جامعة عبد الرحمان ميرة -بجاية
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

الجرائم السيبريانية وسبل مواجهتها في التشريع الجزائري

مذكرة لنيل شهادة الماستر في القانون الخاص
تخصص :علوم جنائية

من إعداد الطالبتين:
-دغيش أحلام
-حمداوي ربيعة

تحت إشراف الاستاذ:
الدكتور حمادي زوبير

لجنة المناقشة

الأستاذ: هلال العيد .....رئيساً
الأستاذ: حمادي زوبير..... مشرفاً ومقرراً
الأستاذ: بن مرغيد طارق.....ممتحناً

السنة الجامعية 2017-2018

إهداء

إلى ملائكي في الحياة...

إلى معنى الحب والحنان ...إلى بسمة الحياة...

إلى سر الوجود إلى من كان دعائها سر نجاحي وبلسم جراحي

إلى أغلى الحبايب أمي الغالية.

إلى مرشدي لطريق النور...

إلى قدوتي ونبراسي في الحياة إلى أبي حفظه الله

أطال الله في عمره

إلى إخوتي وأخواتي

إلى جميع الزملاء والزميلات يونس، سعوبة، و إيمان

و اخص بالذكر زميلتي في العمل حمداوي ربيعة.

دغيش أحلام ✍

إهداء

إلى الذي لا يمكن للكلمات أن تحصي له معروفاً ولا يمكن لي أن أرد له جميلاً.

إلى من كلت أنامله ليقدم لنا لحظة السعادة.

إلى أبي العزيز.

إلى التي رفع الله قدرها فقرن عبادته بالإحسان إليها وشكره بشكرها، فجعل الجنة تحت قدميها.

إلي الغالية أمي.

إلى زميلتي في العمل أحلام دغيش.

إلى كل الزميلات صباح ،إيمان، سعوبة، فيروز، نبيلة ، صبرينة .

إلى كل من سقط من قلمي سهواً

حمداوي ربيعة✍

شكروتقدير

الشكر هو الكلمة الطيبة أصلها ثابت وفرعها في السماء، يلجا إليها الإنسان حينما يثقل كاهله عظيم الإحسان، وإذا كان الاعتراف بالحق فضيلة فان إسداء الشكر لمستحقيه فضيلة، لقوله ﷺ " من لم يشكر الناس لم يشكر الله ".

ومن هذا المقام لا يسعنا إلا أن نتقدم بأسمى آيات الشكر والتقدير والعرفان والاحترام إلى **"الأستاذ الدكتور وداعي عزالدين"** الذي وجهنا في انجاز هذا العمل المتواضع، وكذا" **الأستاذ الدكتور حمادي الزوبير** "الذي تفضل علينا بشرف قبول الإشراف على هذه المذكرة، رغم كثرة مشاغله فشملنا بعلمه الغزير وخلقه الرفيع وفضله الوفير، فأضاء لنا طريق البحث وساعدنا على التقدم فيه وحببنا فيه بعطف الوالد، وتواضع العلماء وكان لتوجيهاته السديدة الأثر البالغ في إثراء هذه المذكرة على النحو الذي نأمل أن تكون عليه، فهو خير معلم ونعم الأستاذ فله منا جزيل الشكر والتقدير والاحترام جعله الله ذخرا لطلبته ومتعه بموفور الصحة والعافية وأحاطه برعايته نسأله عز وجل عنا خير الجزاء وبارك له في وقته و عمله.

كما لا يفوتنا أن نتقدم بجزيل الشكر والعرفان إلى اللجنة الموقرة التي قبلت مناقشة هذه المذكرة.

وإلى كل من كان له الفضل في إتمام هذا العمل ولو بكلمة طيبة.

قائمة أهم المختصرات

1 - باللغة العربية:

1. ج ر.ج.ج.د.ش..... الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية.
2. د.س.ن.....دون سنة النشر.
3. د.ب.ن.....دون بلد النشر.
4. الصفحة .....ص.
5. ص ص ..... من الصفحة إلى الصفحة.

2 – باللغة الفرنسية:

1. *N……numéro*
2. *Op.cit……Opus citatum*
3. *p:……page.*
4. *pp……de la page à la page*
5. *RIDC……Revue internationale de droit comparé*
6. *Vol……volume*

مقدمة

يعرف العالم الراهن منذ نهاية القرن العشرين و بداية القرن الحالي تغيرات واسعة المجال و هذا إثر التطورات البارزة في مجال تكنولوجيا الإعلام و الاتصال، والتي انعكست على كافة جوانب الحياة الاجتماعية، السياسية، والاقتصادية.

ومع هذا التقدم الهائل للتكنولوجيا ظهرت ثورة جديدة تعرف بالثورة المعلوماتية، والتي كانت بداية نشوء عصر جديد ألا وهو العصر المعلوماتي الذي لم يسبق للبشرية معرفته من قبل وهذا لتميزه و فرادة نوعه.

حيث نتج عن هذا الأخير ظهور أدوات واختراعات و خدمات جديدة في شتى الميادين، من أهمها و أبرزها الحواسب الآلية والشبكات المتصلة بها، لاسيما تلك المسماة بالأنترنيت أو الشبكة العنكبوتية التي أثرت في مجال الاتصال والإعلام خاصة وقلبت موازينه، حيث تمكنت من أن تجمع بين مختلف وسائل الإعلام في وسيلة واحدة، فجعلت من العالم مجرد قرية صغيرة بدون عوائق، يتبادل الناس فيها أخبارهم و آرائهم، ويحصلون فيها على مختلف المعلومات بسرعة و دون شقاء.

ومع الانتشار المتزايد لاستخدام الحاسوب و شبكة المعلومات الدولية نشأت مجموعة من الجرائم لم تكن معروفة من قبل مرتبطة بهذه التكنولوجيا، فهذه الجرائم مختلفة عن الجرائم التقليدية من حيث أطرافها، و مكانها و محلها و أساليب ارتكابها، تتمثل في الجرائم الإلكترونية التي تعتبر من الجرائم المستحدثة نظرا لوسيلة ارتكابها.

ومن بين هذه الأخيرة نجد الجرائم السيبريانية و التي هي محور دراستنا، فمصطلح "السيبريانية " هو مصطلح جديد أطلق على الجرائم الواقعة باستخدام الحاسب الآلي المتصل بالانترنيت، يعني أن هذا المصطلح له مدلول ضيق يندرج فقط على السلوكيات الجرمية الواقعة بوسيلة إلكترونية واحدة ألا و هي الحاسوب، و على الشبكة العنكبوتية المتصلة به.

وعلى هذا فالجريمة السيبريانية هي جريمة مستحدثة كونها تطال الكيان المنطقي أي المعنوي للحاسب بما يشمله من برامج و معطيات، فهي تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم و شبكات المعلومات وفي مقدمتها الانترنيت، ويقترفها مجرمون أذكياء يسمون الهاكرز أو الكراكرز، يمتلكون أدوات المعرفة التقنية أو الفنية، و توجد للقضاء على أجهزة الحواسب و شبكات الاتصالات و قواعد البيانات والبرمجيات و

نظم التشغيل، مما يظهر مدى خطورة وهول الجرائم السيبريانية في أنها تمس الحياة الخاصة للأفراد و تهدد الأعمال التجارية بخسائر وخيمة، كما قد تنال من الأمن والسيادة الوطنية للدول، و كذا تشييع فقدان الثقة بالتقنية الرقمية.

ولعل هذا هو ما دفع بكثير من التشريعات الدولية إلى سن و إصدار قوانين جديدة لمواجهة هذه الجرائم السيبريانية أو المعلوماتية المستحدثة، بينما فضلت واختارت بعض الدول القيام بتعديل في بعض قوانينها القائمة فقط، و هنا نجد أن المشرع الجزائري و كغيره من التشريعات الدولية الأخرى قد ساير هذا التطور الحاصل في الميدان التكنولوجي، بحيث أجرى تعديل لقانون العقوبات الجزائري بإصداره عدة قوانين كالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 والذي استحدث نصوصا خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7، والأمر رقم 97-10 المؤرخ في 1997/3/6 المتعلق بحقوق المؤلف والحقوق المجاورة، و الذي ألغى أحكام المواد 390 إلى 394 من قانون العقوبات، وقد قام كذلك بإصدار القانون رقم 09-04 المؤرخ في 2009/8/5 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها.

بالتالي فتكمن أهمية دراسة موضوع هذه المذكرة في أن الجرائم السيبريانية تعد من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني و الدولي على حد سواء، والتي ينبغي على المشرع الجنائي مواجهتها بتشريعات حاسمة لمكافحتها وعقاب مرتكبيها.

ويمكن حصر أهداف هذه الدراسة في محاولة تقديم ماهية شاملة عن الجريمة السيبريانية وذلك بإعطائها تعريف عام لها، و إبراز مراحل نشوئها و تطورها التاريخي وخصائصها، ويتجلى الهدف الرئيسي من الدراسة في تحديد و إبراز أهم أنواع وأصناف الجرائم السيبريانية و الوقوف أمام آليات تصدي المشرع الجزائري لهذه الجرائم.

ولقد جاء اختيار هذا الموضوع وفق مبررات ذاتية و المتمثلة في الفضول العلمي.

أما الأسباب الموضوعية فتتمثل في حداثة الموضوع و ندرة الدراسات القانونية له، وكذا إيمانا منا بأهمية الوقوف على هذا النمط المستحدث من السلوك الإجرامي الذي غزى مجتمعنا مع زيادة استخدام الأنظمة المعلوماتية مناحي الحياة كلها، و كذلك كون الجرائم السيبريانية موضوع يثير إشكالات حديثة في ساحة الفكر القانوني.

أما فيما يخص الصعوبات التي واجهتنا في هذه الدراسة هي عدم إيجاد تعريف محدد لمصطلح " السيبريانية " و هذا عائد لقلة المراجع المتناولة له، كونه مصطلح جديد ومستحدث لا يستخدم قانونيا.

وكذا صادفتنا صعوبة حول مدى انطباق النص الجنائي التقليدي على الجرائم السيبريانية.

يعتبر المنهج ركنا أساسيا لدراسة أي ظاهرة مهما كان نوعها و موضوعها و ذلك لإعطائها صيغة أكثر علمية و موضوعية، و الظاهر أن طبيعة الموضوع هي التي تفرض علينا إتباع منهج معين ملائم، و هذا ما لمسناه من خلال موضوع بحثنا، لذا اعتمدنا على:

المنهج الوصفي حيث تم إتباعه في وصف و تحديد ماهية الجرائم السيبريانية بتبيين مفهومها و أركانها و خصائصها، و كذا أنواعها.

وتم الاعتماد على المنهج التحليلي من خلال تحليل و دراسة النصوص القانونية المتعلقة بآليات و سبل مواجهة المشرع الجزائري للجرائم السيبريانية.

أما المنهج التاريخي فتم توظيفه لتتبع التطور التاريخي لظهور و نشوء الجريمة السيبريانية.

وعليه فالإشكالية التي تتبادر لأذهاننا تتمثل في ما يلي: ما مدى مسايرة المشرع الجزائري للجرائم السيبريانية .

وللإجابة على هذه الإشكالية ارتأينا التعرض في مرحلة أولى إلى جرائم الاعتداء على النظام المعلوماتي (الفصل الأوّل)، والانتقال في مرحلة ثانية إلى جرائم الاعتداء بواسطة النظام المعلوماتي (الفصل الثانّي). غير أنّ الإشكالية لن تكتمل إلا إذا شرعنا مسبقا في ضبط مفهوم الجريمة السيبيريانية وذلك من خلال التعرض إلى النظرية العامة للجريمة السيبريانية (المبحث التمهيدي).

المبحث التمهيدي

نظرة عـــــامة

عن الجريمة السيبريانية

أدى الاستخدام المتزايد للحاسب الآلي في مختلف أشكال الحياة، و كذا سرعة التطور المذهل في مجال المعلوماتية و تكنولوجيا الاتصالات إلى بروز أصناف جديدة من الجرائم تختلف عن الجرائم المعتادة في مرتكبيها ووسائل ارتكابها، تتمثل أساسا في الجرائم السيبريانية، و هي ظاهرة إجرامية تدق ناقوس الخطر لتنبيه المجتمع عن مدى خطورتها وسلبيتها، يرتكبها أشخاص ذو خبرة و احترافية عالية تختلف أهدافهم من شخص لآخر[1].

بالتالي تعددت المفاهيم والتعريفات حول تحديد المعنى الشامل والواسع للجريمة السيبريانية، وعليه سوف نتناول في هذا المبحث المقصود بالجريمة السيبريانية (المطلب الأول)، ومن ثمّ أركانها (المطلب الثاني).

المطلب الأول

المقصود بالجريمة السيبريانية

تتميز الجريمة السيبريانية بطبيعة خاصة مما وجدت صعوبات في وضع تعريف جامع لها ذلك يرجع إلى التطور الذي تشهده و كذلك تنوع و اختلاف وسائل ارتكابها، وعلى هذا سنحاول إعطاء تعريف شامل لهذه الجريمة (الفرع الأول)، استعراض تطورها التاريخي (الفرع الثاني)، مع بيان مميزتها (الفرع الثالث).

الفرع الأول

تعريف الجريمة السيبريانية

تعددت المفاهيم والتسميات المتعلقة بالجريمة السيبريانية، وانعدام وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها اسم جرائم الأنترنيت أو الجريمة المعلوماتية أو جرائم الحاسب الآلي، هذا ما أدى إلى انعدام وجود تعريف محدد مجمع عليه حول الإجرام السيبرياني.

وتجدر الإشارة أنه في الواقع تواجهنا صعوبة في إعطاء تعريف لهذه الآفة الإجرامية وذلك خوفا من حصرها في نطاق ضيق ومحدود في التقدم المعلوماتي الحادث على مستوى

1- **TANO-BIAN Anmonka Jeanine- Armelle**, La répression de la cybercriminalité dans les Etats de l'Union Européenne et de l'Afrique de l'Ouest, Thèse pour obtention du grade de Docteur en droit public, Faculté de Droit, Université de Paris Descartes, Paris, 2015, p 8.

العالم[2].

وننوه إلى أن مصطلح " الجريمة السيبريانية " له مفهوم أضيق من مصطلح " الجرائم المتعلقة بالحاسوب " التي ترتبط بشبكة حاسوبية، فربما هذه الأخيرة تتسع حتى للجرائم التي ليست لها صلة بالشبكة، و كذا أضيق من مصطلح الجرائم الإلكترونية التي لا يقتصر ارتكابها فقط على الحاسوب، و إنما قد تستعمل فيها جميع المعدات و الأجهزة التقنية مثل الهاتف أو الجوال الذكي[3]، بالتالي فالجريمة السيبريانية هي نمط من أنماط الجريمة الإلكترونية، فالثانية أوسع من الأولى نطاقا[4].

وقد ورد تعريفان في إطار ورشة عمل خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاملة الجرمين، أن الجريمة السيبريانية تشمل بمفهومها الضيق (الجريمة الحاسوبية) أي أفعال غير مشروعة موجهة بواسطة عمليات إلكترونية تستهدف أمن النظام الحاسوبي والبيانات والمعطيات المعالجة عن طريق هذا النظام، أما بمفهومها الأوسع (الجرائم المتصلة بالحاسوب) تشمل كل نشاط غير مشروع يرتكب بواسطة أنظمة أو شبكة حاسوبية أو فيما يرتبط بها.

وبتعريف آخر شائع للجريمة السيبريانية هي كل سلوك تستعمل فيه الحواسيب أو الشبكات العنكبوتية كوسيلة أو غاية أو مكان لارتكاب الفعل الجرمي. ويندرج من هذا التعريف عدة عقبات، فإنّه مثلا يشمل الجرائم التقليدية كالقتل لوحة مفاتيح الحاسب الآلي بضرب الضحية حتى الموت.

كذلك يوجد تعريف أدق لوصف الجريمة السيبريانية على "أنها سلوكيات مرتكزة على الحاسوب تعتبر إما غير قانونية أو غير مشروعة من جهة أطراف معينة، ويستطاع الإلمام بها بواسطة الشبكات الإلكترونية العالمية"، بالتالي هذا التعريف يستبعد الحالات التي

2 - **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2011، ص ص 53-54..

3 - **ذياب موسى البداينة**، «الجرائم الالكترونية: المفهوم والأسباب، ملتقى علمي حول الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية» ، الأردن، خلال الفترة من 2 الى 4 سبتمبر 2014، ص03.

4 - **محمد الأمين البشرى** ،« تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت »، حلقة علمية حول الانترنت والإرهاب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، القاهرة، خلال الفترة من 15 إلى 19 نوفمبر 2008.، ص10.

تستعمل فيها الوسائل المادية للقيام بجرائم تقليدية أو عادية، لكنه بذلك قد يسقط جرائم تدرجها اتفاقيات دولية.

كما أن للجريمة السيبريانية تعريف آخر أشمل وأوسع مقارنة بالتعاريف السالفة الذكر، هو أنها جريمة من بين الجرائم الالكترونية التي يتم ارتكابها عن طريق الحاسوب أو الكمبيوتر بواسطة شبكة الانترنيت، من طرف شخص ذو خبرة وذكاء فائق بتقنيات الحاسب الآلي[5].

أو بمعنى آخر هي تلك الجريمة التي تترتب عن استخدام التقنيات الحديثة والمعلوماتية المتطورة المتمثلة بالحاسوب والشبكة العنكبوتية في سلوكات إجرامية، و تكون إما بدافع الحصول على مكاسب مادية أو بهدف الإتلاف والتخريب أو إحداث ضرر بالغير[6].

لذا فعدم وجود تعريف واحد للجريمة السيبريانية ليس بالأمر البالغ الأهمية، لطالما هذا المصطلح لا يستعمل قانونيا. فالمشرع الجزائري قد أطلق عليه مصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال[7]. وعرفها بمقتضى المادة 02 من القانون 09-04 المؤرخ في 05غشت2009 على أنها: « جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية» [8].

وعليه يستوجب في دراستنا إلى الإشارة للأمن السيبرياني الذي تقريبا لا يمكن الفصل بينه وبين الجريمة السيبريانية، فهو يؤدي دور فعال في التنمية لتكنولوجيا المعلومات

5 - **عمرو عيسى الفقي**، الجرائم المعلوماتية: جرائم الحاسب الآلي و الانترنيت في مصر و الدول العربية، المكتب الجامعي الحديث، مصر، د.س.ن، ص84..

6 - **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية و الانترنيت: الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص ص 15-16..

7 - **حفوظة الأمير عبد القادر، غرديان حسام**، « الجريمة الالكترونية و آليات التصدي لها »، مداخلة ألقيت في الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الاتحاد العالمي للمؤسسات العلمي، الجزائر، في 29 مارس 2017.، ص92.

8 - قانون رقم 09-04 مؤرخ في 05 أوت2009، مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج.د.ش عدد 47 لتاريخ 16 أوت 2009.

وخدمة النت، ويعتبر تقوية الأمن السيبرياني وتحصين الأسس الفاصلة للمعلومات عنصرين جوهريين في أمن و سلامة كل الدول، ويعد كبح وصد الجريمة السيبريانية لب الأمن السيبرياني الوطني، وجوهر منهجية تحصين الأسس الحاسمة للمعلومات.

فيمكن تعريف الأمن السيبرياني على أنه أمن الشبكات والنظم المعلوماتية، والبيانات والمعلومات والأجهزة المرتبطة بالشبكة العنكبوتية، لذا فهو النطاق المختص بإجراءات، ومعايير الحصانة والحماية الواجب الأخذ بها، للتصدي للاعتداءات والتهديدات، أو للوقوف من آثارها في أشد و شتى الأوضاع.

ويجمع الأمن السيبرياني و المعلومات علاقة و ارتباط قوي، فعرض المعلومات أو الاطلاع عليها و المتاجرة بها، أو تخريبها واستغلالها، هو ما يكون في معظم الأوقات خلف سلوكيات التعدي على الشبكات و النت.

ويمكن القول أن الأمن السيبرياني مجموعة من أنشطة و مهمات تهدف إلى حماية الأشخاص و الأموال المتصلون بتقنية الاتصال والمعلومات، فيمكن بذلك أن يضمن الحد من الأضرار التي تنجم في حالة تحقق الخطر و التهديد[9]

الفرع الثاني

ظهور الجريمة السيبريانية وتطورها

مرت جريمة الحاسوب بتطور تاريخي وفقا لتقدم التقنية و استعمالها، بذلك فقد عرفت عدة مراحل نبرزها كالتالي:

***المرحلة الأولى**: بدأت من انتشار استعمال الحاسوب والعبث بالبيانات في مطلع الستينات، فبرزت أولى المعالجات التي انحصرت على مقالات و مواد صحفية تناقش التلاعب بالبيانات المخزنة و تدمير أنظمة الحاسوب و التجسس المعلوماتي و الاستخدام الغير المشروع للبيانات المخزنة في نظم الحاسوب، و بذلك ثار جدل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أو ظاهرة إجرامية متطورة، أو أنها جريمة قانونية أم سلوك غير أخلاقي. فاعتبروها في هذه الفترة على أنها سلوكات تدخل في النطاق غير الأخلاقي، و مع

9 - **منى الأشقر جبور**، السيبريانية: هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، مصر، د.س.ن ، ص ص25-26.

ارتفاع نسبة استعمال الحاسوب في فترة السبعينات ظهرت مجموعة من الدراسات المسحية والقانونية التي انصب اهتمامها على جرائم الحاسوب و عالجت عدد من القضايا الجرائم الفعلية، و بالتالي في هذه الحقبة صار الحديث عنها على أنها ظاهرة إجرامية مستحدثة وليست مجرد سلوكيات غير أخلاقية[10].

***المرحلة الثانية:** عرفت هذه المرحلة في الثمانينات ظهور مفهوم جديد ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد و أنشطة نشر و زراعة الفيروسات السيبريانية، التي تقوم بتدمير و إتلاف الملفات والبرامج، وانتشر في هذه الفترة مصطلح (الهاكرز) المعبر عن مقتحمي الأنظمة، نجد في مقدمة غاياتهم سبب التعليم الذي يتمثل في استخدام الحاسوب والإمكانيات المستحدثة في نظم المعلومات، بالإضافة إلى غاية الربع التي كثيرا ما تدفع إلى التعدي على نظم المعلومات، وكذلك الدوافع الشخصية و المؤثرات الخارجية تكون سببا لارتكاب هذه الجرائم[11].

***المرحلة الثالثة:** نتيجة للتطور في العالم المعلوماتي ظهرت أصناف جديدة من الجرائم، التي ما كانت لتبرز لولا الحاسوب، فقد عرفت فترة التسعينات و القرن الحالي نموا هائلا في أنواع الجرائم السيبريانية، وذلك كان لما أحدثته شبكة الانترنيت من تسهيل لعمليات لعمليات دخول الأنظمة واقتحام شبكات المعلومات، بحيث ظهرت أنماط جديدة للجرائم السيبريانية كأنشطة إنكار الخدمة التي تقوم على فكرة تعطيل النظام التقني و منعه من القيام بعمله المعتاد و في هذه المرحلة كذلك نشطت جرائم نشر الفيروسات عبر مواقع الانترنيت لما تسهله من انتقالها إلى العديد من المستخدمين في نفس الوقت.

وقد أظهر تقرير التهديدات الأمنية المتوقعة لعام 2016 الصادر من شركة أنتل سيكيوريتي للأمن الالكتروني، عن سلسلة من التوقعات تشمل تطور شراسة الهجمات على القطاع المالي وسرقة ملايين الدولارات من الأنظمة المصرفية، وتطوير تقنيات جديدة

10 - **بن مكي نجاة**، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017، ص ص16-17.

11 - **سعيدى سليمة، حجازبلال**، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، مصر، 2017، ص58.

لاختراق أنظمة السيارات المتصلة بالانترنيت، و الاستيلاء على مراتب الموظفين[12].

عرفت هذه المرحلة وعيا بمدى أهمية المعلومات و حجم المناظر الناجمة عن الاعتداء عليها و إلزامية حمايتها، وذلك من خلال توفير آليات قانونية فاعلة لصدها و مكافحتها، لما لتقنية المعلومات من آثار واسعة على المجال الإداري و الاقتصادي و السياسي والاجتماعي والثقافي و القانوني للدولة، بالتالي انعكست على كامل زوايا النشاط الإنساني[13].

نستنتج مما سلف أن للجرائم السيبريانية امتدادات تاريخية ترجع إلى الستينات القرن الماضي فهي لم تكن معلومة كما هي عليه الآن، و هذا يستند إلى أن هذه الجرائم مستحدثة تتنوع وتختلف وتتضاعف كل يوم، بالإضافة إلى استخدام الحاسب الآلي والانتشار الواسع لشبكات الانترنيت.

