف ،إلى مجموعة من الموظفين ،و الصحفيين ،ترتب عليه عدم إمكانيةتحميل صور الرؤساء المجتمعين ،حيث كانت الرسائل المرسلة إلى عنوان وزارة الخارجية تحمل عنوان "الظرف الضاحكة"FUNNY JOKES ،و بمجرد فتح الرسالة ،فإن فيروسا غير معروف يبدأ بتدمير القرص الصلب ،ثم يرسل تلقائيا نسخة من البريد الإلكتروني الحامل للفيروس إلى كل عنوان بريدي موجود في الجهاز. أنظر إلى محمد طارق عبد الرؤوف الخن،المرجع السابق،ص.186.

[40] عائشة بن قارة مصطفى،المرجع السابق،ص.42.

أغراض سياسية ،أو التعبير عن موقف فكري، ويمكن تقسيم هذه الطائفة إلى مجموعات متعددة تبعا لتخصصهم بنوع معين من الجرائم ،أو طبقا للوسيلة المعتمدة في ارتكاب الجرائم على سبيل المثال ،طائفة محترفي التجسس الصناعي أو طائفة مجرمي الإحتيال و التزوير[41].

ج الفئة الثالثة:يقصد بها طائفة الحادقون ،يغلب على هذه الطائفة عدم وجود أهداف وأغراض إجرامية لدى أفرادها،فهم لايسعون لإثبات مقدراتهم التقنية،ولا إلى تحقيق مكاسب مادية أو سياسية ،إنما يحركهم الثأر و الرغبة بالإنتقام كأثر لتصرف صاحب العمل معهم،أو لتصرف منشأة ما سبق لهم التعامل معها،ولذلك فهم ينقسمون إلى مستخدمين للنظام بوصفهم موظفين أو علاقة ما بالنظام محل الجريمة ،و إلى غرباء عن النظام،ولايتصف أعضاء هذه الطائفة بالضرورة بالمعرفة التقنية الإحترافية،كما تغلب على أنشطتهم من الناحية التقنية استخدام الفيروسات والبرامج الضارة،[42]الهادفة لتخريب و اتلاف الأنظمة المعلوماتية سواء كان الإتاف كلي أو جزئي،ليس هناك ضوابط محددة بشأن أعمارهم ،وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بإرتكابها،لتوفر ظروف و عوامل تساعد ذلك.

وبالتالي فإن سمات هذه الطائفة تضعها في مؤخرة الطوائف السالفة الذكر،على أساس أنهم أقل خطورة من غيرهم من مجرمي التقنية ،لكن ذلك لايمنع أن تكون الأضرار التي نجمت عن

[41] محمد طارق عبد الؤوف الخن،المرجع السابق،ص.187.

[42] المرجع نفسه.187.

الأنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسسات المستهدفة ،سواء تلك التي يعملون فيها،أو التي تم استهدافها لإلحاق الضر ربها[43].

د الفئة الرابعة:تعتبر طائفة ظهرت حديثا ،يطلق عليها تسمية صغار نوابغ المعلوماتية،أو طائفة صغار السن[44]،ولقد ثار جدل فقهي حول تصنيف هذه الطائفة ضمن مجرمي المعلوماتية ،كغيرهم دون تمييز،وانقسم الفقهاء بصدد ذلك إلى ثلاث اتجاهات:

الاتجاه الأول:وهو الاتجاه الذي يرى أنه من غير الملائم تصنيف هؤلاء الشباب ضمن الطوائف الإجرامية ،لأن لديهم ببساطة ميلا للمغامرة و التحدي و الرغبة في الاكتشاف.

الاتجاه الثاني:يؤيد هذا الاتجاه هذه الفئة على أساس أن لها الفضل في كشف الثغرات الأمنية في تكنولوجيا المعلومات.

الاتجاه الثالث:يصنف هذا الاتجاه هذه الطائفة ضمن مجرمي الانترنت،وذلك باعتبار أن العبث في الحواسب قد يؤدي إلى ارتكاب جرائم والتي قد ينزلق أفرادها في طوائف محترفي الإجرام المعلوماتي[45]

[43] جعفر حسن الطائي،المرجع السابق،ص.16.
[44] باطلي غنية ،المرجع السابق،ص.38.
[45] محمد طارق عبد الرؤوف الخن،المرجع السابق،ص.188.

المبحث الثاني

أركان الجريمة الإلكترونية

سبق وأن أشرنا في معرض حديثنا عن مفهوم الجريمة الإلكترونية بالتعرض إلى الجدل الواقع في تسميتها بين التشريعات المقارنة والتشريع الجزائري ،فرغم الاختلاف التشريعات في تعريفها إلا أنها تنصب في نفس المجرى كذلك تضمن حديثنا خصائص هذه الجريمة من جهة وسمات التي يتصف بها المجرم الإلكتروني من جهة أخرى.

أما في هذا المبحث نتطرق إلى تبيان أركان الجريمة المعلوماتية من الركن المادي المتمثل

في السلوكات المجرمة والتي تختلف من جريمة إلى أخرى (المطلب الأول)،والركن المعنوي الذي يعبر عن إرادة المجرم المعلوماتي(المطلب الثاني).

المطلب

الأول:الركن المادي

يعتبر الركن المادي في الجريمة التقليدية فعل أو السلوك المجرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته كما يجب أن يرتبط السلوك الإجرامي والنتيجة الضارة علاقة سببية.

بمعنى حتى يعاقب المجرم على سلوكه الإجرامي لابد أن يتطابق هذا الفعل المجرم مع النموذج الإجرامي المنصوص عليه في قانون العقوبات.[46]

أما الركن المادي في الجريمة الجريمة الإلكترونية فيتطلب قيام السلوك الإجرامي والنتيجة و العلاقة السببية،مع العلم أنه يمكن تحقق الركن المادي دون حدوث النتيجة كالتبليغ عن الجريمة قبل تحقق نتيجتها[47]

ويتخذ الركن المادي عدة صور بحسب نوع الجريمة،وهو مانقوم بتبيانه في ثلاث فروع متفرقة،السلوك الإجرامي(الفرع الأول)،النتيجة الضارة(الفرع الثاني)،العلاقة السببية(الفرع الثالث).

الفرع الأول

السلوك الإجرامي

مايميز الجرائم الإلكترونية بشكل عام ،هو وجود حاسب آلي وشبكة معلوماتية ،حيث لايمكننا تصور وجود جريمة الكترونية من دون الحاسب الآلي و شبكة الإنترنت،التي يعتبر استخدامها مشروع كأصل عام ،ولكن الخلاف يثور من حيث استخدام هذه الوسائل الحديثة لغايات غير مشروعة و ذلك تعد لوسيلة الإلكترونية من أهم مقومات السلوك الإجرامي في الجرائم الإلكترونية،فالسلوك هذا يتطلب وجود بيئة رقمية من حيث الجهاز الإلكتروني ،و الاتصال

[46] معتوق عبد اللطيف ،المرجع السابق،ص.25.

[47] الحسيناوي علي جبار ،جرائم الحاسوب و الأنترنت،دط،دار اليازوري العلمية للنشر و التوزيع،عمان ،2009،ص.37.

بالانترنت ،لإرتكاب الجرائم الإلكترونية بشكل خاص ،كما و يتطلب الأمر معرفة بكيفية استخدام هذه التقنية مثل كيفية تحميل صور مخلة بالآداب العامة على الجهاز،وإعداد برنامج "فيروس"تجهيزا لنشره عبر الانترنت،إن المنطق التقني الذي ذكرناه يمثل سلوكا ماديا إيجابيا للجرائم الإلكترونية،فهذا يجعل الجرائم الإلكترونية ذات طابع موحد يتمثل في السلوك والنشاط المادي كعنصر أساسي للجرائم الإلكترونية ،و نلمس ذلك من خلال ماعبر عليه المشرع الجزائري في الفصل السابع من ق.ع.ج باستخدام عبارة المساس بأنظمة المعالجة الآلية للمعطيات،حيث قام بتجريم بعض الأفعال المساهمة في حدوث الجريمة الإلكترونية[48]،والتي تعتبر السلوك المادي لهذا النوع المستحدث من الجرائم،ونجد نفس الشيء بالنسبة للمشرع الفرنسي،حيث دل على هذه الأفعال غير المشروعة والتي تعتبر الركن المادي للجريمة الإلكترونية من خلال استخدامه عبارة :

Des atteintes aux systémes de traitement automatisé de données

حيث أدرجها في فصل خاص وهو الفصل الثالث من ق.ع.ف[49].

ويتخذ السلوك الإجرامي في الجرائم الإلكترونية صورتين:

الصورة الأولى تتمثل في السلوك الإيجابي والذي يتطلب مجهود بدني يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف الإعتداء على مصلحة التي يحميها المشرع،ومثال ذلك:كل الأفعال التي يرتكبها الجاني،كفعل الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعاجة الآلية للمعطيات ، نص المشرع الفرنسي على فعل الدخول و البقاء في المادة

[48] الحسيناوي علي جبار ،المرجع السابق،ص.252.

[49] Op-cit

1-1/323 من ق.ع.ف، والتي تنص كالآتي:" :" **فعل الدخول أو البقاء-بطريق الغش-داخل كل أو جزء من نظام المعالجة الآلية للمعطيات،يعاقب عليه بالحبس لمدة سنتين وبغرامة مقدارها 60000أورو**"[50])

كما قام المشرع السعودي بنص في مادة الثالثة من نظام مكافحة الجرائمةالإلكترونية ،على بعض الأفعال التي تعتبر السلوك الإجرامي المكونة للركن المادي لهذه الجريمة،نذكر البعض منها:

الدخول غير المشروع لتهديد شخص أو إبتزازه،أو الدخول غير المشروع إلى المواقع الإلكترونية بهدف تغيير تصاميم الموقع أوإتلافه أو تعديله أو تغيير عنوانه.

فعل التصنت إلى ماهو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.....إلخ بينما يكون السلوك الإجرامي في جريمة السرقة المعلوماتية[51])والإتلاف العمدي للمعلومات والبرامج أو جريمة القرصنة أوالإحتيال المعلوماتي[52])سلوكا إجراميا متعددا يبدأ من الدخول إلى

[50] L'article 323/1-1,www.legifrance.gouv.fr.op cit

[51] السرقة هي نزع المال من حيازة صاحبه دون رضاه وعلمه وإدخاله في حيازة السارق. أما بالنسة لمن يقوم بسرقة البيانات بأخذ نسخه من البيانات أو المعلومات أو برامج معينه وأدخلها في حيازته لكن لم يخرج المعلومات من حيازة مالكها بل أبقاها في حيازته بناء على هذا فإن السرقة لهذا المعنى تعارض تعريف السرقة المنصوص عليها في قانون العقوبات و امكانية أن تكون البيانات أو البرامج محلاً للسرقة لأنها أشياء غير محسوسة وغير مادية يمكن أن تقع السرقة على البرامج والمعلومات وبالتالي تخضع لذات أحكام جريمة السرقة ولأركانها وهما الركن المادي والركن المعنوي في أن الركن المادي يتمثل في السرقة أخذ نسخه عن المعلومات أو البرامج دون إذن صاحبها وعلمه. أما الركن المعنوي يتمثل في القصد الجرمي القائم على العلم والإرادة وذلك لتحقيق مصلحته الشخصيه .. أنظر إلى وسيم طعمة ،السرقة المعلوماتية"دراسة مقارنة"،مجلة جامعة البحث ،جامعة دمشق،العدد 68،سوريا،2017،ص.167-168.

[52] لقد تعددت التعاريف بشأن جريمة الإحتيال عبر الأنترنت،نذكر منها على سبيل المثال:أنها أي سلوك إحتيالي يستخدم فيه الحاسوب الآلي والأنترنت كوسيلة للحصول على امتياز مالي.أنظر إلى محمد طارق عبد الرؤوف الخن،المرجع السابق،ص.37.

نظام الحاسب الآلي أو إلى موقع ما على شبكة الانترنت بوجه غير شرعي ثم القيام بالتلاعب بمحتوياته،ينطوي هذا التلاعب على عدة أنشطة إجرامية من إدخال لبيانات غير صحيحة أو محو أو تدمير لمحتويات هذا النظام ،أو نشر لمواد مخلة بالنظام و الآداب العامة[53]

قد يكون النشاط الإجرامي في الجرائم الإلكترونية وقتيا،أي يبدأ وينتهي بمجرد تمامه ، مثل السرقة المعلوماتية أو الإعتداء على معطيات الحاسب الآلي بإتلافها ،وقد يكون مستمر مثل إنشاء مواقع لتحريض القصر على الفسق أو الإنتحار[54].

أما الصورة الثانية وهي السلوك السلبي،وهو الإمتناع عن اتيان أمر يوجبه المشرع،فمن الممكن التوقف عن عمل معين كان من الواجب مباشرته،وهذا الإمتناع عن قاعدة فرضها المشرع،مثل امتناع المنقذ البحري من انقاذ غريق كان بإمكان انقاذه،أما الإمتناع في الجرائم الإلكترونية يكون مثل،امتناع موظف أمن عن حماية بيانات و معلومات الشركة التي يعمل بها،أو عدم الإبلاغ عن الجريمة لحفاظ على حقوق الغير وخصوصيتهم.

[53] معتوق عبد اللطيف،المرجع السابق،ص.23.

[54] كلعبة الحوت الأزرق blue whale أو تحدي الحوت الأزرق ،وهي لعبة على شبكة الأنترنت ،حيث قام فليب بودكين بإبتكار هذه اللعبة وكان هدفه منها تنظيف المجتمع من خلال دفع الناس إلى الإنتحار الذي اعتبر أنه ليس له قيمة ،تتكون اللعبة من تحديات لمدة 50 يوما وفي التحدي النهائي يطلب من اللاعب الإنتحار ،بدأت هذه اللعبة بالإنتشار الواسع في روسيا ونجم عنها العديد من الضحايا وخلق موجة من الذعر في روسيا ،لتنتشر بعد ذلك في مختلف مناطق العالم ،تعتمد هذه اللعبة على غسل لدماغ المراهقين الضعفاء،وأمرهم بالقيام بأعمال معينة مثل مشاهدة أفلام الرعب و الإستيقاظ في ساعات متؤخرة من الليل ،وايذاء للنفس وبعد أن يتم استنفاذ قواهم في النهاية يتم أمرهم بالإنتحار،أنظر إلى الموقع لإلكتروني www.albawaba.com .

وبالتالي فالسلوك الإجرامي في الجريمة الإلكتروني يتم عن طريق الجهاز الإلكتروني أيا كان نوعه أو شكله،متصلا بشبكة الأنترنت،وبدون هذه الوسيلة لا يمكن مباشرة السلوك الإجرامي،وقد يكون سلوك إيجابي،بمباشرة الفعل من الجاني بإستخدام الوسائل الإلكترونية،وقد يكون سلوك سلبي بإمتناع عن الفعل كان من الواجب اتيانه وهو نادر الحدوث،وفي الغالب يرتكب من قبل موظفين مختصين.

الفرع الثاني

النتيجة الإجرامية

تعتبر النتيجة الإجرامية العنصر الثاني للركن المادي للجريمة ، و هي عبارة عن الضرر الذي نتج عن السلوك الإجرامي سواء كان فعلا أم تركا ، و هو الأثر الخارجي الذي يتولد عن السلوك و يحدث تغييرا يعتد به القانون ، و ذلك طبقا للتصور المادي للجريمة ، أما التصور الشرعي أو القانوني فهو الإعتداء على المصلحة التي يحميها القانون .

وبالتالي تعتبر الأثر المباشر للسلوك الجرمي غير المشروع ،يعرف بعض من الفقه النتيجة الإجرامية على أنها ذلك التغيير الذي يحدث كأثر للسلوك أو الفعل الغير المشروع الذي قام به الجاني ،ويطلق على هذا التغيير الذي يحدث في العالم الخارجي بالمدلول المادي للنتيجة الإجرامية. [55]

[55] خيرت علي محرز ، التحقيق في جرائم الحاسب الآلي ، دط ، دار الكاتب الحديث ، الإسكندرية ، 2012، ص123.

أما المدلول القانوني للنتيجة الإجرامية فهو ذلك الاعتداء على الحق الذي يحميه القانون وهو يمثل التكييف القانوني للنتيجة المادية التي خلفها الفعل غير المشروع.[56] وتعتبر الجريمة الإلكترونية كغيرها من الجرائم و التي يفترض وجود النتيجة الإجرامية فيها،وتختلف النتيجة الضارة في الجريمة المعلوماتية حسب نوع الجريمة المرتكبة.

