



الإجرام المعلوماتي و خطورته Cybercrime and Its Dangers

البقيرات عبد القادر

جامعة الجزائر 1 بن يوسف بن خدة، الجزائر

/

الحاج الطاهر زهير¹

جامعة الجزائر 1 بن يوسف بن خدة، الجزائر

elhadjtaharzoheir80@gmail.com

تاريخ القبول للنشر: 2025-09-12

تاريخ الاستلام: 2025-08-24

ملخص:

إن التقدم الهائل في تقنية المعلومات و ما نتج عنه من إستخدام مفرط لها في شتى مناحي الحياة اليومية للأفراد أو الدول على حد سواء بإعتبار أنها أصبحت وسيلة لا غنى عنها فرضت نفسها بشكل غير مسبوق، إلا أنه رغم ما ترتب على إستعمالها من آثار إيجابية ملموسة على مختلف الأصعدة، فهي لا تخلو من آثار سلبية تتجلى في سوء إستعمال هاته التقنيات الحديثة و بطريقة غير مشروعة، الأمر الذي أدى إلى ظهور طائفة جديدة من الجرائم أطلق عليها إسم الجرائم المعلوماتية، التي أصبحت تشكل تهديدا خطيرا لأمن وإستقرار الدول إضافة إلى إعتدائها على حرمة الحياة الخاصة للأفراد

الكلمات المفتاحية: الجريمة المعلوماتية، المجرم المعلوماتي، انتهاك خصوصية الأفراد، المساس بأمن و استقرار الدول.

Abstract:

The tremendous advancement in information technology, and its consequent excessive use in various aspects of daily life—by individuals and states alike—given that it has become an indispensable tool that has asserted itself in an unprecedented manner, has undoubtedly yielded tangible positive effects on multiple levels. However, despite these benefits, it is not without negative consequences, particularly the unlawful use of such modern technologies. This has led to the emergence of a new category of crimes known as cybercrimes, which have come to pose a serious threat to the security and continuity of states, in addition to infringing upon individuals' right to privacy.

Keywords: keywords must not exceed 05 words.

¹ الحاج الطاهر زهير



مقدمة:

شهد العالم في القرن الواحد والعشرون ثورة تكنولوجية غير مسبوقة نتج عنها ظهور أجهزة الوسائل الإلكترونية أصبحت لا غنى عنها في الحياة الاجتماعية والإقتصادية والأمنية، غير أنه زيادة على الجانب التنموي وتقريب العلاقات بين الناس في جميع أنحاء المعمورة وتسهيل حياة الأشخاص وكذا في مجتمع الدول، إلا أنها كانت سببا مباشرا في ظهور نوع جديد من الجرائم أصبحت تشكل مصدر الخطر بالنسبة للأفراد والمجتمعات.

غير أن إستخدام التقنيات الحديثة ليس له جانب إيجابي فقط بل لأه أيضا جانب سلبي، والذي نتج عن الإستعمال المفرط والغير شرعي لهذه الأجهزة المتطورة، مما أدى إلى ظهور طائفة جديدة من الجرائم عرفت بالجرائم المعلوماتية، هاته الجرائم التي أصبحت تهدد الجميع سواء كانوا مرتبطين بهذه التقنيات الحديثة أم، ذلك لأن مخاطر هاته الجرائم لا تنحصر عند مستعملي أجهزة الحاسب الآلي المرتبط بشبكة الأنترنت وإنما تتسع لتشمل ضحايا آخرين .

و من هنا يدفعنا الأمر إلى طرح الإشكالية التالية وهي : إلى أي مدى أصبحت الجريمة المعلوماتية تشكل تهديدا خطيرا على الأشخاص والدول على حد سواء؟ إنطلاقا من هاته الإشكالية المطروحة تتضح لنا أهمية دراسة الموضوع الحالي من خلال التطرق إلى الإجرام المعلوماتي عن طريق تحديد مفهوم الجريمة المعلوماتية وكذا المجرم المعلوماتي وتبيان مخاطر الجريمة المعلوماتية على الأشخاص وكذا مخاطرها على أمن الدول سواء في المجال الأمني أو في المجال المالي والإقتصادي.

وبغية الإجابة على هاته الإشكالية المطروحة إرتأينا إتباع الخطة التالية :

المبحث الأول: الإجرام المعلوماتي

المطلب الأول: ماهية الجريمة المعلوماتية

المطلب الثاني: المجرم المعلوماتي

المبحث الثاني: خطورة الجريمة المعلوماتية

المطلب الأول : خطورة الجريمة المعلوماتية على الأشخاص
المطلب الثاني : خطورة الجريمة المعلوماتية على الدول
الخاتمة :

1- المبحث الأول : الإجرام المعلوماتي

لقد أدى الإستخدام السيئ و الغير شرعي للحاسب الآلي و الأنترنت إلى ظهور أفعال مجرمة وصفت بالجرائم المعلوماتية و التي تختلف إختلافا جذريا عن أنواع الجرائم الأخرى و كما تختلف أيضا من حيث مرتكب هاته الجرائم الذي يعرف بالمجرم المعلوماتي الذي هو أيضا يتميز بصفات مختلف عن باقي المجرمين التقليديين .

و عليه سوف نتطرق في هذا المبحث إلى مفهوم الجريمة المعلوماتية في المطلب الأول ثم إلى المجرم المعلوماتي في المطلب الثاني .

المطلب الأول : ماهية جريمة المعلوماتية

من أجل تحديد مفهوم الجريمة المعلوماتية بإعتبارها جريمة من نوع خاص لا بد أولا التطرق إلى تعريفها ثم إلى خصائصها ثانيا ثم إلى طبيعتها القانونية ثالثا .

