تاريخ الاستلام:2021/04/23 تاريخ القبول: 2021/08/26

خصوصية الجريمة المعلوماتية بين التجريم و العقاب

The privacy of information crime between criminalization and punishment

د. بولمكاحل أحمد*
جامعة الإخوة منتوري قسنطينة 1 (الجزائر)
boulemkahel.ahmed@gmail.com

د. برني كريمة
جامعة الإخوة منتوري قسنطينة 1 (الجزائر)
berni.karima09@gmail.com

ملخص :

أدى التطور التكنولوجي لوسائل الاتصال واستخدام التقنيات الحديثة إلى إزالة الحدود الجغرافية وظهور نمط جديد في مجال الإعلام والاتصال والذي رافقه التطور الكبير في تكنولوجيات الحواسيب والأجهزة الذكية، أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات الإلكترونية والذي يقصد بها كل المعاملات التي تتم عبر أجهزة مثل الحاسوب ، شبكة الأنترنت و الهواتف الذكية ، والتي أصبحت ضرورة حتمية تفرض وجودها على جميع الدول في ظل عصر الرقمنة .

ونتيجة هذا التطور الكبير والسريع لهذه الأجهزة وضعف القدرة على المرافقة والمراقبة ، ظهر نوع جديد من الجرائم يسمى بالجريمة الإلكترونية أو المعلوماتية أو التقنية ، وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد حتى على مستوى الاقتصاد الوطني للدول ، وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدّة هذا النوع من الجرائم .

الكلمات المفتاحية : الجريمة الإلكترونية ، الحاسوب, شبكة الإنترنت, عصر الرقمنة, وسائل الاتصال.

Abstract

The technological development of means of communication and the use of modern technologies led to the removal of geographical borders and the emergence of a new pattern in the field of information and communication, which was accompanied by the great development in computer technologies and smart devices. This led to the emergence of new tools, inventions and services that resulted in a new type of electronic transactions, which is intended for all transactions It is done through devices such as computers, smart phones, which have become an imperative to impose their presence on all countries in the era of digitization.

As a result of this large and rapid development of these devices and the weakness of the ability to escort and monitor, a new type of crime has emerged called electronic, informational or technical crime.Nowerdays these crimes are threatening the security and safety of individuals, even at the level of the national economy of countries, which requires expediting the necessary measures that would reduce the severity of this type of crime. .

Key words: *Cybercrime, computers, the Internet, the era of digitization, means of* communication.

المؤلف المرسل.

. مقدمة:

إن التحديات التي أفرزها المعاملات الإلكترونية و تكنولوجيات الاتصالات كان لابد لحكومات الدول و هيئتها التشريعية على الخصوص العمل على إرساء بيئة قانونية و تشريعية، ووضع استراتيجيات وآليات قانونية واضحة للتعامل مع هذا الموضوع، ذلك أنه لم يعد التعامل والتصدي للإجرام المعلوماتي اليوم مقتصرا على الطرق والأساليب التقليدية من حيث أنظمة الملاحقة الإجرائية و طرقها التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، بل تعدى ذلك ليصبح ذا طابع إلكتروني متماشيا مع التحولات الراهنة [1] ، التي فرضها العصر الرقمي، و مع تزايد نسبة الجرائم المعلوماتية وتنوع طرقها، مما لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية، ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع ما يؤثر بشكل سلبي على التنمية الاقتصادية.

و رغم الإيجابيات التي وفرها النظام المعلوماتي في شتى الميادين إلا أنه لا يخلوا من بعض المخاطر، لأن المعلومة باعتبارها علم للمعالجة الآلية للمعطيات أصبحت تثير عدة مشكلات من الناحية القانونية ، إذ قد يساير استخدامها للارتكاب الجرائم عن بعد وفي هذا الصدد تقول " روى جودسون " خبيرة بالمركز الوطني الأمريكي للمعلومات " لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديث[2] ، أو قد تكون محلا لاعتداء، وهو الأمر الذي استلزم تدخل المشرع الجزائري من أجل التصدي لمثل هذه الظاهرة ومعاقبة مرتكبيها انطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات. وعلى إثرها قام المشرع بتجريم بعض صور الجريمة المعلوماتية وعاقب مرتكبيها بموجب القانون رقم 15/04، المعدل والمتمم لقانون العقوبات وتناولها تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى المادة 394 مكرر 7 من قانون العقوبات الجزائري، وكذا القانون رقم 09/04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته[3].

ومنه فإن الإشكالية التي يمكن طرحها هي كالتالي:

_ ما مدى فعالية النظام القانوني الذي يتصدى للإجرام المعلوماتي على المستوين الوطني والدولي؟ و كيف ساير المشرع الجزائري بقية التشريعات ذات الخبرة والتجربة في الميدان الإلكتروني للحدّ من الإجرام المعلوماتي؟.