الفرع الثالث

مميزات الجريمة السيبريانية

تتميز الجرائم السيبريانية بمجموعة من الخصائص والسمات التي تنفرد بها وحدها دون الجرائم التقليدية، و من أهمها نذكر ما يلي:

أولا- يستلزم وقوعها وجود حاسب آلي مرتبط بشبكة الانترنيت:

من البديهي أنه لا يمكن تصور قيام هذه الجريمة إلا بوجود جهاز الحاسوب، وتتميز هذه الخاصية من أهم الخصائص التي تتميز بها الجريمة السيبريانية، وزيادة عن ذلك فإن هذه المميزة للإجرام السيبرياني تخرج أفعال مادية التي تقع على أجهزة الحاسب و ملحقاته من حيز الجرائم السيبريانية[14].

إضافة إلى ما ذكرناه سالفا فإن هذه الجرائم تستلزم إلهاما كافيا بالاحترافية والمعارف المعلوماتية، كالمعرفة التقنية بالحاسوب وطريقة تشغيله واستخدامه[15].

---

12 - **سعيدى سليمة، حجاز**بلال ، المرجع السابق، ص59.

13 - **علي جبار الحسيناوي**، جرائم الحاسوب و الانترنيت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص20.

14 - **عمار عباس الحسيني**، جرائم الحاسوب و الانترنيت: الجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، لبنان، 2017، ص48.

15 - **محمود أحمد عبابنة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005،

فهي تعتمد هذه الأخيرة على درجة عالية من الذكاء في القيام بها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، لأنها تتميز بالغموض و صعوبة إثباتها، فكلما تطورت المعرفة التقنية كلما ارتفعت توقعية توظيف هذه المعارف بمظهر غير مشروع، وزيادة خطورة الإجرام السيبرياني[16].

بذلك فالحاسوب هو وسيلة ارتكاب جرائم الانترنيت بصفة عامة، والجريمة السيبريانية بصفة خاصة فلا يمكن وصف هذه الأخيرة بهذا الاسم دون استعمال الحاسوب فهو أداة الدخول على الشبكة العنكبوتية بالتالي قيام الجريمة بأية صورة. و تعتبر الشبكة العنكبوتية هي نقطة ربط بين شتى الغايات المتوقعة لتلك الجرائم، و هو ما جعل هذه الأخيرة تلجأ إلى أنظمة الأمن الإلكتروني للاحتماء بها[17].

لذا فارتباط الحاسوب بالانترنيت أمر ضروري لقيام الجريمة السيبريانية، بحيث أن الحاسب الآلي بواسطته يسمح للانترنيت بالانفتاح على المحيط أو العالم الخارجي، بالتالي هما عنصران متصلان يكملان بعضهما البعض لينتجا فعل إجرامي يتجسد في الجريمة السيبريانية[18].

ثانيا- جريمة عابرة للحدود الدولية:

مما لا شك فيه أن الجريمة السيبريانية تتميز بالطابع الدولي وهو من أبرز الخصائص التي تتسم بها هذه الجريمة، فهي لا تعترف بالحدود بين القارات والدول وبالتالي تسهل ارتكاب الجريمة من جولة إلى أخرى. فهي تكتسب صفة الجريمة الدولية، فمجتمع التقنية

ص36. وانظر كذلك:

ROSE Philippe, La criminalité informatique, 2e édition, que sais-je ?, Paris, 1996, p.64.

16 - **مزيود سليم**، " الجرائم المعلوماتية وواقعها في الجزائر وآليات مكافحتها"، *المجلة الجزائرية للاقتصاد و المالية*، العدد01، أفريل2014، ص97. وراجع أيضاً: يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة، مذكرة لنيل شهادة الماجستير، تخصص قانون عام، كلة الشريعة والقانون، الجامعة الإسلامية، غزة، 2013، ص.24.

17 - **أمير فرج يوسف**، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الانترنيت والكمبيوتر، مكتبة الوفاء القانونية، مصر، 2011، ص ص15-16.

18 - **بن مكي نجاة**، المرجع السابق، ص 20..

السيبريانية لا يقر بالحدود الجغرافية و لا يتقيد بها[19]، فهذا الأخير منفتح عبر الزمان والمكان دون أن يخضع للقواعد العامة للجريمة التقليدية في الحراسة الدولية "حرس الحدود ". فالإجرام السيبرياني هو صنف من الجرائم التي يتم ارتكابها غبر مسافات بحيث لا يتواجد الفاعل في مكان وقوع الجريمة بل يقوم بفعله الإجرامي عن بعد، وهو ما يفي انعدامية وجود المجرم المعلوماتي ماديا في مسرح الجريمة[20].

وقد خلقت هذه الخاصية الكثير من التحديات في مجال الاختصاص القضائي و القانون الواجب التطبيق و متطلبات التحقيق والملاحقة، والضبط والتفتيش، فترتكب بواسطة الحاسوب في دولة ما في حين يثبت الفعل الإجرامي في دولة أخرى[21].

ثالثا-خطورة الجريمة السيبريانية:

تعد الجريمة السيبريانية واقعة إجرامية مستجدة نسبيا تدق أجراس الخطر، لتحسس المجتمع الدولي بمدى حجم مخاطرها، وبشاعة الخسائر والسلبيات الناتجة عنها، فهي تمس جميع القطاعات على الصعيد السياسي والأخلاقي و كذا الأمني والمجتمعي، ويعد المجال الاقتصادي و المالي الأكثر استهدافا للمجرم السيبرياني. فمعظم هذه الجرائم تخص شركات التأمين و البنوك، فهذه الأخيرة ترتكز على أنظمة تمويل والنقل إلكترونيا[22].

وقد وصل المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة و اعتداء في الساعة، تأثر بها (589)، مليون شخص، وانقسمت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب، وكذا الجرائم المرتبطة باختراق الهواتف المحمولة[23].

19 - **BOOS Romain**, La lutte contre la cybercriminalité au regard de l'action des Etats, thèse pour obtention du grade Docteur en droit, option droit privé et sciences criminelles, Faculté de droit, sciences économiques et gestion Nancy, Université de Lorraine, 2016, p 181.

20 - **خالد ممدوح إبراهيم**، أمن الجريمة الالكترونية، الدار الجامعية للنشر، مصر، 2008، ص44.

21 - **تركي بن عبد الرحمن المويشير**، بناء بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص28..

22 - **عمارعباس الحسيني**، المرجع السابق، ص44.

23 - **سعيدى سليمة، حجازبلال**، المرجع السابق، ص65.

تجسدت أهم مخاطر الإجرام السيبرياني في تهديد البناء الثقافي و الاقتصادي للدولة، وكذا المساس بالحياة الخاصة و الأمن القومي والسيادة الوطنية، التي تجعل الانترنيت في عمق دائرة ترويج ثقافة العنف و التطرف، مبينة عن أفكار المتطرفين من كل فئة و جنس.

أما في ما يخص الخطورة في الجانب الأخلاقي، فإن معظم الجرائم السيبرانية تستهدف فضح الأشخاص وأسرارهم وتشويه سمعتهم، الشخصية المهنية والمالية، وهذا راجع لدوافع إما لأجل الانتقام أو الكسب المالي أو المنافسة[24].

رابعا-الجريمة السيبريانية تعتمد على الدراسة الذهنية:

إن كانت الجريمة التقليدية تحتاج إلى بذل جهد كالقتل مثلا، فالإجرام السيبرياني لا يحتاج إلى مجهود عضلي فهو من الجرائم الناعمة و الهادئة، يكفي لمس لوحة مفاتيح الحاسب الآلي لتتم عملية الإتلاف أو الاختراق مثلا، فهي لا تستلزم عنف ولا دماء ولا قتلى، ولا تخلف آثار خارجية بصورة مرئية، بالتالي تعتمد على التفكير العلمي المدروس من طرف محترفي الحاسوب الذين يتمتعون بذكاء ودهاء وخبرة عالية، الأمر الذي يجعل من الصعب كشف جرائمهم، و إثباتها، بالإضافة إلى ذلك فهي جريمة ترتكب في الخفاء مما يصعب تتبع مرتكبيها، و مما ما لا شك فيه ما يزيد من مرونة و نعومة هذه الجريمة أن المجتمع لا يرى المجرم السيبرياني بنفس المنظور الذي يرون به المجرم التقليدي، كون مرتكب هذه الجريمة ينتمي إلى مستوى اجتماعي راقي نسبيا بخلاف المجرمين الآخرين[25].

خامسا-الجريمة السيبريانية صعبة الإثبات:

يعتبر الإثبات أبرز العقبات التي تقف أمام الجهاز الأمني لمعظم الدول، و يمثل الإثبات في الجرائم السيبريانية أكثر تحدي و صعوبة[26]، وهذا راجع لأنّ هذه الجرائم لا تخلف أثر خارجي، فهي لا تتطلب جهد عضلي أو عنف أو سفك دماء أو ترك آثار لجريمة السرقة مثلا، بل هي بيانات ومعطيات تضاف و تتبدل وتتلف أو تحذف من السجلات المحفوظة في ذاكرة الحاسوب[27]. أو بمعنى آخر فإن هذه الجريمة تحدث في محيط

24 - **عمارعباس الحسيني**، المرجع السابق، ص46.

25 - المرجع نفسه، ص51.

26 - **تركي بن عبد الرحمن مويشير**، المرجع السابق، ص31.

27 - **سعيدى سليمة، حجازبلال**، المرجع السابق، ص 73..

إلكتروني يتم فيه نقل المعلومة و تماشيها بالنبضات الالكترونية الغير مرئية، مما لا تخلف آثارا مادية، هذا لأنها من الجرائم المستحدثة[28] التي يصعب اكتشافها، و ما يكتشف منها هو بمحض الصدفة[29].

ومن أسباب صعوبة إثباتها تعود إلى الجاني أو الضحية، وإلى أداة ارتكابها، بحيث تنفذ هذه الجريمة بصورة منظمة من إقليم دولة واحدة باستعمال شبكة الانترنيت، علاوة على ذلك أن المجرم السيبرياني كما أدرجنا سابقا أنه شخص يتميز بذكاء عالي و احترافية تقنية مما لا يترك أثر جانبي للجريمة بالتالي يصعب إثبات هذه الأخيرة[30].

إضافة إلى أن هذه الجريمة تحتاج لإثباتها خبرة فنية، مما يصعب على المحقق التقليدي التحري فيها، بحيث تستوجب هذه الأخيرة معرفة جد عالية بتقنيات الحاسوب و أنظمة المعلومات[31]. وبالتالي فالجرائم السيبريانية لها من الحالة الخاصة ما يعطيها هذه الخاصية، و يعتبر التطور التكنلوجي المتتالي سبب أولي لذلك[32].

المطلب الثاني

أركان الجريمة السيبريانية

قد عرفنا سابقا في المطلب الأول المقصود بالجريمة السيبريانية و أعطيناها تعريفا جامعا وراجحا لها، وتطرقنا أيضا إلى إبراز نشأتها ومراحل تطورها، وأدرجنا أهم المميزات التي تتسم بها. بالتالي سوف نتناول في هذا المطلب أركان الإجرام السيبرياني فمن البديهي والمعلوم أن كل جريمة ما يتطلب المشرع فيها وجود أركان وبدون هذه الأركان لا يمكن تصور قيام أي جريمة.

وتتمثل هذه الأركان في: الركن المادي والذي يتمثل في السلوك الإجرامي أو المادي،

28 - **خالد ممدوح إبراهيم**، أمن الجريمة السيبريانية، المرجع السابق، ص45.

29 - **بن مكي نجاة**، المرجع السابق، ص21.

30 - **نمديلي رحيمة**، « خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة »، مداخلة ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية، الاتحاد العالمي للمؤسسات العلمية، طرابلس، لبنان، يومي 24 و 25 مارس 2017.، ص102.

31 - **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، المرجع السابق، ص46.

32 - **محمود أحمد عبابنة**، المرجع السابق، ص37.

والعلاقة السببية وكذا النتيجة (الفرع الأوّل)، أما الركن الثاني فهو الركن المعنوي والذي يتجسد في القصد الجنائي للجريمة السيبريانية (الفرع الثاني)، والركن الثالث هو الركن الشرعي الذي يتمثل في النصوص القانونية التي تجرم الفعل (الفرع الثالث).

الفرع الأول

الركن المادي للجريمة السيبريانية

يتطلب السلوك المادي في الجريمة السيبريانية وجود محيط رقمي و كذلك توفر جهاز الحاسوب مربوط بشبكة الانترنيت، فيتحقق هذا الركن بضغطه زر أو لمسه شاشة على خلاف الجريمة التقليدية فهي واضحة ويسهل التحقق من وقوع أركانها كالسرقة مثلا، والركن المادي هو ما يعرف بالسلوك الإجرامي الذي يستوجبه القانون كمناط للعقاب على هذه الجريمة على أن يتحقق الضرر للسلوك الإجرامي كشرط لازم لتوقيع العقاب عليه من طرف المشرع، ويستوجب وجود علاقة سببية بين هذا السلوك والنتيجة(الضرر).

بالتالي فالركن المادي للجريمة السيبريانية يتجسد وقت ارتكاب الفعل الإجرامي يتولد منه نتيجة تجمع بينهما علاقة السببية[33]، هذا ما سوف ندرجه كالتالي:

أولا- الفعل الإجرامي في الجريمة السيبريانية

يتمثل السلوك الإجرامي للجريمة السيبريانية في السلوك الخارجي الذي يقوم به المجرم السيرياني، وهو كل فعل مادي يسبب ضرر سواء اتجهت نيته إلى حصول هذا الضرر أو لم تكن كذلك، وهذا السلوك المادي الإيجابي يجعل هذه الجريمة بواسطة الانترنيت ذات ميزة و خاصية موحدة تباشر من حيث النشاط المادي فيها.

بالتالي فإن ارتكاب الجريمة عبر الانترنيت يحتاج بالضرورة إلى منطق تقني، بعدمه لا يستطيع الشخص حتى الاتصال بالانترنيت، وتظهر القيمة الموحدة إلى ضرورة النشاط التقني وإلا فقدت الجريمة أساسياتها.

لذلك يعتبر الاحتجاج بانعدامية وجود قدرات تقنية وقت الاتهام بالقيام بالجريمة

33 - **حنان ريحان مبارك المضحكي**، الجرائم المعلوماتية: دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2014، ص85.

بواسطة الانترنيت من الدفوع الموضوعية الأساسية التي تلتزم محكمة الموضوع بالرد عليه تفصيلا وإلا شاب حكمها عيبا في التسبيب بما يجوز قبول الطعن بالنقض فيه[34].

ثانيا- النتيجة (الضرر):

تعتبر النتيجة هي العنصر الثاني الذي يرتكز عليه الركن المادي في الجريمة السيبريانية، و يستلزم أن تقترن بواصلة أو رابطة سببية بالنشاط الجرمي، والضرر النتج هو التغيير الذي يحصل في المحور الخارجي كنتيجة للسلوك الإجرامي والذي يقيم عليه المشرع أحكاما قانونية. فالنتيجة الضارة لها مفهومان أولهما المفهوم المادي و ثانيهما المفهوم القانوني، فالمدلول المادي يعني المخلفات التي أحدثتها الجريمة في المحور الخارجي و يوقع القانون على حدوثها عقوبة[35].

ويجب أن يكون للجريمة طبيعة مادية ملموسة في المحيط الخارجي لتتم المعاقبة عليها، و لكن توجد بعض الجرائم التي ليس لها نتيجة، و تعرف بالجرائم السلبية، ومن هذا المنبر بدت أهمية الاعتراف بالمدلول أو المعنى القانوني للنتيجة دون الأخذ بعين الاعتبار حصول الضرر أو لا، فمجرد الإخلال بهذه المصلحة ينتج قيام حصول الجريمة من الجهة القانونية[36].

ويطرح موضوع النتيجة الجرمية في جرائم الانترنيت مشاكل عديدة، مثلا مكان و زمان تحقق النتيجة، فلو قام أحد المجرمين في فرنسا باختراق جهاز خادم Server أحد بنوك أمريكا، و هذا الخادم يتواجد في إيطاليا، فكيف يمكن العلم بوقت وقوع الجريمة، فهل هو توقيت بلد المجرم أن توقيت بلد البنك المسروق، أم توقيت جهاز الخادم في إيطاليا، و تطرح أيضا إشكاليات و صعوبات في القانون الواجب التطبيق في هذا الأمر، لأنه هناك أبعاد عالمية في هذا النطاق[37].

ثالثا- العلاقة السببية:

يجب لاكتمال الركن المادي للجريمة السيبريانية أن تكون هناك علاقة سببية بين

34 - **خالد ممدوح إبراهيم**، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص ص99-100.

35 - **حنان ريحان مبارك المضحكي**، المرجع السابق، ص ص 87-88.

36 - المرجع نفسه، ص 88.

37 - **عماد مجدي عبد المالك**، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، مصر، 2001، ص37.

النشاط الإجرامي و بين النتيجة (الضرر) التي وردت جراء هذا النشاط، فيستلزم أن يكون هذا الأخير في حد ذاته هو المؤدي إلى النتيجة الضارة.

ولابد من تواجد العلاقة أو الرابطة السببية في كافة الجرائم العمدية و البحث عن الرابطة السببية لا يطرح إشكالية لأن هذا النشاط الجرمي أفرز حال صدوره إلى حصول النتيجة (الضرر)، و بمفهوم آخر فإن نشاط أو فعل المجرم هو وحده الذي أدى إلى وقوع النتيجة.

وتجدر الإشارة أنه في بعض الأوضاع قد يحصل النشاط الإجرامي و لكن لا تتحقق النتيجة، بالتاي نكون أمام حالة من حالات الشروع في السلوك الجرمي فقط. لكن يواجهنا إشكال في الجانب السيبرياني عند محاولة وصل النشاط الجرمي بالنتيجة الضارة التي حدثت بسببه، نتيجة لصفة هذه الجرائم و طبيعتها المعقدة و الصعبة، فمن المتوقع أن تتولد عدة أضرار من نشاط جرمي واحد[38].

الفرع الثاني

الركن المعنوي

لا يقتصر قيام المسؤولية الجنائية من الجهة القانونية، أن يصدر من الشخص الجاني نشاط إجرامي ذو طابع مادي فقط، و إنما يستلزم زيادة على ذلك توافر الركن المعنوي، فهذا الأخير يعتبر جوهر المسؤولية الجنائية عندما يعتبر الركن المادي مظهرها الخارجي الذي تجسد به الضرر الناجم عن الجرم.

فيستلزم وجود رابطة أو علاقة سببية بين النشاط الإجرامي و إرادة الجاني المنطلقة إلى جعل النتيجة الغير المشروعة كبصمة لسلوكه الإجرامي، و هو الخطأ العمدي فيتطلب أن يدرك المجرم أنه يفعل نشاط غير مشروع، و أيضا أن تكون له الحرية المطلقة في الاختيار للقيام بهذا الفعل الإجرامي، أما الإهمال و الرعونة فينتجان الخطأ الغير العمدي، فهو لا يشترط من المجرم توافر الإرادة[39]. لذا فالركن المادي هو الوضع النفسي للمجرم أو

38 - **حنان ريحان مبارك المضحكي**، المرجع السابق، ص 90.

39 - المرجع نفسه، ص 91.

حالته البسيكولوجية، و الواصلة التي تربط بين ماديات الجريمة و شخصية المجرم[40].

بالتالي الركن المادي هو الاتجاه الذهني أو النفسي للجاني أنه يمثل أساس القانون الجنائي، ففي حيزه تتوافر كامل أساسيات المسؤولية الجنائية، فالرابطة التي تصل بين شخصية الجاني و ماديات الجريمة هي محل الجرم في مفهوم استحقاق العقاب، بالتالي القانون يسلط العقاب عليها[41].

وتجدر الإشارة أن القصد الجنائي في الجرائم العمدية قد يكون قصدا عاما أو خاصا، فالأول يقوم باتجاه إرادة المجرم للقيام بالسلوك الإجرامي مع توافر علمه بكامل عناصر الجريمة. أما الثاني ألا وهو القصد الجنائي الخاص، فيتحقق بالحالة أو الوضعية النفسية الشخصية المرتبطة بالنتيجة الضارة أو الدافع، و ليست متعلقة بالسلوك المادي المكون للمجرم[42].

هذا في الجرائم العمدية، أما الغير العمدية فهي بغير قصد أو واقعة عن طريق الخطأ، سواء لم يكن في حسبان الفاعل نتيجة سلوكه أو عدم سلوكه، و كان في مقدوره أو من واجبه حصولها.

ويكون الخطأ إما عاما أو خاصا، و يقوم الأول بواقعة الإخلال بالقواعد العامة التي تكتسب من خبرة الإنسان العامة، أما الخطأ الخاص فهو الذي يحصل نتيجة لمخالفة القواعد المأخوذة من الشرائع و الأنظمة، فيقوم هذا الخطأ بمخالفة قواعد قانونية ملزمة[43].

وبخصوص الركن المعنوي في الجريمة السيبريانية هو نفسه الركن المعنوي في جميع الجرائم التي تقتضي وجود قصد جنائي عام و خاص فالأول يكون موجودا أو محققا في جميع الجرائم السيبريانية بغير استثناء، إلا أن القصد الخاص قد يتحقق في بعض الجرائم دون الأخرى، لكن هذا لا يعني عدم وجوده في الجرائم الإلكترونية مثلا في جريمة تشويه السمعة عبر الانترنيت، فهذه الأخيرة تقتضي وجود قصد خاص، و عموما يبقى الأمر راجع

40 - **عماد مجدي عبد المالك**، المرجع السابق، ص37.

41 - **خالد ممدوح إبراهيم**، الجرائم المعلوماتية، المرجع السابق، ص ص105-105.

42 - **محمد زكي أبو عامر**، الإجراءات الجنائية، ط7، دار الجامعة الجديدة، مصر، 2002، ص205.

43 - **حنان ريحان مبارك المضحكي**، المرجع السابق، ص ص 93-94-95.

للسلطة التقديرية للقاضي[44].

الفرع الثالث

الركن الشرعي للجريمة السيبريانية

تطبيقا لقاعدة شرعية الجريمة و العقوبة يعني أن القاضي الجنائي ليس له الحق في إنشاء جريمة جديدة أو إصدار عقوبة جديدة لجريمة قائمة، و إنما ليقع ذلك يستلزم صدور نص قانوني بذلك، و ليس بالإمكان متابعة الشخص عن سلوك قام به قبل صدور نص يجرم فعله، أو قيامه بذلك النشاط بعد إلغاء النص المجرم لذلك.

بالتالي فالتشريع يعتبر المرجع الرئيسي للتجريم و تسليط العقوبة، فالقاضي الجنائي ليس بإمكانه تكملة تشريع ناقص أو غير كاف أو تغيير العقوبة المقررة في القانون بعقوبة أخرى[45].لذا ينتج عن مبدأ الشرعية قاعدة هامة و هي عدم رجعية القانون الجنائي، بمفهوم آخر لا يمكن توقيع عقوبة على شخص قد قام بفعل لم يجرمه القانون[46]. هذا إعمالا لما نصت عليه المادة 1 من قانون العقوبات و التي قضت بـ:« لا جريمة و لا عقوبة أو تدبير أمن بغير قانون»[47].

وما يفهم من هذه المادة اعتراف المشرع وتجريم السلوك المرتكب وذلك من خلال توقيع العقوبة في النصوص القانونية، فالمشرع الجزائري استحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم البيانات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات[48].

---

44 - **عاقلي فضيلة**، « الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري»، مداخله ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية ، الاتحاد العالمي للمؤسسات العلمية، طرابلس، لبنان، يومي 24 و 25 مارس 2017.، ص120.

45 - **حنان ريحان مبارك المضحكي**، المرجع السابق، ص55.

46 - **بعرة سعيدة**، الجريمة الإلكترونية في التشريع الجزائري- دراسة مقارنة-، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2015-2016، ص44.

47 - أمر رقم 66-156، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، ج.ر.ج.د.ش العدد 49، المؤرخة في 11 يونيو 1966.

48 - **عاقلي فضيلة** ، المرجع السابق، ص 119.

الفـــــصل الأول

جرائم الاعتداء على النظام المعلـــــــــــوماتي

بعدما تعرضنا في المبحث التمهيدي إلى الطبيعة العامة للجريمة السيبريانية، وذلك من خلال إبرازنا لمفهومها الشامل وذلك من حيث إعطاء تعريف لها، وتبين مراحل ظهورها وتطورها، وكذا مميزات هذه الأخيرة وأركانها، بالتالي فقد ارتأينا في هذا الفصل إلى دراسة جرائم الاعتداء السيبرياني، أي الجرائم التي ترد على المعطيات أو المكونات المنطقية أي المعنوية للحاسوب و الشبكة العنكبوتية، كالبرامج المستعملة و البيانات المخزنة في ذاكرة الحاسب الآلي موضوعا للإجرام، و يقصد بالبرنامج أو الكيان المنطقي مجموعة من الأوامر التي تسمح بتشغيل جهاز الحاسوب أو أنظمة المعلومات المخصصة لمعالجة المعلومات بغية القيام بعملية معينة أو تقديم نتائج محددة[49]، ومن أهم الجرائم الواقعة على النظام السيبرياني نذكر منها جريمة السرقة، الإتلاف، إعاقة النظام السيبرياني، التزوير، خيانة الأمانة، والاستخدام غير المصرح به للنظام السيبرياني، وكذا الجرائم الحاصلة على البيانات الاسمية أو الشخصية المخزنة سيبريانيا، والاختراق.