الفرع الأول : تعريف الجريمة المعلوماتية

إن الجريمة كفعل مجرم و معاقب عليه لا تقوم على أسس ثابتة وإنما متغيرة وتتأثر بالزمان والمكان الذي ترتكب فيه، وعرفت الجريمة بأنها ذلك السلوك الانساني المحظور الذي يخل بسلامة المجتمع وأمنه، وعرفها الدكتور محمود مصطفى الجريمة بأنها " (عبارة عن امتناع أو عمل يرتب القانون على إتيانه عقوبة) (العملي).

وأما بالنسبة للجريمة المعلوماتية فقد أعطيت لها عدة تعريفات بشأنها غير أنها اختلفت هذه التعريفات فيما بينها بحسب المعيار الذي تقوم عليه، ويمكن تقسيمها إلى ثلاثة أقسام، قسم يعتمد في تعريفه للجريمة المعلوماتية على معيار موضوع الجريمة بينما القسم الآخر يستند في تعريفه لها على معيار وسيلة إرتكاب الجريمة وقسم آخر يستند في تعريفه لها على مرتكب الجريمة المعلوماتية .



وعليه سوف نتطرق الى تعريف الجريمة المعلوماتية بحسب المعيار الذي تعتمد عليه إلى اتجاهات ثلاثة :

الإتجاه الأول: التعريفات التي تركز على موضوع الجريمة

لقد استند هذا الإتجاه في تعريف الجريمة المعلوماتية إلى فكرة الجريمة التي تقع ضد الحاسب أو النظام وليس بإعتبار الحاسب وسيلة في إرتكابها، لذلك تم تعريف الجريمة المعلوماتية على أنها نشاط غير مشروع موجه لنسخ أو حذف أو تغيير أو للوصول على المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه (القهوجي، 1997).

وهناك مجموعة من التعريفات الفقهية للجريمة المعلوماتية التي جاء بها فقهاء هذا الإتجاه، فحسب الأستاذ ArtarSolertz فإن الجريمة المعلوماتية تعرف على أنها : " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " (العملي)، وعرفها الدكتور علي القهوجي بأنها : " سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها " (قشقوش، 1992)، وتم تعريفها من قبل مكتب المحاسبة العامة للولايات المتحدة الأمريكية GOA بأنها : "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات وإضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر".

إن اعتماد معيار موضوع الجريمة كأساس لتعريف الجريمة المعلوماتية يعد من أهم المعايير في تعريفها غير أنه لا يحيط بها كاملة مما أدى إلى بروز اتجاه آخر يعتمد تعاريف أخرى للجريمة المعلوماتية تستند إلى مرتكب الجريمة ووسيلة ارتكابها .

الإتجاه الثاني: التعريفات التي تركز على أساس وسيلة ارتكاب الجريمة

هذا الاتجاه اعتمد في تعريفه للجريمة المعلوماتية على أساس الوسيلة المستعملة في ارتكابها، لذلك عرفت هاته الجريمة على أنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب بإستخدام الحاسب الآلي، كما عرفت من

قبل الاستاذ جون فور ستير بأنها "فعل إجرامي يستخدم الكمبيوتر في ارتكابها كأداة رئيسية" (العملي)، كما تم تعريفها على أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة أو هدف لتنفيذ العمل الإجرامي المقصود (عياد، 2007)، كما عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا" (رستم، 1992)، ومن التعريفات التي أعطيت للجريمة المعلوماتية في هذا الاتجاه ما عرفها كل من A.Hard castle, R. ToH بأنها: "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعد عمليات فصلية داخل الحاسب" أو بمفهوم آخري التي يكون للحاسب فيها دورا ايجابيا اكثر من سلبية".

رغم التعريفات التي جاءت في هذا المجال إلا أنها اتسمت بالضيق ذلك أن اشتراط استخدام الحاسب الآلي لوحده في تحديد وصف الجريمة المعلوماتية يبعد كثيرا من الأفعال من دائرة التجريم لذلك جاءت تعريفات أخرى في إتجاه آخر تجعل من مرتكب الجريمة كمعيار لتعريف الجريمة المعلوماتية .

الاتجاه الثالث: التعريفات التي تركز على مرتكب الجريمة

ذهب فقهاء هذا الإتجاه إلى تعريف الجريمة المعلوماتية بالاعتماد على معيار مرتكب الجريمة أي أنه يجب أن تتوافر سمات شخصية في مرتكب الفعل وهي المعرفة و من بين هاته التعريفات ما جاء به David thompson بأنها : "أية جريمة يتطلب لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب" (العملي)، ومن التعريفات أيضا التي تقوم على أساس سمات شخصية مرتكب الفعل عرفتها وزارة العدل الأمريكية بأنها : "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من إرتكابها".

إن اعتماد هذا الاتجاه على معيار شخصي متصل بمرتكب الفعل وضرورة توافره على معرفة بالتقنية هو في حد ذاته إنقاص من الجريمة المعلوماتية في حد ذاتها.



وأمام قصور هاته التعريفات التي جاء بها أصحاب الاتجاه الثلاثة سواء تلك التي تستند في تعريف الجريمة المعلوماتية على موضوع الجريمة أو تلك التي تستند على وسلية ارتكابها أو تلك التي تقوم على اشتراط سمات شخصية في مركب الفعل فقد ظهرت تعريفات أخرى للجريمة المعلوماتية، منها ما جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقة المجرمين المنعقد في فيينا سنة 2000 والذي عرف الجريمة المعلوماتية كما يلي : "يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (القانون رقم 04-09 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ج.ج، العدد 47).