وللإجابة على الإشكالية المطروحة أعلاه، سنحاول تسليط الضوء على الشكل المستحدث للجريمة المعلوماتية مع إبراز أهم الاستراتيجيات والآليات المتبعة من أجل التصدي لهذه الظاهرة, أين احتوى مضمون المقال على قسمين أساسيين حيث خصصنا القسم الأول لدراسة ماهية الجريمة المعلوماتية وإبراز مختلف أنواعها ومجال تحققها، في حين خصصنا القسم الثاني لدراسة مدى خصوصية العقوبة المقررة للجريمة المعلوماتية مع إبراز موقف التشريع الجزائري من الظاهرة, ثم خلصنا إلى خاتمة ضمنها جملة من النتائج و التوصيات.

1_ماهية الجريمة المعلوماتية:

إن الجريمة المعلوماتية بوصفها ظاهرة إجرامية ذات طبيعة خاصة، لا جدال في إعتبارها من أخطر وأعقد الجرائم على الإطلاق وخطورة هذه الجرائم نابعة من طبيعتها المتميزة، من حيث أركانها وحداثة أساليب ارتكابها، فقد اكتنفها الغموض مما صعب مسألة تحديد مفهومها.

وفي هذا المبحث، سنتناول تعريف الجريمة المعلوماتية من خلال الفرع الأول، ثم نعرج لإبراز أنواع الجريمة المعلوماتية من خلال الفرع الثاني.

1.1_تعريف الجريمة المعلوماتية:

لقد تعدد تعريف الجريمة المعلوماتية أو الإلكترونية، فهناك من تناول تعريفها من الزاوية التقنية أو من الزاوية القانونية وترتيبا على ذلك،

اختلفت مصطلحات الجريمة المعلوماتية وظهر مصطلح الجريمة الإلكترونية وجرائم الأنترنت، كما اختلفت وجهات نظر الفقه والقضاء والتشريع حول ماهية الجريمة المعلوماتية .

سنتناول التعريف اللغوي من خلال المقام الأول، ثم التعريف الاصطلاحي من خلال المقام الثاني.

1.1.1_التعريف اللغوي للجريمة المعلوماتية:

لم يتفق الفقهاء على التسمية المحددة للجريمة المعلوماتية لوجود مجموعة من المفاهيم المتقاربة والمشتقة من الإجرام المعلوماتي حيث يطرح إشكالية التشابه والاختلاف بين مصطلحي الجريمة الالكترونية والجريمة المعلوماتي[4]، حيث هناك من عرفها اعتمادا على وسيلة ارتكاب الجريمة، كما عرفها جوم فورستر بأنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة أساسية " ، كما أن هناك جانب من الفقه لا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي، ولذلك عرفت هذه الجريمة بأنها " أية جريمة يكون متطلبا لارتكابها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب "، كما عرفها هشام فريد رستم " أي فعل مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه[5] .

أما من ناحية الفقه، فقد عرفها أنها " الدخول غير المشروع إلى الشبكات الخاصة والعبث بالبيانات الرقمية التي يحويها أو إتلافها أو محوها مما يلحق ضرر بالبيانات والمعلومات ذاتها، وكذلك البرامج و الأجهزة التي يحويها [6] ".

وهناك من عرفها على أنها الجرائم ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة, وغالبا ما تكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الاجهزة, ومن ثم ابتزاز الاشخاص باستخدام تلك المعلومات[7] ".

2.1.1_التعريف الاصطلاحي للجريمة المعلوماتية:

ثمة اختلاف كبير بشأن المصطلحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر و الأنترنت وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات و الاتصالات، فابتداء من مصطلح استخدام الكمبيوتر، مرورا بمصطلح الاحتيال بواسطة الكمبيوتر، والجريمة المعلوماتية، وجرائم الكمبيوتر وجرائم التقنية العالية [8] حيث إنقسم تعريف هذه الجريمة المستحدثة إلى عدة اتجاهات على أساس اختلاف الوسائل والنظم القانونية المتعلقة بها.

حيث يعرفها البعض على أنها " أنها نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسوب الآلي الرقمي وشبكة الأنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الاجرامي "، وهنا لابد من الإشارة إلى اختلاف التسميات لهذا النوع من الجرائم، مثل جرائم الكمبيوتر وجرائم الأنترنت، أو جرائم التكنولوجيا والجريمة الافتراضية، والجريمة السيبرانية أو جرائم التقنية العالية.

كما عرفها البعض بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات، أو نقل هذه البيانات[9] "، وقد إعتمد المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وعرفها بموجب المادة 02 من قانون 04/09 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[10] ".