لكن تقتصر دراستنا على البعض فقط من هذه الجرائم وهي؛ جريمة السرقة، وجريمتي الإتلاف والتزوير السيبرياني، وكذا الجرائم التي تقع على البيانات الشخصية المخزنة سيبريانيا.

وقبل التطرق إلى كل هذا تجدر الإشارة أن الجرائم كإتلاف أجهزة الحاسوب أو سرقتها لا تدخل ضمن المكونات المنطقية أو المعنوية للحاسوب، وإنما هي أفعال مادية تخضع للنصوص التقليدية لانعدام موضوع الجريمة السيبريانية الذي يتمثل في البيانات والبرامج.

وعلى هذا الأساس سنعالج في مرحلة أولى ثلاث جرائم وهي السرقة الإتلاف، والتزوير السيبرياني (المبحث الأوّل)، ثم ننتقل في مرحلة ثانية إلى الجرائم الواردة على البيانات الشخصية المخزنة سيبريانيا (المبحث الثانّي).

49 - **QUEMENER Myriam,** « Concilier la lutte contre la cybercriminalité et l'éthique de liberté», *Sécurité et Stratégie*, vol 01, n°5, 2011, p.56.

المبحث الأول

صور الاعتداء على النظام المعلوماتي

تعتبر المعلومات نتاجا لمعالجة البيانات، وفي ظل التطور التكنولوجي الذي نعيشه ازدادت أهمية هذه الأخيرة، خاصة تلك المحفوظة داخل نظام المعالجة الآلية مع الانتشار الواسع لشبكات الاتصال الخاصة بالحاسوب كثرت وتعددت أصناف صور الاعتداءات على المعلومات، التي تعتمد قيمتها على ما يمنح لها من اعتبارات الخصوصية الأمنية.

وبعد دراستنا للجريمة السيبريانية في المبحث التمهيدي بصفة عامة، استنتجنا أنّ هذه الجرائم السيبريانية قد تحولت إلى ظاهرة عالمية يصعب التحقق منها والحكم عليها، ناهيك عن صعوبة التنبؤ بها ومحاكمة مرتكبيها ذلك لعدم توفر أو وجود دلائل مادية لها في كثير من الحالات أو شهود ضد منفذيها نظراً للتطور الهائل والمستمر لتقنيات الأنظمة السيبريانية.

ومن صور الاعتداءات التي ترد على المعلومات هي سرقة المال المعلوماتي (المطلب الأول)، وإتلافه (المطلب الثاني)، وتزويره (المطلب الثالث).

المطلب الأول

جريمة السرقة السيبريانية

يقصد بالسرقة عموماً اختلاس مال منقول مملوك للغير بنية التملك، وينصرف معنى المنقول في هذا المقام إلى كل ما لديه قيمة مالية يمكن تملكه وحيازته ونقله بغض النظر عن صغر قيمته[50]. فهذه الجريمة تعتبر من أخطر العدوان على المال في العالم المادي، فهي بذلك تحتل المرتبة الأولى في هذا الأمر، حيث جرمتها جميع تشريعات العالم المختلفة.

ومما لا شك فيه، أنّ هذه الجريمة وكغيرها من الجرائم تأثرت بالتطور والتقدم التكنولوجي، الذي ساهم بشكل كبير على إتاحة وتسهيل إمكانية ارتكابها وفي وقت قصير، ومن أماكن بعيدة، إذ باستعمال التقنيات المتطورة في مباشرتها من الحاسوب والانترنيت،

50 - **أحمد خليفة الملط**، الجرائم المعلوماتية: دراسة مقارنة، الطبعة 2، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

بالتالي نتجت جريمة مستحدثة في جرائم الاعتداء على الأموال يطلق عليها اسم السرقة السيبريانية أين تكون المعلومة هي متن الاعتداء و يكون الحاسب الآلي وسيلة لتنفيذها[51].

ولما كانت هذه الجريمة السيبيريانية بهذا القدر الكبير من الخطورة أصحى لزاماً علينا تعريفها (الفرع الأوّل)، وكذا بيان أركانها (الفرع الثانّي)، والوقوف عند نظرة وموقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأوّل

تعريف جريمة السرقة السيبريانية

تختلف السرقة السيبيريانية عن السرقة التقليدية، من حيث أنّها تكون في عالم افتراضي لا العالم الواقعي، كما أنها تقع على المعلومة لا على المال المادي، فالمعلومة لها طابعاً منوياً لا يمكن أن تقع في حيازة مادية مباشرة من طرف مرتكبيها.

وعليه، يقصد بالسرقة السيبيريانية اختلاس معلومات ونقلها من حيازة مالكها إلى الغير باستخدام الانترنت[52]، وذلك من خلال الدخول إلى مواقع وسرقة بطاقات الائتمان مثلاً، الذي يؤدي إلى الحصول على الأموال من قبيل ذلك، أو تحويل السارق السيبرياني أموال بعض العملاء إلى حسابه الخاص وذلك بدخوله إلى حساباتهم المصرفية، باستخدام تقنيات وبرمجيات معينة، أو عن طريق نسخ الملفات أو نقل محتوى المعلومات باستعمال الفيروسات[53].

الفرع الثاني

أركان جريمة السرقة السيبريانية

ترتكز جريمة السرقة السيبريانية على ثلاث أركان لقيامها تتمثل في محل أو موضوع السرقة المتمثل في المعلومات (أولاً)، وركن مادي يتمحور في فعل الاختلاس السيبرياني (ثانياً)، وركن معنوي يتمثل في القصد الجنائي (ثالثاً).

---

51 - **هروال هبة نبيلة**، جرائم الانترنيت: دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2014/2013، ص178.

52 - **KELCI Sevgi**, « Vol, fraude et autres infractions semblables et internet », *Lex-Electronica*, vol 12, n° 1, 2007, p 8.

53 - **هروال هبة نبيلة**، مرجع سابق، ص ص 178-179.

أولاً- المعلومة محلّ السرقة:

يتمثل موضوع السرقة السيبريانية في الشيء الذي يقع عليه الاعتداء ألا وهو المعلومات، ولقيام هذه الأخيرة يستوجب توفر شرطان أساسيان وهما أن يكون موضوع السرقة مالا وأن يكون مملوكاً للغير ومنقولاً[54].

أهم ما يميز السرقة السيبريانية هو موضوعها المتمثل في المعلومات[55] المتكونة من العناصر المنطقية للنظام المعلوماتي وما تحويه هذه العناصر من برمجيات وبيانات صالحة للاستخدام الآلي [56]،

وعلى هذا الأساس أثارت هذه المعلومات جدالاً كبيراً بين أوساط الوفقهاء فيما يخص مدى قابليتها للاعتداء عليها بموجب السرقة، وذلك بسبب طبيعتها غير المادية، فأنقسم الفقهاء إلى تيارين: تيار يستبعد المعلومات من محل جريمة السرقة (أ)، وجانب آخر يعترف بصلاحتة هذه المعلومات بأن تكون موضوعاً لجريمة السرقة (ب).

أ-الاتجاه المنادي بعدم صلاحية المعلومة بأن تكون محلاً للسرقة

ذهب هذا الاتجاه إلى عدم صلاحية المعلومات لأن تكون موضوعاً للاعتداء عليها، وذلك بحجة طبيعتها غير المادية، وأنّ هذه الأخيرة مقصاة من فئة الأموال، وبالتالي لا تصلح أن تكون محلاً لأي حق من الحقوق المالية المتعارف عليها[57]، فحسب زعمهم لا يمكن تصور وقوع جريمة السرقة على الأشياء المعنوية غير المحسوسة، فالأشياء الملموسة هي فقط التي يمكن أن تكون موضوعا لأي حق من الحقوق المالية[58].

ب-الاتجاه المنادي بجواز اعتبار المعلومة محلاً للسرقة:

خلافاً للرأي الأوّل يري أنصار هذا الاتجاه أنّ المعلومات تعتبر مالاً مادياً في نفس ذاتها، أما الكيان المعنوي لها فهو يعكس طبيعة حق صاحب الشيء عليها. ومن ثمّ يجوز الاعتداء

54 - **KELCI Sevgi**, op.cit, p 8.

55 - **هروال هبة نبيلة**، مرجع سابق، ص 179.

56 - **أحمد خليفة الملط**، مرجع سابق ، ص 235.

57 - **هروال هبة نبيلة**، المرجع السابق، ص 180.

58 - **عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، جامعة الشرق الأوسط، د.ب.ن، 2014**، ص 62..

عليها عن طريق فعل السرقة، ودعموا طرحهم هذا بالحجج التالية:

– إنّ كلمة شيء (Chose) الواردة في المادة 311 من قانون العقوبات الفرنسي تشمل على الأشياء المادية و غير المادية، بالتالي من الممكن حيازة المعلومات وسلب حيازتها[59].

– إنّ الاستيلاء على المعلومة يمكن أن يتحقق عن طريق السمع أو المشاهدة من ثم فإن المعلومة يمكن أن تنتقل من عقل إلى آخر و في هذه الحالة يمكن صب المعلومة في إطار مادي، عن طريق تحيزها داخل إطار والاستئثار بها، وينتج ذلك عن قيام الشخص الذي التقط المعلومة عن طريق السمع أو المشاهدة بتدوينها أو تسجيلها على دعامة ثم يعرضها للبيع مثلا، فتنتقل من ذمة مالية إلى أخرى[60].

– إنّ سرقة المعلومات لا الدعامات هي السبب الذي أدانت من أجله محكمة النقض الفرنسية عاملا قام بنسخ مستندات سرية بدون علم ورضا المالك الشرعي، كما أدانت هذه الأخيرة شخصا بتهمة إخفاء معلومات تتعلق بسر التصنيع، وقضت أيضا بالإدانة على شخص آخر لكونه قدم للمحكمة صور منسوخة من مستند مسروق، أعدها بنفسه و بمعرفة شخص مجهول الهوية[61].

– أن المعلومة قابلة للتحديد و القياس مثل الطاقة الكهربائية.

– أن المعلومة منفصلة عن دعامتها المادية هي مال يمكن تملكه لما له من قيمة اقتصادية إذ يمكن للجاني استغلال المعلومات بأن يبرم عقودا مع الغير، بحيث تكون هذه المعلومات - المخزنة المنقولة – محلا لها، وبالتالي حرمان صاحبها من عائدها المادي[62].

– بالتالي نحن نؤيد في رأينا الخاص أنصار الفقه القائل بصلاحية المعلومة للسرقة، ويرجع ذلك أن تحليل الأمور المنطقي يتفق مع التطور التكنلوجي الموجود والمحتمل وجوده فيما بعد بفرض فكرة الكيان المادي للشيء الناتج عن اختلاس المال السيبرياني للبرامج والمعلومات هي وإن لم يكن لها شيء محسوس إلا أنّ لها كيانا ماديا يظهر من رؤيتها على

---

59 - **أحمد خليفة الملط**، المرجع السابق، ص 243.

60 - **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنيت: الجريمة المعلوماتية، مكتبة دار الثقافة للنشر، محفوظة للناشر، الأردن، 2004، ص 151.

61 - المرجع نفسه، ص 152.

62 - **هروال هبة نبيلة**، مرجع سابق ، ص 180.

شاشة النظام السيبرياني، وتنتقل عبر أسلاك وتقنيات عالية الذي تمكن إلى حلها إلى معلومات معينة.

وتجدر ملاحظة أنّ جريمة السرقة لا تقع إلا إذا كان الشيء محل الاعتداء منقول ومملوكا للغير، أي أنه يتم اختلاس المال بسلبه من مالكه الأصلي إلى الحيازة الخاصة للجاني، وهذا ما يتوافق مع الأموال السيبريانية المادية، فالمعلومات تعرف على أنها أصوات وصور ووثائق ومعطيات مهما كانت طبيعتها، فبالتالي تصلح لأن تكون موضوعا للسرقة[63].

هذا من ناحية ومن ناحية أخرى، تشترط القواعد العامة للسرقة أن يكون المال المنقول ملكا للغير وقت الاختلاس، إذ لا تقوم جريمة السرقة إذا كان المال المنقول مملوك للجاني وقت اختلاسه، و لو كان للغير على هذا المنقول حقوق تخوله حبسه وتجعله أولى بحيازته من مالكه[64].

ثانيا- الركن المادي لجريمة السرقة السيبريانية:

يتمثل الركن المادي (السلوك الإجرامي) في جريمة السرقة السيبريانية في فعل الاختلاس، ويقصد به كل فعل يقوم به الجاني و يؤدي إلى انتزاع وأخذ أو الاستيلاء على مال الغير دون رضا صاحب الشيء، ويقوم على عنصرين أساسيين أولهما العنصر المادي، و هو إخراج حيازة المال المملوك للغير كاملا أو ناقصا، وإدخاله في حيازة الجاني. أما العنصر الثاني فهو انعدام علم ورضا المالك أو المجني عليه بخروج المال الذي في حيازته إلى حيازة الجاني[65].

فالاختلاس السيبرياني المرتبط بسرقة المعلومات والبيانات هو استيلاء على هذه الأخيرة دون علم وإرادة صاحبه الشرعي سواء كانت مخزنة على أشرطة ممغنطة أو أسطوانات مدمجة، كما هو الحال عندما يقوم الشخص بتوجيه المعلومات والبيانات الخاصة بالغير إلى حاسوبه الشخصي ويقوم بالاطلاع عليها، وكما يعرف أيضا على أنه

63 - **هروال هبة نبيلة** ، مرجع سابق، ص 181.

64 - **المرجع نفسه**، ص 180.

65 - **KELCI Sevgi**, op.cit, p 8.

الحصول على معلومات التحويلات الالكترونية للنقود أو الخدمات بقصد مشاركة أو حرمان من له الحق فيها[66].

ثالثا- الركن المعنوي لجريمة السرقة السيبريانية:

تعد جريمة السرقة من الجرائم العمدية، ويتخذ الركن المعنوي فيها قصد جنائي عام وخاص. بالنسبة للقصد الجنائي العام لجريمة السرقة فيقوم بانصراف علم الجاني إلى ارتكابه العناصر المكونة للجريمة، فيجب أن يعلم الجاني بأن المال الذي يسرقه أو يختلسه من حائزه الأصلي دون رضاه يدخل تحت تحكمه[67].

وعليه، يكون علم الجاني بالاعتداء على النظام السيبرياني إما بفعل الدخول غير المشروع أو البقاء الغير المشروع فيه، وبانتهاك النظام السيبرياني الخصوصي والمبرمج بسرقة كلمة المرور، و اختراق نظامه الأمني مثلا[68].

أما بالنسبة للقصد الجنائي الخاص، فيتمثل في نية تملك الشيء محل الاعتداء، وذلك بتوجه إرادة الجاني إلى الاستيلاء على المعلومات وتبديل حيازتها وممارسة سلطات المالك عليها. لكن يجب أن يكون هناك تزامن بين النية وفعل الاختلاس، أما إذا كان لاحقا للفعل فلا تقع الجريمة[69].

الفرع الثالث

موقف المشرع الجزائري من السرقة السيبيريانية

لم ينص المشرع الجزائري صراحة على تجريم السرقة السيبريانية، سواء في القانون رقم 04-15 الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، أو القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال، إلاّ أن هذا لا ينمع من إمكانية تطبيق نص المادة 394 مكرر من قانون العقوبات والتي تمنع استخدام منظومة معلوماتية عن طريق الدخول إلى نظام المعالجة الآلية للمعطيات بطريقة غير مشروعة، والتي قضت على ما يلي: « *يعاقب بالحبس من ثلاث أشهر إلى سنة و*

66 - **هروال هبة نبيلة**، مرجع سابق ، ص 182.

67 - **أحمد خليفة الملط**، مرجع سابق ، ص 273.

68 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص 161.

69 - **هروال هبة نبيلة**، مرجع سابق ، ص 186.

بغرامة من 50.000دج إلى 200.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ... »[70].

ويجد تطبيق هذا النص مبرراً له على اعتبار أنّ اختلاس المعلومة تقتضي الدخول إلى النظام المعلوماتي، ومهما يكن يبقى هذا النص غير كافيا، فكان على المشرع الجزائري أن يقتدي بالتشريعات الأجنبية في الدوّل المتطورة، على غرار التشريع الإنجليزي الذي تدخل في سنة 1996 بإضافة المادة 15 (أ) إلى القانون الخاص بالسرقة والتي بموجبها أصبح يعاقب على من يقوم بتحويل إلكتروني غير مشروع للأموال أيا كانت الطريقة التي تم التلاعب في البيانات من أجل إجراء عملية التحويل[71].

المطلب الثاني

جريمة الإتلاف السيبرياني

تعتبر جريمة الإتلاف السيبيرياني من أخطر الجرائم التي تقع على الأنظمة السيبريانية، بحيث يُطلق عليها بمصطلح " تدمير نظام الحاسوب sabotage informatique "، فهذه الجريمة عبارة عن تخريب ومحو تعليمات البرامج والبيانات المتعلقة بالحاسب الآلي[72].

ولما كانت هذه الجريمة بهذه الخطورة كان لابدّ من إزالة الستار عنها والبحث عن تعريفها (الفرع الأوّل)، وبيان أركانها (الفرع الثانّي)، وتحديد موقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأول

تعريف جريمة الإتلاف السيبرياني

يقصد بالإتلاف السيبرياني الأذى الذي يقع على المعلومات كتخريبها أو جعلها بلا فائدة (كتشفيرها باستخدام مفتاح مجهول مثلا)[73]، أو هي المحو أو التشويه الالكتروني

70 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، مرجع سابق

71 - **عباوي نجاة**، الإشكالات القانونية في تجريم الاعتداءات على أنظمة المعلومات، دفاتر السياسة والقانون، عدد 16، 2017، ص.286.

72 - **محمود أحمد عبابنة**، مرجع سابق ، ص100.

73 - **حسن طاهرداود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص93.

للبرامج أو المعلومات كلياً أو جزئياً، على نحو يجعلها غير صالحة للاستعمال[74].

تقع جريمة الإتلاف السيبيرياني في نطاق المعلوماتية بالتعدي على العمل الطبيعي للحاسوب، وذلك بالاعتداء على البرامج، والبيانات المخزنة والمتبادلة بين الحواسيب و شبكاته، ويقتضي ذلك عن طريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو بإتلاف و تخريب المعلومات المخزنة بالحواسيب و المتبادلة عبر الشبكة العالمية global (not) بتغيير نتائجها أو تعديلها أو محوها أو بواسطة التشويش على النظام السيبرياني، الذي يؤدي بدوره إلى إعاقة سير وظائف النظام الآلي بمختلف أشكاله[75].

ولا يقصد بالإتلاف في هذا المنبر الإتلاف الذي تقع أفعاله على المكونات المادية للحاسب، بل ذلك الاعتداء الذي يوجه إلى الجانب المنطقي والمعنوي في الحاسوب، بتدمير برامجه ومعلوماته، هذا لإفقاده قيمة ومنفعة تلك البرامج والمعلومات وجعلها غير صالحة للاستخدام[76].

ويقع الإتلاف على النظام السيبرياني، سواء بالدخول العمدي للنظام السيبرياني، أو نتيجة الخطأ أثناء التواجد بالنظام أو الخروج منه، أو باستخدام الجاني طرق ووسائل فنية للإتلاف[77]، و التي سنعرض البعض و الأهم منها:

أولا: الفيروسات (les virus):

يقصد بالفايرس برنامج تطبيقي تتم كتابته ليقوم بنسخ ونشر نفسه ذاتيا، دون تعاون المالك أو المستخدم للجهاز[78]. فهو يهدف إلى إحداث أكبر ضرر ممكن في النظام السيبرياني بتدمير برامجه وتخريبها.

ومن أهم ميزات الفيروسات: استطاعتها على التخفي والانتشار السريع، وقدرتها على التدمير والاختراق، ومن أبرز الفيروسات التي تستخدم للاعتداء على معلومات وبرامج الحاسوب فيروس حصان طروادة وهو عبارة عن برنامج يتمتع بقدرته العالية على الاختفاء

74 - **عمار عباس الحسيني**، مرجع سابق ، ص 137.

75 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل ومتمم، المرجع السابق.

76 - **محمود أحمد عبابنة**، مرجع سابق ، ص 100.

77 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص222.

78 - **ذيب بن عايض القحطاني**، المدخل إلى أمن المعلومات ، مكتبة الحميضي، الرياض، 2010، ص 122.

داخل البرنامج الأصلي ليعمل أثناء التشغيل ليبدأ نشاطه التدميري، كذلك فيروس القردة، و فيروس السرطان، و كذا الفايروس الإسرائيلي و هو مصمم ليمحو جميع الملفات في يوم محدد من أيام شهور السنة، بالإضافة إلى فيروسات محاكاة الأخطاء وهي تظهر رسالة زائفة على شاشة الحاسوب، و الفيروسات القاتلة والتطورية وكذا النائمة التي تعد من أخطر أصناف الفيروسات بحيث تظهر خطورتها في أنها تبقى منغلقة إلى وقت معين ثم تنطلق لتحقيق أهدافها التدميرية و التخريبية، كفايروس الكريسماس الذي ينتشر عبر البريد الإلكتروني[79].

ثانيا- برامج الدودة: (worn software):

تعبر برامج الدودة عن برمجيات تستغل أي ثغرات في أنظمة التشغيل هي تنتقل من حاسوب إلى آخر، ومن شبكة إلى أخرى عبر الوصلات التي يربط بينهما، لتتكاثر أثناء عملية انتقالها كبكتيريا بحيث تنتج نسخ منها، وتبرز أهدافها في شغل أكبر حيز ممكن من حجم الشبكة بالتالي تقليل وخفض مهارتها وكفاءتها، لتفوت من غايتها لتشرع بعد الانتشار إلى التخريب والتدمير الحقيقي للبرمجيات والأنظمة السيبريانية[80].

ثالثا- القنابل السيبريانية:

تعتبر القنبلة السيبريانية صنفا من أصناف البرامج الخبيثة صغيرة الحجم، يتم إدخالها بطرق غير مشروعة مع برامج أخرى، فهذه البرامج شكليا ليست ملفا كاملا، بل هي شفرة تلتحق بمجموعة من الملفات لنقوم بتجزئتها إلى أقسام متفرقة بالتالي لا يستطاع التعرف عليها بحيث تجمع فيما بينها وفق الأمر المنوط لها في زمان ومكان معينين، فتصميمها يبقيها ساكنة وغير فعالة إلاّ في زمن معين أو واقعة معينة، فهي تستعمل لإتلاف البيانات و المعلومات وتغير برمجيات النظام السيبرياني[81]، وهي بدورها تنقسم إلى قسمين:

أ- القنبلة المنطقية: logie bomb:

يهدف هذا النوع من البرامج إلى إحداث تغيير و تدمير برامج و معلومات النظام في واقعة محددة أو في فترة زمنية منتظمة، فهو يعمل على أساس التوقيت ليحدث تدميرا و

79 - **عمار عباس الحسيني**، مرجع سابق ، ص ص 140- 142.

80 - مرجع نفسه، ص 145.

81 - مرجع نفسه، ص 143.

تغييرا في المعلومات والبرامج عند العمل على أمر معين في الحاسوب، أو برنامج معين[82].

ب- القنبلة الموقوتة: time bomb:

يختلف القنبلة الزمنية أو الموقوتة عن القنبلة المنطقية، في أنها تثير حدثا في وهلة زمنية محددة بالساعة واليوم والسنة، فيتم إدخالها في برنامج وتنفذ في جزء من ثانية أو في يضع ثوان أو دقائق نسبة للتحديد اللازم، ويمكن ضبطها لكي تنفجر بعد عام مثلا[83].

وعليه تعد جريمة الإتلاف السيبرياني من جرائم نظم المعلومات الخطيرة التي تكمن خطورتها في آثارها البالغة السوء على الجهات التي تتعرض لها، فالإتلاف يؤدي إلى عدم تمكين المستفيد من الوصول إلى المعلومة أو كشفها أو استغلالها بالتالي إلحاق ضرر بمصالح صاحب المعلومات[84].

الفرع الثاني

أركان جريمة الإتلاف السيبرياني

غني عن البيان أن لكل جريمة أركان معينة يجب توافرها، فجريمة الإتلاف السيبيرياني كغيرها من الجرائم تتطلب لقيامها -إلى جانب الركن الشرعي طبعاً - تحقق ركنين أساسيين هما الركن المادي (أولاً) والركن المعنوي (ثانياً).