أما بالنسبة المشرع الجزائري قد تنطرق إلى الجريمة المعلوماتية في قانون العقوبات الجزائري تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات في القسم السابع مكرر من الفصل الثالث المواد 394 مكرر إلى المادة 394 مكرر 8 منهم إلا أنه لم يتطرق إلى تعريفها.

غير أن المشرع تطرق لتعريف الجريمة المعلوماتية في القانون رقم 04-09 المؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمكافحة في الفصل الأول منه تحت عنوان أحكام عامة وهذا في المادة الثانية منه بقولها : " يقصد في مفهوم هذا القانون بما يأتي:

أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية" (مؤتمر الأمم المتحدة لمنع الجريمة ومعاقة المجرمين، فيينا 10-17 أبريل 2000).

إن تعريف الجريمة المعلوماتية يجعلها تتميز عن غيرها من الجرائم التقليدية الأخرى بمجموعة من الخصائص، وعليه نتطرق في الفرع الثاني إلى خصائص الجريمة المعلوماتية.

الفرع الثاني: خصائص الجريمة المعلوماتية

باعتبار الجريمة المعلوماتية هي نتاج لتقنية المعلومات، مما يجعلها جريمة من نوع خاص تنفرد بمجموعة من الخصائص نذكرها على النحو التالي :

أولا - خطورة الجريمة المعلوماتية

وذلك لكونها تمس بالإنسان في فكره وفي شخصه وفي حياته الخاصة وكذلك في أمواله كما أنها تمس بأمن وإستقرار الدول والمجتمعات، ولقد قدمت نقابة المحامين الأمريكيين سنة 1987 تقريرا تضمن الحجم الهائل للخسائر التي لحقت بحوالي ثلاثمائة من أكبر الشركات هناك، إذ يشير التقرير إلى معدل الخسارات السنوية لتلك الشركات الذي يتراوح بين 2 إلى 15 مليون دولار سنويا.

ثانيا - الجريمة المعلوماتية من الجرائم العابرة للحدود

من أهم خصائص الجرائم المعلوماتية أنها تتميز بصفة الدولية فهي لا تعترف بالحدود، إذ أنها لا تقتصر على دولة بعينها، ذلك أن التطور التكنولوجي في مجال المحاسبة وبرامجها وشبكات الإتصال وخاصة الإنترنت جعل منها تتصف العالمية، عن طريق الإستخدام الغير المشروع لهذه الوسيلة، فيمكن إرتكاب هذه الجريمة عن طريق كمبيوتر متواجد في دولة (أ) بإختراقه لكمبيوتر أو إتلاف معطياته متواجد في دولة (ب) عن طريق إستخدام كمبيوتر متواجد في دولة (ج)، فالجريمة أرتكبت في بلد والنتيجة الإجرامية في بلد آخر و الوسيلة المستعملة هي كمبيوتر متواجد في بلد غير البلدين السابقين.

ثالثا - لارتكابها يتطلب وجود كمبيوتر ومعرفة تقنية بإستخدامه

يشتمل الحاسب الآلي على المكونات المادية وملاحقاتها وكذلك على المكونات المعنوية والتي تشمل جميع الكيانات وبرامج التشغيل إضافة إلى إتصاله بشبكة الانترنت. ذلك أن الحاسب العنصر المهم الذي يمكن الشخص من تنفيذ الجريمة



أيا كان نوعها (الجنبيهي، 2006)، فالحاسب وما ترتبط به من تقنيات تلعب أدوارا عديدة في هذه الجرائم، فهو إما أن يكون موضوعا للجريمة أو هدفا لها، أو أداة تساعد في تخطيط وتطوير تنفيذها، أو قد تكون مثالا أو نموذجا للجريمة.

رابعا - صعوبة إكتشاف الجريمة المعلوماتية والتحقيق فيها وإثباتها

إن البيئة التي ترتكب فيها الجريمة المعلوماتية هي بيئة إفتراضية رقمية لا تترك خلفها أثارا مادية يمكن من خلالها فك لغز الجريمة والوصول إلى مرتكبها وحتى ولو وجدت هذه الأثار فإنه يصعب المحافظة عليها كدليل إثبات، كما أن ضبطها يصعب إذا لم يتم من قبل مختصين ومؤهلين في التحقيق في مثل هذا النوع من الإجرام، وما يزيد من صعوبة إكتشاف هاته الجريمة هو إمكانية إرتكابها عبر الدول فقد يكون الفاعل في دولة أو قارة و الضحية في دولة أو قارة أخرى مما يصعب إكتشافها والتحقيق فيها وضبط الدليل الإلكتروني من أجل إثباتها، وكذا القانون الواجب التطبيق في هاته الحالات إضافة إلى ضعف التنسيق الدولي، الأمر الذي يؤدي إلى زيادة مرتكبي هاته الجرائم وكذا ضحاياهم، وإنعدام الأثر الخارجي الظاهر يعود إلى أن تنفيذ الجريمة يتم أصلا بالنبضات الكهربائية، حيث تتغير وتمحى الأرقام والدلالات والمعلومات من ذاكرة الحاسب (وهيب، 2014).

كما أن نقص الخبرة الفنية والتقنية لجهات للبحث والتحري في هاته الجرائم يجعل منها تمتاز بخاصية صعوبة التحقيق فيها وإكتشافها، كما أن إكتشافها في بعض الحالات يكون من باب الصدفة فقط، والدليل على ذلك أنه لم يكتشف منها إلا القليل ولم يبلغ عنها إلا البعض فقط بعد إكتشافها الأمر الذي يجعل وجود جهات تحقيق مؤهلة بقدرات فنية وتقنية في هاته الجرائم من أولى الأولويات.