من استقراء نص المادة أعلاه، أن المشرع الجزائري اعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية بين نظام الاتصالات الإلكترونية و المساس بأنظمة المعالجة الآلية للمعطيات، والقانون الواجب التطبيق للجريمة المنصوص عليها في قانون العقوبات.

2.1_ أنواع الجريمة المعلوماتية :

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الإلكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة.

سنتناول دراسة الجرائم الواقعة بواسطة النظام المعلوماتي من خلال المقام الأول، ثم نعرج في لدراسة الجرائم الواقعة على النظام المعلوماتي من خلال المقام الثاني.

1.2.1_ الجرائم الواقعة بواسطة النظام المعلوماتي :

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ولجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حدٌ ذاته أو برامجه كوسيلة لتنفيذ الجريمة، وتنقسم هذه الجرائم بدورها إلى:

_ الجرائم الواقعة على الأموال:

في ظل التحول من المعاملات التجارية إلى المعاملات التجارية الإلكترونية، وما أنجز عنه من تطور في وسائل الدفع و الوفاء، وفي خضم التداول المالي عبر الأنترنيت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم و منها:

_ السطو على أرقام بطاقات الائتمان و التحويل الالكتروني غير المشروع.

_ القمار و غسيل الأموال عبر الأنترنيت.

_ جريمة السرقة و السطو على أموال البنوك.

_ تجارة المخدرات عبر الأنترنيت.

_ الجرائم الواقعة على الأشخاص :

مع تطور شبكة الأنترنيت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للإنتهاك و الإستعمال من طرف هؤلاء المجرمين والمساس بسمعة و شرف الأفراد، ومن أهم هذه الجرائم: جريمة التهديد و المضايقة و الملاحقة، إنتحال الشخصية و التغرير و الإستدراج.

ويضاف إلى هذه الجرائم الإلكترونية الشخصية، جرائم إنتحال الشخصية والإستدراج بإستخدام شخصية شخص آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، أو تتخذ هذه الجريمة منا ما هو إنتحال شخصية الفرد وإنتحال شخصية المواقع.

_ الجرائم الواقعة على أمن الدولة:

تعد هذه الجرائم من أخطر الجرائم الإلكترونية، خاصة الإرهاب المعلوماتي و الجريمة المنظمة المعلوماتية، حيث أتاحت الأنترنيت للكثير من المنظمات الإرهابية الترويج لأفكارها و معتقداتها، و أدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الإلكتروني على الدول، بالإطلاع على مختلف الأسرار العسكرية و الإقتصادية بين الدول المتصارعة[11] ,كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية و تقاليد المجتمعات، مما سهل خلق الفوضى داخل الدولة و المساس بأمنها الداخلي و بنظامها العام.

2.2.1_ الجرائم الواقعة على النظام المعلوماتي:

إضافة إلى هذه الجرائم المعلوماتية التي تقع بإستخدام النظام المعلوماتي، هناك نوع آخر من الجرائم المعلوماتية يمس بالنظام المعلوماتي ويستهدف المكونات المادية للنظام المعلوماتي، أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي.

_ الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي، بالأجهزة الملحقة به والتي تستخدم في تشغيله كالشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية، كأن تكون محل للسرقة وخيانة الأمانة، أو الإتلاف العمد مما يترتب عليها

خسائر جسيمة، و مثالنا على هذا النوع من الجرائم تلك التي وقعت في فرنسا مما أدى إلى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية [12].

– الجرائم الواقعة على البرامج الإلكترونية:

تصنف هذه الجرائم بدورها إلى جرائم واقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أولا، ثم التلاعب به أو تعديله، ومن أمثلتها قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات، وقام بتقييد المصاريف الزائدة في حسابه الخاص.

وكذلك تضم هذه الجرائم الواقعة على برنامج التشغيل، وهي البرامج المسؤولة عن النظام المعلوماتي، من حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام ، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعطيات مثل جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة بسهولة.

2_مدى خصوصية العقوبة المقررة للجريمة المعلوماتية مع إبراز موقف التشريع الجزائري من الجريمة المعلوماتية:

حقيقة أن الإجرام المعلوماتي، خلق ثورة في المجال التجريم والعقاب و الإجراءات الجنائية، فكان لابد من وضع أطر قانونية ملائمة جديدة، أو إدخال تعديلات على القوانين السارية المفعول بما يتلائم والوضع الراهن، من خلال نصوص جزائية جديدة لحماية الأنظمة المعلوماتية، وردع كل مخالفة في استعمالها محليا أو دوليا.

إن الإجرام المعلوماتي، هو إجرام من نوع خاص يأثر فيه التطور المستمر، عجزت النصوص العقابية عن ضم كافة صوره، ولكن هذا لا يمنع من توسيع مجال التجريم والعقاب في حقل الإجرام المعلوماتي[13]، كما أن هذه الجرائم خلقت إشكالا في مدى ملائمة النصوص التقليدية مع خصوصية الجريمة المعلوماتية المستحدثة، إن الجريمة المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي.

