وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم.:القانون العام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

النظام الإجرائي للجريمة المعلوماتية

ميدان الحقوق و العلوم السياسية

الشعبة: الحقوق

التخصص: القانون الجنائي والعلوم الجناية

من إعداد الطالب(ة):

جيلالي جفال

تحت إشراف الأستاذ(ة):

مشرفي عبد القادر

أعضاء لجنة المناقشة

الأستاذ(ة)	برابح هودى	رئيسا
الأستاذ(ة)	مشرفي عبد القادر	مشرفا مقررا
الأستاذ(ة)	مرابط حبيبة	مناقشا

تاريخ المنقشة:22 /2022/06

السنة الجامعية: 2022/2021

شكر و تقدير

.....لا يسعى بعد إتمام هذا البحث إلا أن أحمد الله تبارك و تعالى و أشكره على عظيم نعمه و جليل منته، فهو مبدأ الحمد و منتهاه لا أحصي ثناء عليه كما أتني على نفسه. حباني بنعمة طلب العلم و سهل لي طريقه و سيرني أن أتقدم بجزيل الشكر و الامتنان. عرفا للجميل إلى أستاذي المشرف "**مشرفي عبد القادر**" لقبوله الإشراف على المذكرة رغم مشاغله الكثيرة، فلم يبخل عليا بالعلم و الوقت.....

كما أتقدم بالشكر الجزيل إلى أعضاء لجنة المناقشة الذين منحوا صدورهم من أجل قراءة و تقويم هذه المذكرة.....

كما أتقدم بالشكر لكل ما ساعدني من قريب أو بعيد لإتمام هذه المذكرة.

إهداء

تهدي ثمرة هذا البحث المتواضع إلى:

رمز المحبة والحنان، إلى القلب الناصع بالبياض، إلى منبع الصبر والتفاؤل، إلى التي رعتني حق الرعاية، كانت سندي في الصعاب إلى قدوتي في هذه الحياة.

أمي لحبيبة.

إلى منبت الخير والتضحية، إلى من علمني النجاح والصبر، إلى من حصد الأشواك عن دربي ليمهد إلى طريق العلم، إلى من أجمل اسمك بكل فخر أبي العزيز

.

إن مجال تقنية المعلومات ومجال الاتصالات و الاندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول.

تمخض عن الفكر الإنساني في العقدين الرابع والخامس من القرن الماضي عن ابتكار أعظم ما قدمته الحضارة الإنسانية ألا وهو الحاسوب، مما أهل لحقبة جديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع حيث تطورت وذلك نتيجة لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص وكذا المؤسسات للإعتماد عليه في كافة شؤونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير. تطورا مذهلا، كما ساعد اقترانها INFORMATIQUE حيث في هذه الفترة عرفة المعلوماتية بالتكنولوجيات أخرى) الإلكترونيك، الرقمنة (على تعميم استعمالها وتعدد وظائفها.

فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو انجاز العمليات المعقدة، وإنما عن تكنولوجيا TECHNOLOGIES DE L'information الإعلام والاتصال والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف ، et de la communication المواصلات السلكية واللاسلكية.

حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وإنما تعدت إلى غير ذلك الدول النامية مما زاد من أهمية هذه التكنولوجيات حيث عرفت بما يسمى بعصر المعلومات.

ففي محاضرة ألقاها" كيرك أرثر "مدير إدارة السلامة العامة والعدل التابعة لشركة ميكروسوفت، خلال مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية بالدوحة خلال) شهر أفريل 2015 أكد أن حجم البيانات الرقمية المتنامي سيبلغ بحلول عام 2020 ، أربعين40)

زيتابايت، بعد ما بلغ 1.8 زيتابايت[1] عام 2012 ، إضافة إلى تأكيد أن 1.7 مليار شخص يستخدمون رسائل التواصل الاجتماعي وأن أكثر من 6.8 مليار شخص يستخدمون الهاتف النقال[2] .

ومع التغلغل المتزايد للمعلومات وتكنولوجيا الاتصال في مختلف النشاطات البشرية، إذ اعتبرت فضاء مفتوحا لا حدود له مقارنة بالحدود الإقليمية للدول، وذلك لكون جميع الدول والمنظمات والمؤسسات خاصة المالية المرتبطة ارتباط وثيق بها من أجل ممارسة أعمالهم ونشاطاتهم وتقديم مختلف الخدمات لزبائنهم.

الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى الاستعمال غير الشرعي لهذه المنظمات المعلوماتية، من أجل ارتكاب أعمالهم الإجرامية المختلفة، من جهة الانتفاع بها، ومن جهة أخرى التملص من المسؤولية الجزائية. وأمام هذا الزحف المتزايد للأنظمة المعلومات ظهر شكل جديد من الإجرام وهو ما يعرف بالإجرام او الجرائم المعلوماتية.

إذ أنه وبظهور هذا النوع الجديد من الإجرام جعل من المجتمع الدولي التدخل من أجل وضع حد لانتشاره، فكان لابد من وضع أطر قانونية ملائمة جديدة أو إدخال تعديلات على قوانين سارية المفعول بما يتلاءم والوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في إطار الاتفاقيات الدولية.

فالتقدم العلمي والتكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن أي تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته ويضع الحلول لما قد يطرأ من مشكلات بسبب استعماله، ففي هذه الحالة يمكن للتقدم التكنولوجي أن يصبح أداة للبناء وأساس لكل تطور ويمكن أن يكون أداة لارتكاب الجريمة إذا أسيء استخدامه.

وهو ما يوجب على القانون أن يمتد نصوصه إلى هذه الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تتخذ الجريمة في نصوص منضبطة واحدة إذ أصبحت النصوص التقليدية لا يمكن أن تسرى أو تطبق على هذا النوع من الجرائم مما أدى إلى ظهور مشكلات إجرامية في هذا المجال. والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع

حاسوبية ذاكرة تخزين سعة قياس وحدة هي مليار مليار الف وهو سيكتليون وتعني زيتا: زيتابايت

[1] تساو 1ZB=1000000000000000000000 bites

[2] حسب معهد علم الاجرام والادلة الجنائية .

من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي أيضا معنية بالمكافحة، فكان لابد من إيجاد إطار قانون يناسب لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجريمة المعلوماتية، ومنها إجراءات تطبق فقط على الجريمة المعلوماتية فقط، التي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم 04 .المؤرخ في أوت / 2009 المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته09 تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة وبالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات التي لم تنل حظها) من البحث والتحقيق والمحاكمة (على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها، لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة ويمتد تأثيرها إلى جميع الأصعدة لارتباطه بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها، على الرغم من الصعوبات العديدة التي واجهتنا في إعداد المذكرة نظرا لصعوبة الموضوع وتشعبه.