ففي جريمة تزوير المعلومات أو البيانات والتي تدخل ضمن جرائم المعلوماتية،فإن النتيجة الإجرامية فيها تحريف الحقيقة في البيانات و المعلومات الموجودة في جهاز الكمبيوتر أو في الموقع الإلكتروني ،إذا النتيجة هي الأثر المادي المترتب على القيام بالفعل الغير المشروع،وهي أيضا الأثر القانوني الذي يمثل الإعتداء على خصوصيات الناس ومعلوماتهم بتعديلها أو حذفها أو تحريفها بما يخالف القانون.

أما في جريمة التلاعب غير المصرح به بالمعلومات تكون النتيجة الضارة ،هي وقوع ضرر فعلي على هذه المعلومات و يكون ذلك بالتغيير حالتها عن طريق الإزالة أو التعديل أو المحو.

مما تقدم نستخلص أن الجريمة الإلكترونية هي كغيرها من الجرائم ،يفترض فيها وجود النتيجة الإجرامية كأساس لقيام الركن المادي لهذا النوع المستحدث من الجرائم ،حيث تعتبر من العناصر المكونة للركن المادي والذي يعد من أهم إركان الجريمة ،والذي بدونه لاتقوم الجريمة.

بصدد دراستنا لنتيجة الجرمية ،كأحد عناصر الركن المادي ،فإننا نسلط الضوء فقط على ذكر النتيجة الإجرامية للجريمة المعلوماتية بصفة عامة دون الحديث بالتفصيل عن النتيجة الإجرامية

[56] لورنس سعيد الحوامدة ، "الجرائم المعلوماتاية أركانها و آلية مكافحتها ، دراسة تحليلية مقارنة " ، مجلة الميزان للدراسات الإسلامية و القانونية ، كلية الحقوق ، المملكة العربية السعودية ، 2016، ص. 19-20.

لكل جريمة معلوماتية بالتالي تثير النتيجة الإجرامية في جرائم الإلكترونية مشاكل عديدة،على سبيل المثال مكان وزمان تحقق النتيجة ،فلو قام أحد المجرمين في أمريكا بإختراق جهاز حاسب آلي رئيسي،وهو مايعرف بإسم الخادم server في أحد البنوك في فرنسا ،وهذا الجهاز الخادم موجود في الصين، ومعرفة وقت حدوث الجريمة ،إما بالنظر إلى توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الخادم في الصين وهذا ما يثير إشكالا بالنسبة إلى وقت حدوث الجريمة ،بالإضافة إلى القانون الواجب التطبيق في هذا الشأن.

كما يواجه تحديد الخطر أو الضرر بوصفه نتيجة إجرامية مشاكل أخرى ،كالمتعلقة بجرائم العدوان الفيروسي ،إذ تثير هذه النوعية من الجرائم مشكلة تحديد الضرر وهي من الصعوبات التي تواجه الفكر القانوني المعاصر في هذا المجال ،خاصة إذا اشترط المشرع تحقق نتيجة معينة أما أثر النتيجة الإجرامية ذا البعد الدولي ،سواء في شكل امتداد الضرر أو الخطر إلى مايتجاوز الحدود الإقليمية التي وقع فيها السلوك و النتيجة ،يأخذ هذا الإمتداد شكل العدوان المحدد على مصلحة قائمة ومشروعة في دولة أو دول متعددة. [57]

الفرع الثالث

العلاقة السببية

يقصد بالعلاقة السببية هي العلاقة بين للسلوك الإجرامي فعلا أم تركا و بين النتيجة الإجرامية ، بمعنى أن السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية ، و لولا هذا السلوك ما كانت

[57] خيرت علي محرز ، المرجع السابق ، ص 124-125.

لتحدث النتيجة الإجرامية ، و تبرز الأهمية القانونية لعلاقة السببية من حيث أنها من العناصر الأساسية المكونة للركن المادي للجريمة ، و تحققها يعد شرطا جوهريا من شروط المسؤولية الجزائية ، فإذا أسندنا النتيجة الإجرامية إلى السلوك و كانت هناك إرادة حرة واعية، توفرت أسباب قيام المسؤولية الجزائية ، أما إذا لم يكن هناك علاقة بين النتيجة الإجرامية و السلوك إنتفت المسؤولية الجزائية .

و لكي تكتمل علاقة السببية في جريمة التعدي على الحق في الخصوصية ، يجب أن يكون هناك إتصال بالأنترنت من خلال جهاز إلكتروني ، و من ثم إختراق جهاز ما أو موقع للوصول إلى بياناته الخاصة ، وبعدها يتم نشر هذه البيانات من معلومات أو صور عبر موقع معد مسبقا لذلك ، أو عن طريق المواقع الإلكترونية كمواقع التواصل الإجتماعي ، و تثبت كذلك علاقة السببية في جريمة حيازة صور إباحية لأطفال في حاسوب بمجرد ثبوت الضرر من خلال بث هذه الصور ، فتظهر علاقة السببية بين حيازة الصور و بين ترويجها أو عرضها أو تداولها .

فتعد العلاقة السببية عنصر مهم من عناصر الركن المادي للجريمة، حيث تعتبر حلقة وصل بين السلوك الإجرامي والنتيجة الإجرامية،ذلك بإثبات أن هذا السلوك هو سبب في حدوث النتيجة الضارة .

أما في نطاق الجرائم الإلكترونية ،تعتبر العلاقة السببية أساسية لقيام هذا النوع المستجد من الجرائم ،و المبدأ العام الذي يحكم العلاقة السببية أن الإنسان لا يسأل إلا عن النتائج التي يكون لنشاطه دخلا في إحداثها فاستحقاق العقاب في القانون هو رهن قيام الرابطة السببية بين نشاط الجاني

وبين الواقعة الإجرامية،بالتالي ينبغي لمسألته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية .

ففي جريمة انتهاك الحق في الخصوصية عبر شبكة الانترنت يجب أن يكون هناك دخول غير مصرح به ،بإستخذام الحاسوب و القيام باختراق الخوادم المختلفة في مسارها،ثم بعد ذلك التعدي على الخصوصية موقع ما،وتكون العلاقة السببية قائمة بمجرد ثبوت الضرر الناتج عن السلوك الغير المشروع .[58]

و منه فقد برزت عدة اتجاهات فقهية حول المعيار المناسب لقيام العلاقة السببية و هي كالتالي :

النظرية الأولى : نظرية تعادل الأسباب

و قد قال بها الفقيه الألماني (فون يوري) ، و مضمونها مساواة جميع العوامل التي تساهم في احداث النتيجة الإجرامية ، فهي كلها متعادلة و متساوية من حيث قوة أثرها في حصول النتيجة ، و لما كان سلوك الجاني إحد هذه الأسباب ، فإن يسأل عن النتيجة الإجرامية حتى و لو كانت الأسباب الأخرى مردها فعل الطبيعة ، و مثال ذلك أن يطلق أحدهم النار على آخر ليقتله [59]، و يتم نقله بسيارة الإسعاف التي ترتطم بشجرة سقطت على الطريق فتضاعف من إصابة المجني عليه ثم ينقل إلى المستشفى حتى يتلوث جرحه من العلاج غير المناسب فيموت ، فالجاني و سقوط الشجرة بفعل الطبيعة و تلوث الجرح من المستشفى كلها عوامل ساهمت في وفاة المجني

[58] الحسيناوي علي جبار ، المرجع السابق ، ص 39

[59] خيرت علي محرز ، المرجع السابق ، ص 127 .

عليه بقدر متساوي ، و لذلك تتوفر السببية بين سلوك الجاني و بين النتيجة الإجرامية في هذه الجريمة.[60]

و يؤخذ على هذه النظرية أنها قررت تعادل الأسباب من حيث أثرها في حصول النتيجة ثم إختصرجع نفت إحداها فقط و هو سلوك الجاني للمسؤولية عن هذه النتيجة ، فضلا عن التوسع غير المبرر في إثبات السببية حتى أن الجاني بات مسؤولا عن العوامل النادرة التي تساهم في حصول النتيجة .

النظرية الثانية : نظرية السبب الأقوى أو السبب المباشر

و مضمون هذه النظرية يعني أنها لا تسلم بتساوي العوامل المساهمة في حصول النتيجة الإجرامية ، بل يختار من بينها أقوى هذه الأسباب ، سواء كان سلوك الجاني أو غيره ، و بالتالي يكون ذلك السبب الأقوى هو المسؤول عن النتيجة التي وقعت مع ملاحظة أنه لكي يسأل الجاني لا يشترط أن يكون سلوكه أقوى من بقية الأسباب الأخرى المجتمعة ، و لكن يكفي أن يكون أقوى هذه العوامل على حدى .

ففي المثال السابق ، لو كان إطلاق الرصاص أقوى من أثر سقوط الشجرة و ارتطام سيارة الإسعاف بها ، و كذلك أقوى من أثر التلوث العلاجي للجرح فيكون الجاني مسؤولا عن وفاة المجني عليه ، و لو كان التلوث أقوى في أثره بالنسبة للوفاة فلا يسأل الجاني عن القتل ،و لو كان سقوط الشجرة هو العامل الأقوى ما سئل الجاني او المستشفى .

[60] المرجع نفسه، ص127-128

ويأخذ على هذه النظرية أنها حصرت النتيجة في عامل واحد يؤدي إليها و هو أقوى الأسباب ، و هو أمر قد يؤدي بالجاني إلى الإفلات من العقاب .

النظرية الثالثة : السببية الملائمة

و مضمون هذه النظرية أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله ، أي تلك التي تقع حسب المجرى العادي من الأمور ، و لو لم يكن وصفها بأنها مباشرة أو محققة لهذا الفعل ، و يعد فعل الجاني مناسبا أو ملائما للنتيجة التي وقعت متى كان كافيا بذاته في حصول هذه النتيجة وفقا للمجرى العادي من الأمور ، و ما دامت ظروف الحال تنبئ بأنه قد توقعها أو كان من الممكن له أن يتوقعها ، بصرف النظر عن العوامل الأجنبية التي تدخلت في حصول هذه النتيجة وفقا للمجرى العادي من الأمور ، و ما دامت ظروف الحال تنبئ بأنه قد توقعها أو كان من الممكن له أن يتوقعها ، بصرف النظر عن العوامل الأجنبية التي تدخلت بين سلوك الفاعل و النتيجة ، و سواء كانت هذه العوامل سابقة أو لاحقة أم معاصرة لسلوك الجاني .

و قد قال الفقه الألماني بهذه النظرية ، و العبرة عنده أن تكون النتيجة ممكنة و عادية وفقا للظروف و العوامل التي حدثت ، و على ذلك فلو تداخلت عوامل شاذة في حصول النتيجة لأدى ذلك إلى قطع علاقة السببية بين السلوك الإجرامي و النتيجة الإجرامية ، كأن يموت المصاب بطلق ناري في المستشفى على إثر حريق فيه ، أو تنقلب سيارة الإسعاف التي تنقله فيصاب بارتجاج في المخ يؤدي بحياته ، و المعول عليه أن يتعين تقدير الوقائع في كل حالة على حدى.

و يرى جانب من الفقه أن هذه النظرية لا تخلو من التحكم ، فكون النتيجة ممكنة أو ليست ممكنة مع مراعاة الظروف التي حدثت فيها ، مسألة تقديرية يختلف فيها تقدير الناس ، و لا يصح أن تبنى أحكام القانون الجنائي على أسس تحكمية كهذه.

و لذلك يميل الفقه إلى الأخذ بمعيار موضوعي في التوقع أو الاحتمال حتى يتفادى بعض الحلول التحكيمية التي ينتهي إليها المعيار الشخصي ، و لذلك لا يعتمد على ما يتوقعه الجاني شخصيا ، و إنما يتوقعه الشخص العادي – إن وجد – في مثل ظروفه .[61]

المطلب الثاني

الركن المعنوي للجريمة الإلكترونية

الركن المعنوي هو النصف الآخر للجريمة ، و يمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكاب جريمته ، حيث لا تقوم الجريمة قانونا بدونه ، فلابد من توفر الإرادة الآثمة لدى الجاني عند اقدامه على السلوك الإجرامي ، كما يجب أن تكون الأفعال ارادية ، و إلا انتفى الركن المعنوي للجريمة ، و أن تكون هذه الأفعال متجهة نحو مخالفة القواعد القانونية ، ليترتب على مخافتها الجزاء الجنائي المناسب .

[61] خيرت علي محرز ، المرجع السابق ، ص129-130

فمن المتصور غالبا أن لا تقع الجريمة الإلكترونية إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو إختراق الشبكة ،و الأصل في الجرائم هو العمدية إلا ما استثني بنص.[62]

يتخذ الركن المعنوي في هذا النوع المستجد من الجرائم صورة القصد الجنائي العام بعنصريه العلم والإرادة إذ يجب أن تتجه إرادة الجاني إلى فعل الاعتداء ،كما يجب أن يعلم بأن نشاطه الإجرامي يؤدي إلى ارتكاب سلوك يعاقب عليه القانون.([63]

ولقد ثار جدل فقهي حول مدى ضرورة توافر القصد الجنائي الخاص في بعض الجرائم الإلكترونية فهناك من يرى ضرورة توافر هذا القصد ،في حين يرى البعض الآخر أن القصد الجنائي العام كاف لوحده لقيام الركن المعنوي لجريمة المعلوماتية،وبالتالي لا يتطلب وجود القصد الجنائي الخاص لإكتمال الركن المعنوي ويختلف الركن المعنوي باختلاف النشاط الغير المشروع المقترف من طرف المجرم المعلوماتي لذا نقوم بالعرض القصد الجنائي العام(الفرع الأول)،القصد الجنائي الخاص(الفرع الثاني).

[62] باطلي غنية ، المرجع السابق ، ص 48

[63] معتوق عبد اللطيف ، المرجع السابق ، ص 25

الفرع الأول

القصد الجنائي العام

يراد بالقصد العام ،القصد العادي الذي يتعين توافره في كافة الجرائم العمدية ويكتفي به القانون في أغلب الجرائم وهو ارادة السلوك الإجرامي ونتيجته والعلم بهما.

بمعنى أن للقصد الجنائي العام صورتين العلم والإرادة،أي يتكون من إرادة الفاعل التي تهدف إلى تحقيق عمل يجرمه القانون مع علمه بكل عناصره التي يحددها القانون.[64]

و يختلف القصد الجنائي العام بإختلاف السلوك المؤدي لإرتكاب الجريمة، فهناك بعض من الجرائم المعلوماتية بحكم طبيعتها لا يشترط لقيامها وقيام الركن المعنوي فيها وجود قصد خاص ،كالجريمة الدخول الغير المصرح بها إلى نظام المعالجة الآلية للمعطيات،تتطلب قصدا جنائيا عاما يتمثل في العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة بإعتبار أن المشرع الجزائري سعى لحماية محل الحق وهو جهاز الحاسب الآلي بما يتضمنه من معلومات وبرامج.[65]

[64] حمدي ناصر ، المرجع السابق ، ص 78

[65] معتوف عبد اللطيف ، المرجع السابق ، ص 24

كما اشترط المشرع توافر القصد الجنائي العام في جريمة اتلاف المعلومات،حيث يكفي علم الجاني بأنه يقوم بأعمال من شأنها أن تؤدي إلى تغيير الحالة التي كانت عليها المعلومات أو المعطيات بمحوها أو إتلافها وأن تتجه إرادته إلى تحقيق ذلك.[66]

وبالتالي نجد أن معظم الجرائم المعلوماتية اشترط فيها المشرع القصد الجنائي العام ،حيث اكتفى بالضرورة توافر القصد الجنائي العام لوحده لقيام الركن المعنوي لهذا النوع من الجرائم المستحدثة على غرار التشريعات الأخرى التي دعت إلى توافر القصد الجنائي الخاص إلى جانب القصد الجنائي العام في بعض الجرائم الإلكترونية وهو ما نقوم بتبيانه في الفرع الثاني.

الفرع الثاني

مدى توافر القصد الجنائي الخاص

إن أغلب الجرائم ترتكب بصورة قصدية ، بالتالي يعد القصد الجنائي من بين أكثر عناصر الركن المعنوي تصورا .