وفي هذا المبحث، سنتناول مبدأ الشرعية الجنائية في المجال المعلوماتي من خلال الفرع الأول، ثم المواجهة الزجرية كآلية لمواجهة الجريمة المعلوماتية على المستوى الوطني و الدولي من خلال الفرع الثاني.

1.2 _ مبدأ الشرعية الجنائية في المجال المعلوماتي:

يمثل نظام المعالجة الآلية للمعطيات الشرط المفترض في الجرائم المعلوماتية كافة حسب التشريع الفرنسي، ودون هذا النظام لا يكون هناك مجال للبحث عن أي ركن من أركان الجريمة، وهذا الشرط لازم لتوافر أي *جريمة من الجرائم المعلوماتية*.

إن مبدأ الشرعية الجنائية كأهم مبدأ ضامن للحرية وكمانع للمتابعة لانعدام النص القانوني لتجريم الفعل، وهذا المبدأ يكرس بشكل ملحوظ في المجال المعلوماتي[14]، ليس لسبب آخر غير لحداثة هذا النشاط، بالإضافة لبعض الحالات التي عجز التشريع الجزائري عن تجريمها بنصوص خاصة كغيره من التشريعات المقارنة.

سنتناول الركن الشرعي من خلال المقام الأول، ثم توسيع في الركن المادي والمعنوي للجريمة المعلوماتية من خلال المقام الثاني

1.1.2_الركن الشرعي :

يعد تجريم الأفعال والمعاقبة عليها من أخطر المسائل التي تمارسها السلطة التشريعية، بالنظر لمساس التجريم والعقاب بحرية الأفراد و المجتمعات، وتجد الشرعية أساسها في الدستور 2016 المعدل، وكذا نص المادة أولى من قانون العقوبات، إلا أن مبدأ " شرعية الجرائم وعقوبتها [15] " يتصدر في الوقت الحاضر أهمية بالغة من الوجهة السياسية، فهو من جهة يحدد نطاق حق الفرد من التمتع بالحرية، ومن جهة أخرى يقلص من سلطات القاضي فيما يخص المجال المعلوماتي حيث حالت أسباب كثيرة دون تجريم بعض الأفعال والتي تمس بحقوق وحريات الأفراد، ومن بين هذه الأسباب نجد:

_ سهولة إخفاء الجريمة المعلوماتية:

تتميز الجرائم المعلوماتية بدقتها في التنفيذ و إخفاء معالمها دون مجهود البدني واضح، فهي جريمة يسهل إخفاءها و إخفاء أدواتها و معالمها، لا ربما بكبسة زر واحدة كذلك نقص خبرة الشرطة و جهات الإدعاء و القضاء في الميدان المعلوماتي في حين أن الجريمة المعلوماتية جد متطورة و دقيقة، فبطبيعة الحال فإن إكتشافها و الوقوف على معالمها و مرتكبيها، يتطلب أيضا التطور و الدقة و الخبرة.

_صعوبة الوصول إلى أغلب مرتكبي الجرائم المعلوماتية:

كما سبقت لنا القول، أن مرتكبي الجريمة المعلوماتية يتميزون بالذكاء و تتميز أفعالهم بالدقة، لذى فإنهم لا يتركون ورائهم أي أثر أو خيط للوصول إليهم.

_صعوبة الإثبات:

و ذلك راجع إلى الطبيعة الخاصة للدليل في الجرائم المعلوماتية، فهو ليس بدليل مرئي ملموس حيث يصعب الوقوف عليه و التمكن من الإحاطة به، و أحيانا يقوم المجرم المعلوماتي بترك شفرات و كلمات مرور يستحيل خرقها، كما أنه بإستطاعته محو الدليل بكل بساطة.

كل هذه الأسباب أدت إلى خلق فراغ تشريعي نتج عنه عدم تجريم مجموعة من الجرائم الإلكترونية، و نذكر نموذجين و هما تقنية إلتقاط البيانات المعلوماتية عن طريق دبدبات الحقل المغناطيسي، و تقنية فيروس البريد الإلكتروني. فتقنية إلتقاط البيانات المعلوماتية عن طريق دبدبات الحقل المغناطيسي تعتمد على الحقل المغناطيسي المحيط بجهاز الكمبيوتر لإلتقاط ما يتضمنه من معلومات، بمساعدة بعض الأجهزة غير تلك المستعملة عادة في الولوج لنظام المعالجة الآلية للمعطيات، و قد جرمت بعض الإتفاقيات الدولية و بعض التشريعات المقارنة _ السعودية و الإمارات _ هذه تقنية باعتبارها جريمة مستقلة. في حين أن المشرع قام بتجريم فيروس البريد الالكتروني, حيث استقبال نظام المعالجة الآلية للمعطيات لا يكون دائما سليما بل قد ينطوي أحيانا على بيانات ملوثة بنوع معين من الفيروسات، لاسيما أن هذه الأخيرة تتسلل إلى الحاسوب عبر برنامج سليم ظاهر ثم تنسخ نفسها وتنشر في مجموعة نظام المعالجة الآلية للمعطيات، وتنتقل إلى كل جهاز له إرتباط به، وهي قادرة على تخريب البيانات الموجودة مسبقا، ويعمل هذا الفيروس بعد إرساله من طرف بريد الكتروني مجهول لآخر مستهدف.