وهو الأمر الذي تم إستحداثه في الجزائر بإنشاء خلايا مختصة في مكافحة الجرائم المعلوماتية على المستوى المركزي وكذا المحلي إضافة إلى إنشاء مدرسة عليا للأمن السيبراني.

إن الخصائص الأربعة السالفة الذكر تعد من أهم الخصائص التي تميز الجريمة المعلوماتية عن غيرها من الجرائم إضافة إلى أن الجريمة المعلوماتية لا ترتكب من قبل مجرم عادي تقليدي وإنما من قبل مجرم من نوع خاص وهو ما يطلق عليه بالمجرم المعلوماتي الذي هو محل إعتبار في دراستنا للجريمة المعلوماتية وتحديد خطورتها.

وعليه سنتطرق فيه في دراستنا للمطلب الثاني إلى المجرم المعلوماتي.

المطلب الثاني: المجرم المعلوماتي

لقد أدى ظهور الجريمة المعلوماتية إلى ظهور طائفة جديدة من المجرمين إلى عالم الإجرام، غير أنهم ليسوا بالمجرمين العاديين أو التقليديين بل يتصفون بصفات وخصائص تجعلهم محل إعتبار من قبل جميع المهتمين بالإجرام المعلوماتي سواء كانوا فقهاء أو باحثين أو حتى من قبل الأجهزة الأمنية للدول المكلفين بمكافحة هذا النوع من الإجرام، إن التعرف على السمات التي يتميز بها المجرم المعلوماتي تسعى إلى مواجهة هذا النمط الجديد من المجرمين. ويرى الأستاذ Parker الذي يعد من أهم الباحثين في الجريمة المعلوماتية والمجرم المعلوماتي أن المجرم المعلوماتي حتى وإن كان يتميز ببعض الصفات الخاصة إلا أنه مرتكبا لفعل إجرامي يستحق توقيع العقاب عليه (عطية، 2009) (عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، الإسكندرية 2009).

وسنتطرق في هذا المطلب إلى صفات المجرم المعلوماتي في الفرع الأول ثم إلى أصناف المجرم المعلوماتي في الفرع الثاني.

الفرع الأول: الخصائص المميزة للمجرم المعلوماتي

ينفرد المجرم المعلوماتي بمجموعة من الخصائص التي تجعله ينفرد عن باقي المجرمين شأنه في ذلك شأن الجريمة المعلوماتية، فهو يختلف عن المجرمين التقليديين في عدة خصائص ومميزات، ولقد أطلق عليها الأستاذ Parker بمصطلح Skkam، وهو جمع الأحرف الأولى للكلمات التي تعبر عن خصائصه المميزة وهي المهارة Skills، المعرفة Knowledge، الوسيلة Resources، السلطة Authority، وأخيرا



الباحث Motives (عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، الإسكندرية 2009)، وسنتطرق إلى هاته الخصائص على النحو التالي:

أولا - خاصية المهارة

إن إرتكاب الجريمة المعلوماتية يتطلب من مرتكبها أن يكون متمتعا بقدر كبير من المهارة في مجال تكنولوجيا المعلومات والتي يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو البحث أو مجرد التفاعل مع الآخرين، كما لا يشترط في المجرم المعلومات أن يكون متحصلا على شهادات علمية في مجال تكنولوجيا المعلومات، بل يكفي أن يكون يتمتع بمهارة في عمل الحاسوب والانترنت.

ثانيا - خاصية المعرفة

من بين الخصائص المميزة للمجرم المعلوماتي هي خاصية المعرفة وهو أن يكون المجرم المعلوماتي على معرفة بكافة الظروف التي تحيط بالجريمة المرتكبة في الفضاء الإلكتروني، وفي أغلب الحالات ما يكون مرتكب الجريمة متخصصا، إذ يصعب على الشخص المبتدئ أو الجاهل أن يرتكب جريمته بطريق هاته التقنية إذ يستوجب الدقة والتخصص في هذا المجال لإختراق أنظمة حماية الحاسب الآلي كما في المؤسسات المالية مثلا (عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، الإسكندرية 2009).

ثالثا - خاصية الوسيلة

تعد الوسيلة المستعملة في مجال الجرائم المعلوماتية المتمثلة في الوسائل المطلوبة للتلاعب بأنظمة الحاسب الآلي، وغالبا ما تتميز بالبساطة وسهولة الحصول عليها، غير أنه عندما يكون نظام الحاسب الآلي الذي يحتوي على البيانات المستهدفة غير مألوف، كانت الوسائل المطلوبة أكثر صعوبة في الحصول عليها لكونها تنحصر عند فئة قليلة من الأفراد هم عادة القائمون على تشغيل النظام (الحجازي، 2008).

رابعا - خاصية السلطة

تتمثل السلطة التي يتمتع بها المجرم المعلوماتي في المزايا والحقوق التي تمكنه من ارتكاب الجريمة المعلوماتية فقد تمتد في الشيفرة التي تسمح له بالدخول الى النظام الذي يحتوي على المعطيات، والتي تمنح للمجرم المعلوماتي مزايا متعددة كتعديل البيانات أو محوها، وقد تتمثل هاته السلطة في السماح له بإستعمال الحاسب الآلي أو الدخول إلى مكان تواجد الحاسب الآلي.

خامسا - خاصية الباعث

إن الباعث وراء إرتكاب الجريمة المعلوماتية في أغلب الحالات هو تحقيق مكاسب مادية غير مشروعة، غير أنه في بعض الحالات يكون الباعث في مجرد الرغبة في الإنتقام أو التحدي من أجل إظهار قدرتهم على إختراق وسائل الحماية وأمن الانظمة المعلوماتية وفي بعض الحالات يكون الباعث ينطوي على التفاخر بأنفسهم. وفي بعض الحالات يهدف المجرم المعلوماتي من وراء ارتكاب الجريمة المعلوماتية بدافع حل مشكله شخصيه فقط وليس الجشع. (الحجازي، 2008)

وفي كل الأحوال فإن المجرم المعلوماتي يرتكب الجريمة المعلوماتية بدون عنف لذلك قيل على أنه مجرم غير عنيف.