ومن أسباب اختيار موضوع المتابعة الجزائية في الجريمة المعلوماتية يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها شخصي والآخر موضوعي فالأسباب الشخصية :تمكن في اهتمامي بمجال الجريمة المعلوماتية وما يلقاها من جرائم وكذا من إجراءات خاصة وإن إجراءات المتابعة فيها تختلف كل الاختلاف عن إجراءات المتابعة في الجرائم التقليدية بالإضافة إلى أنه موضوع جديد، ورغبتي الشديدة في الغوص في مجال إجراءاتها وكذا مكافحتها والوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

أما الأسباب الموضوعية :فتكمن فيما يطرحه موضوع الحماية الإجرائية للجريمة المعلوماتية من إشكاليات قانونية التي لا بد من الوقوف نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال أو الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، والقواعد الإجرائية

الحديثة التي جاء بها تعديل الإجراءات الجزائية الجزائري وكذا قانون09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

و نظرا للأهمية البالغة التي تكتسيها مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي الذي يعرف تطورا سريعا في مجال تكنولوجيات الإعلام والاتصال حيث أصبحت هذه ّالأخيرة الركيزة التي تقوم عليها مختلف القطاعات سواء الخاصة أو العامة من أجل ذلك حاولنا في دراستنا هذه إلى محاولة المساهمة في وضع الخطوط العريضة بالتعرف على طرف التحقيق) ابتدائي أو قضائي (والمحاكمة والتعاون الدولي في هذا النوع من الجرائم بالإضافة إلى إلقاء نظرة على مستجدات في مجال الجريمة المعلوماتية، خاصة إجراءات المتابعة إنه وبظهور الإجرام المعلوماتي أثار العديد من المشاكل خاصة الإجرائية في مجال الجريمة المعلوماتية باعتبار أن تلك الجرائم هي جرائم صعبة الكشف عنها و متابعة مرتكبها بالإضافة إلى أنها ترتكب على المسرح الإلكتروني غير مادي يختلف عن مسرح الجريمة التقليدي، مما يجعل قانون الإجراءات الجزائية قاصرا علي إجراءات المتابعة في الجرائم التقليدية فقط ؛على الأمر الذي أدى إلى تدخل المشروع تعديل قانون الإجراءات الجزائية واستحداث قانون خاص يتضمن جميع القواعد الإجرائية التي يمكن من خلالها لجهات البحث والتحقيق والقضاء التحري من أجل الوصول إلى الدليل المناسب لإثبات الجريمة المعلوماتية والتمييز بين إجراءاتها وإجراءات المطبقة على الجرائم التقليدية.

الإشكال المطروح فإلى أي مدى تقيد المشرع الجزائري بالإجراءات العادية في الجرائم المعلوماتية؟ وهل تخضع الجريمة المعلوماتية لقواعد إجرائية عامة أم قرار لها أحكام خاصا؟

ومن هنا نطرح عدة تساؤلات فرعية تتمثل في:

-فيما تتمثل خصوصية الجريمة المعلوماتية من الناحية الإجرائية؟

-ما هي إجراءات البحث والتحقيق في الجريمة المعلوماتية طبقا للتشريع الجزائري؟

-ما هو الجهاز القضائي المختص بمحاكمة المجرم المعلوماتي؟

-ما هي السبل الدولية في مجال مكافحة الجريمة المعلوماتية؟

واعتمدنا في دراستنا هذه على المنهج[3] التحليلي، الوصفي، كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية واختلافها عن النصوص الإجرائية التقليدية وكذا وصف وتحليل مختلف الاتفاقيات الدولية والعربية من أجل مكافحة هذا النوع من الإجرام المعلوماتي.

لقد تطرقت عدة دراسات سابقة إلي الجرائم المعلوماتية من الناحية الموضوعية فقط ؛مع وجود بعض الدراسات التي تطرقت لها من الناحية الإجرائية لكن ليست بالتفصيل الأمر الذي جعلها قاصرة ومن بين هذه الدراسات التي تم الاعتماد عليها في بحثنا هذا:

ومن أجل معالجة الإشكالية التي سبق طرحها وجب تقسيم هذه الدراسة وفقا لخطة منهجية تتمثل في:

فصلين تطرقنا في الفصل الأول إلى ماهية الجريمة المعلوماتية والفصل الثاني الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري .

باتنة لخضر الحاج جامعة. المعلوماتية الجريمة عن والتحري البحث آليات. نعيم سعيداني [3] 202- 2013.

الأنترنت أكبر بوابة علمية تم إكتشافها حتى الآن، من خلاله يستطيع الفرد أن يقوم بالكثير من الأعمال والتصرفات التي كانت تحتاج سابقا إلى مجهود بدني، ولكن كلما ظهرت سبل التسيير على الأفراد من خلال إستعمال الأنترنت، ظهر من يفسد سهولة إستخدام هذه التقنية في أمن وأمان، وهذا ما يضعنا أمام أمرين، ظهور جرائم معلوماتية جديدة من جهة، وقيام ثورة تقنية لمكافحة هذه الجرائم من جهة أخرى، وسنحاول من خلال هذا الفصل تحديد الجريمة المعلوماتية وذلك بتبيان مفهومها وخصائصها في المبحث الأول، لنتطرق فيما بعد في المبحث الثاني إلى أسس قيام الجريمة المعلوماتية.

المبحث الأول: الإطار ألمفاهيمي للنظام المعلوماتي والجريمة المعلوماتية .

مما لا شك أن ثمة تباين أو عدم ثبات حول المصطلحات والتسميات التي أطلقت، ولا زالت تطلق على هذه الظاهرة الإجرامية الجديدة التي باتت تهدد الدول قبل الأفراد، وربما هذا التباين في المفاهيم ، يعود إلى نشأة وتاريخ وتطور تكنولوجيا المعلومات ، واختلاف وجهات النظر بين المختصين، ولقد تعددت التسميات بشأن هذه الجريمة فمرة تسمى جرائم الكمبيوتر والأنترنت، والبعض الأخر يطلق عليها بالغش المعلوماتي أو الجريمة المعلوماتية، أما في الدول الأوروبية فيطلق عليها إسم السيبركرام cyber crim ومن هذا سنتطرق في الطلب الأول إلى تعريف الجريمة المعلوماتية وفي المطلب الثاني إلى خصائص الجريمة المعلوماتية والمجرم المعلوماتي.

المطلب الأول: تعريف التشريعي الفقهي للنظام المعلوماتي.

يعتبر النظام المعلوماتي او نظام المعالجة الآلية للمعطيات فكرة أساسية،ذلك إن هذا النظام هو ركن مفترض بالنسبة للجرائم المعلوماتية وهو الركن الذي يتحكم في وجود أو انعدام الركن المادي الذي ينطوي على الأفعال والوقائع التي تمس أو تهدد النظام المعلوماتي وسنتناول من خلال المبحث الأول مدلول النظام المعلوماتي وفق ما ذهب إليه المشرع الجزائري ومدى تأثره واختلافه عن التشريعات الأخرى بخصوص ضبط مدلوله وعناصره ليتسنى لنا فيما بعد إلى تطبيقات النظام المعلوماتي

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية.

لابد أن نشير في البداية أن المشرع الجزائري عند تطرقه للجرائم المعلوماتية سواء في قانون العقوبات أو قانون الإجراءات الجزائية أو قانون الوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها ،قد استخدم مصطلحين اثنين عند إشارته للنظام المعلوماتي وهو مصطلح معالجة الآليات للمعطيات ومصطلح المنظومة المعلوماتية ففي قانون العقوبات استخدم مصطلحين معا وفي قانون الإجراءات استخدم مصطلح نظام المعالجة آليات لمعطيات أما في قانون الوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام ولاتصال ومكافحتها فقد استخدمه مصطلح منظومتها المعلوماتية في مادته الثانية وقدم تعريفا لهذه الأخيرة ولان هذا التعريف ينطبق تماما على نظام المعالجة آليات للمعطيات ولان المشرع استخدم مصطلحين معا ولم يفرق بينهما في إننا نتخلص إن المشرع الجزائر ي

يوظف هذين المصطلحين كمترادفين أي انه لايميز بينهما فالنظام المعالجة الآلية للمعطيات عنده يعني المنظومة المعلوماتية والعكس صحيح ونحن من جانبنا نؤثر استخدام مصطلح النظام المعلوماتي لثلاث أسباب على الأقل :أولهما عدم تعارضه مع ما جاء في التشريع الجزائري والثاني هو استخدام هذا المصطلح من طرف كثير من القوانين المقارنة التي قد نتطرق لها في دراسة هذه ،إما السبب الثالث فهو استخدام هذا المصطلح من طرف الاتفاقية العربية لمكافحة جرائم تنقية المعلومات لعام ى 2010 والتي صادقت عليها الجزائر في الثامن من سبتمبر 2014 فهذا المصطلح يجمع مختلف القوانين حول المعنى نفسه ،وبالتالي فاستخدامنا لمصطلح النظام المعلوماتي نعني به في الوقت نفسه نظام المعالجة الباليّ للمعطيات والعكس صحيح رغم ذلك فلم يقم المشرع الجزائري بتقديم تعريف لنظام المعالجة الآلية للمعطيات عند نصه على جرائم المساس بأنظمة المعالجة الآلية للمعطيات في تعديله لقانون العقوبات سنة 2004 ،ولكنه تطرق لهذا الموضوع في القانون رقم 09/04 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،إذ جاءت المادة الثانية من هذا القانون تحدد مفهوم بعض المصطلحات ،ومنها مفهوم المنظومة المعلوماتية ،**بحيث** عرفتها بأنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبط ة ،يقوم واحد منها آو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

أولا: التعريف الضيق للجريمة المعلوماتية.

من التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها:" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الألية بقدر كبير لازما لإرتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"[1].

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

كذلك تعرف بأنها:" الفعل غير المشروع الذي يتورط في إرتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في إقترافه الحاسوب بإعتباره أداة رئيسية".

[1] نائلة قورة، جرائم الحاسب الإقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة 2003، ص21.

وعرفت أيضا:" الجرائم التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم في اقترافه الحاسوب بإعتباره أداة رئيسية"[1].

ما يؤخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الإتجاه ركز على معيار موضوع الجريمة والبعض الأخر ركز على وسيلة إرتكابها ، والبعض الأخر على معيار النتيجة.

ثانيا: التعريف الواسع للجريمة المعلوماتية.

في المقابل هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية نتيجة الانتقادات التي واجهت الاتجاه الأول، فحاول الفقهاء تعريف الجريمة المعلوماتية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه المضيف للتصدي للظاهرة الإجرام المعلوماتي.

فعرفها البعض أنها:" كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية بهدف الإعتداء على الأموال المادية أو المعنوية". وبأنها:" إستخدام الحاسب كأداة لإرتكاب الجريمة، بالإضلفة إلى الحالات المتعلقة بالولوج غير المصرح به الحاسوب المجني عليه أو بياناته".

كما تمتد هذه الجريمة لتشمل الاعتداءات المادية، وساءا كان هذا الاعتداء على جهاز الحاسوب ذاته، أو المعدات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الائتمان ، وإنتهاك ماكينات الحسابات الآلية، بما يتضمنه من شبكات تمويل الحسابات المالية بطريقة الكترونية، وتزييف المكونات المادية والمعنوية للحاسوب ، بل وسرقة الحاسوب في حد ذاته أو مكون من مكوناته.

تناول رأي أخر من الفقه تعريف الجريمة المعلوماتية بأنها:" عمل أو امتناع يأتيه الإنسان إضرار بمكونات الحاسوب وشبكات الإتصال الخاصة به، التي يحميها قان ون العقوبات ويفرض لها عقابات".

[1] حنان ريحان مبارك المضاحكي، الجرائم المعلوماتية ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص52.

عرفت في إطار المنظمات الأوروبية للتعاون والتنمية الإقتصادية بأنها:" كل فعل أو امتناع من شأنه أن يؤدي على الإعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية".[1]

جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة 2000 تعريفها كما يلي:" يقصد بالجريمة الإلكترونية أي جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".

لا شك أن هذا الإتجاه ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يسقط من وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك بمجرد مشاركة الحاسوب الألي في النشاط الإجرامي فبعض الجرائم كسرقة الحاسوب الألي أو الأقراص مثلا لا يمكن إعطاؤوها وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محلا لفعل الإختلاس[2].

الفرع الثاني: التعريف التشريعي للجريمة المعلوماتية.

تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها والعربية، فيما يخص القواعد التي أستند إليها أو أتى بها لمكافحة الجرائم المعلوماتية، حيث إتجه إلى خلق نصوص جديدة وخاصة تتعلق بهذا النوع من الإجرام، رغبة منه في تأمين أنظمة المعلومات من إعتداءات المجرمين.

إذ نجد أنه ضمن موضوع الجريمة المعلوماتية في قانون العقوبات أو بموجب نصوص خاصة على سواء.

ويعتبر نظام المعالجة الألية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة ، فإذا تخلق هذا الشرط لا يكون هناك

[1] حنان ريحان مبارك المضاحكي، مرجع سابق، ص26-27.

[2] ونوغي نبيل وزيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، المجلد الرابع، العدد الثالث، الجزائر، 2009/09/01، ص131.

مجال للبحث في مدى توافر أركان أي جريمة من جرائم الماسة بأنظمة المعالجة الألية للمعطيات.[1]

إن نظام المعالجة الألية للمعطيات تعبير يصعب على المشغل بالقانون إدراك حقيقته بسهولة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال الحسابات الألية ، لذلك فالمشرع الجزائري على غرار المشرع الفرنسي لم يقم بتعريف نظام المعالجة الألية للمعطيات بل أو كل مهمة تعريفه لكل من الفقه والقضاء.[2]

أما المشرع الجزائري فقد إصطلح على تسمية الجريمة المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا المعلومات والإتصال ، وتبنى في ذلك تعريف الذي جاءت به الإتفاقية الدولية للإجرام المعلوماتي، بموجب المادة 02 الثانية من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، وعرفها على أنها:" جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية".[3]

وبالتالي تكون الجريمة المعلوماتية أيضا تلك الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ البرنامج معين[4]، والمرتكبة عن طريق أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية[5].

ويلاحظ على هذا التعريف ما يلي:

---

[1] رابح وهيبة ، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد 04، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد ابن باديس ، مستغانم، 12-2014، ص321.

[2] قارة أمال، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة 01، دار هومه 2006، ص101.

[3] المادة الثانية الفقرة" أ" من قانون رقم 09-04 المؤرخ في 05 أوت 2009، جريدة رسمية عدد47، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها الصادرة في 16 أوت 2009.

[4] المادة الثانية الفقرة" ب" من نفس القانون.

[5] المادة الثانية الفقرة "و" من نفس القانون.

-أن المشرع الجزائري قد إعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكتروني، وثانيها معيار موضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الألية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

-كما إعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية، كونه أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه، وهذا ما يوسع نطاق الجرائم المعلوماتية في القانون الجزائري.

وترتيبا على كل هذه التعاريف الفقهية والتشريعية يمكننا القول أن الجريمة المعلوماتية هي:" كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته ويمس بالأشخاص أو الأموال أو أمن الدولة، وهي على غرار الجرائم التقليدية تعرف من خلال أركانها بتوافر القصد الجنائي لإرتكاب هذه الجريمة والركن المادي للجريمة وركنها المعنوي"[1].

المطلب الثاني: خصائص الجريمة المعلوماتية والجرم المعلوماتي.

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية ، وذلك نتيجة إرتباطها بتقنية المعلومات والحاسب الألي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه عن المجرم التقليدي، ومن هذا سنتطرق إلى سمات الجريمة المعلوماتية في الفرع الأول وفي الفرع الثاني إلى سمات المجرم المعلوماتي.

[1] تمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، ورقة علمية في إطار أعمال المؤتمر الدولي الرابع الجرائم الإلكترونية طرابلس، لبنان، 24/25 03/2017، ص100.

الفرع الأول: خصائص الجريمة المعلوماتية.

أولا: جرائم عابرة للحدود.