لقد اختلفت بعض التشريعات حول مدى ضرورة توافر القصد الجنائي الخاص في البعض من الجرائم المعلوماتية ،فنجد أن القضاء الأمريكي لم يقم بالتحديد في بعض الجرائم ما إذا

كانت تتطلب قصد جنائي خاص من جهة،ولا يمانع من جهة أخرى في توافر قصد جنائي خاص في جريمة التهديد بالبريد الإلكتروني.

[66] الشوابكة محمد امين أحمد ، المرجع السابق ، ص 221

أما القانون العقوبات الفرنسي اشترط سوء النية في منطق القصد الخاص حين وجود عدوان على البريد الإلكتروني[67]،وفي جريمة سرقة المعلومات وهي من جرائم المعلوماتية يتطلب فيها لقيام الركن المعنوي قصد جنائي عام و خاص فالقصد العام ينصب في علم الجاني على أن فعل سرقة المعلومات من الحاسب الآلي أو البريد الالكتروني يعد فعل غير مشروع ،ويجب أن يرتبط هذا العلم مع الإرادة وهي الحالة النفسية التي تعكس قيام الجاني بالسلوك المحظور، و قصد جنائي خاص الذي يتمثل في نية التملك للمعلومة التي تم سرقتها وتطبيقا لذلك قضت محكمة النقض الفرنسية بتوافر نية التملك التملك الوقتية في سرقة المعلومات من جهاز الحاسوب،وتتحقق هذه النية منذ سلب و حيازة المستندات خلال الوقت الازم لإعادة نسخها بدون إرادة صاحبها،وهو الأمر الذي يستدعي تدخل التشريعات لمواجهتها بالنصوص خاصة، ويرى اتجاه من الفقه أن نية التملك في جريمة سرقة المعلومات تبدأ بقيام الجاني بالدخول على أدوات الحاسب الآلي من وحدات الإدخال والإخراج و التخزين والمعالجة أو البرامج والبيانات و المعلومات والنظم المخزنة داخل ملفات الحاسب الآلي أو في ذاكرته،كل هذا من أجل الإستيلاء على المعلومات الموجودة بقصد نية التملك و الإضرار بالمجني عليه.[68]

كما يرى جانب من الفقه أن جريمة التعامل في معلومات غير مشروعة تشترط قصد جنائي عام بالإضافة إلى قصد جنائي خاص سواء في صورة الجريمة الأولى وهي التعامل في معلومات

[67] الحسيناوي علي الجبار ، المرجع السابق ، ص 42- 43

[68] لورنس سعيد الحوامدة ، المرجع السابق ، ص 24- 25

صالحة لارتكاب الجريمة أو في صورتها الثانية المتمثلة في التعامل في معلومات متحصله من جريمة.[69]

بخصوص الصورة الأولى ذهب هذا الاتجاه للقول بوجوب توفر قصد خاص إلى حانب القصد العام حتى تقوم جريمة التعامل في معلومات صالحة لارتكاب جريمة ويتمثل القصد الخاص في اتجاه إرادة الجاني إلى الاعداد والتمهيد لاستعمال هذه المعلومات في ارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعلومات غير أن المشرع الجزائري لم يشترط القصد الخاص.

أما الصورة الثانية لهذه الجريمة فقد اشترطت فيها اتفاقية بودابست قصدا خاصا ،وهو نية استخذام المعلومات في جريمة من جرائم طبقا- للفقرة (ب) من المادة 6- حيث أشارت المذكرة التفسيرية لهذه الاتفاقية لأهمية تطلب القصد الخاص، بأنه:"من أجل تجنب خطر العقاب المبالغ فيه ، حيث يتم إنتاج هذه الأجهزة وعرضها في السوق لأغراض شرعية من أجل التصدي لاعتداءات على أجهزة الحاسب الآلي ، فإنه يجب إضافة عناصر أخرى من أجل تضييق نطاق الجريمة ،وبالإضافة إلى اشتراط القصد العام فإنه يجب توافر نية خاصة أو قصد خاص لاستخدام الجهاز من أجل ارتكاب جريمة من الجرائم المشار إليها في المواد من2إلى 5 من الاتفاقية".[70]

نجد أن المشرع الجزائري لم يشترط قصد جنائي خاص في الصورة الثانية من الجريمةالتعامل في معلومات غير مشروعه وذات الوضع بالنسبة للمشرع الفرنسي.

[69] خليفة محمد ، المرجع السابق ، ص 212-213

[70] حمودي ناصر ، المرجع السابق ، ص 85

وبالتالي المشرع الجزائري لم يشترط توافر القصد الجنائي الخاص في هذه الجريمة بصورتيها وبالنسبة إلى الجرائم الأخرى المتعلقة بإعتداء على الأنظمة المعالجة اللآلية للمعطيات بل اكتفى بالضرورة توافر القصد الجنائي العام لقيام الركن المعنوي لهذا النوع المستحدث من الجرائم.[71]

[71] خليفة محمد،المرجع السابق،ص 213-215.

لقد اكتسبت المعلومات في عصرنا الحاضر أبعاد جديدة وأهمية خاصة نتيجة للعولمة و تطور وسائل الإتصال و ارتفاع حدة التنافس بين الدول ، فالدول أصبحت تعد المعلومات ثروة يجب المحافظة عليها وهذه المكانة التي تحتلها المعلومات اليوم ،جعلت التهافت للحصول عليها بشتى الطرق،وجعلها عرضة للسرقة و السطو و القرصنة خاصة بعد دخول الأنترنت إلى قطاع تقنية المعلومات،حيث لايستطيع أحد أن ينكر أهمية الأنترنت لأنها أحد أهم دعائم تكنولوجيا الإتصال و المعلومات ، إلا أن لديها آثار سلبية من بينها ظهور نوع جديد من الجرائم المستحدثة و نتيجة لحداثة هذا النوع من الجرائم،نجد أن التشريعات اختلفت في تعريف هذه الجريمة ،بحيث خولت مسألة تعريفها للفقه وبالنسبة للمشرع الجزائري نجده اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال، هذه الجريمة كأي نوع من الجرائم الأخرى لها خصائص وأركان الخاصة بها.

الفصل الثاني

آليات مكافحة و قمع الجريمة

الإلكترونية

عرف العالم فيالسنوات الأخيرة تطورا مذهلا في تكنولوجيا الإعلام والاتصال، وذلك بسبب ظهور الانترنت والمواقع الإلكترونية والتزايد المستمر في استخدام الحاسب الآلي

فرغم الإيجابيات التيأتى بها التطور في العلوم وانتشار تقنيات تكنولوجيا المعلومات إلا أنه أدى من جهة أخربإلى ظهور نوع جديد من الجرائم، والتي تعرف[5] بالجرائم الالكترونية وتعتبر كنتيجة حتمية للانفتاحالعالمي ولكل تقدم علمي أو تقنيمستحدث[1]

تمثل هذه الجريمة ضربا من ضروب الذكاء الإجرامي، نظرا لسرعة التنفيذ وسهولة الإخفاءإلى جانب ذلك تعدد صورها وأشكالها حيث أصبحت الجريمة تتم وتنظم إلكترونيا مما أضفى على هذا النمط من الجرائم صفة التعقيد وصعوبة الملاحقة[2]

مع تزايد الخسائر والأضرار الناجمة على هذا النوع المستجد من الجرائم والتى تتخطى فى اغلب أحيانها حدود الدول، بات أمر التعاون الدولي لمواجهتها ضرورة حتمية ,باعتبارها ظاهرة عالمية والتيأضحت تهدد كيان المجتمعات نظرا لخطورتها.

مما جعل العديد من الدول تسارع لتطوير بنيتها التشريعية تماشيا مع النوع المستحدث من الإجرام

[1] عبد الله عبد الكريم عبد الله ، المرجع السابق،ص.63.

[2] محمد أحمد سليمان عيسى،التعاون الدولي لمواجهة الجرائم الإلكترونية،المجلة الأكاديمية للبحث القانوني،كلية الحقوق،جامعة عبد الرحمان ميرة، بجاية،العدد الثاني،2016،ص.51.

نظرا لتزايده المستمر ولعجز القوانين العقابية التقليدية على احتواءهذه الظاهرة الإجراميةالمستحدثة[3]لذا نتطرق في هذا الفصل إلى دراسة آليات المعتمدة لمكافحة الجريمة الالكترونية

في (المبحث الأول)وهذا النوع المستحدث من الجرائم من خلال (المبحث الثاني).

المبحث الأول

مكافحة الجريمة الإلكترونية

تعتبر الجرائم الالكترونية أو ما يسمىcyber rimesمن الظواهر الإجرامية التي تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر الخسائر الناجمة عنها ,وذلك باعتبارها من الجرائم الذكية التي تنشا أو تحدث في بيئة إلكترونية ,يقترفها أشخاص من ذوى القدرات التقنية والفنية[4]. حيث أصبحت تهدد المجتمعات ككل نظرا لانتشارها الواسع في مختلف مناطق العالم[5],هذا ما جعل الدول تتحد لمواجهة هذه الظاهرة الإجرامية المستحدثة ,فرغم اختلاف سبل المكافحة إلا أنها تسعى لتصدي لهذه الجريمة[6]وعلى هذا الأساس نقوم بدراسة بعض الآليات المعتمدة لمكافحة الجريمة الإلكترونية سواء على المستوى الدولي (المطلب الأول)و على المستوى الوطني(المطلب الثاني) وتبيان الإجراءات التحقيق المعتمدة لكشف هذه الجريمة.

---

[1]عائشة بن قارة مصطفى،المرجع السابق،ص.41

[4]محمود أحمد عبابنة،المرجع السابق،ص.33.

[5]مصطفى محمد موسى،الجهاز الإلكتروني لمكافحة الجريمة،دط،دار الكتب القانونية،مصر،2006،ص.115.

[6]عبد الله عبد الكريم عبد الله،المرجع السابق،ص16

المطلب الأول

الطرقالمنتهجة لمكافحة الجريمة الالكترونية

إن تشابك العلاقات والمصالح المختلفة بين الدول,وانتشار العولمة بمختلف أشكالها ,ساعد إلى حد بعيد على نمو مستحدث من الإجرام العابر للحدود, و ارتفاع مستوى الإضرار الناجمة عنه,لتصبح الدولة وحدها غير قادرة لمواجهة هذه الجريمة.

مما دفع إلى تزايد قناعة المجتمع الدولي للحاجة الماسة إلى مواجهة فعالة للجريمة الالكترونية ,حيث تعتبر جريمة عالمية تحتاج إلى تكاثف الجهود الدولية المختلفة لمكافحتها, ويظهر التعاون الدولي في مجال مكافحة الجريمة الالكترونية بسن تشريعات خاصة لمواكبة هذا النوع المستجد من الجرائم،[7]فرغم اختلاف الأنظمة والقوانين إلا أنها كلها تسعى لتصدى لهذه الجريمة سوآءا على المستوى الوطني ,أو على المستوى الدولي.

الفرع الأول

مواجهة الجريمة الالكترونية على المستوى الدولي

لقد بذلت جهود دولية عديدة لمكافحة الجريمة الالكترونية وكان لها دور فعال في إطار التصدي لهذا النوع المستحدث من الجرائم من جهة، وكيفية تصدى بعض التشريعات المقارنة لهذه الجريمة من جهة أخرى.

(7) أشرف عبد القادر قنديل،المرجع السابق،ص.99-100.

أولا: مساعي بعض الأجهزة الدولية في مواجهة الجريمة الالكترونية

للمنظمات الدولية دور فعال فيالتصدي للجريمة الالكترونية،باعتبارها من الجرائم العالمية، التي يستوجب فيها التعاون الدولي لمكافحتها وتقتصر دراستنا بعرض بعض الأجهزة الدولية في مجال المواجهة هذا النوع المستحدث من الجرائم.

أ- دور الأمم المتحدة فى مواجهة الجريمة الإلكترونية

اهتمتالأمم المتحدة بموضوع الجريمة الالكترونية ,ووضعته من بين أولويات نشاطها,نظرا لما تسببه هذه الأخيرة من إضرار وخسائر فادحة ,وتؤكد على ان منع هذه الجرائم يتطلب استجابة دولية مشتركة بين أعضاء هذه المنظمة بغية التعاون للحد من انتشارها وتعاظم نتائجها ,من خلال إشرافها على العديد من المؤتمرات الدولية الخاصة لردع الجريمة ومعاقبة المجرمين وإبرامها للاتفاقيات الدولية.[8]

نجد من بين أهم المؤتمرات المبرمة في مجال مكافحة الجريمة الإلكترونية، المؤتمر الثامن المنعقد سنة 1990 الذي توصل إلى عدة توصيات بعد دراسته للتقرير الذي أعدته لجنة الخبراء العشرين، بتكليف من المؤتمر السابع المنعقد بميلانو سنة 1985 حول موضوع حماية نظم المعالجة الآلية و الاعتداءات التي تمس الحاسوب الآلي.

[8] إيمان مسعود سالم ، الجريمة المعلوماتية ، مذكرة لنيل شهادة الماستر ، كلية الحقوق ، جامعة محمد لمين دباغين ، سطيف، 2015 ، ص 32 .

أما بخصوص الاتفاقياتتذكرعلىسبيلالمثال ;

_الاتفاقية المنشئة للمنظمة العالمية للملكية الفكرية في ستوكهولم سنة 1967والتى دخلت حيز النفاذفى 1970,إذ تعتبر هذه المنظمة إحدى الوكالات المتخصصة لأمم المتحدة ,حيث قامت هذهالمنظمة من خلال مجموعة عمل تضم عددا من الخبراء بالعديد من المساهمات بهدف حماية برامج الحاسب الآلي ,وهو ما ذهب إليه اغلب الدول الصناعية ودول العالم الثالث إلى إخضاع برامج الحاسب الآلي لقوانين حماية حق المؤلف, ومنذ ذلك قامت اغلب التشريعات بتعديل قوانينها الخاصة بحق المؤلف ,وأضافت برامج الحاسب الآلي إلى المصنفات الادبية المجمعة وفقا للقانون ,وذلك في "إطار اتفاقية التجارة العالمية "الغات " gatt"

بالتالي لعبت المنظمة العالمية للملكية الفكرية دور في حماية حقوق المؤلف ,و برامج الحاسوب .

_الاتفاقية الخاصة بمكافحة جريمة إساءة استعمال التكنولوجيا لأغراض إجرامية رقم 63_55 التيأبرمتفي 2000/04/12,حيث ركزت على المساهمات التي يمكن أن تقدمها الأمم المتحدة ولا سيما لجنة منع الجريمة وتحقيق العدالة الجنائية ,والترويج لمزيد من الفعالية والكفاءة فى تنفيذ القوانين وإقامة العدل.

كما أكدت على ضرورة منع إساءة استعمال التكنولوجيا لأغراض إجرامية والحاجة للتعاون وتعزيز التنسيق بين الدول والقطاع الخاص على مكافحة وردع هذه الجريمة[9].

ب- دور المجلس الأوروبي فى مواجهة الجريمة الالكترونية

[9] حسين بن سعيد بن سيف الغافري ، الجهود الدولية في مواجهة جرائم الانترنت ، 2007 ، ص ص 1-3 ، مقال متوفر على الرابط الالكتروني التالي : http: //www .minshawi.com

للمجلس الأوروبي دور فعال في سبيل الحد من الجرائم المعلوماتية وذلك من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام ,وحماية الدفق المعلوماتى ومن بين مجهودا الإتحادالأوروبي بصدد مكافحة الجريمة الالكترونية تتمثل فيمايلى :

_التوقيع على اتفاقية الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ,والتى وقعت بين المجلس الأوروبي والسوق الاشتراكية وكان ذلك في 17سبتمبر 1980,وقد بدا السريان الفعلي لهذه الاتفاقية فيأكتوبر 1985,ويقتصر نطاق تطبيقها على الأشخاص الطبيعيين ويسرى على القطاعين العام والخاص بشان الملفات المعدة آليا ,بحيث تقضى بإلزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آليا.[10]

بالإضافة إلى ماصدر عن المجلس الأوروبي من توصيات ,تؤكد على توسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة مثل البيانات الطبية والإحصائية .وفي سنة 1989 قام المجلس الأوروبي بنشر دراسة تتضمن توصيات تبين أهمية تفعيل دور القانون في مواجهة الجرائم المرتكبة عبر الحاسوب الآلي كما استتبعت هذه التوصية بدراسة أخرى سنة 1995 تتمحور حول الإجراءات الجنائية المتعلقة بالجرائم المعلوماتية ,ومحاولة المجلس الأوروبي لتطبيق ماجاء في هذه التوصيات فقد قام المجلس الأوروبي بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي سنة1997.