غير أنه لا يجب أن نستخلص إنعدام خطر الإجرام المعلوماتي بحجة عدم توافر النوايا الإجرامية، ذلك لأنه يمكن أن يترتب عليه أضرار جسيمة على الفرد أو المجتمع ككل يصعب تداركها، وعليه يمكن تصنيف المجرم المعلوماتي إلى أصناف، وهو ما سوف نقوم بالتطرق إليه في الفرع الثاني.

الفرع الثاني : أصناف المجرم المعلوماتي

لقد أسفرت الدراسات المختلفة إلى تقسيم مجرمي المعلوماتية إلى سبعة أنماط من المجرمين في هذا المجال غير أن وجود مجرم معلوماتي في طائفة واحدة لا يعني أنه يمكن أن ينتهي لطائفة أخرى أو عدة طوائف.

الطائفة الاولى: Pranksters وهو المجرمون المعلوماتيون الذين يرتكبون هذه الجرائم بغرض المزاح والتسلية مع الآخرين دون النية إلحاق الضرر بالآخرين.



الطائفة الثانية: Hackers فهم المجرمون المعلوماتيون الذين يهدفون إلى اختراق الحواجز الأمنية الموضوعية داخل أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها وهذا بهدف الفضول وإكتساب الخبرة، وغالبا ما يعودون إلى اختراق هذه الأنظمة بعد تطوير الحماية فيها مما يبعث فيهم روح التحدي (موسى، 2003).

الطائفة الثالثة: Malicious hackers: يهدف هؤلاء المجرمون المعلوماتيون إلى إلحاق الضرر بالغير وليس الحصول على مكاسب مادية وتضم هذه الطائفة مخترعي فيروسات الحاسبات الآلية وموزعيها.

الطائفة الرابعة: Software crackers: وهي طائفة من المجرمين المعلوماتيين المتخصصة في فك شفرات البرامج وليس تخريبها، وهذا بخرق مقاييس الحماية ويقومون بهذه العملية بغرض تحقيق الربح المادي (فريد، 2005).

الطائفة الخامسة: Career criminals: يهدف النشاط الإجرامي لهاته الطائفة من المجرمون المعلوماتيون إلى تحقيق الربح المادي بطرق غير مشروعة وعادة ما يتكثرون في مجموعات أو منظمات إجرامية خطيرة وينطبق على أفعالهم وصف الجريمة المنظمة.

الطائفة السادسة: Extrême advocates: تضم هاته الفئة من المجرمين المعلوماتيين الجماعات المتطرفة الإرهابية التي لها افكار سياسية واجتماعية معتقدات دينية ويرغبون فرضها بالعنف على الغير باللجوء الى هذا النشاط الإجرامي.

الطائفة السابعة: Mercenaries: وتضم هاته الطائفة المجرمون المعلوماتيون الذين يتم إستخدامهم الاقترحام برامج وأنظمة الحاسوب لتدميرها أو سرقتها مقابل مبالغ مالية وعادة ما يتم إستخدامهم من قبل الافراد أو المؤسسات وحتى الحكومات (موسى، 2003).

وبعد تطرقنا في المبحث الأول إلى الإجرام المعلوماتي سنتطرق إلى خطورة هذا النوع من الإجرام على كل من الأشخاص والدول.

2- المبحث الثاني: مخاطر الجريمة المعلوماتية على الأشخاص و الدول

بعد إدراك خطورة وسهولة إرتكاب الجريمة المعلوماتية في آن واحد التي أنتجها الفضاء الافتراضي بدأت فكرة مكافحة هذا النوع من الإجرام تحظى بالاهتمام من قبل الدول والمنظمات الدولية وحتى المؤسسات والأفراد غير أنه مهما كانت طرق الحماية الفنية الموجودة، إلا أنها غير قادرة على تحقيق الأمن المعلوماتي بصفة مطلقة ذلك أنه كلما أحرزت وسائل حماية الأنظمة المعلوماتية تقدما زادت وسائل اختراقها تطورا .

كما أن جرائم المعلوماتية تشكل تهديدا حقيقيا للأفراد و الدول على حد سواء وعليه سنتطرق في هذا المبحث إلى مخاطر الجريمة المعلوماتية على الأشخاص في المطلب الأول ثم إلى مخاطرها على الدول في المطلب الثاني.

المطلب الأول : مخاطر الجريمة المعلوماتية على الأشخاص

للجرائم المعلوماتية المرتكبة على الأشخاص عدة مخاطر ويمكن إيجازها وتقسيمها إلى قسمين من التهديدات والمخاطر الواقعة على حياة الخاصة لأفراد والمخاطر الواقعة على الأموال.

ويمكن التطرق إلى الجرائم المعلوماتية التي تشكل تهديدا على الأشخاص إلى جرائم الاعتداء على حرمة الحياة الخاصة للأفراد جرائم السب والقذف و الجرائم المخلة بالآداب العامة وعلى سنتطرق الى كل من هذه الجرائم المرتكبة في شبكة الإنترنت والتي تشكل تهديدا خطيرا للأفراد بسبب إستفحالها وإنتشارها الواسع.