بمعنى أنها تتعدى الحدود الجغرافية للدول ، إنها جرائم عابرة للقارات لأنه مع انتشار شبكة الإتصالات العالمية والأنترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد أخر.[1]

يعد مبدأ عالمية النص الجنائي صورة عاكسة للتضامن الدولي في مكافحة الجريمة التي تفنن المجرمون في افترافها بالإستفادة من التطور العلمي الذي أتاح لهم ممارسة على المستوى الدولي كالإتجار بالمخدرات والقرصنة والجريمة المنظمة، وعليه فلا يوجد ما يبرره سوى فكرة حماية المصالح العامة والمشتركة للبشرية وهو ما أدى إلى انحصار هذا المبدأ في نطاق ضيق من الجرائم.[2]

ونتيجة للخسائر الكبيرة التي تتسبب فيها هذه الجرائم، تعالت الأصوات الداعية إلى التعاون الدولي المكثف للتصدي لها عن طريق إبرام الإتفاقيات والمعاهدات وتسهيل اجراءات التعاون والمساعدة القضائية بين الدول فقد تتأثر دول عدة بجريمة معلوماتية واحدة تخلق مشكلات كثيرة مثل: تحديد الدولة صاحبة الإختصاص القضائي وحول القانون واجب التطبيق واجراءات الملاحقة القضائية ، فعولمة الجريمة المنظمة تقتضي عولمة مكافحتها أيضا بواسطة التعاون الدولي في صوره المتعددة.

في هذا الشأن سارع المشرع الجزائري الى التصديق على نصوص الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، حيث نصت في مادتها الأولى:" تهدف هذه الإتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجرائم المنظمة عبر الحدود الوطنية"، كما نصت بموجب المادة 21 منها على تجريم إرتكاب أو المشاركة في إرتكاب الأفعال التي

[1] عبد الفتاح مراد، شرح جرائم الكومبيوتر والأنترنت، دار الكتب والوثائق المصرية مصر، 2005، ص42.

[2] عبد الله أوهابية، شرح قانون العقوبات الجزائري القسم العام المؤسسة الوطنية للفنون المصنعة ، الجزائر، 2011، ص157-158.

تقوم بها جماعة إجرامية منظمة في نطاق الإستعمال غير المشروع لتقنية أنظمة المعلومات وتدخل مكافحة الجرائم المعلوماتية ضمن هذا الإطار لأنها تتميز بأنها جرائم عابرة للحدود.[1]

ثانيا: جرائم صعبة الإكتشاف والإثبات.

صعوبة متابعتها وإكتشافها بحيث لا تترك أثر فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم المعلوماتية تم إكتشافها بالصدفة وبعد وقت طويل من إرتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير كم تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات كما يصعب الإحتفاظ الفني بأثارها إن وجدت ، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي مثالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو وضع كلمات سرية ورموز تفوق الوصول إلى الدليل وقد يلجأ مرتكبيها تشفير التعليمات لمنع إيجاد أي دليل يدينه[2].

يرى البعض أن من أسباب صعوبة إكتشاف هذه الجرائم تميزها عن غيرها بحيث أنها لا تترك أثار خارجية ملموسة أو مرئية، كونها تتم بتغير أو محو الأرقام والبيانات الموجودة بأنظمة الحاسب الألي ، فضلا عن إمكانية تدمير أي معلومة قد تستخدم كدليل في أقل من ثانية.[3]

وما جعل الجرائم المعلوماتية صعبة الإكتشاف والإثبات البعد الجغرافي بين الجاني والمجني عليه، إستخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم ترتكب في وقت سريع، ويتم محو أثارها في وقت أسرع لا يتعدى الثواني، مما يزيد الأمر صعوبة عدم وجود خبرة لدى ضباط التحقيق في مثل هذه الجرائم من ناحية التحقيق والبحث عن الأدلة والتحفظ عليها، ومن الصعوبات التي تواجه إثبات هذه الجرائم عدم إقتناع القضاة بكثير من

---

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتاقية العربية لمكافحة جرائم تقنية المعلومات– قانون العقوبات– قانون الاجراءات الجزائية– قوانين خاصة– دار الجامعة الجديدة الإسكندرية 2019، ص80–81.

[2] فضيلة عاقلي، الجريمة الإلكترونية واجراءات مواجهتها من خلال التشريع جامعة باتنة 01 أعمال المؤتمر الدولي الرابع عش، طرابلس، لبنان، 24–2017/03/25، ص07–08.

[3] أيمان مسعود سالم، الجريمة المعلوماتية، مذكرة لنيل شهادة ماجستر كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين ، سطيف 2016، ص20.

الجرائم المستحدثة في هذا المجال، وتعد هذه الخاصية من السمات التي تتميز بها الجريمة المعلوماتية عن غيرها، فقد انتشرت مكاتب تقوم بأعمال السرقة والقرصنة من خلالها يقوم بعض الأشخاص باستئجار قراصنة محترفين لسرقة بيانات الشركات العالمية مقابل مبالغ مالية وبيعها لأشخاص مستفدين ، وكل هذه الأعمال غير مشروعة ، وإن من الأسباب الكامنة في صعوبة إكتشاف وإثبات هذه الجرائم هذه الجرائم عدم تقديم شكاوي من قبل أصحاب الشركات التي يتم إختراقها وذلك خوفا على سمعة الشركة وعلى المستثمرين فيها.[1]

ثالثا: جرائم ناعمة.

تختلف الجرائم المعلوماتية عن الجرائم التقليدية التي تتطلب أحيانا استخدام العنف كما في جرائم القتل والضرب والجرح والسرقة وجرائم الإرهاب...الخ، إلا أن الجرائم المتصلة بالكومبيوتر تمتاز بأنها ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء وإمتلاك الوسائل المناسبة وقدرة على التعامل مع شبكة الأنترنت ، فنقل بيانات من كومبيوتر إلى أخر أو المساس بأنظمة المعالجة الآلية للمعطيات ، أو الدخول غير المشروع للحاسوب أو القرصنة أو السطو الإلكتروني على الأرصدة وبيانات وبطاقات الإئتمان، لا يتطلب أي عنف سواءا مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي فهي جرائم هادئة بطبيعتها.[2]

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في إرتكابها كالقتل، السرقة، وغيرها، فالجرائم المعلوماتية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرام المعلوماتية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكومبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.[3]

---

[1] يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني " دراسة تحليلية مقارنة" رسالة لنيل شهادة الماجستر في القانون العام كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013، ص 16-17 .

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية ، الطبعة 01، دار الثقافة للنشر والتوزيع عمان الأاردن، 2008، ص58.

[3] فضيلة عاقلي، المرجع السابق، ص08.

رابعا: قلة الإبلاغ عن الجريمة المعلوماتية.

غالبا ما نجد أنه لا يتم الإبلاغ عن الجرائم المعلوماتية إما لعدم إكتشاف الضحية ، وإما خشية من التشهير، وأكثر ما يكون ذلك في المؤسسات الإدخارية، ومؤسسات الإقراض والسمسرة، حيث يرجع السبب في امتناع بعض هذه المؤسسات عن الإبلاغ عن تعرضها للجريمة المعلوماتية، الخشية مجالس إدارتها من الدعاية التي قد تنجم عن الإبلاغ عن مثل هذه الجرائم.[1]

كما أن الإعلام عن هذه الجرائم يؤدي أحيانا إلى الكشف عن موطن الضعف أو ما يسمى الثغرة الأمنية في برامج المجني عليه ونظامه المعلوماتي مما يجعل عملية الإختراق سهلة ، إلا أن المجني عليه قد يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية فهو نادرا ما يقوم بالإبلاغ عنها، الأمر الذي يؤثر سلبا في السياسة التي يمكن أن توضع لمكافتحها.[2]

ضرورة تعديل قوانين مكافحة الجرائم المعلوماتية بوجود نصوص تحمى المبلغ عن هذه الجرائم، من حيث سرية التبليغ وسرية التحقيق والمحاكمة في هذا النوع من الجرائم، كذلك اشتمال النصوص على محفزات لمن يبلغ عن هذه الجرائم كمبلغ مالي مثلا يعطي للشخص الذي يبلغ عن هذه الجرائم تشجيعا للتبليغ عنها وبالنتيجة مكافحتها.[3]

الفرع الثاني: خصائص المجرم المعلوماتي.

يتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين.

أولا: الذكاء.

يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج

[1] إيمان مسعود سالم، المرجع السابق، ص20.

[2] نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع منها، مذكرة لنسل شهادة ماجستر، كلية بن يوسف بن خدة جامعة الجزائر، 01، 2017، ص97.

[3] لورنس السعيد الحوامدة، بحث بعنوان: الجرائم المعلوماتية أركانها وألية مكافحتها، " دراسة تحليلية مقارنة" ، كلية الحقوق جامعة طيبة، المملكة العربية السعودية، 2017، ص12.

وإرتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على دراية كبيرة من المعرفة لكي يتمكن من إرتكاب تلك الجرائم.[1]

فهذا المجرم لا يمكن أن ينتمي إلى طائفة المحرمين الأغبياء ، فمن يستعين بجهاز الحاسوب للإيستلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع من الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي يواجهها في إرتكاب جريمته، وتتجلى أهمية صفحة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم إستخدام للعنف في إرتكابه للجريمة.[2]

إذا كان مرتكبي الجرائم التقليدية ليس لمستواهم ولا لدرجة ذكائهم دور كقاعدة في نمط جرائمهم، فإن المجرم المعلوماتي لابد أن يكون من المختصين في مجال المعلوماتية وله دراية وخبرة في مجال التعامل معها وفك رموزها ، فلا يمكن أن يرتكب هذه الجرائم إلا من له مهارة ومعرفة فنية في مجال المعلوماتية ولا يشترط المؤهل العلمي لذلك فيمكن أن يرتكبها شخص ليس له المؤهل العلمي ولكنه على درجة عالية من الذكاء.[3]

ثانيا: ذو طابع إجتماعي.

المجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنه إنسان متكيف إجتماعيا ذلك أنه أصلا فائق الذكاء وهذا ما يساعده على التكيف، وما الذكاء في رأي الكثيرين سوء القدرة على التكيف ولا يعني ذلك التقليل من شأن المجرم المعلوماتي، بل أن الخطورة الإجرامية قد تزيد إذا زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه.[4]

كما يتسم المجرم المعلوماتي في كونه في العادة كائن ذو طابع إجتماعي يتميز بقدرته على التكيف في بيئته الإجتماعية ، بل أن بعضهم يتمتع بثقة كبيرة في مجال عمله،

---

[1] خالد ممدوح إبراهيم ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية 2009، ص133-134.

[2] سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة لنيل شهادة ماجستر في العلوم القانونية، تخصص علوم جنائية كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013، ص51.

[3] ربيعي حسن، أليات البحث والتحقيق في الجرائم المعلوماتية ، رسالة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016، ص36.

[4] عبد الفتاح بيومي حجازي، حول صياغة النظرية العامة في علم الجريمة والمجرم المعلوماتي، منشأة الإسكندرية سعد زغلول ، مصر 2008، ص100.

فالمجرم المعلوماتي لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به فهو يتوافق ويتصالح معه، وتزداد خطورته الإجرامية كلما زاد تكيفه الإجتماعي مع توافر الميول الإجرامي لديه، فشعوره بأنه محل ثقة وأنه خارج إطار الشبهات يدفعه إلى التمادي في إرتكاب جرائمه والتي لا تكتشف عادة.[1]

ومن توابع خصائصه الإجتماعية أنه شخص يشعر بالخوف الدائم من أمر كشف جرائمه وإقتضاح أمره بالرغم من أن هذا الشعور يعالج كافة المجرمين، إلا أنها تصاحب مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من إرتكاب مالي وفقد للمركز الوظيفي، ومرد هذا الخوف أيضا هو إنتمائهم إلى فئة إجتماعية متميزة من حيث التعلم والثقافة وطبيعة العمل.[2]

ثالثا: الخبرة والمهارة.

يتصف مرتكب الجرائم المعلوماتية أيضا على درجة عالية من الخبرة والمهارة في استخدام التقنية المعلوماتية وذلك لأن مستوى الخبرة والمهارة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم بحيث إذا كان شخص مرتكب الجريمة على قد ضئيل من مستوى الخبرة نجد أن الجرائم التي قد يرتكبها ألا تتعدى الإتلاف المعلوماتي إما بالمحو أو بالإتلاف وكذلك بنسخ البيانات والبرامج.

أما إذا كان الشخص على درجة أعلى في المهارة فإن أسلوب إرتكابه للجرائم تختلف حيث يقوم عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الألي وسرقة وإرتكاب جرائم النصب وإرتكاب جرائم التجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مستوى عالي من الخبرة وخبرة كبيرة في إرتكابها.[3]

كما أن المهارة التي يتميز بها المجرم المعلوماتي تمكنه من تكوين تصور كامل لجريمته إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته والكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى التمهيد لإرتكاب جريمته بالتعرف على المحيط الذي

[1] ربيعي حسن، المرجع السابق، ص36.

[2] نهلا عبد القادر المومني ، المرجع السابق، ص80.

[3] خالد ممدوح ابراهيم ممدوح، المرجع السابق، ص135.

تدور فيه، وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانية نجاحها وإحتمالات فشلها وتساعده في ذلك درجة المهارة التي يتمتع بها.[1]

رابعا: المجرم المعلوماتي يتمتع بالسلطة.

يقصد بالسلطة في هذا المجال جملة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من إرتكاب الجريمة، فكثير منهم لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وتتمثل عادة في إمتلاك شفرة الدخول إلى نظام المعلوماتي وإجراء المعاملات، وقد تكون هذه السلطة أحيانا غير مشروعة في حال سرقة شفرة الدخول وقد استغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها بدون بيانات وهمية، وغير صحيحة ويطلب الحاسوب إعتمادها عند إجراء بعض العمليات ومثالها الموظف المشرف على الموظفين بمصالح المحاسبة وصرف الأجور الذي يمكن أن يدرج أسماء بعض الموظفين الوهميين ضمن قائمة الموظفين ثم يمرر عملية صرف الرواتب ويتولى إيداع رواتب الوهميين في حسابه الخاص ولذلك فإن المهتمين بمجال المعلوماتية عادة ما ينبهون أصحاب المؤسسات إلى أخذ الإحتياطات اللازمة عند إختيار المشرفين على هذه المصالح.[2]

[1] سعيداني نعيم، المرجع السابق، ص52.

[2] ربيعي حسن ، المرجع السابق، ص 37-38.

خالد داودي ، الجريمة المعلوماتية، الطبعة الأولى، دار الإعصار العلمي، عمان، 2018، ص 23-24.

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية .

تعتبر الجرائم المعلوماتية من الجرائم الجديدة ، التي لم يتناولها فقهاء القانون إلا في العصر الحديث، فقد ظهرت هذه الجرائم مع ظهور الوسائل التكنولوجية ووسائل الإتصال السريعة ، كل ذلك أثر سلبا في سرعة المعالجة التشريعية لهذه الجرائم، فكونها جرائم مستحدثة وسريعة التطور كان من الصعب على الفقهاء تحديدا أركانها وشرحها وتفصيلها، إلا أن فقهاء القانون الحديث قد بدأوا في وضع الخطوط العريضة لمعالجة هذه الجرائم، من خلال البحث عن صور درجة خطورتها وعليه سوف نقسم هذا المبحث إلى مطلبين المطلب الأول: تناول فيه أركان الجريمة المعلوماتية أما المطلب الثاني نتطرق إلى صور الجريمة المعلوماتية.

المطلب الأول: أركان الجريمة المعلوماتية.