2.1.2_توسيع في الركن المادي والمعنوي للجريمة المعلوماتية:

_ الركن المادي:

يتمثل الركن المادي في الجرائم المعلوماتية بالدخول غير المشروع إلى نظم وقواعد معالجة البيانات، وذلك دون إشتراط إلى وجود تلاعب بهذه البيانات من عدمه، وذلك لأن مجرد الدخول بأي شكل أو وسيلة غير مشروعة للمواقع المعلوماتية أو الأنظمة الحاسوبية يجعل النشاط الإجرامي في هذه الحالة محققا، ويتمثل السلوك الإجرامي في الجريمة المعلوماتية في إرتباط المعلومة الموجودة على الأجهزة الحاسوبية أو النظام

المعلوماتي، و السلوك الإجرامي ليس بحاجة إلى تلك الإجراءات الكثيرة لإرتكاب الجريمة، فقد يتحقق بمجرد ضغطة زر على وسيلة تنفيذ الجريمة، فيتم تدمير النظام المعلوماتي أو إحداث التزوير أو السرقة [16].

وبخصوص النتيجة الإجرامية، فمدى تحققها في العالم الإفتراضي أو إمتدادها للعالم المادي، و مدى إقتصارها على مكان واحد أم إمتدادها لتشمل أقاليم أخرى.

إن النشاط أو السلوك المادي في الإجرام المعلوماتي، يتطلب وجود بيئة رقمية وإتصالات بالأنترنت، ويتطلب أيضا معرفة هذا النشاط والشروع فيه ونتيجته، إذ أن السلوك الإجرامي في كل جريمة يحدده المشرع، فبالنسبة للجريمة المعلوماتية نلاحظ أن السلوك الإجرامي قد يرتبط بالمعلومات المخزنة على الجهاز الحاسوب[17]، التي أدخلت به، أو سرقة صور من الهاتف الذكي.

_الركن المعنوي:

يتحقق الركن المعنوي في الجرائم المعلوماتية في علم الجاني، أنه يرتكب عبر شبكة الأنترنت أفعال كجريمة على الصعيد القانوني وإتجاه إرادته لإرتكاب ذلك الفعل أي لابد من توافر " إرادة آثمة " لديه مع توجيهها نحو القيام بعمل غير مشروع قانونا [18] ، بالإضافة إلى أهمية توفر نتيجة إجرامية ناتجة عن الأفعال السابقة، فتكسب إرادة الجاني طابع التجريم من الفعل الإجرامي المرتكب النابع عن إرتكابها مع توافر علمه بالآثار المترتبة عنه، كما هو الحال في جريمة تقليد المصنفات والبرامج الحاسوبية وعرض المنتجات الأدبية والفكرية دون إذن صاحبها على شبكة الأنترنت، دون إذن مؤلفيها وذلك بتوجه الجاني وإرادته نحو ذلك.

وبالرجوع إلى نظام مكافحة الجرائم المعلوماتية والتشريعات التي نظمت الجريمة المعلوماتية حتى سنة 1990، ركزت في المقام الأول على السلوك الإجرامي وهو الأمر الذي تطلب ضرورة تنوير القوانين والتشريعات التي تأخذ في إعتبارها القسم الخاص بالقصد الجنائي بالجريمة المعلوماتية.

ومن خلال ما تين دراسته، نجد أن طبيعة الجرائم المعلوماتية، تحتم على المشرع صياغة نصوص مرنة وواسعة التفسير سواء بقسم التجريم أو قسم العقوبة، لأن هذا النوع من الجرائم يهدد العديد من المصالح والمراكز القانونية التي إستحدثتها التقنية المعلوماتية، والتي تتطور بشكل سريع يصعب معه وضع نصوص جامدة لا تتحمل التفسير، بحيث كل جريمة على حدى يجب التعامل معها بشكل منفرد، وبالتالي لابد من وجود نص مرن يعطي للسلطة القضائية مساحة واسعة في تقدير العقوبة الملائمة لهذه في هذا المجال المعلوماتي.