كما نجد أيضاأن المجلس الأوروبي قد وقع أيضا على اتفاقية بودابست لمكافحة الجرائم الإلكترونية the budapest convention on cyber cerimes

[10]الحسيناوي علي الجبار ، المرجع السابق ، ص 151.

الموقعة في 2001/11/23 بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأميركية ,ولم تدخل حيز النفاذ إلى غاية سنة 2004بالرغم من أنها أوروبية المنشاة إلا أنها ذات طابع دولي فهي تعتبر اتفاقية جنائية دولية وأداة لمكافحة الجريمة السيبرانية[11]

إلى جانب الجهود المبذولة من طرف الأمم المتحدة والاتحاد الأوروبي في مجال مكافحة هذا النوع المستجد من الجرائم هناك جهاز آخر ساهم في مواجهة الجريمة الإلكترونية.

ج_دور المنظمةالدولية للشرطة الجنائية في مواجهة الجريمة الالكترونية

تهدف المنظمة الدولية للشرطة الجنائية الإنتربول .[12]إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة[13] وكذا مساهمتها في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف.

حيث تركز اهتمامالأنتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطةذات الصلة بها.

---

(11) Haddad (F) , Op-cit,P.22.

(12)منظمة الشرطة الجنائية الدولية ، الأنتربولinterppol ، هي أكبر منظمة للشرطة الدولية ، أنشأت عام 1923 ،مكونة من قوات الشرطة ل192 دولة ، و للمنظمة أربعة لغات رسمية : هي الفرنسية ، الإنجليزية ، العربية ، الإسبانية ، مقرها في مدينة ليون في فرنسا ، توجد مكاتب وطنية للمنظمة في الدول الاعضاء ، و هي منظمة رسمية بين الحكومات تقوم بعدة مهام خاصة في مجال تبادل المعلومات التعاون الدولي للتصدي للجريمة ، أنظر إلى كتاب شحادة يوسف ، الظابطة العدلية علاقتها بالقضاء و دورها في سير العدالة الجزائية (دراسة مقارنة) ، ط1 ، مؤسسة بحسون للنشر و التوزيع للنشر و التوزيع ، بيروت ، ص455 -457 .

(13)بنعمر الحاج عيسى،الأنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود،مجلة الدراسات القانونية السياسية،كلية الحقوق،،جامعة الأغواط، العدد 03،جانفي 2016.ص.252.

وخير دليل على ذلك اختتام أعمالاجتماع الجمعية العامة ال26للشرطة الجنائية الدولية "الأنتربول" بالعاصمة الصينية بكين سنة29_09_2017 بمشاركة نحو1000 من كبار قادة الشرطة والسياسيين في156دولة ,ومن بين أهم القضايا التي تم مناقشتها ضمن اجتماع نجد جرائم الانترنت والقرصنة الالكترونية والمخاطر الناجمة عنها والية التصدي لهذا النوع من الجرائم على المستوى الدولي.[14]

يؤدى الأنتربول دور رائد في مجال مكافحة الجريمة الالكترونية ويتجلى ذلك من خلال تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف من اجل مكافحة هذا النوع من الإجرام ,كما تقوم بتزويد دول الأعضاء بالبيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها ,بإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة فى الدول الأطراف ,حيث تقوم بملاحقة مجرمي المعلوماتية عن طريق تعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود للأنظمة المعلوماتية وشبكات الاتصال بحثا عن الأدلة وبراهين على ارتكاب الجريمة الالكترونيةكلها أمور تستدعى القيام ببعض العمليات الشرطية والأمنية المشتركة ،وهى من شانها متابعة

[14] شبيلي مختار ، الجهاز العالمي لمكافحة الجريمة المنظمة ، الطبعة الثانية ، دار هومة للطباعة و النشر و التوزيع ، الجزائر ، 2016 ، ص 266-267 .

المجرمين الذين يستغلون التكنولوجيا الجديدة لتحقيق أغراضهم الغير الشرعية[15]

وإذا مأردنا تقييم دور منظمة الأنتربول ,فإنها تعتبر من أهم المنظمات الدولية الناجمة والفعالة في أداء مهامها على المستوى الدولي بحيث ساهمت في تحقيق التعاون الدولي بين أجهزة الشرطة في بلدان الأعضاء ,ويرجع هذا إلى كون المنظمة الدولية للشرطة الجنائية تختص بمكافحة الجريمة المنظمة بمختلف أشكالها ومن بينها جرائم الالكترونية ,فهي تعتبر جهاز رئيسي لتحقيق التعاون الدولي في مكافحة الجريمة المنظمة .[16]

د- دور الجامعة العربية في مواجهة الجريمة الالكترونية

إن التطور السريع لتكنولوجيا الإعلام والاتصال وتطبيقاتها جعلتنا نعيش في عالم افتراضي ,حيث فتح مجالات عديدة للاستفادة منها مؤديا فى ذات الوقت إلى زيادة الخروقات والتهديدات التي تمس بأمن الأشخاص والمؤسسات ,فلم يعد احد بمنئ عن مخاطر الجرائم الالكترونية باختلافأساليبها وصورها التي تتخذ المعلوماتية والانترنت مسرحا لها.

مما دفع بالدول العربية إلى محاولة إيجاد طرق تشريعية ناجعة لمواجهة هذه الجرائم ,ومن بين هذه الجهود نذكر القانون العربي الاسترشادي، حيث قامت جامعة الدول العربية من خلال الأمانة العامة لمجلس وزراء العدل العرب في دورته التاسعة عشر، باعتماد هذا القانون النموذجي بالقرار

---

(15) يتجلى ذلك من خلال الإحتيال على الأشخاص بالإدعاء أنهم ممثلين شرعيين لشركات تجارية أو بإستخدام رموز البرامج الخبيثة التي يستخدمونها لسرقة تفاصيل الهوية ، وبتوسيع مجموعات الإجرام المنظم ، وذلك باستغلال الشبكات المعلوماتية لإرتكاب جرائم الإحتيال و السرقة و الإبتزاز،عد إلى شبيلي مختار، المرجع السابق،ص.274.

(16) شحادة يوسف ، المرجع السابق ، ص 456- 458

رقم 459-19 في 08 /10/ 2003 و الذي يعتبر أهم ما بذل من جهود عربية في مجال الحماية التشريعية من الجرائم المعلوماتية .

تضمنت هذا القانون 27 مادة مقسمة إلى أربعة فصول، الباب الأول يتحدث عن الجرائم المعلوماتية من المواد 3 إلى 22،وأهم الجرائم التي تناولتها:

1_ جريمة الدخول غير المشروع إلى الموقع أو النظام المعلوماتي مع تشديد العقوبة إذا كان الغرض من الدخول إما الإتلاف أو الإلغاء أو إلحاق ضرر .[17]

2- جريمة تزوير المستندات المعالجة آليا في النظام المعلوماتي و استعمالها.

3- مختلف الجرائم المخلة بالآداب العامة المرتكبة عبر شبكة المعلومات.

أما الباب الثاني منه فقد تناول التجارة و المعاملات الإلكترونية ، بينما تناول الباب الثالث حماية حقوق المؤلف عبر الوسائل الإلكترونية ، أما في الباب الرابع فتطرق للإجراءات المتعلقة بالجريمة المعلوماتية نجد أن كل من منظمة الأمم المتحدة و المجلس الأوروبي، و المنظمة الدولية للشرطة الجنائية ، و الجامعة العربية قد ساهموا في مكافحة الجريمة الإلكترونية ، رغم اختلاف الأساليب المنتهجة للمكافحة هذه الجريمة،إلا أنها تسعى كلها إلى تحقيق نفس الهدف ،وهو التصدي لهذا النوع المستحدث من الجرائم.

ثانيا:مساعي بعض التشريعات المقارنةفيمواجهة الجريمة الإلكترونية

[17] إيمان مسعود سالم ، المرجع السابق ، 37 .

إن بيان الدور المنوط لبعض التشريعات المقارنة بشأن مواجهة الجريمة الإلكترونية، يتطلب منا عرض موقف بعض هذه التشريعات سواء فيبعض التشريعات العربية أو في بعض التشريعات الأخرى.

أ- جهودبعضالتشريعاتالعربيةفيمواجهة الجريمة الإلكترونية

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقيا لاقتصاديات الدول،مما دفع بهم إلى اتخاذ الإجراءات اللازمة لتصدي لهذا النوع المستحدث من الجرائم،ومن التشريعات العربية التي لها دور في مكافحة الجريمة الإلكترونية نجد:

1-دور المشرعالمصري في مكافحة الجريمة الإلكترونية

بدأ الاهتمام بمكافحة الجرائم المعلوماتية بمصر،بعد انعقاد المؤتمر التأسيسي الأول لجمعيات قانون الانترنت بالقاهرة في سبتمبر 2004 و المؤتمر الدولي الأول لقانون الانترنت بمدينة الغردقة في أوت 2005،و تأسست بذلك الجمعية المصرية لمكافحة الجرائم المعلوماتية سنة 2005 و هدفها نشر الوعي وإعداد الدراسات و المؤتمرات حول الجرائم المعلوماتية.[18]

نجد أن المشرع المصري مازال يعتمد على النصوص التقليدية بخصوص بعض الجرائم كالتزوير الإلكتروني أو الاحتيال أو السرقة المعلوماتية. [19]

[18]الحسيناوي علي الجبار ، المرجع السابق ، ص 174 .

[19]معتوق عبد اللطيف ، المرجع السابق ، ص 97 .

يعد قانون التوقيع الإلكتروني أول قانون يصدر بشأن تجريم بعض الأفعال المتعلقة بالنظم المعلوماتية، حيث قام بتجريم أفعال تتعلق بالحصول على توقيع أو محرر إلكتروني أو وسيط بدون وجه حق.

كما تطرق المشرع المصري في الدستور إلى حرمة الحياة الخاصة التي لايجوز انتهاكها طبقا للمادة 57 منه و التي تنص على مايلي :((للحياة الخاصة حرمة،وهي مصونة لا تمس.

و للمراسلات البريدية و البرقية الإلكترونية و المحادثات الهاتفية و غيرها من وسائل الاتصال حرمة و سريتها مكفولة،ولا يجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب،ولمدة محددة،وفي الأحوال التي بينها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي، وينظم القانون ذلك.))

نجد بأن المشرع المصري من خلال نص المادة تكفل بحماية الحياة الخاصة من كل أشكال الانتهاكات،بحيث لا يجوز التعرض لها أو رقابتها، إلا بمقتضى أمر قضائي مسبب، وفقا لمدة المحددة والأحوال التي نص عليها القانون.[20]

بناء على ما سبق نستخلص أنه رغم المجهودات المبذولة للحد من انتشار الجرائم الإلكترونية في مصر إلا أنها غير كافية لمواجهة هذا النوع المستحدث من الجرائم الذي هو في تزايد مستمر، حيث تعتبر مصر من بين الدول التي تعاني من أزمة انتشار الجرائم الإلكترونية على مواقع

[20] ملتقى لنيل شهادة اليسانس ،الجريمة الإلكترونية،كليةالحقوق،جامعة فرحات عباس،سطيف،2009،ص.116-118.

التواصل الاجتماعي، الأمر الذي أرجعه خبراء في مجال التكنولوجيا إلى عدم الإلمام الأمثل لتلك المواقع، فضلا عن غياب نصوص تشريعية واضحة لتقنين استخدامها.

2-دور المشرع السعودي في مكافحة الجريمة الإلكترونية

احتلت المملكة العربية السعودية المركز السادس عالميا بين الدول التي تنطلق منها الهجمات الإلكترونية نسبة إلى عدد مستخدمي الانترنت في البلاد،فكان لابد لها من إصدار تشريع خاص بذلك ،فقامت بإصدار قانون جديد لمكافحة الجرائم المعلوماتية ،وذلك بصدور المرسوم الملكي رقم17 في 1428/3/8هـ،بناء على قرار مجلس الوزراء رقم 79بتاريخ 1428/3/7،وقد تضمن هذا المرسوم بيان معاني ومصطلحات التي تدخل ضمن الجرائم الإلكترونية والتي عرفتها المادة الأولى على أساس أنها:((أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.))[21]

فقدسعىنظاممكافحةالجريمةالمعلوماتيةإلىالردعهذهالجريمةوذلكمنخلالأنهتظمنعدةمواد،حيثقامالمشرعال سعوديبالتعريفهذهالجريمةمنجهةوتجريمالأفعالالمساهمةفيحدوثهامنجهةأخرى،كالتجريمالدخولغيرالمشرو

[21])الطوئيوائل، مقال صحفي تحت عنوان : مواجهة الجرائم الالكترونية تحتاج إلى سن تشريعات جديدة ، ظر إلى الموقع الالكتروني : www .ahlmasrnews.com

علإلغاءبياناتخاصةأوحذفهاأوتدميرهاأوتسريبهاأوإتلافهاأوتغييرهاأوتدميرهاأومسحالبرامجأوالبياناتالمستخدمةوكذلكإعاقةالوصولإلىالخدمةأوتشويشهاأوتعطيلهابأيوسيلةكانت.[22]

مايمكننا القول بشأن هذا النظام ،هو اعتباره من الجهود الرامية لتصدي لهذا النوع المستحدث من الجرائم ،حيث جاء هادفا للحد من إساءة استخدام النظم المعلوماتية وتحقيق الأمن المعلوماتي،إلا أن هذا النظام لوحده لايكفي لمواكبة التزايد المستمر للجرائم الإلكترونية.

ب_ جهودبعضالتشريعاتالأخربفيمواجهةالجريمة الإلكترونية

أضحى الإجرام المعلوماتي في تزايد مستمر ، إثر الانتشار الواسع لأجهزة الكمبيوتر و شبكات الاتصال الخاصة بها ، و كثرة الاعتماد عليها في مختلف المجالات ، الأمر الذي جعل الدول تقوم بتطوير بنيتها التشريعية لمواكبة هدا النوع المستجد من الجرائم ، و من بين الدول التي سعت إلى مكافحة الجريمة الإلكترونية نجد كل من فرنسا و الولايات المتحدة الأمريكية.

1_ دورالمشرع الفرنسي في مكافحة الجريمة الإلكترونية

يعتبر القانون الخاص بالمعلوماتية و ملفات البيانات و الحريات رقم 78-17 ، المؤرخ في 6 جانفي 1978 ، أول قانون فرنسي ينظم الجوانب القانونية المتصلة بالمعلوماتية و أثرها على الخصوصية و أنشأت من خلاله اللجنة الوطنية للمعلوماتية و الحريات التي تختص بمراقبة سلامة تنفيذ هذا القانون.

[22] المادة الخامسة من نظام مكافحة الجريمة المعلوماتية ،المرسوم الملكي رقم 17 في 8/3/1428،عد إلى الموقع التالي : www.citc.gov.sa

1_قامت فرنسا بتطوير منظومتها القانونية لتتماشى مع مستجدات الإجرام المعلوماتي حيث تضمن قانون العقوبات الفرنسي من خلال التعديلات المتلاحقة عليه نصوصا خاصة بتجريم المساس بنظام المعالجة الآلية للمعطيات بمختلف أشكال الاعتداء حيث أدرجها في الفصل الثالث تحت عنوان :

Des atteintes aux systèmes de traitement automatisé de donnés[23]

حيث تنص المادة 323-1 من ق.ع.ف على ما يلي:

(Le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système automatisé de données est puni de deux ans d'emprisonnement et de d'un système de traitement 6000euros d'amende.)

L'ors qu'il en est résulté soit la suppression ou la modification de donnés contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100000euro d'amende.

[23] محمد طارق عبد الرؤوف الحن ، جريمة الاحتيال عبر الانترنت ، (الأحكام الموضوعية و الأحكام الاجرائية) ، ط1، منشورات الحلبي الحقوقية ، بيروت ، 2011 ، ص 108 .