اشترط المشرع الجزائي القيام أي جريمة وجود ثلاث أركان أساسية وهي الركن الشرعي والركن المادي والركن المعنوي، وهذا هو الحال بالنسبة للجرائم المعلوماتية ، فلقيام الجريمة المعلوماتية لابد من أن يتوفر فيها أركان الجريمة ، وبدون هذه الأركان يصبح هناك خلل في موضوع الجريمة، بحيث أن الركن الشرعي نعني به نص قانوني يحدد الجريمة والجزء الجنائي على سلوكات معينة وهذا ما سنتطرق إليه في الفرع الأول، أما الركن المادي فيتمثل في النشاط الذي يرتكبه الجاني وله مظهر خارجي وهذا ما سنتطرق إليه في الثاني أما الفرع الثالث فسيكون معنون بالركن المعنوي والذي يتمثل في الإرادة الخاطئة لمباشرة السلوك الإجرامي ويكمن في نفس الجاني.

الفرع الأول: الركن الشرعي: تتحقق الجريمة بالفعل الصادر عن الإنسان فيتخذ صورة مادية معينة، تختلف الأفعال المادية بإختلاف نشاطات الإنسان وهذا ما يجعل المشرع يتدخل لتحديد فئة من الأفعال الضارة أو الخطرة على سلامة أفراد المجتمع فينهي عنها بموجب نص قانوني جزائي يجرم هذه الأفعال ويحدد عقوبة من يأتي على إرتكابها.

وتبعا لذلك فلا جريمة ولا عقوبة بدون نص شرعي، وتعتبر الجريمة عمل غير مشروع يجرمه القانون ويعاقب عليه ، وذلك بالنظر لما يقرره القانون الجنائي.[1]

[1] أحسن بوسقيفة، الوجيز في القانون الجزائي العام، الطبعة الثالثة عشر، دار هومه، الجزائر، 2013، ص64..

وتعتبر الجريمة عمل غير مشروع يجرمه القانون ويعاقب عليه وذلك بالنظر لما يقرره القانون الجنائي والقوانين المكملة له من أوامر ونواهي تجرم وتعاقب على كل سلوك أو فعل ترى فيه السلطة المختصة بالتشريع أنه يرقى لدرجة التجريم بما يشكله من مساس بمصالح الجماعة بتعريضها بوجه عام للخطر.

ويقوم الركن الشرعي للجريمة على النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له، تطبيقا لمبدأ شرعية الجرائم والعقوبات لا جريمة ولا عقوبة أو تدابير أمن بغير قانون.

وقد خصص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويشتمل ثمانية مواد تهتم بذكر كل أنواع الإعتداءات على الأنظمة المعلوماتية، وإن كان من المستحسن أن يعتمد المشرع الجزائري شمل هذا النمط من الجرائم المستجدة بنص قانوني خاص بها وإلى غاية تكريس ذلك يبقى المنهج المعتمد من طرفه سلميا نوعا ما ويتفق مع وجود ظاهرة إجرامية مستجدة تستلزم ضرورة التدخل لتجريمها وافراد عقوبات مناسبة لها، تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير مجرمة قانونا لذا فقد عمد المشرع إلى وضع نصوص خاص بالجرائم الماسة بأنظمة المعالجة الألية للمعطيات ليساير بذلك كل الإتجاهات التشريعية المعاصرة في هذا الشأن.[1]

الفرع الثاني: الركن المادي.

جرائم المعلوماتية تتخذ عدة أشكال تتعدد بتعدد صور الإعتداء الواقع على نظام المعلوماتية بحذ داته والتي نوردها كما يلي:

1 الدخول والبقاء غير المرخص بهما في النظام

يقصد بفعل الدخول هنا وهو الركن المادي لجريمة الإعتداء على نظام المعالجة الألية للمعطيات ذلك الدخول المعنوي أو الإلكتروني بإستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفة الإجرامي

[1] ونوغي نبيل وزيوش عبد الرؤوف، المرجع السابق، ص133.

إنطلاقا من كونه قد تم دون وجه حق أو دون ترخيص هو ما يستشف من المادة مكرر من قانون العقوبات الجزائري.

لا حظ من خلال هذه المادة أن المشرع الجزائري إعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها تحقق النتيجة الإجرامية، أي أنه جرم مجرد الدخول إلى نظام المعالجة الألية للمعطيات بأكمله أو إلى جزء منه فقط، بشرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ.

نعتقد أن المشرع الجزائري أصاب كثيرا عندما جرم مجرد الدخول إلى نظام المعالجة الألية للمعطيات عن طريق الغش أي بدون ترخيص وبغض النظر عن ما إذا كان النظام المعتدى عليه محاطا بحماية فنية أم لا لأنه بذلك يكون جعل من هذا التدبير بمثابة تدبير تحفظي وقائي سيساهم بشكل كبير في التصدي لظاهرة الإجرام المعلوماتي، من خلال غلق الباب أمام المجرمين من التهرب من المسؤولية الجزائية عن فعل الإعتداء ، بحجة أن النظام المعندي عليه لم يكن محاطا بحماية فنية، وفي تفادي ارتكاب جرائم أكثر شدة على نظام المعالجة ومعطياته كإتلاف النظام أو محو وتعديل معطيات النظام.[1]

أما فيما يخص فعل البقاء غير المرخص به في نظام المعالجة الألية للمعطيات فيقصد به استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السيطرة عليه، بمعنى أخر هو بقاء شخص داخل نظام المعالجة ملك الغير بعد الدخول إليه خطأ أو صدفة، رغم علمه بأن بقاءه فيه غير مرخص.[2]

إعتبر المشرع الجزائري على غرار المشرع الفرنسي فعل البقاء غير المرخص به في نظام المعالجة الالية للمعطيات جريمة مثلها مثل جريمة الدخول الغير مرخص به، وذلك بموجب المادة 394 مكرر من قانون العقوبات وحدد لهاتين الجريمتين نفس العقوبة.

ومن خلال نص نفس المادة [3] أورد المشرع الجزائري طرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الألية ، بحيث يتحقق الظرف الأول إذا نتج عن

---

[1] هذا ما أخذ به المشرع الفرنسي من خلال نص المادة 1/323 من قانون العقوبات الفرنسي، وحذا حذوه المشرع الإنجليزي في نص المادة الأولى من قانون اساءة استخدام الكومبيوتر لعام 1990.

[2] قارة أمال، المرجع السابق، ص44.

[3] الفقرة الثانية من المادة 394 مكرر من قانون رقم 04-15 المتضمن تعديل قانون العقوبات.

الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام، ويتحقق الثاني حينما يترتب عن الدخول أو البقاء تخريب نظام إشتعال المنظومة وإعاقته عند أداء وظيفته، زهذا بتوفر علاقة سببية بين فعل الدخول أو البقاء غير المرخص به والنتيجة الإجرامية التي حددتها المادة في محو أو تعديل بيانات النظام أو تخريب تشغيل النظام ذاته.

2 الإعتداء على معطيات المعالجة الألية:

يقصد بالإعتداء هنا ذلك الإعتداء الذي يهدف إلى الإضرار بمعلومات الكومبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها، تكاملها أو بتعطيل قرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم، يتحقق الإعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة، ويتخذ أحد الشكلين التاليين:

-الإعتداء على المعطيات الداخلية للنظام:

لقد جرم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الألية من خلال المادة 394 مكرر 1 من قانون العقوبات، وحدد في ذات المادة صور الإعتداء على معطيات النظام الداخلية على سبيل الحصر ولم يدع أي مجال للإجتها فيها، مما يدل على أن أي إعتداء لا يحمل إحدى هذه الصور : الإدخال، المحو،التعديل فهو مستبعد ولا يخضع لأحكام المادة 394 مكرر 1:

فبالنسبة للإدخال: يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها أليا.