أولا - المخاطر الواقعة على حرمة الحياة الخاصة للأفراد

تكفل جميع الدساتير و المواثيق الدولية حماية الحياة الخاصة للأفراد، غير أن الجريمة المعلوماتية تشكل تهديدا كبيرا لهذا الحق المكفول دستوريا والمحمي قانونا، وهذا من خلال إستغلال المعلومات الشخصية المحفوظة في نظام المعلومات في غير الهدف الذي جمعت من أجله هذه البيانات الشخصية أو الدخول الى البيانات المخزنة دون إذن صاحبها وإطلاع الغير لها او ابتزاز صاحب هذه المعلومات الشخصية و الخاصة به.



لقد أقرت جميع الدساتير والمواثيق الدولية والقوانين الداخلية للدول حرمة الحياة خاصة للأفراد وهي منصوص عليها في الدستور الجزائري الجديد (دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020، ج.ر.ج.ج، العدد 62، الصادرة بالتاريخ 2020/12/30). في المادة 39 منه بقولها: "تضمن الدولة عدم إنتهاك حرمة الإنسان". غير أن النظام المعلوماتي أصبح يشكل تهديدا خطيرا على حرمة الحياة الخاصة للأشخاص من خلال استغلال الفضاء في المساس بحياة الأشخاص الخاصة عن طريق ارتكاب وقائع مجرمة ومعاقب عليها. يقوم المجرم المعلومات بإعداد ملف خاص بشخص المجني عليه يحتوي على بياناته الشخصية بدون علم وإذن صاحبها، وقد يكون قد تم تجميع هذه المعلومات والبيانات الخاصة بالشخصية علم صاحبها بإذنه وهذا لكون المكلف بحفظها قام بإعلام واطلاع الغير عبر شبكه التواصل الاجتماعي دون أن يأذن له صاحب هذه المعلومات الشخصية بنشرها (الملط، 2006).

فقد تكون هذه المعلومات والبيانات الشخصية معالجة معلوماتيا بغية الاحتفاظ بها في النظام المعلوماتي بإعتباره وسيلة لتخزين البيانات الخاصة بالأشخاص أو الموظفين...الخ، ويقوم المجرم المعلوماتي بإختراق النظام المعلوماتي وأخذ هاته البيانات والمعلومات الشخصية التي تتعلق بأسراره المكتوبة، وكتاباته، صوره، سيرته الذاتية، حياته الشخصية والعائلية وتكون هذه المعلومات الشخصية محلا للجريمة المعلوماتية التي تؤدي إلى المساس بالحياة الخاصة للأفراد. وقد يكون المجرم المعلوماتي مرتكب جريمة مساس بحرمة الحياة الخاصة للفرد بشخص عادي يتقن استعمال أجهزة وأنظمة الحاسوب ومتمرس في إختراق أنظمة المعلوماتية، وقد يكون موظف عهدت اليه هذه البيانات والمعلومات الشخصية بحكم وظيفته أو بمناسبتها.

ولقد نص المشرع الجزائري في المادة 303 مكرر من قانون العقوبات على جنحة المساس بحرمة الحياة الخاصة للأشخاص بقولها: "يعاقب بالحبس من ستة 6 أشهر الى ثلاث 3 سنوات وبغرامة من 50,000 دينار جزائري الى 300,000 دينار

جزائري كل من تعتمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضا.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه..."

وعليه فالفرد له أسرار خاصة به لا يجوز للغير الاطلاع عليها بعدما قام بتخزينها في حاسبه الخاص به، ذلك أن الدخول للنظام المعلومات يخلق أوضاعا جديدة على المجتمع في مجال حماية الحياة الخاصة للأشخاص، وإن الحصول غير المشروع على هذه المعلومات الشخصية السرية هو إعتداء على الشخص الإنساني ذاته (الحسيني، 1995).

وفي بعض الحالات يتم جمع وتخزين البيانات الشخصية الخاصة بالفرد بصفة شرعية وبموافقة صاحبها غير أن المكلف بحفظها يقوم بإفشائها أو تسريبها للغير بغية الإضرار بهذا الشخص (عفيفي).

كما أن مخاطر الجريمة المعلوماتية تزداد أكثر بالنسبة للمعلومات المجمعة بينك المعلومات، وذلك أن هذه البنوك تحوز على بيانات خاصة بعملائها وأعضائها ويمكن أن تكون هدفا كافيا لإنتهاكها (عبابنة، 2005).

ثانيا- جرائم القذف والسب

تعد جرائم القذف والسب من أكثر الجرائم وقوعا عبر شبكة الأنترنت إذ يتم بواسطتها الاعتداء والمساس بشرف وكرامة وإعتبار الأشخاص مما يؤدي إلى إحتقار الناس والمجتمع للمجني عليه بعد إسناد إليه واقعة غير حقيقية (الطوالبة، 2008). ولقد نص المشرع الجزائري على جرمي القذف والسب والعقوبات المقررة لها في المواد من 296 إلى 299 من قانون العقوبات في القسم الخامس من الفصل الأول تحت عنوان الاعتداء على شرف واعتبار الأشخاص على حياتهم الخاصة وإفشاء الأسرار.



فقد يكون القذف أو السب عبر البريد الإلكتروني أو شبكة الانترنت بإسناد واقعة أو صورة أو رسالة لا تعبر عن شخص المجني عليه ومن شأنها أن تمس بشرفه وبإعتباره وكرامته، وبهذا تكون للجريمة المعلوماتية مخاطر على شرف وسمعة واعتبار الأشخاص وتهدد مكانتهم في المجتمع وبين عائلاتهم وذوئهم.

ثالثا - الجرائم المخلة بالآداب العامة

تعتبر شبكة الإنترنت أكبر تهديد للروابط العائلية وللقيم التي تحكم المجتمعات، بعدما أصبحت مرتعا للفاحشة والزيلة، و مكانا لتفريغ العقد والمكبوتات لكثير من مرتادي هذا الفضاء السيبراني، وقيامهم بصناعة ونشر الإباحية الجنسية بجميع الوسائل من صور وفيديوهات وحوارات وجعلها في متناول المرتادين لهذا الفضاء الإلكتروني .