أولا-الركن المادي:

يتمثل لب وجوهر الإتلاف يتمثل في تخريب الشيء محل الإتلاف، وإنقاص منافعه وجعله غير صالح للاستخدام، ويتحقق النشاط الإجرامي لهذه الجريمة بكامل الأفعال التي تتوصل إلى إتلاف النظم السيبريانية، ويطلق على هذا السلوك عدة تسميات كالتدمير والإتلاف، و التخريب و محو البرامج والبيانات.

ومن متطلبات الإتلاف وجود وسائل و برامج خبيثة كالفيروسات مثلا، أو أي طريقة أخرى تتوصل إلى نفس النتيجة.

82 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص 240.

83 - **محمود أحمد عبابنة**، مرجع سابق ، ص 104.

84 - **حسن طاهرداود**، مرجع سابق ، ص39.

وترتيبا لذلك تعتبر هذه الجريمة من جرائم الضرر، أي تلك الجرائم التي تستلزم وقوع نتيجة إجرامية تنجم عن نشاط أو سلوك الجاني، وليس مجرد قيام النشاط الإجرامي، وهذا الشأن من البديهي أنه ينتج عن جريمة الإتلاف التي تستوجب حصول محو أو تلف أو تدمير أو إحداث خلل دائم للبيانات بحيث لا يستطيع المالك الانتفاع بالمعلومات بصورة كلية أو جزئية، بالتالي فهذه الأخيرة تستلزم بعد ذلك قيام العلاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية التي وقعت، أي أن تكون نتائج الإتلاف بشتى أشكاله، تترتب على ذلك السلوك الإجرامي[85].

ثانيا- الركن المعنوي:

تعتبر جريمة الإتلاف السيبرياني من الجرائم العمدية التي تقوم على ركن معنوي، يتحقق بتوفر القصد الجنائي العام، الذي ينبني على العلم والإرادة، فيستوجب على الجاني العلم بأنه يقوم بالاعتداء على الأموال السيبريانية المملوكة للغير، وأنه سينتج من سلوكه إتلاف أو تعطيل أو محو المعلومات، بالتالي يحرم صاحبه من الانتفاع بها بشكل كلي أو جزئي، وبالإضافة إلى إلزامية توافر العلم يستلزم أن تتجه إرادة الجاني إلى تحقيق نتيجة سلوكه، وهذا بفعل حصول الإتلاف الذي ينتج توافر الضرر الناجم عن نشاطه الإجرامي[86].

الفرع الثالث

موقف المشرع الجزائري من جريمة الإتلاف السيبيرياني

نص المشرع الجزائري على تجريم كل نشاط أو فعل ينتج إتلاف المال السيبرياني المعنوي من خلال نص المادة **394 مكرر1** من قانون العقوبات الجزائري، والتي تتضمن ما يلي: « يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة 500.000دج إلى 4000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها»[87].

85 - **عمار عباس الحسيني**، مرجع سابق ، ص ص 152-153.

86 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص 221.

87 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، مرجع سابق.

و نفهم من هذه المادة أن المشرع الجزائري قد عاقب كل شخص أدخل بطريق الغش أو أزال أو عدا معطيات في نظام المعالجة الآلية بالحبس من 6 أشهر إلى 3 سنوات وفرض غرامة مالية قدرها 500.000دج إلى 4000.000دج.

لكن في رأينا هذا لا يعتبر وافيا وكافيا لحماية النظم المعلوماتية، من الاعتداءات الكثيرة والمتزايدة من قبل المتلفين أو المخربين والذين يعتمدون على مناهج وطرق فنية تتطور بتطور النظام المعلوماتي.

المطلب الثالث

جريمة التزوير السيبرياني

لعل من أكثر جرائم نظم المعلومات شيوعا وذيوعا على الإطلاق جريمة التزوير السيبرياني، التي ترتكب سواء على شبكة الانترنيت أو ضمن جرائم الحاسب الآلي، فلا تكاد تخلوا جريمة من الجرائم إلا ويكون من تفاصيلها جريمة تزوير البيانات بشكل أو بآخر[88].

وتعتبر هذه الأخيرة من الجرائم المنصوص على تجريمها في كافة القوانين والتشريعات[89].

وعلى هذا الأساس، يتعين علينا التعرض في مرحلة أولى إلى تعريف جريمة التزوير السيبيرياني (الفرع الأوّل)، ثم ننتقل في مرحلة ثانية إلى بيان أركانها (الفرع الثاني)، لنقف في الأخير عند موقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأول

تعريف جريمة التزوير السيبرياني

تعتبر جريمة التزوير السيبرياني من أخطر أشكال الغش التي تقع على المعلومات نسبة للدور المهم والخطير الذي أضحى يقوم به الحاسب الآلي الآن، والذي دخل شتى المجالات وصارت تجري من خلال كم هائل من العمليات ذات الآثار القانونية المهمة

88 - **حسن طاهر داود**، مرجع سابق ، ص 45.

89 - **منير محمد الجنيهي، ممدوح محمد الجنيهي**، جرائم الانترنيت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي، مصر، 2006، ص 92.

والخطيرة[90].

ولهذا تعرف هذه الجريمة بأنها كل تغير للحقيقة بقصد الغش و محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا، هذا ما أورده الفقه الفرنسي[91].

وما يهمنا في دراستنا هو جريمة التزوير في المجال السيبرياني، وذلك يكون إما بإدخال بيانات خاطئة إلى قواعد البيانات أو بتعديل البيانات الموجودة عمدا بهدف ارتكاب جريمة من جرائم نظم المعلومات، و هذا الفعل لا يشترط معرفة بالبرمجة و لكن يستوجب معرفة بسيطة بطريقة استعمال التطبيق كتطبيقات الحسابات في البنوك[92].

ويمكن تعريف جريمة التزوير السيبرياني أيضا على أنها تغيير حقيقة في مستندات معلوماتية وذلك بهدف استخدامها، بحيث أن التزوير السيبرياني يتضمن إتلاف المعلومات وتحريفها سواء كان ذلك بالإضافة أو المسح أو الحذف، والتزوير هنا يظهر في نسخ الأقراص مدمجة على أقراص أخرى مثلا، أو قد يقع على تزوير بيانات ذلك إثر الدخول بطريقة مشروعة أو غير مشروعة[93].

بالتالي فمن الوسائل والأساليب المتبعة لتزوير بيانات الحاسوب وسيلة تعديل البيانات باستخدام بعض البرامج المعاونة الجاهزة (utilities) التي صممت خصيصا لتعديل البيانات في مواقعها مباشرة (suparzapping)، فهذا الصنف من البرامج خطير، لأنه لا يبقى دليلا يبين التعديل أو القائم به، و بهذا يستوجب تجديد الأشخاص المرخص لهم باستخدام هذه البرامج في نطاق ضيق[94].

90 - **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومه للطباعة النشر والتوزيع، الجزائر، 2007، ص ص 133-134.

91 - **أحمد خليفة الملط**، مرجع سابق ، ص 431.

92 - **حسن طاهرداود**، المرجع السابق، ص 45.

93 - **حفصي عباس**، جرائم التزوير الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الاسلامية، جامعة أحمد بن بله، وهران،2014-2015، ص ص 18-19.

94 - **حسن طاهرداود**، مرجع سابق ، ص 46.

الفرع الثاني

أركان جريمة التزوير

تقوم جريمة التزوير السيبرياني كغيرها من الجرائم إضافة إلى الركن الشرعي على ركنين أساسيين: و هما الركنين المادي (أولاً)، والمعنوي (ثانياً).

أولا- الركن المادي:

يتمثل الركن المادي لهذه الجريمة في النشاط الذي يقوم به الجاني وهو تغيير الحقيقة يرد على محرر، و يكون ذلك بالطرق التي أوردها القانون، بالتالي حدوث الضرر قائم أو متوقع الحصول جراء هذا التغيير[95].

عليه سوف نقوم بتفصيل هذه العناصر كل عنصر على حدى:

أ- تغيير الحقيقة:

إن التزوير في لبه كذب يرد في محرر، بالتالي لم يكن يتوقع حدوث بدون تغيير للحقيقة، لذا فلا تزوير بلا تبديل الحقيقة، حتى و إن نشأ ضرر للغير نتيجة للبيانات الصحيحة، و يكون التبديل المغاير للحقيقة إما كليا أو جزئيا[96]، وبمفهوم آخر، يقصد بتغيير الحقيقة اختلاف حقيقة مخالفة أو تحريف حقيقة قائمة، فأساس تغيير الحقيقة هو التزييف والكذب[97].

وعليه يتصور حدوث التزوير في النطاق السيبرياني بواسطة تبديل الحقيقة على الشرائط والمستندات التي تمثل مخرجات الحاسوب، طالما ن التغيير بحد ذاته مس البيانات الموجودة في الحاسب الآلي، و الذي يظهر في افتراض ارتجاج الثقة في المحررات الرسمية وقت التزوير السيبرياني في المحرر الرسمي[98].

---

95 - **محمد على العريان**، مرجع سابق، ص 163.

96 - **عمار عباس الحسيني**، مرجع سابق، ص 173.

97 - **محمد على العريان**، مرجع سابق، ص 163.

98 - **عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر والانترنيت، دار النهضة العربية، القاهرة، مصر، 2009، ص 202.

ب- المحرر السيبرياني:

يستوجب لوقوع جريمة التزوير السيبرياني أن تكون تغيير الحقيقة واردة على محرر مكتوب أي محرر موجود من الأصل، ولا تهم اللغة التي كتب بها هذا المحرر سواء أكانت وطنية أو أجنبية[99].

أصبح التزوير السيبرياني يمتلك أهمية نسبة لاعتباره من أبرز جرائم تكنولوجيا الحواسيب في عصرنا هذا، حيث أن المشرع الجزائري أورد في المادة 323 مكرر من القانون المدني تعريفا للإثبات بالكتابة على أنها: « ***ينتج الإثبات بالكتابة من تسلسل حروف وأوصاف و أرقام و أي علامات أو رموز ذات معنى مفهوم مهما كانت والوسيلة التي تتضمنها وكذا طرق إرسالها***».

وبصدور القانون 05-10 المعدل و المتمم للقانون المدني الجزائري[100] انتقل المشرع من النظام الورقي في الإثبات إلى النظام الإلكتروني، وهذا ما نصت عليه قواعد الإثبات المدني في القانون الفرنسي التي نصت على قيمة الوثيقة السيبرانية في الإثبات بالكتابة كقاعدة عامة[101].

لذا استوجب الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات في القانون المدني الجزائري وفقا لنص المادة 323 مكرر ق. م. ج، والوسيلة السيبرانية المستعملة هي القرص الصلب أو القرص المرن أو وسائل سيبرانية بالتالي يتبين من خلال هذا الأخير أن المشرع الجزائري اعتمد المفهوم الواسع للكتابة.

والمحرر المعالج آليا هو دعامة مادية تصلح لأن تدون عليها المعلومات و يقصد به في المجال السيبرياني كل شيء مادي متميز (قرص صلب أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، ويستوي بعد ذلك لوقوع و حصول فعل لتغيير الحقيقة على هذا المستند الشكل الذي يكون عليه،

---

99 - **محمد على العريان**، مرجع سابق ، ص 164.

100 - أمر رقم 75-58 ، مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج.ر.ج.ج.د.ش عدد 78 لتاريخ 30 سبتمبر 1975. (معدّل ومتمّم)..

101 - **أحمد حسام طه تمام**، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة ، دار النهضة العربية، القاهرة، مصر، 2000، ص 427.

فيدخل فيه إلى جانب الشرائط و الأقراص الممغنطة المسجل عليها البرامج أو المعطيات أو البطاقات البنكية بصفة عامة والوثائق والخطابات.

وتبعا لذلك لا يصلح أن تكون المستندات غير المعالجة آليا محلاً لهذا النوع من الجريم ، إذ تخرج في ذلك الأوراق المعدة لتسطير المعلومات عليها، والأقراص الممغنطة التي لم يسجل عليها أي شيء، والملاحظات التي تكون على شكل كتب والتعليمات التي تنص على استخدام البرامج وكذا البطاقات البنكية التي لم تدخل في الخدمة لأنها مازالت في مرحلة الإعداد فقط[102].

ج- وسائل و طرق التزوير السيبرياني:

حدد المشرع الجزائري طرق و وسائل جرائم التزوير التقليدية على سبيل الحصر في قانون العقوبات في المواد: 214، 215، 216، و التي تتمثل في:

- وضع إمضاءات أو أختام مزورة.
- تعيير المحررات أو الأختام أو الإمضاءات أو زيادة الكلمات.
- وضع أسماء أو صور أشخاص آخرين مزورة.
- التقليد والاصطناع.

لكن بتقدم التكنولوجيا فقد ظهرت جريمة التزوير السيبيرياني، لذا فإن هذه الطرق لا يمكن أن تكون على سبيل الحصر في هذه الأخيرة، نتيجة لسرعة و تطور و تغير أشكال التكنولوجيا، لهذا لا يستطاع حصر طرق التزوير في المجال السيبرياني، فقد تخلت معظم التشريعات الجنائية على فكرة تحديد طرق التزوير عند التجريم السيبرياني في قانون العقوبات، بالتالي فإن هذا التزوير يقع بأي وسيلة يتم عن طريقها تغيير الحقيقة[103].

د- الضرر:

يعتبر الضرر عنصرا من عناصر الركن المادي لجريمة التزوير السيبرياني، بحيث لا تكتمل هذه الجريمة إلا بحصوله أو احتمال حصوله، لذا و لقيام هذه الأخيرة يجب أن

102 - **حفصي عباس**، مرجع سابق ، ص ص 68-69-70.

103 - المرجع نفسه ، ص ص 40-42.

يؤدي فعل التزوير الذي قام به المجرم إلى وقوع ضرر للغير[104].

ويقصد بالضرر ذلك الأذى الذي يصيب المتضرر في حق من حقوقه أو في مصلحة من مصالحه المشروعة، و يمكن أن يكون الأذى ماديا أي في أموال الشخص أو جسده، وإما يكون معنويا الذي يمس اعتباره و شرفه[105]، أو هو كل إخلال أو احتمال الإخلال بمصلحة يحميها القانون[106].

وعليه في حالة انعدام الضرر لا تقوم جريمة التزوير بطبيعة الحال فالقاضي ملزم بأن يظهر في محكمه توافر عنصر الضرر، و إلا كان هذا الأخير معيبا و بغض النظر عن نوع الضرر ماديا كان و أو أدبيا، عاما أو خاصا، حالا أو محتمل الحدوث.

وقد اعتبر المشرع الجزائري عنصر الضرر من المسائل الموضوعية لا القانونية لذلك فإنه لم ينص عند تعريفه لجريمة التزوير على عنصر الضرر[107].

ثانيا- الركن المعنوي:

يشترط لقيام جريمة التزوير السيبرياني تحقق الركن المعنوي و هو القصد الجنائي، ذلك أن جريمة التزوير من الجرائم العمدية، فلابد من توافر القصد الجنائي العام و هو العلم والإرادة، و كذا القصد الجنائي الخاص الذي يتمثل في نية استعمال المستند السيبرياني المزور و ذلك فيما زور لأجله[108].

أ- القصد الجنائي العام:

يتمثل القصد الجنائي هنا في علم الشخص الجاني بأنه يقوم بتغيير الحقيقة، و ذلك في المستند السيبرياني عن طريق الحاسوب، و يكون على دراية و علم بأن هذا التغيير سيحدث ضررا أو احتمال حدوثه.

104 - **أحمد خليفة الملط**، مرجع سابق ، ص ص 469-470.

105 - **عمار عباس الحسبني**، مرجع سابق ، ص 176.

106 - **محمد علي العريان**، مرجع سابق، ص 142.

107 - **حفصي عباس**، مرجع سابق ، ص 80-81.

108 - **حنان ريحان المبارك المضحكي**، مرجع سابق، ص 215.

ويمكن استخلاص هذا القصد من طبيعة الركن المادي، ذلك أن الجاني يجب أن يكون لع علم بأنه يقوم بتزوير المستندات السيبريانية، غير أنه إذا ثبت أن الشخص لم تكن له معرفة أو علم بأنه يقوم بتزوير هذه الأخيرة فهنا ينتفي القصد الجنائي[109].

ب- القصد الجنائي العام:

يعتبر القصد الجنائي الخاص نية أو الهدف الذي يرمي الجاني إلى تحقيقه من جراء قيامه بالسلوك الإجرامي و المتمثل في تزوير المستند السيبرياني، أي ضرورة ارتباط العلم بنية الشخص المرتكب للجريمة، و التي تتمثل في نية استعمال المستند المزور، وذلك فيما زور لأجله.

وفي حالة تخلف هذه النية ينتفي القصد الجنائي، فلا عبرة بالباعث أو السبب الذي دفع بالجاني إلى ارتكاب جريمة التزوير، فيكفي أن تتوفر لديه نية استعمال المستند المزور[110].

الفرع الثالث

موقف المشرع الجزائري من التزوير السيبيرياني

نلاحظ أن المشرع قد جرم في نص المادة 394 مكرر1 من قانون العقوبات الجزائري كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أي معلومة أو غيرها بتعديل المعطيات، و عاقب على هذه الأفعال بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000ج إلى 4000.000دج.

و على إثر مضمون هذه المادة نفهم أن نشاط الجاني يأخذ شكلين:

1- إدخال معطيات غريبة في نظام المعالجة الآلية، فهذا الإدخال قد يترتب إما جريمة الإتلاف و التخريب المشار إليها سالفا، و إما يترتب جريمة التزوير السيبرياني وهذا بإدخال معلومات أو معطيات جديدة في أنظمة المعالجة الآلية بغاية التزوير.

109 - **حفصي عباس**، مرجع سابق ، ص 78.

110 - **أحمد خليفة الملط**، مرجع سابق ، ص 176.

2- أما الشكل الثاني فهو إفساد و تخريب المعطيات التي يتضمنها أو يحتويها نظام المعالجة الآلية، لذا فالتخريب هنا قد يكون بهدف تعديل أو إزالة معطيات من نظام المعالجة، و هذا بغاية تغيير الحقيقة في محرر أو مستند إلكتروني.

إلا أن هذه المادة يدخل في نطاقها فقط التزوير الواقع على المعطيات الكامنة في نظام المعالجة الآلية، و كذا مستخرجات الحاسوب التي يتجسد فيها شكل المحرر، أما المستخرجات الأخرى ألا و هي الدعامات كالشرائط الممغنطة لا تدخل فيما جرمه المشرع الجزائري في المادة المذكورة أعلاه.

ومجمل القول يمكن اعتبار جريمة لتزوير السيبرياني هو ذلك التلاعب بالمعلومة المحفوظة في جهاز الحاسوب سواء بحذف أو تغيير كل أو بعض المعلومات المنشئة لنظام المعالجة الآلية، أو هي مستخرجات الحاسوب، وكذا المستند المعلوماتي، و من هذا المنبر وجب على المشرع الجزائري تقديم تعريف واسع للمحرر ليشمل كل الوسائل المستحدثة لمواكبة التقدم المعلوماتي الذي يترتب عنه نشوء أفعال جرمية حديثة[111].

المبحث الثاني

الجرائم الواردة على البيانات الشخصية المحفوظة سيبريانيا

من المسائل البالغة الأهمية التي يجدر بنا التطرق إليها هي تحديد نوع الاعتداءات التي يمكن أن تمس بالحياة الخاصة بالأفراد، والتي يمكن عبر الوسط السيبرايني، وتجدر الإشارة أن المخاطر التي تهدد الحياة الخاصة كثيرة ومتعددة أفرزتها مختلف التطورات، التي حدثت بظهور شبكة الانترنيت لذا فقد تتعرض الحياة الخاصة للأفراد إلى اعتداءات تمس بخصوصية البيانات والمعلومات المتعلقة بهم، ولكن قبل الدخول والتعرض إلى ماهية هذه الاعتداءات والجرائم يجب أن نقف عند تعريف البيانات الشخصية أو المعلومات الخاصة بالأفراد، فتعرف هذه الأخيرة على أنها مجموعة معلومات تتعلق بحالة الإنسان المادية، الصحية، الشخصية، و الاجتماعية و غيرها، من أمثلتها اسم الشخص و عنوانه، حالته المادية، وثروته، وضعه الصحي وغير ذلك من البيانات التي يحرص الأفراد على

111 - **بن عقون حمزة**، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2011-2012، ص ص 173.-174، 179.

إحاطتها بنوع من الكتمان والسرية، كذلك أقدمت الدول إلى تنظيمها و تخزينها في بنوك المعلومات، و هي ليست بنوكا كتلك البنوك التقليدية التي تحفظ فيها الأموال النقدية والعينية، وإنما هي بنوكا سيبريانية لتجميع وتخزين البيانات أو المعلومات التي تتعلق بالجوانب المهنية أو العائلية، أو المالية، أو الصحية، أو الوظيفية للأشخاص[112].

لذا فقد تتعرض هذه البيانات إلى اعتداءات خطيرة، و لعل أبرز هذه الأخيرة تتمثل في جريمة المعالجة السيبريانية للبيانات بدون ترخيص (المطلب الأول)، وجريمة جمع وتخزين هذه البيانات بطريق غير مشروع (المطلب الثاني)، وكذا جريمة الإفشاء غير المشروع للبيانات الشخصية (المطلب الثالث).

المطلب الأول

جريمة المعالجة السيبريانية للبيانات الشخصية دون تصريح

تعتبر جريمة المعالجة السيبريانية للمعلومات الشخصية، من الجرائم الواقعة على البيانات الشخصية والخاصة بالأفراد، بذا فكل من يرتكب هذه الجريمة يقوم بالمساس بالحياة الخاصة للأفراد، فإنه يلقى عقوبة ذلك لقيامه بالاعتداء على حرمة الحياة الخاصة للأشخاص عن طريق معالجة البيانات الشخصية دون تصريح.

ولما كان الأمر كذلك فإنه سنقوم بداية بتعريف هذه الجريمة (الفرع الأوّل) ثم نبين أركانها (الفرع الثاني)، لنبرز أخيراً موقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأول

تعريف المعالجة السيبريانية للبيانات الشخصية دون تصريح

يمكن تعريف هذه الجريمة على أنها الفعل الذي يقوم به الجاني، و ذلك بجمع البيانات الشخصية، سواء كانت بشكل مشروع أو غير مشروع، وتخزينها في ذاكرة الحاسوب، وذلك قبل أو بعد تحليل البيانات الشخصية والاحتفاظ بها، دون اتخاذ

112 - **PRADEL Jean**, « Les infractions relatives à l'informatique », *R.I.D.C*, vol 42, n°42, 1990, p.817.

الإجراءات التي يحددها القانون[113].

الفرع الثاني

أركان جريمة المعالجة السيبريانية للبيانات الشخصية

يتعين لقيام هذه الجريمة توافر ركنين أساسيين[114]، أولهما الركن المادي الذي يتمثل في المعالجة السيبريانية للبيانات الشخصية دون مراعاة الإجراءات الأولية التي يتطلبها القانون (أولاً)، وثانيهما الركن المعنوي المتمثل في القصد الجنائي (ثانياً).

أولا- الركن المادي:

يتمثل السلوك المادي لهذه الجريمة بأية معالجة للبيانات الشخصية دون اتخاذ الإجراءات الأولية التي يستلزمها القانون، و تتمثل هذه المعالجة في جمع البيانات وتسجيلها أو تحليلها أو تعديلها أو تصنيفها ثم حفظها أو محوها، وتتحقق أفعال هذه الأخيرة إما في شكل إدخال البيانات أو تصنيفها أو توزيعها أو دمجها مع بيانات أخرى، أو تحليلها كي تقدم معلومة معينة ذات معنى خاص أو استرجاع البيانات الشخصية، بالتالي هذه الجريمة تنشأ بمجرد مباشرة الشخص بفعل المعالجة على البيانات الشخصية، أنشطة المعالجة في الأحوال التي لم يمنح له فيها ترخيص بذلك، من طرف الجهة المختصة، و تنشأ أيضا في الأحوال التي يلغى فيها الترخيص أو نفاذ مدته، ولكن أفعال المعالجة تبقى قائمة[115].

ثانيا- الركن المعنوي:

تتخذ هذه الجريمة في ركنها المعنوي صورة العمد أو الخطأ، فيثبت القصد الجنائي العام بعلم الشخص الجاني بالصفة الشخصية للبيانات، و كذا أن يعلم بأن من طبيعة الحاسوب والمتصل بشبكة الانترنيت إجراء معالجة سيبريانية للبيانات دون مراعاة الإجراءات المنصوص عليها في القانون.

---

113 - عمار عباس الحسيني، المرجع السابق، ص 238..

114 - غني عن البيان بأنّه يجب أن يتوفر في كل جريمة الركن الشرعي المتمثل في وجود نص قانوني يجرم الفعل.

115 - **عمارعباس الحسيني**، مرجع سابق، ص ص 238-239.