وأما المحو: يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الألية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

أما التعديل: يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمطيات أخرى.

ولا يشترط اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني إحداهما لكي يكتمل الركن المادي لجريمة الإعتداء على معطيات نظام المعالجة.[1]

[1] ونوغي نبيل وزيوش عبد الرؤوف، المرجع السابق، ص135.

يرجع سبب تجريم المشرع الجزائري للأفعال المذكورة أعلاه بنص مستقل عن جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة، واللتان تمثلان الطريق العادي للوصول إلى المعطيات الموجودة داخل النظام وإرتكاب جريمة محو أو إدخال أو تعديل ضدها إلى وجود طرق أخرى لإقتراف هذه الأفعال عن بعد أي دون الدخول أو البقاء في النظام، كإستخدام مثلا القنابل المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات ، وقد أصاب المشرع في ذلك لأنه بوضعه نص المادة 394 مكرر 1 يكون قد جرم أفعال المحو والإدخال والتعديل الواقع على معطيات النظام مهما كانت الوسيلة المستعملة والطريقة المتبعة لتحقيق ذلك:

-الإعتداء على المعطيات الخارجية للنظام:

يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دورفي تحقيق نتيجة معينة تمثل في المعالجة الألية للمعطيات، وقد نص عليها المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات على النحو التالي:" يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1000.000 إلى 5000.00 دج كل من يقوم عمدا أو عن طريق الغش بـ:

1 تصميم أو بحث أو تجميع أو مراسلة عن طريق منظومة معلوماتية يمكن أن 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"[1].

يتبين لنا من نص هذه المادة أنها جاءت عامة ومطلقة، فهي تقرر الحماية الجنائية لكل من المعطيات الداخلية والخارجية للنظام معا.

3 الإعتداء على سير نظام المعالجة الألية:

لقد أغفل المشرع الجزائري وضع نص صريح خاص بتجريم الإعتداء على سير نظام المعالجة الألية للمعطيات، غير أنه يمكن استخلاص ذلك من خلال النصوص التي

[1] نص المادة 394 مكرر 2 من قانون رقم 04-15 المتضمن تعديل قانون العقوبات.

استحدثها بخصوص تجريم الإعتداءات الواقعة على أنظمة المعالجة أو على معطيات هذه الأنظمة سواء كانت معطيات داخلية أم خارجية.

فالإعتداء على النظام بتخريبه كما نصت عليه المادة 394 مكرر من شأنه أن يعيب عملية النظام، والإعتداء على معطيات الداخلية للنظام باستعمال برامج الفيروسات وبرامج القنابل المعلوماتية من شأنه كذلك التأثير في سير أو حسن سير النظام المعلوماتي.

يمكن أن تتخذ الأفعال الماسة بسير النظام عدة صور نذكر منها:

التعطيل: يمكن أن يصيب التعطيل الأجهزة المادية للنظام كتحطيم الأسطوانات أو قطع شبكة الإتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي إلى عرقلة سير النظام.

الإفساد: هو جعل نظام غير صالح للإستعمال بإحداث خلل في نظام سيره وفقدان توازن في أداء وظائفه، كان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ومثل هذا الفعل إلن لم يؤدي إلى تعطيل نظام المعالجة كلية فإنه يحول دون تحقيقه لوظائفه بشكل صحيح.

إذا كان حقيقة يمكن للقاضي الجزائي استخلاص الحماية الجزائية لسير نظام المعالجة الألية للمعطيات من النصوص القانونية التي تجرم أفعال الإعتداء على أنظمة المعالجة ومعطياتها إلا أنه كان الأجدر بالمشرع الجزائري إضافة نص خاص بتجريم الإعتداء على سير النظام لرفع اللبس والحرج عن القاضي الجزائي الذي تفرضه عليه قاعدة التفسير الضيق للنص الجزائي.

تجدر الإشارة إلى أن المشرع الجزائري جرم كل من الإشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة وجعل العقوبة لهما تساوي العقوبات المقررة للجريمة ذاتها، وقد تشمل هذه العقوبات المذكورة في القسم السابغ مكرر من قانون العقوبات عقوبات أصلية تتمثل في الحبس والغرامة، وعقوبات تكميلية هي مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع وأماكن الإستغلال إذا ارتكبت الجريمة بعلم مالكها، كما أن المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي ارتكب احدى الجرائم المعلوماتية إلى 05 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي مع إقراره

المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين و/أو شركاء في نفس الجريمة التي إرتكبها الشخص المعنوي.[1]

الفرع الثالث: الركن المعنوي.

عرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها، وبالتالي يكون مطابق للواقع، يسبق الإرادة، أما هذه الأخيرة فتتمثل في الإتجاه من أجل تحقيق السلوك الإجرامي، ويتخذ القصد الجنائي عدة صور منها القصد العام والقصد الخاص.

-القصد الجنائي العام: هو الهدف الفوري المباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها.

-القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم فلا يكفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم من هنا نتساءل عن القصد الذي يجب وافره في الجريمة المعلوماتية.

إن المجرم الإلكتروني يتوجه من أجل ارتكاب فعل غير مشروع أي غير مسموح مع علم هذا المجرم بأركان الجريمة وبالرغم من أن بعض المحترفين يبررون أفعالهم بأنهم مجرد فضوليون وأنهم قد تسللوا صدفة، فلا انتقاء للعلم كركن للقصد الجنائي، وكان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الإطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية.

فالقصد الجنائي متوافر في جميع الجرائم المعلوماتية دون أي استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم المعلوماتية تتطلب أن يتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الأنترنت، أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الظروف المشروع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص.[2]

---

[1] براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، العدد02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2016، ص136-136.

[2] ونوغي نبيل وزيوش عبد الرؤوف، مرجع سابق، 136-137.

المطلب الثاني: صور الجريمة المعلوماتية.

يصنف الفقهاء والدارسون جرائم الكومبيوتر والأنترنت ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند اليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظام الحاسوب وأخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات جرائم ترتكب على نظام الحاسوب وأخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات بالإستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لإرتكاب الجريمة ، وغيرهم يؤسس تقسيمه على تعدد محل الإعتداء، وكذا تعدد الحق المعتدي عليه، فتوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة، ومن الملاحظ أن هذه التقسيمات لم تراعي خصائص هذه الجريمة وموضوعها، والحق المعتدي عليه لدى وضعها الأساس أو معيار التقسيم، وعليه ونظر الطبيعة ونظرا لطبيعة هذا النوع المستحدث من الجرائم تعددت تصنيفاتها، سنتطرق لها في أربعة فروع.

الفرع الأول: الجرائم الواقعة على الكومبيوتر.

أولا: الدخول والبقاء غير المصرح به لنظام المعالجة الآلية.

تكون الجريمة في صورتها البسيطة إذا كانت مجرد دخول وبقاء غير مشروع، وإما إذا توافرت ظروف معينة ينتج فيها عن الدخول والبقاء غير المشروع تغيير في المعطيات فتحقق الصورة المشددة.[1]

1 -**فعل الدخول:** أي الإطلاع على المعلومات التي تمت معالجتها دون التصريح والدخول قد يكون مباشرا أو غير مباشرا بالنسبة للدخول المباشر فله عدة صور حيث أن الجاني يمكنه الإستيلاء على المعلومات المخزنة بعده طرق سواء بطبعها أو استخدام شاشة النظام، أو قراءة ما هو مكتوب أو استخدام ما هو مكبر الصوت.

أما الولوج غير المباشر يكون عن طريق إمكانيات حديثة يتم من خلالها الولوج والإستفسار من المراكز المعلوماتية عن بعد، فتكون المعلومات مهددة بالإلتقاط والتسجيل

[1] أمال قارة، الجريمة المعلوماتية، مذكرة لنسل شهادة ماجستر، كلية الحقوق والعلوم السياسية، بن عكنون، 2002، ص41-42.