Lorsque les infractions prévues au deux premiers alinéas ont été commises a l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat. La peine est portée a cinq ans d'emprisonnement et à 150 000 d'amende).[24i]

نجد أن المشرع الفرنسي طبقا لنص هذه المادة قد جرم بعض الأفعال المساهمة فى حدوث الجريمة الإلكترونية من فعل الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات،ويعاقب على ذلك بالحبس لمدة سنتين وغرامة مقدارها 60000 أورو، أما إذا نتج عن ذلك حذف أو تعديل للمعطيات الموجودة في النظام أو تحريف لمجريات النظام، فتكون العقوبة الحبس لمدة 3 سنوات وغرامة تقدر ب 100000أورو.وفي حالة ارتكاب الجرائم المنصوص عليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة يتم رفع العقوبة إلى السجن لمدة خمس سنوات وغرامة 150000أورو،بينما فى المادة 323_3 من نفس القانون من نفس القانون فقد جرمت إدخال بطريقة احتيالية معطيات إلى النظام المعالجة الآلية من استخراج ونسخ وإرسال وحذف أو تعديل البيانات التي يحتوي عليها ويعاقب عليها بالسجن لمدة خمسة سنوات وغرامة قدرها 150000أورو.كما تطرق ق ع ف إلى ذكر حالة استخدام أداة أو برنامج معلوماتي أو أية معطيات يمكن أن ترتكب بها أي جريمة من الجرائم المذكورة في المواد 323-1 إلى 323-3،ويعاقب على ذلك بنفس العقوبة المقررة للجريمة نفسها أو بالعقوبة أشد.

---

[24]Articles 323-1 , Code pénal partie législative - Dernière modification le 06 mai 2018 - Document généré le 11 mai 2018Copyright (C) 2007-2018 Legifrance ,
Site : www.legifrance.fr .

وبالخصوص العقوبات المقررة للأشخاص الطبيعيين ،الذين ارتكبوا الجرائم المنصوص عليها في المواد السالفة الذكر،إلى جانب العقوبات الأصلية عقوبات تكميلية تتمثل في:المنع من الحصول على الحقوق المدنية و العائلية حسب اجراءات المادة 131-26 من قانون العقوبات الفرنسي.[25]_المنع من ممارسة الوظائف العامة،أو أي نشاط مهني أو اجتماعي،ومصادرة المواد التي استخدمت في ارتكاب الجريمة أو المعدة لذلك،وإذا كان الفعل مرتكبا من طرف إحدى المؤسسات فيكون العقاب بالإغلاق و الطرد من الصفقات العامة و نشر الحكم حسب شروط المادة 131-35 من قانون السالف الذكر. إلى جانب العقوبات المقررة للشخص الطبيعي هناك عقوبات أخرى للشخص المعنوي وفقا للشروط المنصوص عليها في المادة 121-2 من ق ع ف ، حيث يعاقب بالغرامة المنصوص عليها في المادة 131-"39 ، و المنع المنصوص عليه في البند الثاني من المادة السالفة الذكر. كما نص كذلك هذا القانون على معاقبة الشروع في ارتكاب أي من الجرائم المنصوص عليها سابقا بنفس العقوبة التامة.[26]نجد أن المشرع الفرنسي قد بذل مجهودات معتبرة في مجال التصدي لهذا النوع المستحدث من الجرائم من خلال تطوير بنيتها التشريعية لمواجهة هذه الجريمة التي أصبحت تهدد كيان المجتمعات على حد سواء.

2-د ور المشرعالأمريكي في مكافحة الجريمة الإلكترونية

لقد سعى المشرع الأمريكي لتصدي لهذا النوع المستجد من الجرائم، ويظهر ذلك من خلالإصداره لقانون فلوريدا لسنة 1978 المتعلق بجرائم الحاسوب، الذي يعتبر أول قانون خاص

[25] خليفة محمد ، المرجع السابق ، ص 67-68

[26]الحن محمد طارق عبد الرؤوف ، المرجع السابق ، ص 109-110 .

بالجريمة المعلوماتية في الولايات المتحدة الأمريكية، حيث اعتبر أن مجرد الدخول غير المصرح به إلى الحاسوب حتى ولو لم يكن بدافع الإضرار يعتبر جريمة في حد ذاتها.

كما قام أيضا بإصدار قانون فدرالي متعلق بجرائم الحاسب الآلي سنة 1984 والذي أطلق عليه قانون الاحتيال وإساءة استخدام الحاسب الآلي the computer froudand abuse act

إلا أن هذا القانون لم يجرم إتلاف المعلومات و البيانات ،وإنما اقتصر التجريم فيه على إعاقة أنظمة الحاسبات الآلية و بسبب الانتقادات التي وجهت له على هذا الأساس تم تعديله سنة 1986.[27]

لحماية حرمة الحياة الخاصة من الانتهاكات قام أيضا بإصدار قانون الخصوصية (PA) privacyact لسنة 1974،و قانون خصوصية الاتصالات الإلكترونية (ECPA) عام 1986 electronic communication privacyact

وفي حماية الأموال من الاعتداءات عليها عبر الانترنت أصدر في سياق ذلك قوانين متتالية تتواكب مع التطور العلمي و التقني في مجال المعلومات [28]،بإصدار القانون الفيدرالي لحماية أنظمة الكمبيوتر (CSPA) لسنة 1977 COMPUTER SYSTEM PROTECTION ACT

[27] عبابنة محمود أحمد ، جرائم الحاسوب و أبعادها الدولية ، ط1، دار الثقافة للنشر و التوزيع ، عمان ، 2009 ، ص 142-143.

[28] الحن محمد طارق عبد الرؤوف ، المرجع السابق ، ص 104-105.

نظرا للتطور الهائل الذي توصلت إليه الدول الأجنبية وعلى رأسها الولايات المتحدة الأمريكية في مجال تكنولوجيا المعلومات، فإنها بذلك أكثر معرفة بالجرائم المعلوماتية، وأكثر تطور في سن التشريعات لمكافحتها.[29]

الفرع الثاني:

مواجهة الجريمة الإلكترونية على المستوى الوطني

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني، وما يصاحبها من أضرار من جهة، ومحاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، قام من خلال ذلك إلى إصدار قوانين عامة وخاصة.

أولا القوانين العامة المنظمة للجريمة الإلكترونية

سعى المشرع الجزائري إلى تنظيم الجريمة الإلكترونية بقوانين عامة هادفا بذلك إلى ردع هذا النوع المستحدث من الجرائم.

أ_الدستورالجزائري:

[29]الحن محمد طارق عبد الرؤوف ، المرجع السابق ، ص 105-106.

كفل الدستور الجزائري حماية الحقوق الأساسية و الحريات الفردية ،و السهر على أن تضمن الدولة عدم انتهاك حرمة الإنسان ، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى،تحذر كل مساس بهذه الحقوق،ومن بين المبادئ الدستورية نجد بحسب المواد التالية:[30]

المادة 38 التي تنص على مايلي ((الحريات الأساسية وحقوق الإنسان و المواطن مضمونة))

بالتالي المشرع الجزائري سعى لحماية الحقوق من جميع أشكال الانتهاكات.

بينما نصت المادة 44 على مايلي((حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن،حقوق المؤلف يحميها القانون ، لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي،الحريات الأكاديمية و حرية البحث العلمي مضمونة وتمارس في إطار القانون،تعمل الدولة على ترقية البحث العلمي و تثمينه خدمة للتنمية المستدامة للأمة.

---

(30) دستورالجمهوريةالجزائريةالديمقراطيةالشعبية،الصادربموجبالمرسومالرئاسيرقم 96-438،المؤرخفي 07 ديسمبر 1996،المصادقعليهفياستفتاء 28 نوفمبر 1996،جرعدد 76 صادرفي 8 ديسمبر 1996،معدلومتمم:

- قانونرقم 02-03 مؤرخفي 10 أفريل 2002 يتضمنتعديلالدستور،جرعدد 25 صادرفي 14 أفريل 2002.

-قانونرقم 08-19 مؤرخفي 15 نوفمبر 2008،يتضمنتعديلالدستور،جرعدد 63،صادرفي 16 نوفمبر 2008.

-قانونرقم 16-01 ،مؤرخفي 06 مارس 2016 ،يتضمنتعديلالدستور،جرعدد 14،صادرفي07 مارس 2016.

لايجوز انتهاك حرمة حياة المواطن الخاصة،وحرمة شرفه و يحميها القانون،سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة.))[31]

يفهم من سياق نص المادة ،أن المشرع سعى لحماية حق المؤلف من جهة لايجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ و الإعلام،إلا بمقتضى أمر قضائي،وحماية الحياة الخاصة من كل أشكال الاعتداءات.

ب-قانون العقوبات الجزائري

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل ق.ع.ج.بموجب قانون رقم 04-15 المؤرخ في 10نوفمبر 2004 المتمم لأمر رقم 66-156 المتضمن قانون العقوبات، الذي أفرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن 8 مواد من المادة 394مكرر إلى 394 مكرر 7 ونص على عدة جرائم وهي كآتي:

-الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

-إدخال أو إزالة أو تعديل_بطريق الغش-معطيات في نظام المعالجة الآلية.

[31]المادة 44 من القانون رقم 16- 01 ، المتضمن دستور الجمهورية الجزائرية الشعبية ، المرجع السابق .

_تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

_حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.[32]

وقد ضاعف المشرع العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات العمومية ،بالإضافة إلى ذلك نجد أن المشرع الجزائري اتبع نفس نهج المشرع الفرنسي من خلال إقراره لمسؤولية الشخص المعنوي بموجب المادتين 18 مكرر، و 18مكرر1 من قانون رقم 04-15،وشدد عقوبة الغرامة على الشخص المعنوي إلى خمس مرات للحد الأقصى للعقوبة المقررة للشخص الطبيعي .

كما تم التطرق لعقوبة الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم.

ونص هذا التعديل أيضا على عقوبة مصادرة وسائل ارتكاب الجريمة –الأجهزة والبرامج–وإغلاق المواقع التي تكون محلا لها، علاوة على إغلاق المحل أو المكان الذي ارتكبت فيه الجريمة.[33]

---

[32] المادة 394 مكرر2 من قانون رقم 06-23 مؤرخ في20/12/2006 يعدل و يتمم الأمر رقم66/156 مؤرخ في 18 صفر عام 1386، اللموافق ل 8 يونيو 1966و المتضمن قانون العقوبات.

[33]بن بورنانكاتية ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة تخرج لنيل شهادة الماستر في الحقوق ، قسم: القانون الخاص ، تخصص : القانون الخاص و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة ، بجاية ، 2014 ، ص ص 37-39 .

طبقا لنص المادة 394 مكرر6 والآتي نصها:((مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم،علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها)) [34]

أدخل المشرع الجزائري تعديل آخر على ق.ع.ج بموجب قانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006، ومس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث تم تشديد العقوبات الحبس والغرامة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون رقم 04-15.[35]

ج-قانون الإجراءات الجزائية

لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بالجريمة المعلوماتية ، محاولة منه تطوقها و القضاء عليها،أو على الأقل الحد من انتشارها،

حيث وضع قواعد و أحكام خاصة لسلطة التحري و المتابعة ،الغرض منها هو مواجهتها،وقد وردت هذه الأساليب في قانون الإجراءات الجزائية.

متابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية ،كالتفتيش والمعاينة والضبط ...إلخ

---

[34] المادة 394 مكرر6 من الأمر رقم 66-156 ، المؤرخ في 8/جوان/ 1966 ، يتضمن قانون العقوبات ، ج.ر، عدد 71 ، معدل و متمم . راجع موقع الأمانة العامة للحكومة : www .joradp.dz

[35] بورنانكاتية ، المرجع السابق ، ص 41 ,

كما قام باستحداث أساليب أخرى خاصة كاعتراضالمراسلات، المراقبةالإلكترونية، التسرب،تسجيل الأصوات

والتقاطالصور [36]نتطرقإليهافيالفرعالثانيمنالمطلبالثاني،وبالتاليندأنق.إ.ج.جساهمفيمتابعةالجريمةالإلكترونيةمنخلالنصهلقواعدالإجرائيةفيالتحقيقفيهذهالجريمةوالمساهمةفيكشفالحقيقةبإزالةالغموضومعاقبةمرتكبيها.

ثانيا:القوانين الخاصة في مجال مكافحة الجريمة الإلكترونية

نظرا لاتساع نطاق الجريمة الإلكترونية،التي أصبحت لا تقتصر على جريمة واحدة وإنما اتسعت إلى عدة جرائم ، وعلى أساس أن القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الإلكترونية الحديثة ،مما دفع بالمشرع الجزائري إلى استحداث قوانين خاصة لمواكبة هذا النوع المستحدث من الجرائم.

أ-قانون البريد والمواصلاتالسلكية واللاسلكية

سعى قانون البريد والاتصالات لمواجهة هذه الظاهرة الإجرامية،من خلال المواد التي تضمنها لهذا الغرض،بات من السهولة إجراء التحويلات المالية عن الطريق الإلكتروني نظرا لتطور تكنولوجيا الإعلام والاتصال.

كما نص القانون السالف الذكر إلى استخدام حوالات دفع عادية أو الكترونية أو برقية.

[36] بن بورنانكاتية، المرجع السابق، ص35.

بينما نصت المادة 23 منه على مايلي :((**يجوز إنشاء و/أو استغلال شبكات المواصلات السلكية و اللاسلكية مهما كان نوع الخدمات المقدمة،وفق الشروط المحددة في هذا القانون وفي النصوص التنظيمية المتخذة لتطبيقه.**

لا تشمل أحكام هذه المادة منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي.))[37]

بحسب هذه المادة يجوز كأصل عام إنشاء استخدام شبكات الاتصال السلكية واللاسلكية، باختلاف نوع الخدمة المقدمة، لكن وفقا لشروط المحددة قانون، باستثناء منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي.

كما نصت المادة 93 الفقرة الأخيرة كمايلي:((لايمكن بأي حال من الأحوال انتهاك سرية المراسلات.))،بمعنى أنه يجب احترام سرية المراسلات.[38]

تطرق أيضا القانون السالف الذكر إلى معاقبة كل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه،يعاقب فيه الجاني بالحرمان من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية و الاسلكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس سنوات.

[38] قانون البريد و المواصلات السلكية و اللاسلكية ، رقم 03-2000 مؤرخ في 05/08/2000 ،ج ر.ج.ج ، العدد48 ،معدل و متمم.

[38] أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس ، يومي 24-25|03|2017، ، 2017 ، ص 131 .

ب-قانون التأمينات

تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي ،في نصوص قانونية عديدة تخص البطاقة الإلكترونية ،التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني.

حدد هذا القانون الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية وفقا لنص المواد التالية:ففي المادة 93 مكرر2 من ق.ت.إ نصت على مايلي: ((دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به،يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 100000دج إلى 200000دج،كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو مفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة.)) [39]

طبقا لنص المادة ،نجد أن المشرع الجزائري يعاقب كل من يستخدم البطاقة الإلكترونية،أو المفتاح الإلكتروني لهيكل العلاج أو لمهني الصحة ، لأغراض غير شرعية،كما قام أيضا المشرع وفقا لهذا القانون بتجريم مجموعة الأفعال الغير المشروعة،من القيام عن طريق الفش بتعديل أو حذف كلي

[39] المادة 93 مكرر2 من قانون رقم 18-01، مؤرخ في 23 يناير 2008، يتمم القانون رقم 83-11، المؤرخ في 2 يونيو 1983، المتعلق بالتأمينات الإجتماعية.

أو جزئي للمعطيات التقنية أو الإدارية التي تتضمنها البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني سواء لهيكل العلاج أو لمهني الصحة.[40]

كما عاقب كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستخدام المعطيات التي تتضمنها البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو لمهني الصحة.

ج-قانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

نص هذا القانون على مراقبة الاتصالات الإلكترونية و ذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية ، حيث نصت المادة 4 منه على الحالات التي يسمح فيها للسلطات الأمنية باللجوء إلى المراقبة الإلكترونية و هي : الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

حالة توفر معلومات عن احتمالاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية .

[40]أعمال مؤتمر الجرائم الإلكترونية ، المرجع السابق .،ص130-131.

في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة و اشترط المشرع إجراء عمليات المراقبة بإذن مكتوب من السلطة القضائية المختصة.[41]

كما نص كذلك هذا القانون على قواعد إجرائية تساهم بدورها في كشف الجريمة و معالمها، من تفتيش و حجز للمعطيات المعلوماتية و حفظ المعلومات المتعلقة بحركة السير .

فيما يخص التفتيش فقد أجازت المادة 5 من القانون 04-09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية الدخول بغرض التفتيش و لو عن بعد إلى :

أ_ منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها .

ب_ منظومة معلوماتية.