و يتعين كذلك أن تتجه إرادة الجاني إلى إجراء المعالجة السيبريانية مهما كان شكل هذه الأخيرة وفي مختلف صورها، و بغض النظر عن الإجراءات اللازم اتخاذها قبل القيام بالمعالجة.و تجدر الإشارة أنه لا عبرة بالدوافع والبواعث التي دفعت لارتكاب سلوكه الإجرامي أو فعله.

أما بالنسبة للخطأ في هذه الجريمة فقد اختلف الفقه بشأنه، فهناك من يرى أن الخطأ يمكن تصوره في هذه الجريمة كما هو الحال في الإهمال، لكن الجانب الآخر من الفقه يرى أن هذه الجريمة من الجرائم العمدية فحسب[116].

الفرع الثالث

موقف المشرع الجزائري من المعالجة السيبيريانية للبيانات الشخصية

جرم المشرع الجزائري الاعتداءات الواقعة على البيانات الشخصية المخزنة سيبريانيا من خلال قانون العقوبات الجزائري في المادة 394 مكرر2 من القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال، و التي تنص على: « يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000دج إلى 10.000.000دج كل من يقوم عمدا و عن طريق الغش بما يأتي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن و ترتكب بها الجرائم المنصوص عليها في هذا القسم.
2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم»[117].

116 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص 89.

117 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، مرجع سابق.

المطلب الثاني

جريمة الجمع و التخزين غير المشروع للبيانات الشخصية

لقد اتسع على نحو كبير استخدام الحواسيب لجمع وتخزين البيانات الشخصية أو الاسمية لأغراض متعددة فيما يعرف ببنوك ومراكز معلومات الوطنية، ومع ايجابيات استخدام الحواسيب في هذا المجال ظهر كذلك الشعور بسلبياتها و مخاطرها، نظرا لأن عملية الجمع والتخزين تعد في حد ذاتها جريمة إذا كانت قد اتخذت صورة غير مشروعة.

لذلك سنحاول تعريف الجريمة (الفرع الأول)، وتبيان أركانها (الفرع الثاني)، وإبراز موقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأول

تعريف جريمة الجمع والتخزين غير المشروع للبيانات الشخصية

أطلقت عدة تسميات على هذه الجريمة فهناك من سماها بجريمة التسجيل و الحفظ غير المشروع، ومنهم من سماها وأطلقوا عليها تعبير المعالجة غير المشروعة، وبعض النظر عن هذه التعابير والأوصاف المختلفة لهذه الجريمة فالمقصود من جميع هذه الأفعال من جمع أو تسجيل أو حفظ، تخزين، معالجة هي أفعال تتم في مجال الأنشطة المتعلقة بالمعالجة الآلية للبيانات الشخصية في نظم أو بنك المعلومات. ومثال ذلك أن يتولى شخص مكلف بجمع و تجميع البيانات أو المعلومات التي تخص شخص آخر، فيقوم بالإطلاع عليها دون إذن صاحبها[118].

وكما تجدر الإشارة أن فعل الحفظ و التخزين يستمد صفته الغير مشروعة إما من الأساليب المستخدمة للحصول على هذه البيانات أو من مضمون و طبيعة هذه البيانات، كما و يعتبر فعل الجمع و التخزين الغير المشروع انتهاكا للحياة الخاصة للأفراد[119].

---

118 - **خالد ممدوح 'براهيم**، الجرائم المعلوماتية، مرجع سابق ، ص ص 124-125.

119 - **محمد عبد الله أبو بكر السلامة**، جرائم الكمبيوتر والانترنيت، منشأة المعارف، الإسكندرية، مصر، 2006، ص108.

فالبيانات والمعلومات الشخصية التي ترتبط بالحياة الخاصة للأفراد لا يسمح أو يحظر تجميعها و تخزينها أو معالجتها داخل الحاسوب[120].

وعليه فيتمثل محل أو موضوع هذه الجريمة في المعلومات الشخصية فتعرف هذه الأخيرة على أنها تلك المعلومات الخاصة و المتعلقة بحالة الفرد الصحية أو المالية أو الوظيفية، و بالتالي فإن الحماية تمتد لتشمل جميع البيانات التي تستوجب طبيعتها عدم جمعها و تخزينها باستثناء بعض الجهات التي يسمح لها بجمع هذه المعلومات.

الفرع الثاني

أركان جريمة الجمع والتخزين غير المشروع للبيانات الشخصية

إن جريمة جمع وتخزين غير المشروع للبيانات الشخصية تعتبر كباقي الجرائم الأخرى وبالتالي يتطلب لقيامها ركنين مهمين وهما: الركن المادي والذي يتمثل في السلوك الإجرامي(أولاً) ، والركن المعنوي المتمثل في القصد الجنائي (ثانياً).

أولا- الركن المادي:

يتمثل الركن المادي هنا في السلوك الإجرامي والذي يتجسد في فعل الجمع والتخزين على نحو غير مشروع[121]، وتتحقق عدم المشروعية إما في الطرق والأساليب الغير مشروعة المستخدمة للحصول على هذه البيانات، أو من حيث مضمون و طبيعة هذه البيانات التي منع القانون تخزينها[122].

أ- استخدام الأساليب الغير المشروعة للحصول على البيانات الشخصية:

يعتمد الحصول على المعلومات و البيانات الشخصية على عدة أساليب وبالتالي يكون كذلك بطريقة غير مشروعة إما بواسطة الغش أو التدليس، ومن ضمن هذه الأساليب والطرق نذكر التقاط الارتجاجات والتي تسببها الأصوات في الجدران الإسمنتية للغرف و ترجمتها باستخدام الحاسب الآلي و الذي يكون مزود ببرنامج خاص، أو بواسطة مراقبة

120 - **نهلا عبد القادر المومني**، الجرائم المعلوماتية ، دار الثقافة للنسر والتوزيع، عمان، الأدرن، 2008، ص 175.

121 - المرجع نفسه، ص 126.

122 - **عمار عباس الحسيني**، مرجع سابق ، ص 241.

واعتراض أو التقاط الرسائل التي يتم مبادلتها عبر البريد الإلكتروني، أو باستعمال أسلوب آخر و الذي يتمثل في توصيل أسلاك بطريقة خفية إلى الحاسوب الطي يتضمن البيانات الشخصية، ومما لا شك فيه أن الزيادة في استعمال شبكات المعلومات والبريد الإلكتروني سيؤدي إلى زيادة في استخدام الأساليب الغير المشروعة[123].

ب- طبيعة و مضمون البيانات التي يتم جمعها أو تخزينها:

تتمثل طبيعة هذه البيانات في أن تكون غير صالحة للجمع أو التخزين و ذلك لسبب راجع لمضمونها، فقد منع القانون المعالجة الآلية لهذه البيانات دون وجود موافقة أو تصريح مؤكد متى كانت هذه المعلومات تبين بطريقة مباشرة أو غير مباشرة الأفكار الدينية أو السياسية، الأخلاقية الشخصية، أو الانتماءات، وهذا في غير الحالات التي أوردها لقانون.

ولكن في الحقيقة تعيين من له الحق في تخزين المعلومات و جمعها و تحديد نوعية هذه المعلومات يشكل من أهم الصعوبات و الإشكاليات التي تواجه الحياة الخاصة في مجال السيبريانية[124].

وبمعنى آخر تضفي صفة عدم المشروعية على جمع وتخزين البيانات أي أن تكون هذه الأخيرة غير صالحة للجمع و التخزين بسبب مضمونها.

وواقعيا فإن عدم وجود ضوابط قانونية في هذا المجال قد يؤدي إلى إمكانية جمع وتخزين ونقل كم هائل من المعلومات التي ترتبط بأدق التفاصيل الخاصة بالأفراد[125].

ثانيا- الركن المعنوي:

تعتبر جريمة جمع و تخزين البيانات الشخصية من الجرائم العمدية التي يجب أن يتخذ فيها الركن المعنوي القصد الجنائي العام و الذي يتمثل في العلم و الإرادة بحيث يجب على المجرم أن يكون عالما بان البيانات التي يقوم بحفظها هي معلومات شخصية تتعلق بشخص معين، و يستلزم عليه أن يكون عالما كذلك بعدم مشروعية أفعال المعالجة تلك،

123 - **محمد عبد الله أبو بكر السلامة**، مرجع سابق ، ص 108.

124 - المرجع نفسه، ص 108-109.

125 - **نهلا عبد القادر المومني**، مرجع سابق ، ص ص 174-175.

ومن جانب آخر يستلزم أن تتجه إرادته إلى تخزين أو معالجة هذه البيانات مخالفا بذلك القيد أو الحظر الذي أدرجه أو أورده القانون.

أما القصد الجنائي الخاص فيغيب في هذه الجريمة ذلك أنه لا عبرة بالدوافع أو البواعث التي أرغمت أو دفعت بالمجرم إلى فعل أو القيام بهذه الجريمة، سواء أكان الدافع الحصول على فائدة مادية أو دفع ضرر عنه، أو حتى تحقيق مصلحة للغير[126].

الفرع الثالث

موقف المشرع الجزائري من جريمة الجمع والتخزين غير المشروع للبيانات الشخصية

أشار المشرع الجزائري للاعتداءات الواقعة على البيانات الشخصية المخزنة سيبريانيا في قانون العقوبات الجزائري وذلك في المادة 394 مكرر2 من القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال، و التي تنص على: « يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000دج إلى 10.000.000دج كل من يقوم عمدا و عن طريق الغش بما يأتي:

3- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن و ترتكب بها الجرائم المنصوص عليها في هذا القسم.»[127].

يُستنتج من خلال هذه المادة أن المشرع الجزائري قد جرم أعمال تصميم أو بحث أو تجميع المعطيات مختزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية عن طريق الغش أو بطريقة غير مشروعة.

المطلب الثالث

جريمة الإفشاء غير المشروع للبيانات الشخصية

على الرغم من تعدد بنوك المعلومات و كثرة المعلومات و البيانات المخزنة، غير أن تلك

126 - **عمار عباس الحسيني**، مرجع سابق، ص 241.

127 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، مرجع سابق.

البيانات تحظى بحرمة وبقدوسية كباقي صور الخصوصية، فقد تشمل أسرار الأفراد الشخصية أو أوضاعهم الذاتية في مختلف الاتجاهات و المجالات، والحفاظ عليها من العلن مهمة ذات طابع إنساني وأخلاقي، و في حالة تعرضها للإفشاء فإنه يعاقب الشخص الذي ارتكب هذا الفعل المشين.

وبهذا سنتعرض إلى تعريف هذه الجريمة (الفرع الأول)، وأركان هذه الأخيرة (الفرع الثاني)، وإبراز موقف المشرع الجزائري أخيراً (الفرع الثالث).

الفرع الأول

تعريف جريمة الإفشاء الغير المشروع للبيانات الشخصية

من المبادئ الأساسية أنّ تخزين البيانات لا يعني أن هذه الأخيرة قد انتقلت من الخصوصية إلى العلانية، كما أن الموافقة على التخزين لا يقصد به الحرية في تداول هذه البيانات و نقلها، وبالتالي ففعل الإفشاء يشكل في حد ذاته جريمة معاقب عليها[128].

ويعرف فعل أو سلوك الإفشاء على أنه تداول المعلومات الشخصية أو الاسمية من طرف شخص مسموح له بتخزين و حفظ المعلومات أو معالجتها إلى خص أو جهة أخرى غير مسموح لها بالاطلاع على هذه المعلومات، و لذا لا يدخل ضمن هذا الفعل اختراق هذه الأخيرة من قبل جهة مختصة قانونا لتخزينها، لأن هذا السلوك يدخل ضمن جريمة أخرى، وعليه فإنه يجرم كل فعل يرتكبه الشخص من شأنه الكشف عن البيانات الشخصية و ذلك بمناسبة تسجيل أو تقل أو أي شكل من أشكال معالجة تلك البيانات الشخصية الاعتبارية لصاحب الشأن أو حرمة حياته الخاصة في هذه المعلومات[129].

وتجدر الإشارة إلى أنه هناك اختلاف بين جريمة الإفشاء الغير المشروع للبيانات الشخصية وبين جريمة إفشاء الأسرار العادية، و تتمثل أبرز أوجه التباين بينهما فيما يلي:

- أن موضوع جريمة إفشاء الأسرار العادية هي معلومات ذات طبيعة سرية لكن جريمة إفشاء المعلومات الشخصية موضوعها تلك البيانات التي تم تخزينها وتسجيلها في

128 - **نهلا عبد القادر المومني**، مرجع سابق ، ص 177.

129 - **بولين أنطونيوس أيوب**، الحماية القانونية للحياة الشخصية في المجال المعلوماتية، دراسة مقارنة، د.ب.ن، 2009، ص 104.

النظام المعلوماتي.

– الركن المادي في جريمة إفشاء الأسرار العادية لا تحتاج إلى تحقيق الضرر لكن الضرر مطلوب أو لازم لقيام جريمة إفشاء البيانات الشخصية.

– عدم إمكانية تصور حدوث جريمة إفشاء الأسرار العادية عن طريق الخطأ غير أنه يمكن أن تحدث جريمة إفشاء البيانات الشخصية إلى أثر الخطأ.

الفرع الثاني

أركان جريمة الإفشاء غير المشروع للبيانات الشخصية

إن هذه الجرائم وكغيرها من الجرائم الأخرى تقتضي وجود وكنين أساسيين لقيامها هما الركن المادي (أولاً) والمعنوي (ثانياً).

أولا- الركن المادي:

يتجسد السلوك أو النشاط المادي لهذه الجريمة بتوفر صورتين و هما:

أ- **الصورة الأولى**: تتمثل في تلقي أو حيازة البيانات و المعلومات الشخصية والاسمية مهما كان القصد من حيازتها سواء بغاية نقلها أو معالجتها أو تخزينها أو حفظها بأي شكل من الأشكال، و بالتالي يجب أن تثبت أو تتحقق واقعة حيازة الشخص للمعلومات الاسمية أو الشخصية حتى يستطيع القيام بتصنيفها أو حفظها.

ب- **الصورة الثانية:** تتحقق هذه الصورة بقيام الجاني بإفشاء المعلومات الشخصية إلى شخص آخر لا يحق له الاطلاع عليها، وبالتالي إذا كان إفشاء البيانات إلى جهة يحق لها أو يجوز لها الاطلاع على هذه الأخيرة فهنا ينتفي السلوك الإجرامي في هذه الجريمة[130].

و يستوجب لقيام الركن المادي لهذه الجريمة توافر ثلاث شروط و هي:

1. أن يسبب فعل الإفشاء ضررا بالمجني عليه صاحب البيانات طلك لارتباط فغل الإفشاء بالاعتداء على شرف الشخص و خصوصية حياته الشخصية.

130 - **آدم عبد البديع حسين**، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة القاهرة، 2000، ص 581.

2. أن يكون هذا الإفشاء دون علم ورضا المجني عليه وبالتالي لا يمكن أن تقوم هذه الجريمة إذا ثبت رضا الشخص المهني بالأمر بهذا الإفشاء.
3. أن يتم فعل الإفشاء قد وجه لشخص ليس له الحق في الاطلاع على هذه المعلومات الخاصة و الشخصية[131].

ثانيا- الركن المعنوي:

بالنسبة لركن المعنوي فهو القصد الجنائي في هذه الجريمة، ويظهر في صورتيه العمد والخطأ، بحيث يتمثل عنصر العد بتوافر القصد الجنائي العام والذي يقوم بوجود العلم والإرادة، فيجب على الجاني أن يكون على علم بأنه يقوم بفعل الإفشاء الغير المشروع للبيانات الشخصية، الذي يمثل اعتداء على الشرف وعلى حرمة الحياة الخاصة للأفراد، ويتطلب كذلك اتجاه إرادته إلى إتيان هذا الفعل.

أمّا عنصر الخطأ فيتحقق إذا كان فعل الإفشاء قد وقع نتيجة الإهمال أو التساهل أو رعونة و قلة انتباه و احتياط، أو عدم إعطاء هذه البيانات قدرا من الأهمية، مما يؤدي إلى تسريبها و إفشائها[132].

الفرع الثالث

موقف المشرع الجزائري من جريمة الإفشاء غير المشروع للبيانات الشخصية

تعرض المشرع الجزائري للاعتداءات الواقعة على البيانات الشخصية المخزنة سيبريانيا من خلال قانون العقوبات الجزائري في المادة 394 مكرر2 من القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال، و التي تنص على: « يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000دج إلى 10.000.000دج كل من يقوم عمدا و عن طريق الغش بما يأتي:

131 - **محمد أمين أحمد الشوابكة**، مرجع سابق ، ص 102.

132 - المرجع نفسه، ص 104.

4- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن و ترتكب بها الجرائم المنصوص عليها في هذا القسم.

5- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم»[133].

بالتالي من نص هذه المادة نستنتج أن المشرع الجزائري قد جرم أعمال تصميم أو بحث أو تجميع أو توفير أو نشر أو الإيجار في المعطيات مختزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية مكن أن ترتكب بها إحدى جرائم الغش المعلوماتي، كما جرم أيضا أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من النشر المعلوماتي، ونص بمعاقبة مرتكبيها و ذلك بالحبس من شهرين إلى ثلاث سنوات وبغرامة مالية[134]

133 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل ومتمم، مرجع سابق.

134 - **بن تواتي خليل**، جرائم المساس بالأنظمة المعلوماتية، مذكرة ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2017/2016، ص 47.

الفصل الثاني

جرائم الاعتداء بواسطة النظام المعلوماتي

بعد أن عالجنا في الفصل الأوّل جرائم الاعتداء على النظام المعلوماتي، و المتمثلة في جريمة السرقة. التزوير، و الإتلاف، و الجرائم الواردة على البيانات الشخصية المخزنة سيبريانيا، فإننا سنتطرق في هذا الفصل إلى الصنف الثاني من الجرائم السيبرياينة وهي تلك الواقعة بواسطة النظام المعلوماتي.

فالعديد والكثير من الأفعال الجرمية ترتكب عن طريق الاستعانة بنظم الحاسوب ومكوناته، و بصفة خاصة شبكة الانترنيت، و الحاسوب في هذه الجرائم يكون بمثابة الأداة في يد المجرم، يستعملها كيفما أراد لتحقيق العديد من الأهداف والغايات الجرمية الغير مشروعة والمعاقب عليها قانونا، و من ثم فإن الإجرام السيبرياني لا يكون حاصلاً في تلك الحالات على الحاسوب أو أحد مكوناته، وإنما يقع بتلك النظم والشبكات بغرض إتمام العديد من المبتغيات الإجرامية، وبمعنى آخر إن النظام المعلوماتي هي الوسيلة والأداة الأساسية لارتكابها.

ومن الصعب حصر جميع الجرائم السيبريانية التي قد تقع تحت هذه الطائفة إلا أننا سنتناول بعض وأهم وأخطر صور هذه الجرائم، ولعل أبرزها هي الجرائم الماسة بالاعتبار و الآداب العامة، فهي من الجرائم الواقعة على الأشخاص، بحيث تؤثر على الآداب العامة للمجتمع و ذلك يمس شرفهم و كرامتهم و تشويه سمعتهم أمام الغير، وكذا بنشر الفسق والرذيلة بإنشاء مواقع مخصصة لذلك، ترمي لهدم مكارم الأخلاق والمبادئ المؤسسة للمجتمعات (المبحث الأوّل).

وكذا الجرائم الماسة بأمن الدولة، التي تعدّ أخطر الأفعال الجرمية والاعتداءات الواقعة بواسطة النظام المعلوماتي، فهذه الأخيرة تقترف ضد الدولة بصفتها شخصا من أشخاص القانون العام الداخلي أو شخصاً من أشخاص القانون الدولي العام، لذا فالأفعال الإجرامية المرتكبة تحت طائلتها ترمي إلى هدم البنية التحتية للدولة من خلال أفعال الإرهاب و التجسس السيبرياني (المبحث الثانّي).

المبحث الأوّل

الجرائم الماسة بالاعتبار والآداب العامة

عرف عالمنا في الآونة الأخيرة تطورا بارزا في مجال تكنولوجيا المعلومات، بحيث أثر سلبيا عليه، بإنتاجه لجرائم مستحدثة، وفريدة من نوعها، تتباين عن مثيلاتها التقليدية، و ذلك في طرق و وسائل أو موضوع ارتكابها.

ومن الجرائم التي أفرزها هذا التقدم الجرائم الماسة باعتبار الأشخاص و المخلة بالآداب العامة، ويقصد بالاعتبار المكانة التي يحتلها كل فرد سواء في المجتمع، هذا من الجهة الموضوعية، أما من الجهة الشخصية هو إحساس كل فرد بكرامة العيش كغيره من أفراد المجتمع، وذلك من خلال الاحترام المتبادل بينه و بين الآخرين، بشرط عدم المبالغة أو التقليل من ذلك الشعور أو الإحساس كي لا ينعكس عليه سلبا.

من بين الجرائم الماسة بشرف واعتبار الشخص، جريمتي القذف (المطلب الأوّل) والسب (المطلب الثانّي) اللتان تتجسدان في توجيه عبارات وإشاعات كاذبة، و ألفاظ مشينة غايتها النيل من شرف الغير و كرامته و اعتباره، و تعرضه لازدراء الناس والنفور منه، لما تم إسناده إليه من الجاني.

أما الآداب العامة فيقصد بها مجموعة القواعد والنظم والتقاليد السائدة التي تحكم السلوك السوي أخلاقيا في مجتمع معين وفي وقت معين فالآداب العامة ليست أمرا ثابتا في سائر المجتمعات فهو يحتم على جميع أفراده احترام قواعده و يعاقب كل من يخالفها بالاحتقار و الاستنكار، و الإخلال بهذه الآداب يشكل و ينتج لنا عدة جرائم من بينها جريمة التحريض الجنسي المعلوماتي، الذي وجدت غايتها في المجال الكوني الرقمي للشبكة العنكبوتية، بحيث يقوم الجاني باستغلال التقدم الحاصل في البيئة السيبريانية، وذلك بترويج حالات الفساد الأخلاقي، المتمثلة في نشر العديد من الصور الفاضحة والأفعال الفاحشة أو إنشاء مواقع تحت ممارسة الجنس، سواء أكانت موجهة إلى كل الأشخاص عامة أو إلى فئة منهم كالقصر، و هي الفئة الحساسة أكثر عرضة لهذه الأفعال (المطلب الثالث).

المطلب الأول

جريمة القذف السيبرياني

تعد جريمة القذف من الجرائم التقليدية المنصوص عليها في أغلب النصوص العقابية، لما لها من أثر سلبي على ذات الإنسان ذلك لأنها تنال من شرفه و اعتباره، وكرامته و تعرضه لبغض الناس واحتقارهم و قد صارت في وقتنا الراهن ومع تقدم التكنولوجيا ووسائل الاتصال تتم عبر وسائل وطرق مستحدثة منها شبكة الانترنيت والحاسوب.

ولما كانت هذه الجريمة من أكثر الجرائم انتشارا ارتئينا إلقاء الضوء عليها وذلك من خلال تعريفها (الفرع الأوّل)، وبيان أركانها (الفرع الثاني)، وتحديد موقف المشرع الجزائري منها (الفرع الثالث).

الفرع الأول

تعريف جريمة القذف السيبرياني

يعتبر القذف من أبرز وأكثر الجرائم شيوعا وانتشارا في نطلق الشبكة العنكبوتية[135]. فغالبا ما يقوم بالقذف أشخاص ضعفاء النفوس، فيعملون على التشهير بأصدقائهم وزملائهم و أرباب عملهم، أو حتى الزعماء السياسيين للبلدان، ومن مبتغياتهم التشفي وحب البروز و جذب الأنظار[136].

وعليه يعرف القذف على أنه إسناد حادثة أو واقعة معينة تستلزم عقاب أو احتقار من أسندت إليه، و الإسناد يقصد به « نسبة أمر أو حادثة إلى شخص محدد بإحدى الوسائل المعلوماتية»[137].

أما في تعريفه التشريعي، فلم نلقى مفهومه في الشكل السيبرياني أو المعلوماتي هذا ما قادنا إلى العودة لتعريفات القذف بشكله التقليدي، و قد أوردت المادة 296 من قانون العقوبات الجزائري تعريفا للقذف و ذلك بنصها على ما يلي:

135 - **خالد ممدوح إبراهيم**، أمن الجريمة الإلكترونية، مرجع سابق، ص 71.

136 - **محمد أمين الرومي**، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، مصر، 2004، ص 133.

137 - **محمد عبد الله أوبكر السلامة**، مرجع سابق، ص 196.

« يعد قذفاً كل ادعاء بواقعة من شأنها المساس بشرف و اعتبار الأشخاص أو الهيئة المدعى عليها به، أو إسناد إليهم أو إلى تلك الهيئة، و يعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى و لو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم، و لكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة ».

فيستخلص من نص المادة أم القذف هو أي ادعاء و افتراء بواقعة من شأنها خدش شرف و كرامة الشخص أو الهيئات المدعى عليها، و ذلك باستعمال أية طريقة من طرق العلن، فقد ميز المشرع بين صنفين تتحقق بهم العلانية و هما:

-الصنف الأول: العلانية بواسطة الكلام أو الصياح.
-الصنف الثاني: العلانية بواسطة الكتابة أو المنشورات أو اللافتات أو الإعلانات.