2.2_المواجهة الزجرية كآلية لمواجهة الجريمة المعلوماتية على المستويين الوطني و الدولي:

لقد أدت الخصائص التي تتميز بها الجريمة المعلوماتية إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس نصوص تقليدية مع ما قد تشكله من مساس بمبدأ الشرعية الجنائية والتفسير الضيق للنصوص، حيث أن الجريمة المعلوماتية غيرت العديد من المفاهيم في القانون الجنائي، نظرا لظهور مجموعة من القيم الحديثة ذات طبيعة خاصة تتمثل أساسا في المعلومات والمعطيات والتي هي ليست منقولات مادية[19]، كما أن النصوص الجنائية التقليدية غير قادرة على مواكبة هذه التغيرات التي تجعل مبدأ الشرعية الجنائية نعمة على المجرم المعلوماتي مما يمكنه من الإفلات من العقاب، ويصبح نقمة على القضاء الذي يجد نفسه عاجزا على تأويل النص لما في ذلك من خرق لمبدأ الشرعية الجنائية.

سنتناول بعض القوانين الخاصة التي تحتوي على عقوبات ردعية كآلية لمواجهة الجريمة المعلوماتية على المستوى الوطني من خلال المقام الأول، ثم نتناول طرق آليات المكافحة الزجرية على المستوى الدولي من خلال المقام الثاني.

1.2.2_آليات مواجهة الجريمة المعلوماتية على المستوى الوطني :

إن الجريمة المعلوماتية لا تتخذ صور الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات فقط بل تأخذ عدة صور أخرى يمكن إيجادها في نصوص جزائية متفرقة، ولأجل هذا نجد أن المشرع الجزائري نص على أحكام خاصة لمكافحة الإجرام المعلوماتي ، من خلال نصه على محاربة الإعتداءات المتعلقة بالأنظمة المعالجة الآلية للمعطيات، إذ نص على ثلاث أصناف من الجرائم وهي:

_ الدخول أو البقاء غير الشرعي في نظام المعالجة الآلية للمعطيات.

_ إعتداءات على النظام في حدٌ ذاته.

_ الإعتداء على معلومات النظام.

وبهذا يمكن حصر الصور المجرمة للاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وفقا لقيام ركنها المادي والمعنوي وأن المشرع الجزائري قد جرم الأفعال الماسة بنظام المعالجة الآلية للمعطيات أو ما سميت بالغش المعلوماتي بموجب القسم 07 مكرر من قانون العقوبات ، فقد عاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000دج، وفي حال إدخال بطريق الغش معطيات تكون نفس العقوبة على المحاولة, وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

أما إذا ترتب عنها تخريب نظام إشتعال المنظومة، تكون العقوبة من 06 أشهر إلى سنتين حبس والغرامة من 50.000دج إلى 150.000دج، وتعاقب المادة 394 مكرر 1 على المساس بمنظومة معلوماتية بالإدخال، الإزالة أو التعديل بطريق الغش، بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج.

في حين نصت المادة 396 مكرر 3 مضاعفة العقوبة المقررة لجرائم الغش المعلوماتي، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ويعاقب المشرع على الإتفاق بين الأطراف أو المشاركة في الجرائم المعلوماتية إذا جسدت بأفعال مادية.

كما نصت المادة 39 مكرر 2 من قانون العقوبات، التي تشمل وصفين لجريمة الإعتداء العمد على المعطيات خارج النظام، ففي الوصف الأول تكون في المعطيات وسيلة لإرتكاب جريمة من جرائم الإعتداءات الماسة بنظام المعالجة الآلية للمعطيات مثل " التصميم ، البحث ، التجميع ، النشر ، والإيجار في المعطيات المعالجة أو المخزنة، أو مرسلة الموجودة خارج النظام "، ونجد أن المشرع الجزائري يشترط في قيام الجريمة أن تكون المعطيات المعدة خصيصا لإرتكاب جريمة من هذه الجرائم، أما الوصف الثاني تكون في المعطيات محصلة أو نتيجة لإرتكاب جرائم الإعتداءات الماسة بنظام المعالجة للمعطيات وتتحقق بإتيان أحد الأفعال المتمثلة في حيازتها أو إفشائها، ونشرها أو إستعمالها مثل أعمال الجوسسة، الإرهاب التحريض على الفسق وفساد الأخلاق.

وأقر بمصادرة الأجهزة والبرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي علاوة على إغلاق المحل إذا كانت الجريمة قد إرتكبت بعلم صاحبها، كما يعاقب على الشروع بذات العقوبة.

2.2.2_آليات مواجهة الجريمة المعلوماتية على المستوى الدولي:

إن التعاون الدولي مهم عند التعامل مع الجرائم المعلوماتية، لما سيلحقه تطور في أساليب متشابه لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية، لأن هذه الجرائم هي عابرة للقارات ولا حدود لها، وعدم التعاون فيما بين الدول سيؤدي إلى زيادة القيود على تبادل المعلومات عبر الحدود مما يعطي المجرمين الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية [20].