وتزداد خطورة الجرائم الإباحية المرتكبة عبر شبكة الأنترنت عندما يكون ضحاياهم قصر و تستهدف هاته الجرائم تحقيق الكسب المادي ومن أبرز الصور الإباحية عبر شبكة الانترنت التي يكون ضحاياها قصر تكون في حالتين، الأولى عن طريق عرض صور و أفلام ومحاادثات منافية للأخلاق والآداب العامة، والثانية عن طريق التحريض على الفسق والفجور (سلاف).

ومن هنا تبرز أهمية حماية الأطفال من مخاطر الجرائم المعلوماتية، وهذا عن طريق الحملات التحسيسية والدور الذي تلعبه أيضا الأسرة في حماية أطفالهم من مخاطر الانترنت وكذا تفعيل الآليات التقنية و الفنية للوقاية و الحماية من هاته المخاطر.

المطلب الثاني : مخاطر الجريمة المعلوماتية على الدول

لقد إمتد تأثير شبكة الانترنت والمواقع الالكترونية على الدول، إذ يقول "توماس فريدمان" أن الدول يتحكم فيها قطاع إلكتروني من المستثمرين المسيطرين على رأس المال في الاقتصاد العالمي وأصبحت شبكات التواصل الاجتماعي وسيلة لبث ونشر الافكار الرجعية والطائفية الهدامة، الأمر الذي أصبح يشكل تهديدا للأمن

القومي للدول، ويشكل خطرا على سيادتها وإستقرارها الاجتماعي، الاقتصادي والأمني.

وعليه سنتطرق الى مخاطر الجرائم المعلوماتية على الدول من حيث أنها تشكل تهديدا على أمنها القومي وكذا إقتصادها الوطني.

أولا - مخاطر الجريمة المعلوماتية على أمن وإستقرار الدول

أخذت وسائل التواصل الإجتماعي صور جديدة على ما كانت عليه في السابق، حيث أصبحت هاته الصورة تتسم بالعنف بشتى أنواعه وكذا التشجيع والتحريض عليه، و أصبحت مجالال خصبا لنشر الأفكار المتطرفة و الهدامة التي تحت على التخريب و العنف و الترهيب و هذا ما يوصف بالإرهاب الإلكتروني الذي أصبح يشكل تهديد حقيقيا للدول ويمس بأمنها وإستقرارها كما أن التنظيمات الإرهابية أصبحت تقوم بتجنيد الاشخاص عن بعد وتوجههم للقيام بأعمال عدائية وتخريبية ضد مجتمعاتهم وحتى أهاليهم و أوطانهم ومن هنا فقد أصبح الإرهاب المعلوماتي يشكل تهديدا خطيرا للأمن الدول و إستقرارها، و لقد نص المشرع الجزائري في قانون العقوبات في القسم الرابع مكرر من الفصل الاول من الباب الاول بجرائم الموصوفة بأفعال إرهابية أو تخريبية من المادة 87 إلى المادة 87 مكرر 18 منه، فجرم فعل الإشادة بالأعمال الإرهابية و تمويلها بأية وسيلة كانت في المادة 87 مكرر4، كذلك القيام بطبع أو نشر الوثائقي او المطبوعات او التسجيلات التي تشيد بالأفعال الإرهابية في المادة 87 مكرر5 كما نصت المادة 87 مكرر11 في فقرتها الأخيرة على تجريم ومعاقبه كل من يستخدم تكنولوجيات الإعلام و الإتصال لإرتكاب الأفعال المذكورة في هذه المادة، و نصت المادة 87 مكرر12 على تجريم ومعاقبه كل من يستخدم تكنولوجيات الإعلام وإتصال لتجنيد الاشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة"، وعليه فقد جاء النص في قانون العقوبات



الجزائري صراحة على الافعال الإرهابية التي ترتكب في الفضاء الإلكتروني بإعتبارها تشكل تهديدا للأمن القومي للدولة.

ثانيا - مخاطر الجريمة المعلوماتية على الإقتصاد الوطني

إن حماية الإقتصاد الوطني لدولة ما لا يقل أهمية عن حماية أمنها القومي ذلك أن قوة الدول تقاس بأمنها و إقتصادها، ولهذا أصبحت الأنظمة المعلوماتية وسيلة للمساس بإقتصاد الدول و إستقرارها المالي، من خلال إستخدام شبكة الإنترنت في إجراء عمليات تحويل مبالغ مالية ضخمة من حسابات إلى أخرى بغرض إخفاء مصدرها الغير مشروع وهو ما يعرف بجريمة غسيل الأموال (الطائي، 2007)، هاته الأخيرة التي ترتكب على نطاق واسع في الفضاء الإلكتروني بإعتباره مجالا خصبا لارتكابها تحت ستار التجارة الإلكترونية، ونقل الأموال من دولة إلى أخرى تحت هويات غير معروفة وفي بعض الأحيان هوية صاحب المال والمحمول له تكون عبارة عن تشفيرات فقط دون الهوية الكاملة للأطراف، و لقد ظهرت طرق جديدة لغسل الأموال القدرة مش عبر شبكة الانترنت وذلك عن طريق إستخدام الانترنت في المقامرة والنشاطات المصرفية المرتبطة بها وكذلك بالنسبة للعمليات البنكية عبر شبكة الانترنت مقارنة مع الاستخدام السابق للأموال (الحجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية، 2008).