لذا فتعد هذه الجريمة إظهارا لسلبيات الشخص المستهدف، أو تشييعا لأسراره التي قد يتم الحصول عليها بطريقة أو وسيلة غير مشروعة و ذلك بعد الاطلاع على جهازه، أو القيام بنشر الأخبار عنه[138]، وذلك إما قوليا كما هو الأصل في الجرائم التقليدية أو كتابيا[139]، أو وجاهيا عن طريق حظوظ عن طريق الاتصال المباشر، أي بواسطة المبادلات المعلوماتية الصوتية، أو غيابيا عبر المبادلات الإلكترونية الكتابية أو الفديوهية، و هي إما تكون بين طرفيات انترنيت مرتبطة، و إما غير مرتبطة[140].

الفرع الثاني

أركان جريمة القذف السيبرياني

في حقيقة الأمر أن التشريع الجزائري ونخص بالذكر قانون العقوبات لم يورد نصوص قانونية تعالج القذف السيبرياني، لكن هذه لا يمنع من إمكانية تطبيق عليه النصوص الخاصة بجريمة القذف التقليدية، بما فيها تعريف هذه الجريمة و أركانها، وطرق و آليات التصدي لها.

138 - **بن مكي نجاة**، مرجع سابق، ص 57.
139 - **حنان ريحان مبارك المضحكي**، مرجع سابق، ص 317.
140 - **هروال هبة نبيلة**، مرجع سابق ، ص 82.

فمن هنا فإنّ قيام هذه الجريمة يتطلب توافر ركنين أساسيين وهما الركن المادي و الذي يتمثل في فعل و محل و علانية الإسناد (أولا)، المعنوي المتجسد في القصد الجنائي بصورتيه (ثانيا)

أولا-الركن المادي:

يتمحور الركن المادي لجريمة القذف، إما بشكله التقليدي أو السيبرياني في ثلاث عناصر و هي: فعل الاسناد (أ)، ومحل الإسناد (ب)، والعلنية (ج).

أ- **فعل الإسناد:**

يقصد به نسبة شأن أو حادثة إلى شخص معين و بكل و شتى الرسائل التي تعبر عن المعنى المراد إيصاله[141]. لذا يتجسد في إسناد واقعة معينة أو أمر ما إلى شخص محدد، إما أن يكون هذا الأخير شخص طبيعيا أو معنويا، أو ليس له شخصية قانونية كالهيئات مثلا و هذا بأية طريقة من طرف طرق التعبير عن المقصود أو المعنى، كتابة أو إشارة، أو قولا، و يثبت الإسناد على وجه الشك أو القطع.

وفي هذا المنبر يجب التنويه إلى أن هذا الشرط في القانون الجزائري يتوافر بالإسناد أو الإخبار، بمعنى آخر أن المشرع الجزائري اتبع نهج باقي المشرعين كالمصري و الفرنسي و الأردني...، فلم يميزوا بين الإسناد الذي يدل على نسبة الواقعة إلى الشخص المقذوف على وجه التأكيد، و بين الإخبار الذي يفيد معنى الحكاية عن فم الغير أو تبين الخبر المحتمل الصدق والكذب، وإنما ألموا بالعقاب كل صور التعبير التي من أمرها أن تهدم شرف واعتبار الأشخاص أو الهيئات المدعى عليها به، حتى وإن كان ذلك بوسيلة تدل على الشك والغموض، أو سواء كان حضوريا أو غيابيا، بشتى الوسائل قولية كانت أو كتابية، أو بالإشارة[142].

ب-محل الإسناد:

إضافة إلى العنصر الأول المذكور سابقا المتضمن إسناد أمر غير لائق إلى الغير، فيستلزم أن يكون هذا الشأن أو الأمر محددا أو معينا، فيجب أن تتحدد الواقعة وتجعل

141 - **محمد عبد الله أبو بكر السلامة**، مرجع سابق، ص 169.

142 - **هروال هبة نبيلة**، مرجع سابق، ص ص 77-78.

من أسندت إليه موضوعا للعقاب وفقا للقانون أو موضوعا للاحتقار من جانب أهل بلده أو من يعاشرهم، أو أن تكون مخلة وماسة بعرض وسمعة الشخص أو أحد أفراد عائلته أو أقربائه[143].

لذا يعتبر قاذفا من يسند إلى غيره أنه مثلا قد أزنى بامرأة، أو أنه سرق مالا من شخص معين، أو قام بالاحتيال عليه، فهذا ما يميز القذف عن السب ذلك أن في تعيين الواقعة يجعلها أقرب إلى التصديق، فخلو الإسناد من هذا التحديد للحادثة يعد سببا وليس بقذف[144].

جـ- العلانية في الإسناد:

تعتبر العلانية أهم عنصر في جريمة القذف، فيقصد بالعلانية اتصال معرفة الأشخاص بالتعبير الوارد عن فكرة المتهوم أو شعوره و إحساسا هاو رأيه بواسطة إحدى الطرق والوسائل التعبيرية التي تتمثل في:

-الصياح أو القول إذا حصل الجهرية أو ترديده في أماكن عامة أو مباحة.
-الأعمال أو الإشارات أو الحركات إذا وقعت في طريق عام أو في محفل أو معرض لأنظار الناس.
-الكتابة و الرسوم و الصور و الإشارات الأفلام و غيرها إذا عرضت في مكان عام، أو إذا وزعت أو بيعت إلى أكثر من شخص، أو عرضت للبيع في أي مكان سواء عام أو خاص[145].

ثانيا-الركن المعنوي:

بما أن جريمة القذف السيبرياني جريمة عمدية فيتطلب لقيامها ثبوت القصد الجنائي بصورتين العام و الخاص، و المتمثل في العلم و الإرادة، فيستلزم أن يعلم الجاني أن الواقعة التي يسندها أو ينسبها إلى المجني عليه تكون موضوعا للعقاب والازدراء من طرف أهله وناسه.

143 - **هروال هبة**، مرجع سابق ، ص 78.
144 - **عمارعباس الحسيني**، مرجع سابق ، ص 383.
145 - **هروال هبة**، مرجع سابق ، ص ص 78-79..

أما صورة الإرادة فتتجسد في إرادة الجاني في نشر و إذاعة البيانات أو الوقائع التي تتضمن القذف، أما إذا ثبت أن الجاني كان مكره على ذلك فلا يكون القصد الجنائي لديه، وكذل في نفس الوضع إذا كانت تلك العبارات قد خرجت نتيجة زلة لسان أو نتيجة جهل اللغة، أو صدور عبارات سالفة أو آتية تنفي المفهوم المستنتج من ألفاظ القذف[146].

الفرع الثالث

موقف المشرع الجزائري من جريمة القذف السيبيريانية

تنص المادة 144 مكرر من قانون العقوبات إمكانية وقوع جريمة القذف السيبرياني لما تكون موجهة لرئيس الجمهورية إذا تمت بأية وسيلة إلكترونية أو معلوماتية أو أية آلية لبث الصوت أو الصورة، و هذا بنصها على ما يلي:

« يعاقب بغرامة من 100.000دج إلى 500.000دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت و الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى...» [147].

يتضح من خلال نص هذه المادة أن المشرع الجزائري قد جرم فعل القذف الموجه لرئيس الجمهورية، و الذي يتم بصورة معلوماتية أي سيبريانية أو إلكترونية، فهذا الأمر يفسر اعتراف المشرع بجريمة القذف السيبرياني هذا ما نفهمه من العبارات الواردة في نص المادة أعلاه.

أما بخصوص العقوبة المقررة لجريمة القذف السيبرياني عامة فنجد أن المشرع الجزائري لم يضع لها نصوص خاصة، لكن خذا لا يمنعنا من إمكانية تطبيق غليها النصوص التقليدية لجريمة القذف، بحيث نصت المادة 298 من قانون العقوبات على:

« يعاقب على القذف الموجه إلى الأفراد بالحبس من شهرين إلى ستة أشهر وبغرامة من 25.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين.

---

146 - **محمود نجيب حسني**، شرح قانون العقوبات- القسم الخاص- جرائم الإعتداء على الأشخاص ، دار النهضة العربية، مصر، 1978، ص ص 566-567.

147 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل ومتمم، مرجع سابق.

و يضع صفح الضحية حدا للمتابعة الجزائية.

ويعاقب على القذف الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من شهر إلى سنة وبغرامة من 20.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين فقط إذا كان الغرض هو التحريض على الكراهية بين المواطنين أو السكان».

نستخلص من هذه المادة أن العقوبة المقررة لجريمة القذف تختلف حسب ما إذا كانت موجهة إلى أفراد عاديين، أو موجهة إلى أشخاص ينتمون إلى بعض المجموعات العرقية أو الذهبية أو إلى دين معين بهدف التحريض على الكراهية بين المواطنين أو السكان، فعقوبة الأولى تتمثل في الحبس من شهرين غلى ستة أشهر وبغرامة من 25.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين.

أما العقوبة المسلطة على الثانية فهي الحبس من شهر إلى سنة و بغرامة من 20.000دج إلى 100.00دج أو بإحدى هاتين العقوبتين.

أما بخصوص القذف الموجه لرئيس الجمهورية الذي سبق و أن ذكرناه و المتمثل عقوبته في غرامة من 100.000دج إلى 500.000دج، هذا وفق المادة 144 مكرر من قانون العقوبات و هي العقوبة نفسها للقذف الموجه ضد أحكام القضاة، هذا ما ورد في المادة 147 التي أحالت عقوبة هذه الأفعال إلى المادة 144 مكرر من قانون العقوبات.

و خلاصة القول هي أن المشرع الجزائري قد أقر مواجهة نوعا ما كافية لجريمة القذف سواء في صورتها السيبريانية أو التقليدية.

المطلب الثاني

جريمة السب السيبرياني

تعد جريمة السب أو القدح السيبرياني من أكثر الجرائم مساس بشرف واعتبار الفرد في مجال الشبكة المعلوماتية أي الانترنيت. بحيث يساء استعمالها للنيل من كرامة الغير، و ذلك بخدش شرفه والإساءة إليه[148]، ولما كانت جريمة السب السيبرياني من الجرائم المستحدثة من حيث طرق و وسائل ارتكابها بظهور الشبكة العنكبوتية، ارتأينا إلى عرض

148 - **PETIT Marie-Noëlle**, « Cybercriminalité : du virtuel au réel », Rhizome, vol 3, n°63, 2016, p.14

هذه الجريمة من الجانب المفاهيمي لها(الفرع الأول)، وإبراز أركان قيامها و مدى توفير المشرع الجزائري سبل لمواجهتها (الفرع الثاني).

الفرع الأول

تعريف جريمة السب السيبرياني

من الملاحظ أننا لم نجد تعريفا للسب السيبرياني بالذات، لكن مع هذا فمعنى هذا الأخير مستنتج من تعريفه التقليدي، فما التباين إلا بوسيلة القيام بالجريمة التي تستوجب شكلها المعلوماتي، أي أن تكون قد حدثت بواسطة الحاسب الآلي و النت، فالنصوص التقليدية ذات الطابع العام تسمح بتدارك هذا الشكل السيبرياني[149].

لذا فالمقصود بالسب هو كل تعبير يخدش الشرف و الاعتبار[150]. أو هو مس شرف شخص و كرامته عمدا بغير أن يتضمن انساب واقعة محددة إليه[151].

وهذا ما جاءت به المادة 297 من قانون العقوبات الجزائري و التي تنص على ما يلي: « ***يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة***»[152].

فمن خلال هذه المادة نخلص إلى أن السب هو ألفاظ و تعابير فضة و سيئة، تفيد القدح و تحقير الشخص، دون أن يتضمن ذلك إسناد أية حادثة معينة، وهذا ما يميز السب عن القذف ففي هذا الأخير يتضمن إسناد الواقعة أما السب فلا.

الفرع الثاني

أركان جريمة السب السيبرياني

تعتبر جريمة السب السيبرياني وكغيرها من الجرائم الأخرى، التي يستلزم لقيامها توافر ركنين أساسيين، أولاهما الركن المادي و المتمثل في السلوك الإجرامي المعلوماتي الذي ينطوي على عبارات تمس شرف و كرامة المجني عليه، أما اركن الثاني وهو الركن المعنوي

149 - **عمار عباس الحسيني**، مرجع سابق ، ص 387.

150 - **محمد عبد الله أبو بكر السلامة**، مرجع سابق ، ص 196.

151 - **خالد ممدوح إبراهيم**، الجرائم المعلوماتية، مرجع سابق، ص. 123.

152 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، مرجع سابق.

المتجسد في القصد الجنائي.

أولا -الركن المادي:

يتجسد الركن المادي لجريمة السب السيبرياني في السلوك الإجرامي المتمثل في التلفظ بعبارات تمس اعتبار و شرف و كرامة الشخص المجني عليه بإسناد واقعة، لكن بشرط أن لا تكون هذه الأخيرة معينة أو محددة، لأن إذا تم تحديدها نكون أمام جريمة القذف، الذي سبق و أن تطرقنا إليه، و مثالا على عبارات و ألفاظ السب كقول الشخص الجاني إلى شخص آخر (يا حمار)، أو (يا زاني)، أو (يا مخادع)... أو قد تكون بصيغة (أن ذلك الشخص أو فلان حمار، زاني، أو سكير، أو سارق، أو نصاب...إلخ).

لذا فالسلوك الإجرامي في هذا المنبر قد يأتي كتابيا أو شفاهيا، و إن كان الشكل الغالب في جريمة السب السيبرياني أن يكون الإنساب قد ورد بشكل مكتوب على شبكة النت، إما على واحدة من المواقع الإلكترونية، أو في إحدى صفحات التواصل الاجتماعي " كفي سبوك "، أو " واتس آب " ...، لكن هذا لا يمنع من أن يصدر السب السيبرياني بصيغة قولية، مثل الذي يسجل لنفسه مقطعا فيديوهيا أو صوتيا فقط ينطوي على ألفاظ سب مسلطة للغير، بحيث يقوم بإطلاقه في شبكة النت، وهذه الصورة لقت انتشارا كبيرا في عصرنا هذا، و من جانب آخر قد يكون الفعل الإجرامي في شكل رسوم كاريكاتورية و غيرها منشورة على شبكة النت، لذا فإطلاق ألفاظ السب بشكل معلوماتي أو سيبرياني من أمره أن يحقق العلانية التي يشترطها المشرع في تطبيق النص المدرج هذه الجريمة[153].

وتجدر الإشارة إلى أن ألفاظ السب يستلزم أن تكون مسلطة لشخص محدد، لأن مفاد الشرف و الاعتبار المعتدى عليه في هذه الجريمة يشترط تحديدا للشخص المجني عليه، من غير أن يكون التعيين مفصل بصورة دقيقة، و إنما بإمكان فئة من الأشخاص التعرف عليه[154].

ثانيا- الركن المعنوي:

جريمة السب جريمة عمدية، يتضمن الركن المادي فيها القصد الجنائي العام لدى

153 - عمار عباس الحسيني، المرجع السابق، ص ص 389-390.

154 - مرجع نفسه، ص90.

الجاني بصورتيه و هما العلم و الإرادة، فتنصرف إرادة الجاني إلى إشاعة الأمور التلفظ بعبارات ماسة بشرف و اعتبار و كرامة المجني عليه، مع علم الجاني كذلك بمعنى تلك الألفاظ التي صدرت عنه التي من شأنها خدش شرف و عرض الشخص[155].

الفرع الثالث

موقف المشرع الجزائري من جريمة السب السيبيريانية

بخصوص آليات التصدي لجريمة السب السيبرياني، فكما أشرنا سابقا أن المشرع عرف السب في المادة 297 من قانون العقوبات حيث تتضمن لقيام هذه الجريمة توافر العلن والذي يستنتج من الوسائل والطرق المنصوص عليها في المادة 296 من قانون العقوبات، والتي نفسها بالنسبة لجريمة السب و هي التي تطرقنا إليها سابقا في جريمة القذف، رغم سكوت المشرع عن النص عليها في المادة 297 من قانون العقوبات[156].

ونستخلص من خلال المواد 144 مكرر و 144 مكرر2 من قانون العقوبات إمكانية وقوع جريمة السب بواسطة الانترنيت، بحيث نصت المادة 144 مكرر على: « *يعاقب بغرامة من 100.000دج إلى 500.000دج، كل من أساء إلى رئيس الجمهورية بعبارات تتضمن اهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى...* »[157].

وكذا المادة 144 مكرر2 بنصها على: « *يعاقب بالحبس من 3 سنوات إلى 5 سنوات و بغرامة من 50.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين فقط كل من أساء إلى الرسول (صلى الله عليه و سلم) أو بقية الأنبياء أو استهزأ بالمعلوم من الدين بالضرورة أو بأية شعيرة من شعائر الإسلام سواء ع طريق الكاتبة أو الرسم أو التصريح أو أية وسيلة أخرى...* »[158].

يتضح من خلال هاتين المادتين اعتراف المشرع الجزائري بجريمة السب السيبرياني من خلال عبارة " بأية وسيلة إلكترونية أو معلوماتية " الواردة في نص المادة 144 مكرر، وعبارة

155 - هروال هبة نبيلة، مرجع نفسه، ص 81..

156 - المرجع نفسه، ص 88.

157 - أمر رقم 66-156يتضمن قانون العقوبات، معدل و متمم، المرجع السابق.

158 - المرجع نفسه.

" بأية وسيلة أخرى " المدرجة في نص المادة 144 مكرر2، هذا ما يسمح بإدخال السب الواقع على النت ضمن هذه الوسائل.

وبخصوص العقوبة المقررة لجريمة السب فهي تتباين حسبما إذا كان موجهة لأفراد عاديين، أم إلى أشخاص ينتمون إلى الطبقة العرقية المذهبية، أو السب الموج إلى رئيس الجمهورية، أو الرسول (ص) والرموز الدينية فنصت المادة 298 مكرر و 299 من قانون العقوبات على ما يلي:

المادة 298 مكرر: « *يعاقب على السب الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من 5 أيام إلى ستة أشهر و بغرامة من 20.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين فقط* ».

المادة 299: يعاقب على السب الموجه إلى فرد أو عدة أفراد بالحبس من شهر إلى ثلاثة أشهر و بغرامة من 20.000دج إلى 100.000دج

و يضع صفع الضحية حدا لمتابعة الجزائية ».

بالإضافة إلى هذا فقد سبق و أن ذكرنا أعلاه نص المادتين 144 مكرر و 144 مكرر2، اللتان ورد فيهما العقوبة المقررة للسب الموجه لرئيس الجمهورية، و ذلك بتسليط غرامة مالية من 100.000دج إلى 500.000دج، و كذا العقوبة المقررة للسب الموجه إلى الرسول صلى الله عليه و سلم و كذا ضد رموز الدين، و هي الحبس من 3 سنوات إلى 5 سنوات و بغرامة من 50.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين فقط »[159].

بالتالي نخلص إلى أن المشرع الجزائري اعترف بجريمة السب السيبرياني أو المعلوماتي، و قد أوفاه حقه من خلال التصدي له و مواجهته بعقوبات صارمة.

المطلب الثالث

جريمة التحريض الجنسي السيبرياني

إذا كان لشبكة الانترنيت وجه إيجابي فإن لها وجه سلبي أيضا، و من هذه الأوجه وجود مواقع على الشبكة تحرض على ممارسة الجنس والدعارة و الفجور، سواء مع صغار

159 - أمر رقم 66-156، يتضمن قانون العقوبات معدل و متمم، مرجع سابق.

السن أو مع الكبار، و تعد جرائم التحريض الجنسي من بين الجرائم الأكثر شيوعا في المجتمعات العربية في الوقت الحالي، فهذه الأخيرة تخل بالنظام العام و الآداب العامة لما تحمله من فسق و رذيلة للمجتمع.

لذا سنتناول في هذا المطلب التعريف بهذه الجريمة (الفرع الأول)، ونبين أركانها (الفرع الثاني) وموقف المشرع الجزائري من خلال التصدي لها (الفرع الثالث).

الفرع الأول

تعريف جريمة التحريض الجنسي السيبرياني

لقد أمست شبكة النت فضاء واسعا لتجميع الصور الفاضحة والأفلام والفيديوهات الخليعة، التي تنشر عن طريق مواقع مخصصة لذلك، من أهدافها جني منافع مادية، وتلقب بالمواقع الجنسية الإباحية، وبواسطة الدردشة الإباحية والقوائم البريدية الجنسية، التي أضحت تغزو مجتمعنا و تدخل بيوت و مكاتب الجميع، و هي تمس الصغير والكبير، والذكر و الأنثى من دون استثناء[160].

لذا فالتحريض الجنسي فالتحريض الجنسي السيبرياني يحتمل شكلان، الشكل الأول يتمثل في التحريض على القيام بجرائم جنسية معلوماتية، بمعنى آخر أن التحريض في هذه الحالة يتم في صورة سيبرياينية أو تقليدية واقعية مادية، أما الشكل الثاني يتمثل في التحريض السيبرياني أو المعلوماتي على إتيان هذا الفعل الجنسي السيبرياني فقط، و ذلك من خلال صنع مواقع لنشر الصور والأفلام الإباحية لدفع الغير على التعامل بها وتداولها عبر الانترنيت.

وعلى هذا يمكن تعريف التحريض الجنسي السيبرياني بأنه حث الغير معلوماتيا على ارتكاب جرائم تقليدية أو سيبريانية، ذات طابع جنسي و ذلك بواسطة توزيع و نشر صور وفيديوهات وأفلام خليعة، بصورة علنية فاضحة[161]، عبر مواقع إلكترونية معدة لذلك، ويكون الحدث أكثر عرضة للتأثر بهذه المشاهد الجنسية الشنيعة، على عكس الكبار الذي يتوفر لديهم اكتمال العقل فباستطاعتهم الرفض أو القبول بهذه المنشورات الجنسية

160 - **هروال هبة نبيلة**، مرجع سابق، ص 155.

161 - **حسن طاهرداود**، مرجع سابق، ص 93.

المعلوماتية[162].

وبمعنى آخر يتحقق التحريض الجنسي سيبريانيا من خلال الكثير من الأعمال المادية التي تتمثل في عض أو توزيع أية صور و أفعال وأقوال بذيئة فاسقة وفاضحة، تخل بالنظام العام والآداب العامة، عن طريق شبكة النت، ويتحقق أيضا بصنع وخلق العديد من المواقع الجنسية الإباحية على النت لمداولتها و جذب الغير لها، أو أيضا تبادل رسائل البريد الإلكتروني التي تتضمن شتى الصور و الأقوال و الإشارات و الأفعال الماجنة بين مستعملي الشبكة العنكبوتية[163].

وهذا التحريض له مظهران، أولهما يتمثل في التحريض الفردي والمدعو بـ "التحريض الخاص" و الذي تكون فيه أفعال الحمل والدفع على ارتكاب جريمة التحريض الجنسي موجهة إلى شخص محدد أو أشخاص محددين، بغير وجود طريقة معينة لوقوع هذا الصنف من التحريض بها، فقد يتم كتابيا أو شفاهيا أو بالإشارة.

أما المظهر الثاني للتحريض فيكون موجها للجمهور عامة، أي التحريض الجماعي غير المحدد للأشخاص بذاتهم أو أنفسهم، بالتالي هم غير معروفين ومعلومين بالنسبة للمحرض، و لا يحث هذا الصنف الأخير من التحريض إلا إذا تم بأحد طرق العلنية التي ذكرناها سابقا في الجرائم الماسة بالشرف، و ربما هو الأقرب إلى التحريض السيبرياني الذي في معظم الأحيان تأتي فيه طرق التحريض موجهة لأشخاص غير محددين[164].

الفرع الثاني

أركان جريمة التحريض الجنسي

جريمة التحريض الجنسي كغيرها من الجرائم التي تقتضي لارتكابها تحقق ركن مادي والمتمثل في السلوك الإجرامي ألا وهو فعل التحريض، وركن معنوي المتجسد في القصد الجنائي لذا سنتناول كل ركن على حدة.

---

162 - **محمد أمين الرومي**، مرجع سابق، ص 130.

163 - **محمد عبد الله أبو بكر السلامة**، مرجع سابق، ص 199.

164 - **عمار عباس الحسيني**، مرجع سابق، ص 408.

أولا- الركن المادي:

إن جريمة التحريض الجنسي تعتبر من جرائم الخطر و ليست من جرائم التي تقتضي تحقيق نتيجة، و بالتالي فإن النشاط الإجرامي في جريمة التحريض السيبرياني قد تحدث باستعمال أية وسيلة معلوماتية و أبرزها شبكة النت، و سواء تم ذلك بنشر الصور الجنسية أو مقطع فيديو، أو نشر روايات جنسية يهدف من ورائها تحفيز و تشجيع الأشخاص على ممارسة الجنس و أفعال الفجور، أو تشجيعهم على الانضمام للممارسات والأنشطة الجنسية و الإباحية المعلوماتية.