يلاحظ بأن التفتيش في الوضعيات المشار لها يأخذ مجالين إما أن يكون في مجال أعمال التحقيق تقوم به السلطات القضائية المختصة و إما ان يكون في مجال أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطات المختصة ، و في كلتا الحالتين يكون جهاز الكمبيوتر هو المستهدف بمختلف مكوناته . كما أجاز هذا القانون تسخير كل شخص له دراية بعمل المنظومة المعلوماتية التي تتضمنها ، و ذلك قصد مساعدة السلطات المكلفة بالتفتيش من خلال تزويدها بكل المعلومات الضرورية لإتمام مهمتها .

[41] زبيحة زيدان، المرجع السابق، ص 129

يسمح هذا القانون للسلطات التي تباشر التفتيش في منظومة معلوماتية ، بنسخ المعطيات محل البحث ، و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في ق.إ.ج.[42]

يعتبر قانون 04/09 كخطوة أولى للجزائر في مجال مواجهة الجريمة الإلكترونية من ناحية و سد للفراغ التشريعي الذي كان يعتري القانون الجزائري من ناحية أخرى ، لكن هذا لا يكفي لردع الجرائم الإلكترونية بمختلف أنواعها .

ثالثا : دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

تعتبر هذه الهيئة قفزة نوعية في إطار مسار الإصلاحات التي تنتهجها الجزائر مؤخرا ذات الطابع القانوني و الأمني و السياسي لتعزيزدولةالقانونويتجلىدورهذهالهيئةفيمايلي:

– تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها.

– مساعدة السلطات القضائية و المصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال،من خلال جمع المعلومات و انجاز الخبرات القضائية.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم.

[43]زبيحةزيدان،المرجعالسابق،ص 131.

المطلب الثاني

القواعد الإجرائية للتحقيق في الجريمة الإلكترونية

يعتبر التحقيق من أهم الإجراءات التي تتخذ بعد وقوع الجريمة ،لما له من أهمية في تثبت من الحقيقة، من خلال كشف الغموض الذي يعتري الجريمة ،و إسناد الدليل على مرتكبيها بأدلة الإثبات، لغرض الوصول إلى إدانة المتهم من عدمه.[43]

تعد البيئة الرقمية مسرحا لارتكاب الجريمة الإلكترونية، والتي تستدعي كافة الإجراءات من أجل الوصول إلى الدليل بالنسبة الذي لايخلو أي جريمة ، مهما كانت طبيعتها مادية أو تقنية ، كما هو الحال بالنسبة لهذا النوع المستحدث من الجرائم ، الذي يقوم على الدليل الرقمي،ومن الإجراءات التي ساهمت إلى حد بعيد في كشف معالم الجريمة ، نجد إجراءات عامة وإجراءات خاصة.

الفرع الأول

القواعد الإجرائية الكلاسيكية للتحقيق في الجريمة الإلكترونية

تعد الجريمة الإلكترونية من الجرائم التي لايترك أثر مادي في مسرح الجريمة ،فضلا عن أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة،أي سهولة طمس معالم الجريمة،لذلك عمل المشرع الجزائري في هذا المجال على دعم الإجراءات العامة والت نتطرق إليها على النحو الآتي:

---

[43]خالد ممدوح ابراهيم،المرجع السابق،ص،119.

أولا: المعاينة

المعاينة من أهم مراحل التحقيق في الجرائم المستحدثة نظرا لما يمكن أن توفره من أدلة إثبات للجريمة ،و تزداد أهميتها في إثبات الجرائم المرتكبة عبر الانترنت،في أنها تقوم على معاينة جملة من البرمجيات أو الأقراص وكل ما يتعلق بجهاز الحاسب الآلي ،وذلك راجع إلى الطبيعة الخاصة للمعاينة في هذا المجال،وبالتالي جوهر المعاينة هو الملاحظة و فحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة لإثبات حالته و التحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة ،يجوز الالتجاء إلى المعاينة في كافة الجرائم[44] ،إلا أن غالبية التشريعات بما فيها التشريع الجزائري ،يقتصر ها على الجنايات و الجنح الهامة ،بحيث تعد إجراء وجوبيا في الجنايات و جوازيا في الجنح ،وهي قد تتم في مكان عام أو خاص ،فإذا كانت في مكان عام،مأمور الضبط القضائي لا يحتاج إلى إذن أو ندب سلطة تحقيق بإجرائها،أما إذا كانت بمكان خاص ،لابد لصحتها ،إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

بخصوص أهمية هذا الإجراء في الجريمة المعلوماتية ، يكمن في كشف غموض جرائم الانترنت،وضبط الأشياء التي قد تفيد في إثبات وقوعها و إسنادها إلى مرتكبيها[45]

ثانيا:التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش ،بقدر ما اعتبره إجراء من إجراءات التحقيق و أحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة من جهة وخطورته فيما قد يترتب عنه

[45] خالد ممدوح ابراهيم،المرجع السابق،ص111.

[46] المرجع نفسه ، ص .212.

من مساس بالحرية الأشخاص وبكرامتهم من جهة أخرى،خير دليل على ذلك اهتمام الدستور الجزائري بأهمية هذا الإجراء من خلال نص المادة 40 منه و التي تنص على مايلي:((فلا تفتيش إلا بمقتضى القانون و في إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة.))[46]

نستخلص من فحو المادة أن التفتيش يعتبر من الإجراءات المخولة لضباط الشرطة القضائية حسب نص المادة 1/5 قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذلك قانون الإجراءات الجزائية .

ثالثا :الضبط

يتمثل الضبط في العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها التحفظ عليها ،و يعتبر الضبط هو الهدف من التفتيش والنتيجة المباشرة و المستهدفة،ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط.

يختلف الضبط في الجريمة المعلوماتية عن ضبط في الجرائم الأخرى من حيث المحل لأن الجريمة الإلكترونية يرد فيه الضبط على الأشياء ذات طبيعة معنوية من حيث البيانات و المراسلات و الاتصالات الإلكترونية و على الأشياء ذات الطبيعة المادية،كالكمبيوتر وملحقاته و الأقراص الصلبة الخارجية والمرنة[47].

(47) المادة 40 من قانون رقم 08-19 مؤرخ في 15 نوفمبر 2008، يتضمن تعديل الدستور، ج ر عدد 63، صادر في 16 نوفمبر 2008

[47]خالد ممدوح ابراهيم،المرجع السابق،ص.221.

الفرع الثاني

القواعد الإجرائية المستحدثة للتحقيق في الجريمة الإلكترونية

نظرا لتطور الكبير الذي شهده العالم في ميدان التكنولوجيا الرقمية ، وما أفرزه من أضرار وخيمة تمس بالنظام العام،والذي نتج عنه ظهور نوع مستحدث من الجرائم الذي أصبح يهدد كيان المجتمعات،الأمر الذي دفع بالمشرع الجزائري إلى استحداث أساليب أخرى للبحث والتحري عن الجريمة ،من خلال تعديله لقانون الإجراءات الجزائية ،وفقا لقانون رقم 22/06 المؤرخ في 2006/7/20 وهو ما يسمى بأساليب البحث و التحري الخاصة.

أولا:اعتراض المراسلات

يعتبر إجراء من إجراءات التحري المستحدثة و الذي يقصد به التتبع السري و المتواصل للمراسلاتالخاصة بالمشتبه به ودون علمه ،ذلك باعتبارهإجراء تحقيقي يباشر خلسة وتنهك فيه سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانون بهدف الحصول على دليل مادي للجريمة ،والتي تستخدمها في مواجهة الإجرام الخطير ،وتتم عبر وسائل الاتصال السلكية و اللاسلكية [48].

[48]زبيحةزيدان،المرجعالسابق،ص 55.

نجد وفقا لنص المادة 65مكرر5 من ق إ.ج.ج[49] أن اعتراض لم يقتصر فقط على المكالمات الهاتفية، بل تم توسيعه إلى مختلف أنواع الاتصال السلكية واللاسلكية، أما بخصوص أداة الاعتراض، فإن المشرع لم يحدد وسيلة معينة فقد تكون تقليدية أو مستحدثة.

ثانيا: التسرب

لقد تطرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 65مكرر12من قانون إ.ج.ج بعد تعديله بالقانون 22/06 والتي تنص على مايلي:((يقصد **بالتسرب قيام ضابط أوعون شرطة قضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيقالعملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.**

يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض،هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر14 أدناه،ولايحوز تحت طائلة البطلان،أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم.))

وبالتالي نستخلص طبقا لنص المادة، أن التسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة المشتبه في ارتكاب جناية أو جنحة بإيهامهم أنه فاعل أصلي بغرض كشف الحقيقة، ويبطل هذا الإجراء إذا كان الهدف من التحريض على ارتكاب الجريمة.

كما نص المشرع الجزائري على التسرب في قانون مكافحة الفساد [50].

[49]المادة 65مكرر5 من قانون الاجراءات الجزائية أمر رقم 66-156،مؤرخ في8 جوان 1966،يتضمن قانون الاجراءات الجزائية ، ج ر،عدد 84،معدل و متمم.

نجد أن المشرع الجزائري من خلال قانون مكافحة الفساد ،لم يعرف لنا التسرب حيث استخدم مصطلح اختراق للدلالة عنه و بالإشارة إليه فقط باعتباره من إجراءات التحري.

ثالثا : مراقبةالاتصالات الإلكترونية

نجد المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الإلكترونية،لكن بعض التشريعات قد قامت بتعريفها مثل التشريع الأمريكي الذي عرفها على أساس أنها "عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر"[51]

إلا أننا يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر خلسة ،و تنتهك فيه سرية الأحاديث الخاصة ،تأمر السلطة القضائية في الشكل المحدد قانون يهدف الحصول على دليل غير مادي للجريمة المعلوماتية،و يتضمن من ناحية استراق السمع إلى إلى الأحاديث ومن ناحية أخرى حفظه بواسطة أجهزة متخصصة لذلك.

ونجد أن المشرع من خلال قانون 06-01 قد أشار إلى هذا الإجراء دون تقديم تعريف له.بينما في بينما في القانون09-04 في المادة 3 منه قد حدد كيفية مراقبة الاتصالاتالالكترونية على النحو الآتي((مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد

---

[50]قانون رقم 06-01 مؤرخ في 20 فيفري 2006،يتعلق بالوقاية من الفساد و مكافحته ج ر عدد 14، صادر في 08 مارس 2006،المتمم بالأمر رقم 10-05،مؤرخ في 26أوت 2010،ج ر عدد 50،صادر في 1 سبتمبر 2010 معدل و متمم بالقانون رقم 11-15 مؤرخ في 02 أوت 2011،ج ر عدد 44، صادر في 10 أكتوبر 2011.

[51]زبيحةزيدان،المرجع السابق،ص-ص،126-127.

المنصوص عليها في القانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية))[52]

وبالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء وفي الحالات المحددة حصريا في المادة4 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المبحث الثاني

قمع الجريمة الإلكترونية

تعد ظاهرة الجرائم المعلوماتية أو الجرائم التقنية العالية ،ظاهرة مستجدة،تنشأ في الخفاء وتوجه لنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات ،فهي تعتبر من الجرائم التقنية التي تعاني منها المجتمعات في الآونة الأخيرة من انتهاك لحقوق والخصوصيات،لذا سعت مختلف التشريعات لردع هذا النوع من الجرائم من خلال تطوير بنيتها التشريعية ،الهادفة إلى توقيع عقوبات جزائية على مرتكبي هذا النوع من الجرائم المستحدثة من جهة،ونجد أن المشرع الجزائري من جهة أخرى رغبة منه لتصدي لظاهرة الإجرام الإلكتروني ، سعى إلى الحيلولة دون ارتكابها،وذلك بتوقيع عقوبات مختلفة ،سواء بالنسبة لشخص الطبيعي أو الشخص المعنوي.

[52]المادة 3 من قانون 09-04،المرجع السابق.

المطلب الأول

مضمونالعقوبة

لمواجهة الجريمة الإلكترونية فرضت التشريعات المختلفة جزاءات ردعية تتناسب مع خطورة هذه الجريمة التي أصبحت تهدد كيان المجتمعات، خاصة مع تنامي معدلات الجريمة وتطور أشكالها وتهديدها المباشر، دق ناقوس مجتمعات العصر الراهن لحجم المخاطر الناجمة عن هذه الظاهرة الإجرامية، هذا ما جعل المشرع الجزائري يعاقب من جهة الاتفاق الجنائي في الجريمة الإلكترونية (الفرع الأول)، ومن جهة أخرى الشروع فيها (الفرع الثاني)

الفرع الأول

العقاب على الاتفاق الجنائي في الجريمة الإلكتروني

لقد اختلف الفقه حول مدى ملائمة تجريم المشرع للاتفاق الجنائي ، فهناك من يرى أن الاتفاق الجنائي هو عزم إجرامي بحد ذاته ، مبررين ذلك بأن المعاقبة عليه تظهر من خلال العزم الجنائي الجماعي في مظهره الخارجي المادي ، فكل عضو فيه يعلن عزمه إلى سائر الأعضاء أين تتحدد إرادتهم على ارتكاب الجريمة . و بالموازاة مع خطورة هذه الظاهرة و تهديدها للأمن العام ، فنجد أن هذا الرأي يتماشى مع القانون من ناحية العقاب على الاتفاق الجنائي فيسلط العقوبة على تكوين الاتفاق الجنائي من جهة ، و يضفي الطابع الوقائي من هذه الجريمة الذي يكون بواسطة إحباط الاتفاق الجنائي المكون بين الجناة و لخططهم الإجرامية [53].

[52]إيمان مسعود سالم ، المرجع السابق، ص.38-39.

بينما يرى اتجاه آخر من الفقه أن تجريم مجرد العزم الإجرامي هو مرحلة مبكرة مقارنة مع التحضير للجريمة، كما أنها تعود للمرحلة النفسية بينما يلي التحضير للجريمة هذه المرحلة[54]

لذا لو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة لوجب على المشرع أن يجرم مرحلة التحضير أولا.

لقد تنبه كلا من من المشرع الجزائري و الفرنسي للنقد المقدم من الجانب الفقهي الثاني ، فلم يقوما بتجريم مجرد العزم على إعداد جرائم المعطيات ، و إنما تطلبا أن يجسد العزم بفعل أو عدة أفعال مادية ، فقد انتقلا من المرحلة النفسية إلى المرحلة التحضيرية للتجريم.[55]

أولا : مبدأ المعاقبة على الأعمال التحضيرية

نجد أن المشرع الجزائري لا يجرم الاتفاق الجنائي في الأصل إلا في الجنايات و عليه فقد أراد كلا من المشرعين الفرنسي و الجزائري عدم التوسع في تجريم الاتفاق و رفع سقف التجريم إلى الأعمال التحضيرية بدلا من تجريم العزم المجرد ، و نلاحظ أن المشرع الجزائري قد نص على الاتفاق الجنائي في نص المادة 394 مكر 5 من ق.ع ج على ما يلي : ((يعاقب كل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم ، و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة ذاتها))[56]

و يقابل هذا النص المادة 4/323 من القانون الجنائي الفرنسي.

---

[54]باطلي غنية ، المرجع السابق ،ص196.

[55]المرجع نفسه ،،ص.197.

[55] المادة 394 مكرر5من القانون رقم 66-156،مرجع السابق.

ويعتبر هذا خلافا للقواعد العامة حيث أن العقاب لايتقرر إلا في الجرائم التامة ،أو التي تقف عند حد الشروع،وبالتالي لكي يكون هناك العقاب لابد من وجود البدء في نشاط إجرامي يؤدي إلى ارتكاب الجريمة .

بينما الأعمال التحضيرية التي تسبق البدء في التنفيذ فلا عقاب عليها،ومنه نستخلص من خلال المادتين السالفتي الذكر أنهما تعتبران استثناء على القاعدة العامة،والغرض من ذلك توفير الحماية والوقاية لنظم المعالجة الآلية للمعطيات ضد مخاطر التي تنشأ عن نشاط غير مشروع الذي قد يهدف من خلال ذلك المجرم المعلوماتي إلى البدء في التحضير لارتكابإحدى الجرائم المنصوص عليها في القسم السابع مكرر من ق.ع.ج.

كما عاقب المشرع الفرنسي على هذا النشاط الإجرامي بنفس عقوبة الجريمة التي تم التحضير لها ،فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة أشد قمعا.[57]

ثانيا:أركانالاتفاق الجنائي

يعتبر قوام جريمة الاتفاق الجنائي في الجريمة التي نحن بصدد دراستها، ركنان، الركن المادي الذي يتم استخلاصه من نص المادة 394 مكرر5 من ق .ع.ج و المادة من 323 ق.ع.ف.