إضافة الى جريمة غسيل الأموال عبر شبكة الانترنت التي تمس بالإقتصاد الوطني للدولة هناك أيضا جرائم إقتصادية ترتكب عبر شبكة الانترنت منها عملية الإحتيال والنصب عبر الشبكة، بقيام المجرمين بإستهداف ضحاياهم من خلال إيهامهم بالفوز بمبالغ مالية ضخمة في حالة قيامهم بدفع بعض الدولارات فقط وذلك عن طريق إتباع بعض الخطوات من صنع هؤلاء المجرمين، كإرسال رقم حسابك، رقم هاتفك، رقم حسابك البنكي و إسم البنك... إلخ و هذا بعد إنتحال إسم أو صفة أو مهنة منظمة قانونا بغية سلب أموال الغير، وما ينطبق على الأشخاص الطبيعية ينطبق على الأشخاص المعنوية من المؤسسات المالية والصناعية وكذلك على الدول، إذ يترتب عليه الإضرار بإقتصاد الدول، كذلك

إختراق بطاقات إئتمان لعدد من البنوك في الدول وبعد بذلك يترتب خسائر للإقتصاد من جراء هذا العمل الإجرامي الذي ما كان ليتم لولا شبكة الانترنت، وفي دراسة أجريت سنة 2018 من قبل شركة مايكروسوفت أن الجرائم المعلوماتية كبدت دولة ماليزيا خسائر قدرت بـ 12.2 مليار دولار أمريكي وعليه تعتبر شبكة الانترنت تهديدا خطيرا للإقتصاد الدول.

الخاتمة

أدى التطور التقني والعلمي إلى ظهور تكنولوجيات المعلومات والاتصالات التي أصبحت لها دورا كبيرا في حياتنا اليومية غير أن الإستخدام السيئ لهاته التقنيات الحديثة أدى إلى ظهور طائفة جديدة من الجرائم على قدر كبير من الخطورة على الأشخاص وكذا الدول و أصبحت تشكل تهديدا خطيرا على الأمن العالمي ككل بسبب ما لها من أضرار فتاكة قد يصعب إزالتها . الأمر الذي إستدعى ضرورة تظافر جميع الجهود الوطنية و الدولية من أجل التصدي لهذا النوع من الإجرام الحديث والحد من آثاره السلبية على الفرد و المجتمع و المؤسسات و الدول، و حصرها في الإطار المنفعي الإيجابي الذي وجدت من أجله دون سواه.

قائمة المصادر والمراجع:

المراجع باللغة العربية:

الدساتير:

- دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020، ج.ج.ج، العدد 62، الصادرة بالتاريخ 2020/12/30.

القوانين:

- قانون العقوبات الجزائري
- القانون رقم 04-09 المؤرخ في 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، ج ج ج، العدد 47

الكتب:

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



- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للحركة الحديثة)، الطبعة الأولى، دار البداية، الأردن 2007
 - خالد عياد العملي، إجراءات التحري والعلمية في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع سنة 2011.
 - طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.
 - عبد الفتاح بيومي الحجازي، التزوير في الجرائم الكمبيوتر والإنترنت، مصر 2008.
 - عبد الفتاح بيومي الحجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية)، دار الفكر الجامعي، الإسكندرية، 2008
 - عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة).
 - علي القهوجي، الحماية الجنائية لبرامج الحاسوب، الدار الجامعية للنشر، الإسكندرية، سنة 1997.
 - علي حسن الطوالة، الجرائم الإلكترونية، مؤسسة فخراوي للدراسات والنشر، الطبعة الأولى، مملكة البحرين، 2008.
 - عمر الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسوب وأبعادها الدولية، طبعة الثانية، القاهرة، 1995.
 - محمود أحمد عابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005.
 - مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، الطبعة الأولى، مصر، 2003.
 - منير وممدوح الجنبلي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية، 2006.
 - نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، مطابع الحلبي الحقوقية، 2005.
 - هدى حامد قشقوش، جرائم الحاسوب الإلكتروني في التشريع المقارن، القاهرة، 1992.
 - هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتب الآلات الحديثة 1992.
- المجلات العلمية:**
- بلطرس آسية، مخاطر المعلوماتية وإنعكاساتها على النمو المعرفي للطفل وعلاقته الأسرية، المجلة العملة للتكنولوجيا وعلوم الإعاقة المجلد 02، العدد 05 ديسمبر 2020، ص 31، 32، جامعة الجزائر 2 أبو القاسم سعد الله (جامعة الإخوة منتوري، قسنطينة، الجزائر 2017).

- بولغيلمات سلاف، كلية الحقوق جامعة باجي مختار عنابة، مجلة العلوم الإنسانية، العدد 48 ديسمبر 2017، المجلد ب.
- حكيم غريب، مداخل، مخاطر مواقع التواصل الاجتماعي على الأمن المجتمع الرهانات والإستراتيجيات، المدرسة الوطنية العليا للعلوم السياسية الجزائر، مداخل قدمت في الندوة النقاشية العلمية الدولية حول : عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية 11 افريل 2017.
- مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بإرتكابها، بحث، مجلة العلوم القانونية والسياسية، المجلد الثالث، العدد الأول، كلية القانون والعلوم السياسية، جامعة ديالا، العراق، 2014.
- مؤتمر الأمم المتحدة لمنع الجريمة ومعاقة المجرمين، فيينا 10-17 أفريل 2000.

المراجع باللغة الأجنبية:

- Donn B.Parker, «Fighting computer crime Anew framework for protection information», Gohn willey& sons inc, usa, 1998.
- Richard Totty and Anthony Hardcastel, Computer_Related crime in "Information Technology & The Law", Chris Edwards and Nigel Savage U.K, 1986.