وعليه لا يشترط أن يكون فعل التحريض موجها و صادرا إلى مجموعة معينة ومحددة، فقد يكون موجها إلى الكبار وكذلك إلى الصغار، و في الحقيقة أن أصحاب المواقع الجنسية وبهدف تحقيق نجاح تحريضهم على أفعال الفجور والجنس يقومون بنشر مقاطع الفيديو أو الصور الإباحية أو بنشر ألفاظ كتابية مغرية ويتم اختيارها وتحديدها، وذلك من أجل إغراء الغير و دفعه على القيام بأفعال جرمية جنسية[165].

ثانيا- الركن المعنوي:

تعد جريمة التحريض الجنسي السيبرياني من الجرائم العمدية و القصدية، و التي تستوجب توافر القصد الجنائي العام[166]، والذي يقصد به أن يكون الجاني على علم أن سلوكه سيترك أثر في نفسية الشخص الآخر أي المُحَرَضْ و أن الوسائل التي استعملها الجاني من شأنها أن تدفع الغير على القيام بفعل الجنس، وأن تتوجه إرادة الفاعل أي المحرض إلى توليد رغبة لدى الغير أي الشخص المُخَاطَب.

ويُرى أن التحريض الجنسي السيبرياني للقيام بجريمة جنسية إباحية يقتضي في أغلب الأحيان توافر القصد الخاص والذي يتجسد في تشجيع الغير وتحفيزه على القيام بأفعال الفسق أو الفجور أو معاونته في ذلك[167].

165 - **عمار عباس الحسيني**، مرجع سابق، ص ص 410-411.

166 - **حنان ريحان مبارك المضحكي**، مرجع سابق، ص 239.

167 - **عمار عباس الحسيني**، مرجع سابق، ص 411.

الفرع الثالث

موقف المشرع الجزائري من جريمة التحريض السيبيرياني

تظهر مواجهة المشرع الجزائري لجريمة التحريض السيبرياني أو المعلوماتي والتصدي لها في النصوص القانونية الواردة في قانون العقوبات وذلك من المادة 342 إلى غاية المادة 349 من قانون العقوبات الجزائري والتي ورد فيها العقوبات المقررة لجريمة التحريض الواقعة على القصر[168].

ومثال على ذلك نص المادة 342: «*كل من حرض قاصرا لم يكمل الثامنة عشر سنة على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له و لو بصفة عرضية، يعاقب بالحبس من خمس سنوات إلى عشر سنوات و بغرامة من 20.000دج إلى 100.000دج ...*»[169].

يتضح من خلال هذه المادة نجد أن المشرع الجزائري عاقب كل من يقوم بتحريض قاصر على الفسق و أفعال الفجور و فساد الأخلاق أو قام بدفعه و حثه على تلك الأفعال و ذلك بتسليط عقوبة الجبس من خمس سنوات إلى عشر سنوات و بغرامة من 20.000دج إلى 100.000دج.

وقد نصت المادة 347 من قانون العقوبات: « يعاقب بالحبس من ستة أشهر إلى سنتين و بغرامة من 20.000دج إلى 100.00دج كل من قام علنا بإغراء أشخاص من أي من الجنسين بقصد تحريضهم على الفسق و ذلك بالإشارة و الأقوال أو الكتابات أو بأية وسيلة أخرى ... »[170].

فنفهم من خلال هذا النص أن المشرع الجزائري جرم فعل التحريض الموجه للأشخاص عامة دون استثناء أي للكبار أو الصغار، و كذلك للذكر أو الأنثى، و يكون هذا الأخير شفهيا أو كتابيا أو بأية وسيلة أخرى، فهذه العبارة الأخيرة "بأية وسيلة أخرى" تسمح لنا بإمكانية تطبيق هذا النص على جريمة التحريض الجنسي الواقع عبر الانترنيت، لأن مدلولها عام وشامل لكل الطرق و الوسائل بما فيها التحريض السيبرياني.

168 - **هروال هبة نبيلة**، مرجع سابق، ص 170.

169 - أمر رقم 66-156، يضمن قانون العقوبات، معدل و متمم، مرجع سابق.

170 - المرجع نفسه.

ونرى أيضا أنه بالمكان تطبيق نص المادة 394 مكرر2 من قانون العقوبات على التحريض الجنسي السيبرياني، إذ نص المشرع على معاقبة كل من خولت له نفسه القيام عن قصد و بواسطة الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار حيازة أو استعمال لأي غرض كان المعطيات المجملة أو المخزنة أو المحفوظة معلوماتيا، وبالتالي إذا كانت هذه المعطيات و البيانات تتضمن صورا جنسيا فتعتبر هذه جريمة إباحية، جنسية يعاقب عليها حسب العقوبة المقررة في المادة 394 مكرر2 وهي الحبس من شهرين إلى ثلاث سنوات و بغرامة من 100.000دج إلى 10.000.000دج[171].

المبحث الثاني

الجرائم الماسة بأمن الدولة

تملك الدولة باعتبارها شخصية معنوية مصالح و حقوق عامة مثلها مثل الأفراد ترمي إلى حمايتها و ذلك بتجريم الأفعال والسلوكات التي تضر بها وبمصالحها وتعرضها للخطر، وتوقيع العقاب الرادع لها.

وتتمثل المصالح والحقوق التي تعمد الدولة حمايتها على صعيد أمنها هي تلك المرتبطة بكيانها في شكليه الخارجي و الداخلي، فلما كان الشكل الأول من هذه المصالح يتعلق بسيادة الدولة على الصعيد الخارجي و سلامتها و هيبتها الدولية، فإن الشكل الثاني منها يرتبط بنظام الحكم الداخلي و الدستور ومؤسساته ووحدة وأمن الشعب.

وعلى إثر ذلك فإن الجرائم التي ترتكب في كيان الدولة الخارجي تسمى الجرائم الحاصلة على أمن الدولة الخارجي، أما الجرائم التي تقترف في كيان الدولة الداخلي تسمى الجرائم الواقعة على أمن الدولة الداخلي.

وعليه يمكن تعريف الجرائم الواقعة على أمن الدولة عامة بأنها مجموعة الجرائم التي تمس بشكل مباشر الدولة في وجودها و استمرارها و سيادتها و أراضيها ومواطنيها، أو تنال من نظام الحكم وتعرض مؤسسات الدولة الدستورية للخطر، وكذا هيئاتها العمومية، الحكومية و غير الحكومية، الاقتصادية والسياسية، وكل ما يمس بكيان الدولة وأمنها.

171 - أمر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، المرجع السابق.

وعلى ذلك تعتبر الاعتداءات الحاصلة على أمن الدولة من بين أخطر الاعتداءات لما لها من تهديد على مصالح الدولة، ولقد تأثرت هذه الجرائم كغيرها من الجرائم بالتقدم التكنولوجي وما أنتجه من تقنيات عالية و متطورة من بينها الشبكة العنكبوتية والتي سهلت للمجرمين المعلوماتيين القيام بجرائمهم في وسط افتراضي يصعب فيه إثبات هذه الاعتداءات مما قدم لهم رخصة ارتكاب العديد من الجرائم المستحدثة الماسة بأمن الدولة، والتي من أهمها و أبرزها جريمتي الإرهاب السيبرياني (المطلب الأول)، و التجسس السيبرياني (المطلب الثاني)، اللذان وجدا من الحاسوب والانترنيت الأرضية الممتازة لتحقيق غايتها الجرمية بكل سهولة و بدون أي جهد عضلي.

المطلب الأول

الإرهاب السيبرياني

لقد ظهر وانتشر مصطلح الإرهاب السيبرياني نتيجة للقفزة الكبيرة التي حققتها التكنولوجيا المعلوماتية، والاستعمالات اليومية الكثيرة للحاسوب والانترنيت في شتى مجالات الحياة، هذا الأخير دفع بأكثر من ثلاثون دولة إلى التوقيع على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الانترنيت في بوداباست عام 2001، وهذه الظاهرة تعد من أخطر أنواع الجرائم الواقعة في الفضاء السيبرياني، لما تخلفه من أضرار و خسائر جسيمة لكل دول لعالم، التي بالإمكان أن تنتجها عملية ناجحة واحدة الإرهاب السيبرياني[172].

ولما كان الإرهاب السيبرياني من أخطر الجرائم المعروفة في عصرنا فإنه كان لزاما علينا تعريفها (الفرع الأول)، وبيان الأركان التي تقوم عليها (الفرع الثانّي) و تحديد آليات مكافحة المشرع الجزائري لها (الفرع الثالث).

الفرع الأول

تعريف الإرهاب السيبرياني

كان يعرف الإرهاب فيما مضى أنه قيام جماعة إرهابية بتفجير قنبلة في مكان ما، أو قتل شخصية ما، و غيرها من العمليات الروتينية التي تعود عليها كل الأشخاص وشتى

172 - **علي عدنان الفيل**، الإجرام الإلكتروني- دراسة مقارنة، مكتبة زين الحقوقية و الأدبية، لبنان، 2011، ص 59..

الدول، وهذا بغرض نشر الإرهاب في دولتهم أو أية دولة أخرى لا ينتمون إليها، للوصول إلى مبتغياتهم و التي كانت تتمثل أكثرها في معارضة نظام الحاكم أو الرئيس.

أما في الوقت الراهن و مع تقدم تقنيات ووسائل الاتصال، تغيرت وتطورت تلك الطرق، التي يسعى الإرهابيين بها إلى تحقيق غاياتهم، فقد أمسى الإرهاب السيبرياني هو المنتشر في الوقت الراهن، و أضحى اختراق المواقع الإلكترونية وإتلافها، وتبديل محتوياتها، والولوج على الشبكات و التلاعب بمضمونها و ذلك بحذفها أو الاستيلاء عليها، و غيرها من الأفعال التي تعد طرق الإرهاب حاليا في محاولة تحقيق أهدافهم[173].

و لقد تعددت التعاريف والمفاهيم حول هذه الظاهرة الخطيرة ألا و هي الإرهاب السيبرياني، فعرف على أنه العدوان أو التخويف أو التهديد المادي أو المعنوي، باستعمال الطرق المعلوماتية، الصادرة من دولة أو جماعة أو شخص على الإنسان في دينه أو نفسه أو عرضه و شرفه، أو عقله أو ماله بدون حق بمختلف أنواعه و مظاهر العدوان والإفساد[174].

وعرف أيضا بأنه مجموعة من الاعتداءات غير المشروعة، أو تهديدات بهجمات ضد الحواسيب و شبكات النت أو المعلومات المحفوظة إلكترونيا، و هذا من أجل الانتقام أو التهديد، أو إجبار الدول و الحكومات و المجتمع الدولي بكامله لتحقيق غايات سواء كانت سياسية أو دينية أو اجتماعية، لذا فلكي يطلق على شخص ما بأنه إرهابي على الانترنيت، وليس فقط مقتحم، يجب أن تؤدي اعتداءاته أو هجماته إلى ضرر كافي لإحداث الخوف والرعب و نشره في المجتمع[175].

وهناك أيضا من ذهب إلى تعريفه بأنه استخدام للمصادر المعلوماتية، و المتجسدة في أجهزة الحاسوب و شبكات النت و المعلومات، بهدف التخويف و الإجبار لمبتغيات سياسية[176].

173 - **منير محمد الجنبيهي، ممدوح محمد الجنبيهي**، مرجع سابق ، ص ص 106-107.

174 - **بن مكي نجاة**، مرجع سابق، ص 65.

175 - **علي عدنان الفيل**، مرجع سابق ، ص 60.

176 - **أمير فرج يوسف**، مرجع سابق، ص206.

لذا فنطاق الإرهاب عبر الحاسب الآلي و الانترنيت شاسع و كبير، بالأخص مع تزايد و انتشار الحواسيب و الشبكات في العالم، و الحرص على اتصالها بالشبكة العنكبوتية، ولهذا النوع من الجرائم أمثلة عديدة نذكر منها اختراق أنظمة الملاحة الجوية في أبراج المراقبة بالمطارات الكبيرة.و تهديد سلامة الملاحة الجوية.

بالتالي التسبب في حوادث وسقوط بعض الطائرات، كذلك اقتحام أنظمة إدارة معامل إنتاج الطاقة الكهربائية لإحداث انقطاع التيار عن مكان ما، وما قد يتزامن مع ذلك من جرائم أخرى، و كذلك استخدام الفيروسات و الديدان لإتلاف أجهزة الحاسوب والمواقع الإلكترونية، فهي تعتبر وسيلة وطريقة جيدة للقيام بأفعال الإرهاب السيبرياني[177]، كالذي حدث في العام 2000، عندما أدى انتشار فايروس الحاسب الآلي " I love you" إلى إتلاف وتدمير معلومات قدرت قيمتها بـ عشر مليارات دولار أمريكي[178].

بالتالي فالإرهاب السيبرياني يسعى إلى المساس بالبنى التحتية و الأساسية للدول، والتي أضحت في فجر المعلوماتية ترتكز كليا و بصفة كبيرة على المعلومات الرقمية، فيمكن له أن يتسبب في شل أنظمة القيادة، و الاتصالات، أو قطع شبكات الاتصال بين الوحدات و القيادة أو إعاقة أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها، أو اقتحام النظام المصرفي، وإلى غيرها من الأفعال التخريبية[179].

وبهذا صار الإرهاب السيبرياني من أخطر ما يواجه العالم حاليا، حيث أضحى باستطاعة الإرهابي من خلال لمسة زر على الحاسوب، اختزال 90% من العمليات الإرهابية، وأيضا حيازة قنبلة حقيقة و هو قاعد في منزله وبأدنى التكاليف عن طريق المواقع المعدة لذلك[180].

الفرع الثاني

أركان جرائم الإرهاب السيبرياني

إن الإرهاب السيبرياني مثله مثل الجرائم الأخرى التي تحتاج لقيامها توافر أركان،

177 - **تركي بن عبد الرحمن المويشير**، مرجع سابق، ص 78.

178 - **علي عدنان الفيل**، مرجع سابق، ص 60.

179 - **هروال هبة نبيلة**، مرجع سابق، ص 338.

180 - مرجع نفسه، ص 336.

والمتمثلة في الركن المادي و المعنوي، و هذا ما سوف نعالجه على النحو الآتي:

أولا- الركن المادي:

يتمثل الركن المادي في السلوك الإجرامي، و يتباين هذا السلوك بين جريمة الإرهاب السيبرياني، و جريمة الإرهاب في شكلها التقليدي، بحيث هذا الأخير يقوم على أنشطة التخريب و القتل و التدمير، و كذا السلوكات التي تهدف إلى خلق حالة فزع ورهبة لدى الأشخاص و كل هذه الأفعال ترتكب بطريقة تقليدية، كالأسلحة، و المتفجرات، و المواد الملتهبة و السامة...إلخ.

أمّا الإرهاب السيبرياني فيختلف سلوكه الإجرامي، بحيث يعتمد على التقنية الرقمية المتطورة، أي أن هناك رابطة بين الحاسب الآلي والنت من جانب و بين الجاني من جانب آخر[181]، فهذا الفعل الإجرامي السيبرياني يتمثل في مجموعة من الوسائل التي تعمد التنظيمات و الجماعات الإرهابية إتباعها في أجل تحقق أهدافها المتمثلة في استدراج الأفراد الانخراط في مثل هذه التنظيمات، فهذه الطرق و الوسائل كثيرة و متعددة لذا نذكر البعض منها فقط، وهذا على النحو الآتي:

أ- الدعاية:

تتمثل الدعاية في قيام الإرهابيون بإنشاء و تصميم مواقع لهم على الشبكة العنكبوتية، لنشر أفكارهم و الدعوة إلى مبادئهم المنحطة، و لإظهار مدى قوة الجماعات الإرهابية، بمعنى آخر تعليم الغير بشتى الطرق و الوسائل التي تعاون على القيام بالعمليات الإرهابية، كإنشاء مواقع الويب لتبيين كيفية صنع المتفجرات أو أدوات تستخدم في الأعمال الإرهابية، و كذا توضيح طريقة اختراق و تدمير المواقع و البريد الإلكتروني، و كيفية نشر الفيروسات و غير ذلك من الأساليب المتبعة للدعاية الإرهابية[182].

ب- جمع المعلومات:

تتميز الشبكة العنكبوتية بتوافر وكثرة المعلومات فيها، مما يجعلها تعد الموسوعة المعلوماتية الشاملة لمختلف الثقافات و المصادر، فهي ثرية بالمعلومات الهامة والحساسة

181 - **عمار عباس الحسيني**، مرجع سابق، ص 357.

182 - **علي عدنان الفيل**، مرجع سابق، ص 84.

التي يرمي الإرهابيون لحيازتها، كأماكن تواجد المنشآت النووية و القيادة العسكرية، و كذا مصادر الطاقات و توليدها، ومعرفة مواعيد الرحلات الجولة و البحرية، و المعلومات المهمة الخاصة بآليات مواجهة الإرهاب، وإلى غيرها من المعلومات التي تعد البنية الأساسية التي يطمح إليها الإرهابيون[183].

ج- نشر تدريبات إرهابية:

إنّ العمليات الإرهابية تقتضي تدريبات خاصة، و تعد هذه الأخيرة أهم خواطر وهواجس الجماعات الإرهابية[184]، لذا فبالإمكان استعمال النت لنشر مواد تدريبية، كالتوجيهات الخاصة بطريقة استعمال الأسلحة، واختيار الأهداف، وهذه المواد مقدمة على مجال شاسع ليتلقاها جميع الأفراد.

د- تمويل الإرهاب:

بواسطة الشبكة العنكبوتية وعن طريق الاستعانة بالإحصائيات السكانية المستخرجة من المعلومات الشخصية الموجودة على شبكة النت، وكذا من خلال الاستكشافات والاستفسارات التي توجد في المواقع الإلكترونية[185]، يقوم الإرهابيون بعدة طرق من أجل الحصول على التمويل، فبإمكان المنظمات الإرهابية استخدام أنظمة الدفع الإلكتروني للحصول على تبرعات مالية، وهذا باستقطاب الأشخاص ذوي القلوب الرحيمة، وباستطاعتها كذلك أن تستخدم المواقع الإلكترونية لنشر معلومات عن طريق التبرع بالتالي وضع حساب مصرفي لجمع التبرعات المحتملة، وبإمكانها أيضا استخدام بطاقات الائتمان، لذا فكلا الطريقتان محتملتا الكشف، ولتجنب هذا الأخير تستعين المنظمات الإرهابية بلاعبين لا يشتبه فيهم كالمنظمات الخيرية.

هـ- إتلاف البنى التحتية للأنظمة المعلوماتية:

زيادة إلى جرائم السيبركرام (ciber crim) العادية كالاحتيال و السرقة، و غسيل الأموال، بالإمكان أن يصبح تدمير المواقع الإلكترونية و النظم المعلوماتية هدفا للإرهاب،

183 - **أمير فرج يوسف**، مرجع نفسه، ص ص 233-234.

184 - **علي عدنان الفيل**، مرجع سابق، ص 83.

185 - المرجع نفسه، ص ص 81-82.

وتزايد الارتكاز على تكنولوجيا المعلومات يجعل البنى الحساسة أشد عرضة للهجمات[186]، فتقوم التنظيمات الإرهابية بشن اعتداءات إلكترونية، تمس وتدمر نظم المعلومات وإلحاق الضرر بها، و تستهدف هذه الهجمات كل من المجال العسكري، و السياسي، والاقتصادي.

ويقصد بالتدمير في هذه الحالة الدخول الغير المصرح على نقطة وصل أساسية أو ثانوية مرتبطة بشبكة الانترنيت، بواسطة نظام آلي (server-pc) أو العديد من النظم المتصلة شبكيا، بغية إتلاف نقطة الاتصال أو النظام[187].

واستخلاصا لبعض هذه السلوكات والوسائل المنتهجة من طرف الإرهاب السيبرياني، نجد أن هذا الأخير قد اعتمد على أفعال و أنشطة متطورة تؤدي إلى نتائج وخيمة و خطيرة، خاصة بعد ارتكاز الكثير من الأنشطة الحكومية و غير الحكومية على الحاسب الآلي والشبكة المعلوماتية في تسيير أعمالها[188].

ثانيا-الركن المعنوي:

إن جريمة الإرهاب السيبرياني جريمة عمدية تتطلب تحقق العلم و الإرادة، أي يجب أن يعلم الشخص أن سلوكه يعتبر سلوكا إجراميا و معاقب عليه قانونا، و أن تتجه إرادته إلى تحقيق النتيجة الجرمية الضارة في بعض صور جرائم الإرهاب السيبرياني التي تتطلب وجود هذه النتيجة[189].

إضافة إلى هذا فقد رأى الدكتور عمار عباس الحسيني أن هذه الجريمة تتطلب قصدا خاصا يتمثل في تحقيق الرعب و الذعر بين الناس و إشاعة الفوضى و الدمار وإلا فبماذا تتميز جريمة الإرهاب عن جريمة القتل أو التخريب أو الإتلاف في صورها التقليدية[190].؟؟؟

186 - **علي عدنان الفيل**، مرجع سابق ، ص 37.

187 - أمير فرج يوسف، مرجع سابق، ص ص 238-239.

188 - عمار عباس الحسيني، مرجع سابق، ص ص 358-359.

189 - حنان ريحان مبارك المضحكي، مرجع سابق، ص 286.

190 - عمار عباس الحسيني، مرجع سابق، ص 360.

الفرع الثالث

موقف المشرع الجزائري من جريمة الإرهاب السيبيرياني

يتضح موقف المشرع الجزائري من خلال مواجهته لجريمة الإرهاب السيبرياني، لذا فنظرا للأزمات التي عانت منها الدولة الجزائرية جراء أنشطة الإرهاب سارعت بوضع القانون رقم 09-04 للتصدي لها، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و المتمم لقانون العقوبات، بحيث سمحات المادة 04 منه[191] باللجوء إلى المراقبة الإلكترونية و ذلك في أربع حالات مدرجة على سبيل الحصر من بينها:

-الوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب و الجرائم الماسة بأمن الدولة، و في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة، أو الدفاع الوطني أو النظام العام أو الاقتصاد الوطني[192].

-وكذا بما جاءت به المادة 87 مكرر4 من قانون العقوبات الجزائري التي تنص على: « يعاقب بالحبس المؤقت من 5 سنوات إلى 10 سنوات و بغرامة مالية من 100.000دج إلى 500.000دج، كل من يشيد بالأفعال المذكورة في المادة 87 مكرر أعلاه أو يشجعها أو يمولها بأية وسيلة كانت»[193].

-لهذا فهذه المادة تجرم تشييد الأفعال المذكورة في المادة 87 مكرر أو التشجيع على ارتكابها أو تمويلها بأية وسيلة كانت، وعلى إثر هذا فعبارة " بأية وسيلة كانت " تسمح بإمكانية شمول شبكة الانترنيت، بالتالي يعاقب كل من ارتكب هذه الأفعال وكانت بواسطة شبكة الانترنيت بالسجن المؤقت من 5 سنوات إلى 10 سنوات وبغرامة مالية من 100.000دج إلى 500.000دج، ومن بين هذه الأفعال نذكر:

191 - قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتمثلة بتكنولوجيا الإعلام والاتصال، مرجع سابق.

192 - هرول هبة نبيلة، مرجع سابق، ص359.

193 - أ مر رقم 66-156، يتضمن قانون العقوبات، معدل ومتمم، المرجع السابق.

-بث الرعب في أوساط السكان و خلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المس بممتلكاتهم.

-الاعتداء على رموز الأمة و الجمهورية.

-الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مستند قانوني.

-تخريب أو إتلاف وسائل الاتصال.

-تمويل إرهابي أو منظمة إرهابية...، و إلى غيرها من الأفعال المذكورة في نص المادة 87 مكرر.

وكذلك باستطاعتها تطبيق نص المادة 394 مكرر3 من قانون العقوبات و التي تنص: « *تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد*»[194].

يفهم من نص هذه المادة أن المشرع الجزائري يشدد العقوبات إذا استهدفت هذه الجرائم المعلوماتية الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، و كما نص أيضا في المادة 394 مكرر2 فقرة 2 على: « يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة من 1000.000دج إلى 10.000.000دج كل من يقوم عمدا و عن طريق الغش بما يأتي:

2.حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم »[195].

بالتالي فيستخلص من هذه المادة أن المشرع عاقب و جرم أفعال حيازة أو جمع أو نشر أو إفشاء أو استخدام معطيات مخزنة لأي غرض كان فمن هذا المنبر يسمح لنا بضم فعل نشر الأفكار الإرهابية، وعلى هذا بمقدورنا أن نستخلص أن المشرع الجزائري قد اعترف بالإرهاب الواقع عبر الانترنيت من خلال تجريمه والمعاقبة عليه.

194 - أ مر رقم 66-156، يتضمن قانون العقوبات، معدل و متمم، المرجع السابق.