الذي يتمثل في الاتفاق أو الاجتماع المجسد في فعل مادي بغرض التحضير لارتكاب جرائم هذا القسم،مع اشتراط فعل المشاركة ،أي تعدد الجناة،أما الركن المعنوي يتجسد في القصد الجنائي.

[57]محمد خليفة ، المرجع السابق ، ص 111.

أ-الركن المادي في الاتفاق الجنائي

يتخذ الركن المادي في جريمة الاتفاق الجنائي ثلاثة عناصر وهي كآتي:

1-فعل الاتفاق

يقوم هذا الركن على الاتفاق ذاته، الذي يتمثل في انعقاد إرادتين أو أكثر و اجتماعهما على موضوع معين،ولهذا الاتفاق طبيعة مادية ملموسة إذ يفترض تعبير كل واحد منهم عن إرادته و يعلم بها أطراف الاتفاق الأخرى ، و يتحقق أن إرادتهم تسير باتجاه واحد و هو هدف معين ، و تتلاقى في نفس الموضوع ، بالتالي يجب أن تترجم هذه الإرادة في شيء مادي كالعبارات المكتوبة و يقوم الاتفاق بغض النظر عما استغرقهانعقاد الإيرادات من وقت قصير أو طويل ، و سواء كان الاتفاق منظما مفصلا فيتخذ شكل الجمعية الإجرامية ، أو كان عارضا اقتصر أعضاؤه بمجرد العزم على جريمة معينة دون تعيين لكيفية تنفيذها أو تحديد دور كل واحد منهم[58]

2_ موضوع الاتفاق :

يستمد الاتفاق صفته الإجرامية من موضوعه،واستنادالنصالمادة394 مكرر5 من ق.ع.ج

التي نصت على مجرد الاتفاق بغرض الإعداد أو التحضير لجريمة من جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات. من خلال هذه المادة نلاحظ أنه إذا كان موضوع الاتفاق أعمال تحضيرية و الإعداد لتلك الجرائم ، فإن الاتفاق يكسب صفته الجنائية ، و لو كانت الأعمال في

[57] طبقا لنص المادة 176من قانون رقم 04-15،المرجع السابق،بينما المادة 394 مكرر5 و الخاصة بالإتفاق في جرائم المعطيات التي تشترط للعقاب على الإتفاق أن يكون مجسدا بفعل أو عدة أفعال مادية،أي التحضير لوحده لايكفي ، كالقيام بإقتناء برامج خبيثة كالفيروسات أو برامج إختراق يتم من خلالها الدخول إلى أنظمة المعالجة الآلية للمعطيات

ذاتها مشروعة ، مثل الاتفاق على كيفية تصميم المعطيات و تجميعها و نشرها هو في الأصل مشروع ، لكنه يصبح غير مشروع إذا كان الاتفاق على تعليم ذلك بغرض استعماله في الجرائم التي تنص عليها المادة 394 مكرر 2ف1 من ق.ع.ج .

3_ وجوب تعدد الجناة :

تتطلب جريمة الاتفاق تعددا ضروريا للجناة ، و الحد الأدنى لهذا التعدد هو شخصان ، بينما لا يرد قيد على الحد الأقصى يجب أن يكون الجناة المتفقون مسؤولون جنائيا ، فإذا كان أحدهم غير مسؤول جنائيا ، فيجعل الاتفاق غير قائم ، كأن يكون أحدهم فاقد للإدراك أو التمييز لتعاطيه مخدرا دون علم منه ، أو مجنونا إلا أن هذا لا ينفي المسؤولية للمتفقين الآخرين ، الذين يتم معاقبتهم لوحدهم.[59]

ب_ الركن المعنوي:

تعد جريمة الاتفاق الجنائي واحدة من الأحكام التي تشترك فيها جميع الجرائم الواقعة على معطيات الحاسب الآلي ، و التي لابد لقيامها قصد جنائي عام و المتمثل في العلم و الإرادة .

1_ العلم:

يجب توفر العلم لدى كل عضو من أعضاء الجماعة بماهية الفعل أو الأفعال موضوع الاتفاق ، التي يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها ، وذلك باعتبار أن من يجهل الغرض من الاتفاق و هو ارتكاب جناية أو جنحة أو التحضير لهما لا يعد القصد الجنائي متوفرا لديه.

[59] زبيحةزيدان،المرجع السابق،ص.107.

2_ الإرادة:

لابد من توفر الإرادة لدى كل عضو من أعضاء الاتفاق و الهادفة إلى تحقيق نشاط إجرامي معين، و لابد أن تكون هذه الإرادة جدية ، فالذي يدخل الاتفاق بقصد الوشاية ببقية المتفقين أو بغرض الإطلاع على أمرهم ، لا يعد القصد الجنائي متوفرا لديه لغياب الإرادة الجدية[60].

الفرع الثاني

العقاب على الشروع في الجريمة الإلكترونية

يهدف العقاب على أية جريمة إلى تحقيق الردع العام فالعقاب على الشروع بوصفه جريمة لابد من تحقق عدوان على المصالح محل الحماية القانونية ، و أن العدوان يأخذ في الشروع صورة الخطر الذي يهدد هذه المصالح ، حيث ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما قد تحدثه من قلق و اضطراب في الجماعة[61].

و نجد أن مجال الشروع في الجنايات هو الأصل لشدة خطورتها ، أما بالنسبة للجنح فلا يكون إلا في الخطيرة منها بواسطة نص ، و لأن المشرع رأى في جرائم المساس بأنظمة المعالجة الآلية للمعطيات خطورة كبيرة الأمر الذي جعله يقرر إخضاعها للشروع بعدما نص على العقاب على الاتفاق الجنائي المجسد بأعمال مادية .

---

(59) محمد خليفة ، المرجع السابق، ص.116-117.

(60) باطلي غنية،المرجع السابق،ص.204.

أولا : أركان الشروع في الجريمة الإلكترونية

تطرقت المادة 30 من ق.ع.ج ، للشروع تحت عنوان المحاولة ، فنص على ما يلي : ((كل محاولة لارتكاب جناية تبتدئ بالشروع في تنفيذ الجناية أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى و لو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها)) و بالتالي فالشروع جريمة ناقصة ، و هذا و هذا النقصان لا يحتوي الركن المعنوي ، بينما يمس الركن المادي ، باعتبار أن الفاعل يقوم بأفعال تعتبر بدءا في التنفيذ لكنه لا يتوصل إلى النتيجة لأسباب خارجة عن إرادته ، كما نصت المادة 394 مكرر 7 من ق.ع.ج على أنه : ((يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها)).[62]

لولا وجود نص قانوني لما أمكن العقاب على الشروع لأن الشروع في الجنح لا يكون إلا بنص قانوني صريح.

و عليه فإن المشرع يعاقب على محاولة ارتكاب أي جريمة من جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، و لأن المشرع قد جرم الاتفاق الجنائي المجسد بالأعمال التحضيرية بصفتها مرحلة من مراحل الجريمة التي تسبق الشروع، فكان لزاما عليه أن يجرم الشروع لأنه مرحلة لاحقة [63].

---

(61) تقابلها المادة 323/7 من قانون العقوبات الفرنسي..

(62)محمد خليفة ، المرجع السابق،ص.119-120.

ثانيا: خصوصية الشروع في الاتفاقالجنائي:

هناك اختلاف فقهي حول وجود الشروع في الاتفاق الجنائي . فيرى جانب من الفقه أنه لا يوجد شروع في الاتفاق الجنائي ، و ذلك باعتبارالاتفاق حالة نفسية تتم بتلاقي الإرادات و لا تحمل بداية و لا نهاية فهو يقع كاملا و لا يحتمل بدءا في التنفيذ.

أما الرأي الثاني يخالف الرأي الأول باعتبار أنه ليس صحيحا أن الشروع في الاتفاق غير متصور فالعقاب على الشروع متعين إذا كان الاتفاق جناية، إذ لا يتطلب العقاب نصا خاصا و إذا كان الاتفاق جنحة فلابد من وجود هذا النص ، و هو ما أخذ به المشرع الجزائري عندما نصعلى جميع جرائم المعطيات بما فيها جريمة الاتفاق الجنائي ، ثم أخضع ذلك بالنص على الشروع في الجرائم السابقة .بناء على ذلك نقترح إخراج جريمة الاتفاق الجنائي من نظام الشروع ، و قصر هذا الأخير على على جرائم المعطيات الأخرى و هذا هو الذي عمل به ق.ع.ف من خلال نصه على الجرائم التي تخضع للشروع دون جريمة الاتفاق الجنائي.[64]

المطلب الثاني

أنواع العقوبات الإلكترونية المقررة للجريمة الإلكترونية

تختلف الجريمة الإلكترونية بحسب الفعل المرتكب لكل نوع منها ، الأمر الذي يجعل التشريعات تسلط عقوبات خاصة لكل نوع على حدا و يتجلى ذلك من خلال العقوبات المقررة سواء بالنسبة

(63) باطلي غنية،المرجع السابق،ص.205.

للشخص الطبيعي من جهة (الفرع الأول) ، و بالنسبة للشخص المعنوي من جهة أخرى (الفرع الثاني).

الفرع الثاني

العقوبات المقررة للشخص الطبيعي

نجد أن المشرع الجزائري قام بتوقيع عقوبات على الشخص الطبيعي و التي تختلف باختلاف الفعل المرتكب

أولا: العقوبات الأصلية

إن العقوبات الأصلية المطبقة تمثل المؤشر الصريح للخطورة التي يضفيها المشرع على الأفعال التي يجرمها ق.ع.ج ، و عليه نتطرق إلى عرض هذه الجرائم بحسب العقوبات المقررة لها.[65]

أ_العقوبات المقررة لجرائم الاعتداء على سير النظام :

سنتناول العقوبات المقررة لكل من جريمتي الدخول و البقاء غير المشروع سواء في صورها البسيطة أو المشددة .

– عقوبة جريمة الدخول أو البقاء غير المشروع

نصت على هذه الجريمة المادة 394 مكرر من ق.ع. ج سواء في صوتها البسيطة أو في صورتها المشددة

[64]باطلي غنية،المرجع السابق،ص.205 –206.

1-عقوبة الجريمة في صورتها البسيطة

يعاقب المشرع الجزائري على هذه الجريمة طبقالنصالمادةالسالفةالذكربالحبس من 3 أشهر إلى سنة و الغرامة من 50000 دج إلى 200000دج[66]، بينما المشرع الفرنسي يعاقب على فعل الدخول أو البقاء بطريقة الغش إلى جزء أو كل من نظام المعالجة الآلية للمعطيات بعقوبة الحبس لمدة سنتين و غرامة قدرها 60000 أورو . و نجد أن المشرع الجزائري من خلال نص المادة السابقة الذكر ، ترك للقاضي السلطة التقديرية بأن جعل له حدا أدنى و حدا أقصى في تقدير العقوبة بحسب الوقائع المعروضة أمامه ، حيث يختلف الباعث من شخص لآخر ، فليس باعث الفضول الاكتشاف كباعث الجوسسة و الربح ، وعلى هذا وجب اختلافالتقدير.

2_ عقوبة الجريمة في صورتها المشددة

ضاعفت الفقرة الثانية و الثالثة من المادة 394 مكرر من ق.ع.ج عقوبة جريمة الدخول أو البقاء غير المشروع إذا ترتب عن هذا الأخير إما حذف أو تغيير المعطيات ، سواء في حدها الأدنى الذي أصبح ستة أشهر بعدما كان ثلاثة أشهر ، أو في حدها الاقصى إلى سنتين بعدما كانت سنة واحدة . و بالنسبة للغرامة تكون من 50000 دج إلى 300000 دج.[67]

ثانيا :العقوبات المقررة لجرائم الاعتداء على المعطيات

---

[65]تقابلها المادة 323/1 من قانون العقوبات الفرنسي.

[66]حمودي ناصر،الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري،المجلة الأكاديمية للبحثالقانوني،كلية الحقوق، جامعة أكلي محند أولحاج،العدد الثاني،2016،ص.73-74.

سنتناول العقوبات الأصلية التي أقرها المشرع الجزائري لكل من جريمتي الاعتداء العمدي على المعطيات الموجودة داخل النظام ثم العقوبات الأصلية لجريمة التعامل غير المشروع في المعطيات.

أ_ عقوبة جريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام

نصت المادة 394 مكرر1 منٌ ق.ع.جعلى العقوبة الأصلية لمرتكب جريمة الاعتداء العمدي على المعطيات بالحبس لمدة تمتد من 6 أشهر إلى ثلاث سنوات و غرامة من 500000دج إلى 4000000دج

ب_ عقوبة التعامل غير المشروع بالمعطيات

تكون عقوبة جريمة التعامل غير المشروع بالمعطيات عن طريق تقرير عقوبتان أصليتان هما الحبس والغرامة.

1_ عقوبة التعامل في معلومات صالحة لارتكاب الجريمة

يعد التعامل في المعطيات فهو ينطوي على العديد من الأفعال والأعمال و العمليات السابقة على استعمال المعلومات مثل و بحثها و تجميعها، وصولا إلى توفيرها و نشرها أو الاتجار فيها حيث يعاقب المشرع على القيام العمدي أو عن طريق الغش بالأفعال السابقة الذكر بالحبس من شهرين إلى ثلاث سنوات و بغرامة من من 1000000دج إلى 10000000دج.[68]

[66] المادة 394 مكرر2 من قانون رقم06-23،المرجع السابق.

2_ عقوبة التعامل في معلومات متحصلة من الجريمة

أضاف المشرف الجزائري صورة ثانية من صور التعامل في معلومات غير مشروعة ، تتمثل في التعامل في معلومات متحصلة من جريمة و ذلك في حالة ارتكاب فعل من الأفعال التي حصرتها الفقرة الثانية من المادة 394 مكرر 2 و هي : الحيازة أو الإفشاء أو النشر أو الاستعمال و التي يعاقب عليها بنفس العقوبة المقررة في الصورة الأولى من جريمة التعامل غير المشروع في المعطيات.[69]

ثانيا: العقوبات التكميلية

بالإضافة إلى العقوبات الأصلية المفروضة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، قرر المشرع عقوبات تكميلية تتمثل في المصادرة و الغلق بالنسبة للقانون الجزائري.

أ_ المصادرة:

و هي تشمل كل الأجهزة و الوسائل التي تم استخدامها في ارتكاب إحدى الجرائم المعلوماتية و ذلك مع مراعاة الغير حسن النية.

ب_ الغلق:

تشمل عقوبة الغلق من ناحية، غلق المواقع التي تكون محلا لإركاب الجريمة المعلوماتية ، و من ناحية أخرى ، غلق المحل أومكانالاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.[70]

---

[69] حمودي ناصر ،المرجع السابق،ص-ص81-83.

[69] باطلي غنية، المرجع السابق ، ،ص.221.

الفرع الثاني

العقوبات المقررة للشخص المعنوي

لقد تضمن تعديل ق.ع.ج لسنة 2004 إقرار للمسؤولية الجنائية للأشخاص المعنوية بنص عام و هو نص المادة 18 مكرر من القانونرقم 15/04 السالف الذكر، و من خلال ذلك نقوم بتبيان شروط مسائلة الشخص المعنوي[71]

أولا: شروط تقرير المسؤولية على الشخص المعنوي

نصت المادة 394/ مكرر4 منٌ ق.ع.ج :((يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي .)) و تقابلها نص المادة 2/221 من ق.ع.ف التي تنص ((يمكن للأشخاص المعنوية أن يسألو جنائيا عن الجرائم المرتكبة في هذا القسم طبقا للمادة 4/121)) ، و كذا المادة 7/121 تنص على أنهم يسألوا في الحالات التي تنص أو اللائحة عن الجرائم التي ارتكبوها لحسابهم أو من طرف أعضائهم أو ممثليهم ، أما الجماعات المحلية و التجمعات التابعة لها ل يسألون جنائيا إذا كانت الجرائم التي ارتكبوها أثناء ممارستهم نشاطهم و القابلة لأن تكون موضوعا لاتفاق يمثل الخدمة العامة .

---

[70]براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري،المجلة النقدية للقانون والعلوم السياسية،كليةالحقوق ،جامعة ملودمعمري،تيزي وزو ،ص،130.