حيث أنه من المهم وجود ترسانة تشريعية وقضائية وفنية في مجال مكافحة الجريمة المعلوماتية، بل و أن تكون هذه القوانين متجانسة وملائمة مع قوانين مختلف الدول، وملائمة هذه الدول مع نصوص الإتفاقية التي صادقت عليها من جهة أخرى، وذلك بهدف خلق منظومة قانونية موحدة تهدف إلى تحقيق أمن معلوماتي ومتابعة المجرمين، هذا ما كرسته الدولية المبدلة في إطار مكافحة الجريمة المعلوماتية، و يمكن إعتبار إتفاقية بودابست بشأن الإجرام السيبيري سنة 2001 و ليدة هذه الجهود التي يتوخى من ورائها مكافحة الجريمة المرتكبة عبر الأنترنيت، حيث إعتمدت هذه الأخيرة من طرف لجنة وزراء بالمجلس الأوروبي رفقة تقريرها التفسيري خلال دورتها 109بتاريخ 8 نوفمبر 2001، و ذلك في إطار التأكيد و الإقناع بضرورة الحاجة إلى اتباع سياسة جنائية موحدة تهدف إلى تحقيق الأمن المعلوماتي و متابعة المخلين به[21] .

كما أن الجهود الدولية لم تكن بخيلة العطاء، حيث إن مجلس أوروبا لم يكتفي بإتفاقية بودابست بل بذل جهود عديدة من قبل نذكر منها: إتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الطابع الشخصي سنة 1981.

أما فيما يخص الجهود المبذولة على المستوى العربي، فلا مناص من الإقرار بأن التعاون العربي الإقليمي هو اللبنة الأساسية في مواجهة هذه الأنواع من الجرائم نظرا لأنها غالبا ما تتم في أماكن مختلفة بإستخدام تقنيات حديثة، و هذه الإتفاقية التي تم المصادقة عليها جاءت مطابقة لإتفاقية بودابست خاصة على المستوى الإختصاص القضائي و تسليم المجرمين.

3.خاتمة :

اتسمت الجريمة المعلوماتية بطبيعة خاصة وجدت صعوبة في وضع تعريف شامل جامع وموحد لها, فقد اختلفت المفاهيم حولها بإختلاف الزوايا التي ينظر إليها، كما تميزت بسرعة تنفيذها والتطور المتسارع في إرتكابها، مما أعطاها خصوصية أكثر من الجرائم التقليدية المرتكبة.

وفي ظل هذه الخصائص للجريمة المعلوماتية، أضحت القوانين عاجزة عن التصدي لها نظرا للعدد الهائل من هذه الجرائم المتطورة بتطور تقنية المعلومات، حيث أصبح مبدأ " لا جريمة ولا عقوبة إلا بنص " لا يتسع للتصدي لهذا النوع من الجرائم بل يجب التوسع في تفسيره لإيجاد التكييف القانوني الصحيح للجرائم المعلوماتية.

و من خلال ما سبق عرضه و التفصيل فيه توصنا إلى رصد مجموعة من النتائج و مجموعة أخرى من التوصيات نوردها على التوال تباعا:

النتائج:

من جملة ما توصلنا إلى رصده كنتائج ما يلي

1_ أنه في مجال الجريمة المعلوماتية تظهر الجرائم الواقعة بواسطة النظام المعلوماتي و كذا الجرائم الواقعة على النظام المعلوماتي.

2_أن لمبدأ الشرعية الجنائية في المجال المعلوماتي خصوصية من حيث الركن المادي و الركن المعنوي للجريمة.

3_ أنه لمجابهة الجريمة الإلكترونية فقد أوجدت التشريعات الوطنية و الدولية مجموعة من الآليات لمواجهة الجريمة المعلوماتية على المستويين الوطني و كذلك الدولي.

4_ خطى المشرع الجزائري خطوات إيجابية في مجال سن تشريعات حديثة لمواجهة الجريمة المعلوماتية، وبالتالي أصبح للقاضي آليات البث في قضايا الجريمة المعلوماتية، بما يضمن عدم المساس بمبدأ الشرعية الجنائية.

التوصيات:

من جملة ما توصلنا إلى رصده من توصيات ما يلي

1_ وجوب تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلائم وأنواع الجرائم الإلكترونية، أو إصدار قانون خاص ومستقل للجرائم المعلوماتية وطرق مكافحتها.

2_ لا يكفي مواكبة المشرع العقابي الجزائري لنصوص التشريعات المقارنة بدون تجسيدها من ناحية التطبيقية والإستعانة بخبراء ومختصيين في مجال تشخيص الجريمة، و منه يجب العمل على تكوين فرق الضبطية القضائية لتختص بهذا النوع من الجرائم المستحدثة في مجال التقنية والمعلومات.