195 - المرجع نفسه.

المطلب الثاني
جريمة التجسس السيبرياني

إضافة إلى جريمة الإرهاب السيبرياني تعد جريمة التجسس السيبرياني ثاني أخطر جريمة تهدد أمن الدولة، فالتجسس ظاهرة منتشرة و شائعة في الوسط المعلوماتي بكثرة، وتعتبر أشد الاعتداءات خطرا لما لها من أضرار وخيمة تهدد مختلف المجالات الاجتماعية والأمنية و حتى السياسية إضافة إلى الخسائر و الأضرار المادية الفادحة والتي تمس الكثير من القطاعات الحكومية و الغير الحكومية. و يجدر الذكر أن التجسس السيبرياني لا يستهدف معلومات خاصة بدولة أخرى فقط بل يطال المعلومات داخل الدولة الواحدة مثل المعلومات التجارية أو العلمية[196]. ونظرا لأهمية دراسة هذه الجريمة الخطيرة، خصصنا الفرع الأول لتعريفها و الفرع الثاني لتوضيح أركانها (الفرع الثاني) و سبل التصدي لها من طرف المشرع الجزائري (الفرع الثالث).

الفرع الأول
تعريف جريمة التجسس السيبرياني

تجمع البيانات الحساسة في نظام الحاسب في أغلب الأحيان، و إذا كان هذا النظام متصل بالشبكة العنكبوتية فإنه يسهل على المجرمين الوصول إلى هذه البيانات وذلك بالاستعانة بشبكة النت واستخدام التقنيات المتعددة لتحقيق غايتهم وهو اختراق حواسيب الضحايا.

وعليه يمكن تعريف التجسس السيبرياني بأنه كل اختراق لشبكة المعلومات إما بالصدفة أو بواسطة اختراق شفرات الشبكة عمدا[197].

ويتحقق التجسس متى قام الشخص باقتحام الأنظمة المتواجدة على الحسب الآلي ويقوم بسرقة تلك المعلومات المهمة و الحساسة ذات السرية، بهدف استخدامها للإضرار بصاحب النظام المخترق[198].

196 - **عمار عباس الحسيني**، مرجع سابق ، ص 314..

197 - **عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، (دراسة مقارنة).ط2، منشورات حلبي الحقوقية، بيروت، لبنان، 2007، ص462.

198 - **تركي بن عبد الرحمن المويشير**، مرجع سابق ، ص 82.

وقد تحدث عملية الاقتحام إما بصفة عشوائية أي أن المخترق لا يعرف صاحب الجهاز و قد يقوم المخترق باقتحام جهاز معين مملوك لشخص يعرفه[199].

وفي تعريف آخر للاعتداء بأنه الاعتداء الذي يقع على الدولة وذلك بمحاولة التحصل على بيانات سرية تخص الدولة، وسواء ارتكب فعل التجسس من جاسوس وطني أو جاسوس أجنبي. وعلى ذلك فإن هذه الجريمة تصنف أساسا من الاعتداءات التي تقع على أمن الدولة و تعد كجناية كونها تهدد الأمن و الاستقرار الخاص بها[200].

وتستهدف أعمال التجسس السيبرياني معلومات و بيانات من شانها أن تمس بالدولة، كالمعلومات العسكرية، الاقتصادية، و البيانات الخاصة بالسكان و الوضع الاجتماعي، فتتمثل الأولى في الاستراتيجيات العسكرية و المشاريع الحربية وكذا الخطط المتعلقة بصناعة الأسلحة وكل البيانات التي تخص المجال الأمني وهي معلومات حساسة تخص دولة معينة، و تجمع هذه المعلومات في نظام الحاسوب أو يتم تخزينها في قرص ممغنط أو وضعها في مواقع معينة و خاصة عبر شبكة الانترنيت، و على هذا فإنه يمكن للمقتحمين أن يستعملوا الطرق التقنية المتطورة للوصول إلى هذه المعلومات السرية ليس هذا فقط بل قد يصل الأمر إلى حد إتلاف و تخريب هذه المعلومات، أما الثانية فتتجسد في البيانات الاقتصادية ذات الطبيعة التجارية و المالية التي تتعلق بالوضع الاقتصادي للدولة، و الثالثة تتمثل في البيانات المتعلقة بالسكان و الوضع الاجتماعي و ترتبط أساسا بحالة السكان و ذلك من حيث الدين مثلا أو الوضع المعيشي للأفراد و غير ذلك.

و متى كانت هذه البيانات مخزنة في نظام الحاسب و توافر اتصال بشبكة النت يسهل للجواسيس اختراق النظام و التحصل على المعلومات الخاصة بالدولة[201].

الفرع الثاني

أركان جريمة التجسس السيبرياني

جريمة التجسس السيبرياني كغيرها من الجرائم التي تحتاج لقيامها توفر أركان، الركن المادي و هو السلوك الإجرامي و المتمثل في فعل التجسس، و ركن معنوي المتجسد في

199 - **محمد أمين الرومي**، مرجع سابق، ص 137.

200 - **حنان ريحان مبارك المضحكي**، مرجع سابق، ص ص 278-279.

201 - **نهلا عبد القادر المومني**، مرجع سابق ، ص ص 211، 213، 215

القصد الجنائي لذا سنتعرض لكل ركن على حدة.

أولا-الركن المادي:

يتمثل السلوك الإجرامي في جريمة التجسس السيبرياني في فعل الدخول غير المصرح به إلى النظام المعلوماتي كخطوة أولى[202]، و كذا يتمثل في الأساليب و الوسائل المتطورة في مجال تكنولوجيا المعلومات المستخدمة في جريمة التجسس كخطوة ثانية، وهذه الأساليب متطورة و متعددة لذا يصعب تحديدها فهي تتطور و تتجدد بتقدم التكنولوجيا، لكن بإمكاننا الإشارة فقط إلى أهم و بعض هذه الأساليب و المتمثلة في:

أ-استخدام هوائيات متصلة بحاسوب آلي:

يستعمل هذا الأسلوب للتجسس على البيانات المجمعة في الحاسب بحيث بواسطة الهوائيات يتم رصد الموجات الكهرومغناطيسية المنبثقة من الحاسب أثناء تشغيله مع استطاعته معالجتها و ترجمتها إلى معلومات واضحة[203].

ب-استخدام تقنية أبواب المصيدة:

يطلق كذلك عليها الأبواب الخفية، و يتحقق عمل هذه التقنية بتخليف فجوات وذلك بالسماح بالولوج إلى البرنامج مرة أخرى أثناء تحضيره، و هذه الفجوات من الواجب إلغائها في النسخة النهائية للبرنامج، غير أنه يمكن أن يتم تركها قصدا، و على هذه يستطيع أي شخص إذا لقي هذه الأبواب و الفجوات أن يتحصل على البيانات الواردة في الحاسب[204].

ج-إخفاء معلومات داخل معلومات:

يتمثل هذه الأسلوب في قيام المجرم بإخفاء المعلومة السرية ضمن معلومة أخرى عادية و ذلك داخل الحاسوب، و بعد ذلك يلقى وسيلة ما لتسريب تلك المعلومة العادية والمعلومات السرية ضمنها، و بهذه الطريقة لا يستطيع أحد أن يشك بأن المعلومات السرية

202 - **عمار عباس الحسيني**، مرجع سابق ، ص 331.

203 - **نهلا عبد القادر المومني**، مرجع سابق ، ص 216.

204 - المرجع نفسه، ص 217.

قد تم تسريبها[205].

ويعتبر هذا الأسلوب من بين الأساليب المستحدثة و المتطورة للتجسس على البيانات، و يتسم هذه الأسلوب بأن الكشف عن المعلومة المخفاة أمر صعب، إن لم يكن مستحيلا أحيانا[206].

د- إدخال ملف التجسس إلى المجني عليه:

وبهذا الأسلوب يمكن للمقتحم أو المخترق أن يعلم بكل كلمات السر المسجلة في الجهاز، وكذلك يسمح هذا الأسلوب للمخترق إذا كان للمجني عليه كاميرا أو ميكروفون أن يسمع و يشاهد كل ما يقوم به المجني عليه في النطاق الذي يغطيه الميكروفون أو الكاميرا، أما عن كيفية إدخال ملف التجسس إلى حاسوب المجني عليه يتم بثلاث طرق إما بواسطة البريد الإلكتروني، أو برامج المحادثة، أو عندما يقوم الشخص بالدخول إلى موقع غير معروف ويقوم بتنزيل برامج مجانية، و قد يكون من بينها ملف التجسس[207].

كما وتجدر الإشارة إلى أن المعلومة موضوع التجسس يستوجب أن تكون سرية وحساسة، فإذا كانت هذه الأخيرة من المعلومات المسموحة و المنشورة عبر المواقع المتاحة للجميع وقام أحد بالاطلاع عليها فهذا يعتبر تجسسا سيبريانيا كون أن المعلومة كانت مسموح للجميع الدخول والاطلاع عليها، فيجب أن تكون المعلومة من الأسرار الخاصة بالدولة، كالمعلومات العسكرية و السياسية والخاصة بالاقتصاد الوطني التي لا يمكن لأحد الاطلاع عليها[208].

ثانيا- الركن المعنوي:

تعد جريمة التجسس السيبرياني من الجرائم العمدية و التي تقتضي توافر قصد جنائي عام، و المتمثل في العلم و الإرادة، فيجب على الجاني أن يكون على علم بأنه يقوم بنشاط مجرم و ذلك بالولوج إلى النظام المعلوماتي بطريقة غير مشروعة، و أن هذا السلوك يتضمن الاطلاع على بيانات حساسة و سرية، أما معلومات عسكرية، سياسية، أو

205 - **منير محمد الجنبيهي**، ممدوح محمد الجنبيهي، مرجع سابق ، ص 109.

206 - **حسن طاهر داود**، مرجع سابق ، ص 67.

207 - **بن مكي نجاة**، مرجع سابق، ص 48.

208 - **عمار عباس الحسيني**، مرجع سابق، ص 332.

اقتصادية، زيادة علة ذلك يستوجب توافر عنصر الإرادة لدى الجاني، أي اتجاه إرادته إلى الدخول للنظام المعلوماتي و الاطلاع على المعلومات السرية، غير أنه إذا كان دخوله و اطلاعه عليها وقع عن طريق الخطأ فهذا لا يكفي لقيام الجريمة، إلا أن هناك بعض التشريعات التي استوجبت زيادة على القصد العام توافر قصد خاص و المتجسد في نية إلحاق الخسارة و الضرر بالشخص المعني[209].

الفرع الثالث

مواجهة المشرع الجزائري لجريمة

التجسس السيبيرياني

تتبدى مواجهة المشرع الجزائري لجريمة التجسس السيبرياني من خلال نص المادة 394 مكرر3 من قانون العقوبات الجزائري و التي تنص على الأتي: « *تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد* »[210].

ومن خلال هذه المادة نجد أن المشرع قرر مضاعفة العقوبات الواردة في القسم المتعلق بالمساس بأنظمة المعالجة الآلية، وهذه العقوبات واردة في النصوص 394 مكرر، 394 مكرر1 و 349 مكرر2، بحيث وردت العقوبات في هذه النصوص كالآتي:

المادة 349 مكرر: « *يعاقب بالحبس من ثلاث (3) أشهر إلى سنة (1) و بغرامة من 50.000دج إلى 200.000دج ...* ».

المادة 394 مكرر1: « *يعاقب بالحبس من ستة أشهر (6) إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 4.000.000دج ...* ».

المادة 394 مكرر2: « *يعاقب بالحبس من شهرين (2) يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 10.000.000دج ...* »[211].

---

209 - **عمار عباس الحسيني**، مرجع سابق، ص 334.

210 - أمر رقم 66-156يتضمن قانون العقوبات، معدل و متمم، المرجع السابق.

211 - المرجع نفسه.

و عليه فإن العقوبات المذكورة في النصوص أعلاه تضاعف في حالة ما إذا كانت الجريمة موجهة ضد أمن الدولة أو استهدفت الدفاع الوطني وكذا الهيئات والمؤسسات التابعة لها، وبما أ جريمة التجسس السيبرياني من بين الجرائم الماسة بأمن الدولة، فتطبق عليها العقوبات المضاعفة.

وعلى ذلك ومن كل هذا نستنتج أن المشرع الجزائري أقر على إمكانية حدوث فعل التجسس عن طريق الانترنيت وكذا جرم هذا السلوك وذلك بتوقيع عقوبات رادعة له.

خـــــــــاتمة

في ختام هذه الدراسة المتعلقة بالجرائم السيبريانية وسبل مواجهتها في التشريع الجزائري، ومن خلال ما توصلنا إليه في بحثنا اتضح لنا أن الانترنت تلعب دورا كبيرا في نشر هذا النوع من الإجرام المستحدث، والذي أصبح خطرا على أمن واستقرار المواطنين في المجتمع، يمكن أيضا أن نستخلص النتائج الآتية:

- الجريمة السيبريانية متعددة التعاريف، وذلك لحداثة هذه الظاهرة الإجرامية ولم يوجد للآن إجماع على تعريف موحد لها وهذا ما أدى إلى القول بأن هذه الجرائم تقاوم التعريف.

- تتمتع الجريمة السيبريانية بطبيعة قانونية مغايرة تماما لطبيعة الجريمة التقليدية.

- القوانين التشريعية بخصوص جرائم السيبريانية تبدو قاصرة على مواجهة هذا النوع من الجرائم المستحدثة.

- الدليل في الجرائم السيبريانية يختلف عن نظيره في الجرائم العادية وهو ما يزيد في تعقيد

الوضع في جرائم الكمبيوتر وتجعلها صعبة الاكتشاف والإثبات.

- الجرائم السيبريانية تستهدف المعطيات ذات الطبيعة المعنوية أي الكيان المنطقي للحاسوب.

الحلول المقترحة:

- وجوب الاتفاق على ضرورة تبني مصطلح الجرائم السيبريانية للدلالة على جرائم الإنترنت

والحاسوب دون غيره من المصطلحات الغير دقيقة.

- ضرورة القيام بحملات توعية حول مخاطر الجريمة السيبريانية، وذلك بدراسة كل جريمة على حدا حتى يتسنى الإلمام بها.

- تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي، والأجهزة الحاسوبية

وهذا لتفادي وقوع الجرائم الماسة بشرف واعتبار الأشخاص.

- تجنب تحميل أي برنامج مجهول المصدر لتفادي التعرض لإتلاف البرامج المتواجدة في جهاز الحاسوب.

- المسارعة في الإبلاغ للجهات الأصلية فور التعرض لأي جريمة سيبريانية، وذلك لمتابعة

المجرم المعلوماتي.

- سد الفراغات القانونية التي تعاني منها النصوص القانونية الجزائرية.

قـــــائمة المراجـــــع

أولاً- باللغة العربية:

1 – الكتـــــب:

1. **أحمد حسام طه تمام**، الجرائم الناشئة عن استخدام الحاسب الآلي،(دراسة مقارنة) د. ط، دار النهضة العربية، القاهرة، مصر، 2000.
2. **أحمد خليفة الملط**، الجرائم المعلوماتية،(دراسة مقارنة) الطبعة ،2 دار الفكر الجامعي، الإسكندرية، مصر، 2000.
3. **أمير فرج يوسف**، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الانترنت و الكمبيوتر، مكتبة الوفاء القانونية، مصر، 2011.
4. **بن مكي نجاة**، السياسة الجنائية لمكافحة الجرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017.
5. **بولين انطونيوس أيوب**، الحماية القانونية للحياة الشخصية في مجال المعلوماتية،(دراسة مقارنة)،د.ب.ن، 2009.
6. **حسن طاهر داود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.
7. **حنان ريحان المبارك المضحكي**، الجرائم المعلوماتية،(دراسة مقارنة)، منشورات الحلبي الحقوقية،بيروت، لبنان،2014.
8. **محمد أمين الرومي**، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر، 2004.
9. **محمد أمين أحمد الشوابكة**، جرائم الحاسوب والانترنت الجريمة المعلوماتية، مكتبة دار الثقافة للنشر و التوزيع،عمان، الأردن، 2005.
10. **محمد زكي أبو عامر**، الإجراءات الجنائية، ط7، دار الجامعة الجديدة، مصر،2002.
11. **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الإسكندرية، مصر، 2004.
12. **محمد عبد الله ابو بكر السلامة**، جرائم الكمبيوتر والانترنت ، منشاة معارف،الإسكندرية، مصر 2006.

13. **محمود أحمد عبابنة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

14. **محمود نجيب حسني**، شرح قانون العقوبات القسم الخاص جرائم الاعتداء على الأشخاص، دار النهضة العربية،القاهرة، مصر، 1978.

15. **منير محمد الجنبيهي، ممدوح محمد الجنبيهي**، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، مصر،2006.

16. **منى الأشقر جبور**،السيبيريانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، مصر، د.س.ن.

17. **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع،عمان، الأردن، 2008.

18. **سعيدى سليمة حجاز بلال**، جرائم المعلومات و الشبكات في العصر الرقمي، دار الفكر الجامعي، مصر، 2017.

19. **عبد الفتاح بيومي حجازي**،مكافحة جرائم الكمبيوتر و الانترنت، دار النهضة العربية، مصر، 2009.

20. **عبد الله عبد الكريم عبد الله**، جرائم المعلوماتية والانترنت الجرائم الالكترونية،منشورات الحلبي الحقوقية،بيروت، لبنان، 2007.

21. **عمرو عيسى الفقى**، الجرائم المعلوماتية جرائم الحاسب الآلي والانترنت في مصر والدول العربية، المكتب الجامعي الحديث، مصر،د.س.ن.

22. **عفيفى كامل عفيفى**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، (دراسة مقارنة).ط2، منشورات حلبي الحقوقية، بيروت، لبنان، 2007.

23. **علي جبار الحسيناوي**، جرائم الحاسوب و الانترنت، دار اليازوري العلمية للنشر والتوزيع،عمان، الأردن، 2009.

24. **علي عدنان الفيل**، الإجرام الالكتروني، (دراسة مقارنة) ،مكتبة زين الحقوقية والأدبية،عمان، لبنان، 2011.

25. **عماد مجدي عبد الملك**، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر، 2011.

26. **عمار عباس الحسيني**، جرائم الحاسوب و الانترنت الجرائم المعلوماتية، منشورات زين الحقوقية،بيروت، لبنان، 2017.

27. **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومه للطباعة النشر و التوزيع، الجزائر، 2007.

28. **خالد ممدوح إبراهيم**،أمن الجريمة الإلكترونية، الدار الجامعية للنشر، مصر، 2008.

29. .....، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009.

30. **ذيب بن عايض القحطاني**، المدخل إلى امن المعلومات، مكتبة الحميضي، الرياض، 2010.

2 – الرسائل والمذكرات الجامعية:

أ-رسائل الدكتوراه:

1- **أدم عبد البديع ادم حسين**، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي(دراسة المقارنة)، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة القاهرة، 2000.

2-**هروال هبة نبيلة**، جرائم الانترنت (دراسة مقارنة)، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق و العلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2013-2014.

3-**حفصي عباس**، جرائم التزوير الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه،تخصص شريعة وقانون، كلية العلوم الإنسانيةوالعلوم الاسلامية، جامعة أحمد بن بله، وهران،2014-2015.

4-تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته،كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية،الرياض، 2009.

ب-مذكرات الماجستير:

1-**بن عقون حمزة**، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة،2011-2012.

2-**يوسف خليل يوسف العفيفي**، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة، مذكرة لنيل شهادة الماجستير، تخصص قانون عام، كلة الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

3-عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، مذكرة ماجستير، تخصص قانون عام، جامعة الشرق الأوسط، د.ب.ن، 2014

ج-مذكرات الماستر:

1-**بعرة سعيدة**، الجريمة الالكترونية في التشريع الجزائري(دراسة مقارنة)، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة ،2015-2016.

2- **بن تواتي خليل**، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق و العلوم السياسية، جامعة محمد لمين دباغين، سطيف،2016-2017.

3– المقـــــالاتوالملتقيات:

1-**حفوظة الأمير عبد القادر ، غرديان حسام**، «الجريمة الالكترونية و آليات التصدي لها»، مداخلة ألقيت في الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الاتحاد العالمي للمؤسسات العلمي، الجزائر، في 29 مارس 2017.ص ص.83-106.

2-.**ذياب موسى البداينة**،«الجرائم الالكترونية: المفهوم والأسباب، ملتقى علمي حول الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية»، الأردن، خلال الفترة من 2 الى 4 سبتمبر 2014.

3-**عباوي نجاة**، الإشكالات القانونية في تجريم الاعتداءات على أنظمة المعلومات، دفاتر السياسة والقانون، عدد 16، 2017، ص ص 279-292.

4-**عاقلي فطيلة**، «الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري»، مداخله ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية، الاتحاد العالمي للمؤسسات العلمية، طرابلس، لبنان، يومي 24 و 25 مارس 2017.ص.115-136.

5-مزيود سليم، «الجرائم المعلوماتية وواقعها في الجزائر وآليات مكافحتها»، *المجلة الجزائرية للإقتصاد و المالية*، العدد01، أفريل2014، ص ص 94-107.

6-**محمد الأمين البشرى**،« تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت»، حلقة علمية حول الانترنت و الإرهاب، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، القاهرة، خلال الفترة من 15 إلى 19 نوفمبر 2008.

7-**نمديلي رحيمة**، «خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة»، مداخلة ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية، الاتحاد العالمي للمؤسسات العلمية، طرابلس، لبنان، يومي 24 و 25 مارس 2017.ص ص.95-114.

4-النصوص القانـــونية:

1- أمر رقم 66-156، مؤرخ في 08 يونيو 1966، يتضمن قانون العقوبات، معدل ومتمم، ج.ر.ج.ج.د.ش عدد 49، لتاريخ 11 يونيو 1966.(معدّل ومتمّم).

2- أمر رقم 75-58، مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج.ر.ج.ج.د.شعدد 78 لتاريخ 30 سبتمبر 1975. (معدّل ومتمّم).

3-قانون رقم 09-04، مؤرخ في 05 أوت 2009،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،ج.ر.ج.ج.د.شعدد 47 لتاريخ 16 أوت 2009.

ثانيًا – باللغة الفرنسية:

I –OUVRAGES

1-**ROSE Philippe**, La criminalité informatique, 2e édition, que sais-je ?, Paris, 1996.

II–THESES DE DOCTORAT

1-**BOOS Romain**, La lutte contre la cybercriminalité au regard de l'action des Etats, thèse pour obtention du grade Docteur en droit, option droit privé et sciences criminelles, Faculté de droit, sciences économiques et gestion Nancy, Université de Lorraine, 2016.

2- **TANO-BIAN Anmonka Jeanine- Armelle**, La répression de la cybercriminalité dans les Etats de l'Union Européenne et de l'Afrique de l'Ouest, Thèse pour obtention du grade de Docteur en droit public, Faculté de Droit, Université de Paris Descartes, Paris, 2015.

III – ARTICLES :

1-**KELCI Sevgi**: « Vol, fraude et autres infractions semblables et internet », *Lex-Electronica*,vol 12, n° 1, 2007, pp. 1 - 22.

2-PETIT Marie-Noëlle, « Cybercriminalité : du virtuel au réel », *Rhizome*, vol 3, n°63, 2016, pp.14-14.

3-**PRADEL Jean**, « Les infractions relatives à l'informatique », *R.I.D.C*, vol 42, n°42, 1990, pp.815-825.

4-QUEMENER Myriam,« Concilier la lutte contre la cybercriminalité et l'éthique de liberté», *Sécurité et Stratégie*, vol 01, n°5, 2011, pp.56-67.

الفـــــــــهرس

ملخص باللغة العربية

يعتبر الانترنت أهم الاختراعات التي توصل إليها العقل البشري والتي فرضت نفسها في الوقت الحالي. ومن بين المخاطر التي تسببها هذه الوسيلة نجد أخطرها وأكثرها تعقيداً ما يصطلح عليها بالجريمة السيبريانية.

تعد الجريمة السيبريانية من أحدث الجرائم المرتبطة بالانترنت، والتي تشكل خطرا جسيما على الأمن الإنساني.

وعلى هذا الأساس، تهدف هذه الدراسة إلى ألقاء الضوء على هذه الجريمة لاسيما البحث في أنواعها وكيفية تعامل المشرع الجزائري معها.

Résumé en langue française

Toute invention humaine porteuse de progrès peut être aussi génératrice de comportements illicites. Le coté élogieux d'internet occulte la face la plus redoutable ; et parmi les menaces liées à cet outil, une démarque par sa dangerosité et sa complexité : la cybercriminalité.

Celle-ci est l'une des nouvelles formes de criminalité ou de délinquance sur le réseau internet, dont les conséquences se relèveêtreparticulièrement grave pour la sécurité humaine.

A cet effet, cette étude porte un peu de lumière sur la question de la cybercriminalité, sa typologie et surtout le traitement de la législation algérienne à leurs égards.