ثانيا :أنواع العقوبات المقررة على الشخص المعنوي

نص المشرع الجزائري في المادة 18 مكرر من ق.ع على العقوبات التي تطبق على الشخص المعنوي فيما يخص الجنايات و الجنح و هي كالآتي .

_حل الشخص المعنوي ، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات ، الإقصاء من الصفات العمومية لمدة لا تتجاوز 5 سنوات ، المنع م

بشكل مباشر أو غير مباشر إنعئيا لمدة 5 سنوات، مصادرة الشيء المستعمل في ارتكاب الجريمة ، نشر أو تعليق حكم الإدانة ، الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ، و مساءلة الشخص المعنوي لا تغني عن مساءلة الشخص الطبيعي و ذلك طبقا لأحكام المسؤولية الجزائية. بالإضافة إلى هذه العقوبات هناك عقوبات مقررة في حالة الاعتداء على الجهات العامة و التي تطرقت إليه المادة 394 مكرر 3 ق.ع.ج . التي تنص((تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد))[72]

نستنتج بناءعلىما سبقأن الجريمة الإلكترونية ، ظاهرة إجرامية مستجدة و التي تعاني منها المجتمعات ،وجاء تطور هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات و تكنولوجيا التي يسرت سبل التواصل و انتقال المعلومات، إلا أن هذا التقدم لا يخلو من العيوب وذلك باستخدامه في الأشياء غير المشروعة الأمر الذي دفع بالدول إلى العمل ملياً للحد من هذه

[72]المادة 394 مكرر3 من قانون رقم 04-15المرجع السابق.

الجرائم من خلال التوعية والوسائل الوقائيّة الأمنية وغيرها ،بحيث بات لزاما أن يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و السياسة الجنائية علي وجه الخصوص ، بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية ، لهذا الاعتبار تكاثفت الجهود الدوليةوالوطنية لمواجهة الآثار السلبية المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات.

خاتمة

نستخلص من خلال ما قد سبق دراسته نجد أن موضوع الجريمة الإلكترونية يعد من المواضيع البالغة في الأهمية نظرا لخطورتها ، مما يتطلب دراسة دقيقة و عميقة حولها ، الأمر الذي جعلنا نلاحظ و جود آليات معتمدة لمكافحة هذه الجريمة على الصعيد الدولي تبيينا لدور التشريعات المقارنة في مواجهتها من جهة ، و أخرى معتمدة على الصعيد الوطني وفقا لمجهودات قد قامت بها أجهزة الدولة من جهة ثانية .

فنرى أن المشرع الجزائري سعيا منه لتدارك الفراغ التشريعي الذي وقع فيه بخصوص مجال مكافحة الجرائم الإلكترونية ، قد قام بإدراج تعديلات خاصة على ق.ع.ج ، و استحداث قانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، محاولة منه للتقليص من هذه الجرائم المستحدثة و العابرة للحدود .

من بين النتائج التي توصلنا إليها نجد :

1_ الجرائم المعلوماتية من بين الجرائم المستحدثة و العابرة للحدود .

2_ هي من الجرائم المختلفة من حيث خصائصها عن الجريمة التقليدية ، كما أنها صعبة الإثبات و الإكتشاف كما يقل الإبلاغ فيها .

3_ الجرائم الإلكترونية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق و يتصف المجرم المعلوماتي فيها بالذكاء و السرعة كذلك يكون متميزا بالدقة و التخصص في مسائل تكنولوجيا المعلومات.

4_ هي من بين الجرائم التي تتوافق مع غيرها من الجرائم في مدى توفر القصد الجنائي العام.

5_ إسراع الدول إلى إيجاد حلول قانونية ردعية للحد من انتشار هذه الجريمة، كذلك تسخير الكفاءات البشرية للوقاية من تأثير هذه الجرائم على الأمن العام وكذا حماية المواطنين من خطورتها.

6_ تفطن المشرع الجزائري لهذا النوع من الجرائم بواسطة إحداثه لتعديلات في ق.ع.ج و ق04/09،إلا أن ذلك لايعتبر كافيا مع حداثة هذا النوع المستحدث من الجرائم الذي هو في تزايد مستمر.

أمابالنسبةللاقتراحاتالتييمكنتقديمهاهيكالآتي:

1_ نقترح من وجهة نظرنا أنه على المشرع استحداث تعريف قانوني خاص لهذا النوع المستجد من الجرائم ، نظرا لإزدياده و خطورته . الأمر الذي يستوجب إضفاء تعريف يبين نوعية الجريمة لعدم الوقوع في الخطأ خاصة من ناحية التكييف .

2_ على المشرع أن يقوم بتطوير بنيته التشريعية تماشيا مع التطور السريع والملحوظ لهذه الجريمة.

3-إنشاءأقساممتخصصةبالجرائمالإلكترونية.

4-ضرورةتخصيصشرطةجنائيةخاصةوخبراءمنذويالكفاءةالعاليةفيمجالالأنترنت.

5_ حبذا لو سار المشرع على قدم المساواة مع نظيره الفرنسي مثلا ، خصوصا من ناحية التكييف الدقيق للإتفاق الجنائي لفعل الشروع من جهة أخرى . و للوسائل و الأجهزة المسخرة و المتنوعة لقمع الجريمة من جهة مغايرة .

6_ ضرورة إبرام معاهدات و إتفاقيات دولية لردع الجريمة الإلكترونية .

7_ على السلطات المختصة الإكثار من الحملات التوعوية للمواطنين من أجل وضعهم في الصورة لتوخي الحيطة و الحذر من هذه الجرائم التي تتزايد أكثر فأكثر .

قائمة المراجع:

I: باللغة العربية

أولا :الكتب

1 –أمير فرج يوسف،الجريمة الإلكترونية و المعلوماتية و الجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت،الطبعة الأولى،مكتبة الوفاء القانونية،مصر،2011.

2–أحمد خليفة الملط ،الجرائم المعلوماتية،الطبعة الثانية،دار الفكر الجامعي،الإسكندرية،2006.

3–أشرف عبد القادر قنديل،الإثبات الجنائي في الجريمة الإلكترونية،دط ،دار الجامعة الجديدة،الإسكندرية،2015.

4– الحسيناوي علي جبار ،جرائم الحاسوب و الأنترنت،دط،دار اليازوري العلمية للنشر و التوزيع،عمان ،2009 .

5–الشوابكة محمد أمين أحمد،جرائم الحاسوب و الأنترنت"الجريمة المعلوماتية"،ط1،دار الثقافة للنشر و التوزيع،عمان،2004.

6–العريان محمد علي،الجرائم المعلوماتية،دط،دار الجامعة الجديدة،الإسكندرية،2011.

7–باطلي غنية،الجريمة الإلكترونية"دراسة مقارنة"،دط،منشورات الدار الجزائرية،الجزائر،2015.

8–بيومي حجازي عبد الفتاح،جرائم الكمبيوتر و الأنترنت في التشريعات العربية , دراسة مقارنة مع التطبيق على نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية .دط ، دار النهضة العربية ، الاسكندرية ،2009 .

9- _____ ، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر و الانترنت ، ط1 ، دار الكتب القانونية ، 2007.

10- جعفر حسن الطائي ، جرائم تكنولوجيا المعلومات رواية جديدة للجريمة الحديثة ، الطبعة الأولى ، جامعة عمر المختار ، 2007

11- خالد ممدوح ابراهيم،فن التحقيق الجنائي في الجرائم الإلكترونية،ط1،دار الفكر الجامعي،الإسكندرية،2010 .

12- خيرت علي محرز ، التحقيق في جرائم الحاسب الآلي ، دط . دار الكاتب الحديث ، الاسكندرية ، 2012 ،

13- خليفة محمد ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن ، دط ، دار الجامعة الجديدة ، الاسكندرية ، 2007.

14- شيماء عبد الغني محمد عطا الله ، الحماية الجنائية الالكترونية دط ، دار الجامعة الجديدة ، الاسكندرية . 2007 .

15- شحادة يوسف ، الضابطة العدلية علاقتها بالقضاء و دورها في سير العدالة الجزائية ، "دراسة مقارنة" ، ط1 ، مؤسسة يحسون للنشر و التوزيع ، بيروت ، د.س.

16 - شبيلي مختار ، الجهاز العالمي لمكافحة الجريمة المنظمة ، الطبعة الثانية ، دار هومة للطباعة و النشر و التوزيع ، الجزائر ، 2016 .

17-عبد الله عبد الكريم،الجرائم الإلكترونية،دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية و الأنترنت مع الإشارة إلى جهود مكافحتها محليا و عربيا ودوليا،ط1،منشورات الحلبي الحقوقية،بيروت،2007.

18 – عبابنة محمود أحمد ، جرائم الحاسوب و أبعادها الدولية ، ط1، دار الثقافة للنشر و التوزيع ، عمان ، 2009 .

19- عائشة بن قارة مصطفى،حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن،دط،دار الجامعة الجديدة،الإسكندرية،2010.

20- عفيفي كامل عفيفي ،جرائم الكمبيوتر و حقوق المِؤلف والمصنفات الفنية و دور الشرطة و القانون"دراسة مقارنة"،دط،منشورات الحلبي الحقوقية،الإسكندرية،2007.

21- محمد عبد الله أبوبكر سلامة،جرائم الكمبيوتر و الأنترنت،دط،منشأة المعارفالإسكندرية،2005.

22-محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر الانترنت ، (الأحكام الموضوعية و الأحكام الاجرائية) ، ط1، منشورات الحلبي الحقوقية ، بيروت ، 2011.

23- مصطفى محمد موسى ، الجهاز الالكتروني لمكافحة الجريمة ، دط ، دار الكتب القانونية ، مصر ، 2006 .

ثانيا : االمذكرات الجامعية :

1- إيمان مسعود سالم ، الجريمة المعلوماتية ، مذكرة لنيل شهادة الماستر في قانون الأعمال ، كلية الحقوق ، جامعة محمد لمين دباغين ، سطيف ، 2016.

2- بعرة سعيدة،الجريمة الإلكترونية في التشريع الجزائري"دراسة مقارنة"،مذكرة مكملة لنيل شهادة الماستر في العلوم الجنائية،جامعة محمد خيضر ،بسكرة،2015

3- بن بورنان كاتية ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة تخرج لنيل شهادة الماستر في الحقوق ، قسم: القانون الخاص ، تخصص : القانون الخاص و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة ، بجاية ، 2014.

4- معتوق عبد الطيف،الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن،مذكرة لنيل شهادة الماجستير في العلوم الجنائية،كلية الحقوق،جامعة الحاج لخضر ،باتنة،2015.

ثالثا : المقالات

1-بنعمر الحاج عيسى ، الأنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود ، مجلة الدراسات القانونية و السياسية ، كلية الحقوق ، جامعة الاغواط ، العدد 03 ، جانفي 2016،ص 252.

2-حمودي ناصر،الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري،المجلة الأكاديمية للبحث القانوني،كلية الحقوق ،الجامعة أكلي محند أولحاج،العدد الثاني،2016،ص.73_74.

3_ محمد أحمد سليمان عيسى ، التعاون الدولي لمواجهة الجرائم الالكترونية ، المجلة الأكاديمية للبحث القانوني ، كلية الحقوق ، جامعة عبد الرحمان ميرة ، بجاية ، العدد 2 ، 2016 .ص52-53.

رابعا : النصوص القانونية

1-الدستور :

دستورالجمهورية الجزائرية الديمقراطيةالشعبية،الصادربموجبالمرسومالرئاسيرقم 96-438،المؤرخفي 07 ديسمبر1996،المصادقعليهفياستفتاء 28 نوفمبر 1996،جرعدد 76 صادرفي 8 ديسمبر 1996،معدلومتمم:

- قانونرقم 02-03 مؤرخفي 10 أفريل 2002 يتضمنتعديلالدستور،جرعدد 25 صادرفي 14 أفريل 2002.

-قانونرقم 08-19 مؤرخفي 15 نوفمبر 2008،يتضمنتعديلالدستور،جرعدد 63،صادرفي 16 نوفمبر 2008.

-قانونرقم 16-01 ،مؤرخفي 06 مارس 2016 ،يتضمنتعديلالدستور،جرعدد 14،صادرفي07 مارس 2016.

2-النصوص التشريعية

أ_ أمر رقم 155/66 ، المؤرخ في 8 / جوان /1966 ، يتضمن قانون الاجراءات الجزائية ، ج.ر ، عدد 47 ، صادرفي 09 جوان 1966،معدلومتمم.

ب_ أمر رقم66-156، مؤرخ في جوان 1966، يتضمن قانون العقوبات ، ج،ر ، عدد 49، صادر 1966/06/11 ، معدلومتمم.

ج_ قانونرقم 06-01،مؤرخفي 20 فيفري 2006،يتعلقبالوقايةمنالفسادومكافحتهجرعدد 14،صادرفي 08 مارس 2006 ،المتممبالأمررقم 10-05 ،مؤرخفي 26 أوت 2010 ،جرعدد 50،صادرفي 1 سبتمبر 2010،معدلومتممبالقانونرقم 11-15،مؤرخفي 02 أوت 2011،جرعدد 44،صادرفي 10 أكتوبر 2011.

د_ قانونرقم 2000-03،مؤرخفي 5 أوت 2003،يحددالقواعدالعامةالمطبقةعلىالبريدوالمواصلاتالسلكيةواللاسلكية،جرعدد 48،صادرفي 6 أوت 2000 معدلومتممبموجبالقانونرقم 06-24،المؤرخفي 26 ديسمبر 2006،المتضمنقانونالماليةلسنة2007،جرعدد 85،الصادرفي 27 ديسمبر 2006،المعدلوالمتممبموجبالقانونرقم 14-10،المؤرخفي 30 ديسمبر 2014،المتضمنقانونالماليةلسنة 2015،جرعدد 78،الصادرفي 31 ديسمبر 2014.

هـ_ قانون رقم 18-01، مؤرخ في 23 يناير2008،يتمم القانون رقم 83-11 ، المؤرخ في 21 رمضان عام 1403، الموافق ل2 يونيو سنة 1983المتعلق بالتأمينات الإجتماعية.

3 النصوص التنظيمية

أ _ مرسوم رئاسي رقم 261/15 ، مؤرخ 8 أكتوبر 2015، يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

خامسا: مواقع الأنترنت

أ-المداخلات:

_ أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس ، يومي 24-25|03|2017، 2017،

أنظر الموقع التالي : .www.jilrc.com

ب-المقالات:

1-الحوتالأزرق،www.albawaba.com

تاريخالنشر:أفريل 2018،تاريخالإطلاع: الأحد2018/05/22 ،علىالساعة، 12; 20.

2-مقالصحفيعنالجرائمالإلكترونيةبإسمخديجةبودومي،wwwdw.com

تاريخالنشر:فيفري2018،تاريخالإطلاع:الثلاثاء،2018/03/5،علىالساعة،15: 16.

3-الطوئيوائل ، مقال صحفي تحت عنوان : مواجهة الجرائم الالكترونية تحتاج إلى سن تشريعات جديدة ، www .ahlmasrnews.com

II : باللغة الفرنسية

A/Ouvrages

1_ Eric (F) , Philippe (R) , Cybercriminalité , (Enquête sur les mafias qui envahissent le web) , Dunod , Paris . 2006 .

2_ Eric ,freyssinet , La cybercriminalité ou mouvement , La voisier, France , 2012.

B / Textes juridiques

1-Code pénal français: www.legifrance.fr .

2-Loi n 2004_ 575, du 21 juin 2004 pour la confiance dans l'économie numérique, J.O.F.R n°143 du 22 juin 2004, p.11168

C/ Mémoires

HADDAD Fella, : VHEKKOUR TASSADIT , La cybercriminalité Mémoire de fin d'études pour l'obtention de master IIOption droit privé de sciences criminelles Faculté de droit et de science criminelles , Université Abderahmane mira , Bejaia , 2012.

الـــفـــهـرس

ملخص :

تعتبر الجريمة الالكترونية من الجرائم المستحدثة التي تعاني منها المجتمعات في وقتنا الراهن ، الأمر الذي جعلها تقوم بتطوير بنيتها التشريعية تصديا لهذا النوع الخطير من الجرائم على مستويين الوطني و الدولي الذي يؤثر على استقلال الدول من جميع النواحي.

Résume :

La cybercriminalité est l’un des nouveaux crimes que connaissent les sociétés aujourd’hui, qui a développé sa structure législative pour faire face à ce type grave de criminalité aux niveaux national et international, ce qui affecte la stabilité pays à tous égards