3_ ضرورة تأهيل ضباط الشرطة والمحققين تأهيلا يستطيع معه كل منهم التعامل مع هذا النوع من الجرائم.

4_ ضرورة تأهيل القضاة وتدريبهم حتى يستطيعون التعامل مع الأدلة الرقمية الناتجة عن الجريمة المعلوماتية، و بالتالي تصبح الأحكام القضائية الصادرة أكثر دقة،

5- مع ضرورة استحداث قطب جزائي متخصص لمكافحة والتصدي لمثل هذه الجرائم .

_عقد إتفاقات دولية ثنائية من أجل تسليم المجرم المعلوماتي، كما يجب على الدول العربية المضي لعقد إتفاقات دولية وإقليمية وعربية للتعاون على مكافحة الجرائم المعلوماتية على المستوى التشريعي، والتنسيق فيما بينهم لتعاون أجهزة الشرطة لتبادل البيانات والمعلومات.

4.التهميش و قائمة المراجع :

(1) أنظر : _ أمال قارة ، الحماية الجزائية للجريمة المعلوماتية في التشريع الجزائري ، دار الهومة للنشر والتوزيع ، الجزائر ط 02 ، 2008 ، ص 10 .

(2) أنظر : _ مكرر سمية ، الجرائم المعلوماتية وطرق مواجهتها ، قراءة في المشهد القانوني والأمني ، ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ، الأردن ، 2014 .

(3) أنظر : _ الأمر رقم 66-156 المؤرخ في 8 جويلية 1966 ، المتضمن قانون العقوبات ، الجريدة الرسمية ، عدد 49 القانون رقم 09/04 ، المؤرخ في 05 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، الجريدة الرسمية ، عدد 47 ، الموافق 16 أوت 2009 .

(4) أنظر : _ ذياب موسى البداينة ، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية و الدولية ، ملتقى علمي الأردن ،2014/09/04 ، ص 23 .

(5) أنظر – محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2004 ، ص 43 .

(6) أنظر: _ سوبر سفيان , رسالة لنيل ماجستير في العلوم الجنائية وعلم الإجرام ،كلية الحقوق ، جامعة أبو بكربلقايد تلمسان ، الجزائر ، 2010 ، ص 16 .

(7) أنظر: _ مجلة تكنولوجيا المعلومات ، قسم نظم المعلومات ، بدون نشر و بدون سنة.

(8) أنظر: _ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن , دار الجامعة الجديدة للنشر ، 2008 ، ص 77 .

(9) أنظر: _ محمد علي العريان ، الجرائم المعلوماتية ، المرجع السابق ، ص 66 .

(10) أنظر: _ نص المادة 02 من قانون 04/09 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، الجريدة الرسمية ، عدد 47 ، الموافق 16 أوت 2009 .

(11) أنظر: _ نذى قشقوش ، الحماية الجنائية الإلكترونية عبر الأنترنت ، دار النهضة العربية ، القاهرة ، ص 10 .

(12) أنظر: _ الموقع الالكتروني ، مجلة القانون العام والقانون الخاص http://droit-pub.bligspot./2012/

(13) أنظر: _ عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة ، ط01 ، دار النهضة العربية ، منشأة المعارف الإسكندرية ، 2010/2009 ، ص 102 .

(14) أنظر: _ نور الدين الواهلي ، الاختصاص في الجريمة الإلكترونية ، سلسلة ندوات ، محكمة الإستئناف بالرباط مطبعة الأمنية ، العدد07 ، 2014 ، ص 117 .

(15) أنظر: ـ نص المادة 01 من قانون العقوبات رقم 15/04 ، المؤرخ في 10 نوفمبر 2004 ، المعدل والمتمم لقانون العقوبات .

(16) أنظر: ـ الإتفاقية الدولية حول الإجرام المعلوماتي أبرمت بتاريخ 2001/11/20 ، من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/22 .

(17) أنظر: ـ منى شاكر فراج العسيلي، مقال على الخط http//kenanaonline,com تاريخ 2018/10/02 .

(18) أنظر: ـ خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01، دار الفكر الجامعي، الإسكندرية 2008 ، ص 36 .

(19) أنظر: ـ أمين أعزان ، الجريمة المعلوماتية في التشريع المغربي , مجلة العلوم القانونية ، العدد01 ، 2016 .

(20) أنظر: ـ عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت ، ط01 ، دار الفكر الجامعي الإسكندرية ، 2009 ، ص 84 .

(21) أنظر: ـ نور الدين الواهلي ، الاختصاص في الجريمة الالكترونية ، سلسلة ندوات ، محكمة الاستئناف بالرباط مطبعة الأمنية ، العدد07 ، 2014 ، ص117 .