غير المشروع في أي لحظة، كالقيام مثلا بتوصيل نظام معلوماتي بالنهاية الطرفية ومعرفة كلمة السر أو الشفرة المناسبة.[1]

2 -**فعل البقاء:** يعتبر البقاء جريمة إذا تم طباعة نسخة من المعلومات في الوقت الذي نسمح له فيه بالرؤية فحسب، كما نجده أيضا في الخدمات المفتوحة للجمهور مثل: الخدمات التلفزيونية التي يمكن للمجرم من خلال طرق غير مشروعة الحصول على الخدمات دون مقابل، أو زيادة مدة استفادته من الخدمة، ألا أنه قد يجتمع فعلا الدخول والبقاء غير المشروعين معا، وذلك في حالة ما إذا لم يكن من حق الجاني الدخول إلى النظام.[2]

يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة إلى هذا الموضوع حيث خطى المشرع هذه الخطوة بالمبادرة إلى تقديرها قانون العقوبات بمقتضى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع بمحتوى المادة 394 مكرر إلى 394 مكرر7، ويبدو أن المشرع لم يكتف بذلك بل قطع أشواطا أخرى في اتجاه فرض حماية جنائية على حياة الأفراد الخاصة حين بادر بتعديل جديد لقانون العقوبات وهو الذي جاء به القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 والذي مس االمادة 303 واقراره إعادة الأفراد تحسبا للإستخدام السيئ لوسائل التكنولوجيا الحديثة عن طريق الكومبيوتر أو الهاتف النقال وما يرتبط بهامش االتقنيات.

يلاحظ أن المشرع الجزائري جرم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية واعتبر هذا التصرف في حد ذاته يشكل جريمة إذ يستخلص لأول مرة وهلة أن مجرد اختراق جهاز كومبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية بعد إنتهاء النظام المعلوماتي بطريقة شرعية.[3]

ثانيا: جريمة التلاعب بمعطيات الحاسب الألي.

جريمة التلاعب الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول والبقاء غير المصرح بها، أما قانون العقوبات الفرنسي فينص عليها بعد جريمة إعاقة وإفساد

[1] أحمد خليفة ملط، الجرائم المعلوماتية، الطبعة 02، دار الفكر الجامعي الاسكندرية، 2006، ص191-192.

[2] أمال قارة، المرجع السابق، ص42.

[3] زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار النهضة للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص48-49.

أنظمة المعالجة نظرا للتشابه الكبير بينهما وبين جريمة التلاعب بالمعطيات بحيث يصعب في الكثير من الأحيان التمييز بينهما وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده، وقد اكتفى المشرع الجزائري نتيجة إفساد النظام كطرف مشدد فقط لجريمة الدخول واستبعادها كجريمة قائم بذاتها والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والتعديل، ويكفي توافر أحدهما لقيام الجريمة لا يشترط اجتماعها حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن المادي للجريمة لكن القاسم المشترك في هذه الأفعال جميعها هو إنطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل.[1]

نلاحظ أن المشرع بادر برفع العقوبة في المادة 394 مكرر 1 وجعلها تبدأ من ستة أشهر إلى ثلاث سنوات وبغرامة من 5000.000 دج إلى 2000.000 دج على خلاف ما نصت عليه المادة 394 مكرر، ذلك أنه وإن اعتبر المشرع مجرد الدخول إلى المنظومة المعلوماتية أو جزء منها أو البقاء فيها بطرق تدليسية بشكل جريمة دون اقترانه بأي تصرف أخر، كما تفطن المشرع إلى تصور ما قد يترتب عن فعل الدخول أو البقاء من المساس بالمعطيات أو البيانات المخزنة من خلال التجوال في النظام سواء كان المساس عن عمد أو عن غير عمد.[2]

الفرع الثاني: الجرائم الواقعة على الأشخاص.

أولا: جرائم القذف والسب وتشويه السمعة.

تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة ، حيث يستعمل الجاني حسب القواعد العامة جرائم القذف والسب عبارات بديئة تمس شرف المجني عليه، بل إن إرادته اتجهت لذلك بالذات، وبالتطور أصبحت الإنترنت إحدى هذه الوسائل إذ لم نقل أكثرها رواجا فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع مشاهدتها أو الإستماع إليها ، وبتحقيق بذلك ركن

[1] ابتسام مهوب، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماجستر كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي ، أم البواقي ، 2014، ص15-16.

[2] زبيخة زيدان، المرجع السابق، ص53.

العلنية الذي تطلبه الكثير من التشريعات في السب العلني، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني.[1]

ثانيا: صناعة ونشر الإباحة.

إذا كان لشبكة الأنترنت وجه ايجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع لشبكة الأنترنت تحرص على ممارسة للكبار والصغار على حد سواء وتقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال.[2]

ثالثا: جريمة التهديد والمضايقة.

يقصد بالتهديد الوعيد بالشر، وهو زرع الخوف في النفس بالضغط على إرادة الإنسان وتخيفه من أضرار ما سيحلقه أو يلحق أشياء له صلة بها، ويعد تهديد الغير من خلال البريد الإلكتروني واحد من أهم الاستخدامات غير المشروعة للأنترنت حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها.

رابعا: انتحال الشخصية والتعزيز والإستدراج.

يقصد بانتحال الشخصية ما يعود عليه المجرم من استخدام شخصية شخص أخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للإهتمام بخصوصية وسرية المعلومات الشخصية للمستفدين على شبكة الإنترنت.[3]

الفرع الثالث: الجرائم الواقعة على الأموال.

أولا: السرقة عبر الانترنت.

تعرف السرقة بأنها اختلاس شيء منقول مملوك للغير بدون رضاء بنية امتلاكه، وتتم سرقة المال المعلوماتي إن أمكن الوصف عن طريق اختلاف البيانات والمعلومات، وبإفادة منها بإستخدام السارق للمعلومات الشخصية مثل ، الإسم ، العنوان، الأرقام الخاصة بالمجني عليهم، والإستخدام غير الشرعي لشخصية المجني عليه ليبدأها عملية السرقة

[1] سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة ماجستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2014، ص26.

[2] محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، بدون سنة، ص08.

[3] سمية مزغيش، المرجع السابق، ص27.

المتخفية عبر الأنترنت بحيث يؤدي بالغير إلى تقديم الأموال الإلكترونية أو عادية إلى الجاني عن طريق التحويل البنكي.[1]

ثانيا: جرائم التحويل غير المشروع للأموال أو جرائم الإحتيال الإلكتروني.

يعرف النصب أو الإحتيال على أنه من جرائم الإعتداء على ملكية مال منقول يلجأ فيه الجاني بواسطة إحدى وسائل الإحتيال المعنية قانونا، على الحيازة الكاملة عمد بطريقة الحيلة أو الخداع على مال مملوك للغير.[2]ثالثا: جرائم الإستخدام غير المشروع لأدوات الدفع الإلكتروني.

تعتبر تقنية الدفع الإلكتروني للأموال من أهم التطبيقات الحديثة للمعلوماتية فقد كسرت حاجز التعامل بالنقود وكذلك عوائق المبادلات المالية، فأصبحت تتم بسهولة وسيولة كبيرة ولا تستعرق من الزمن سوى لحظات، غير أنها وبقدر تطمينات المؤسسة المالية بمدى أمنها إلا أنها تبقى الهدف الأول لمجرمي المعلوماتية، نظرا لما تدره من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة.[3]

الفرع الرابع: الجرائم الواقعة على أمن الدولة.

أولا الجريمة المنظمة.

تعرف الجريمة المنظمة بأنها تعبير عن المجتمع اجرامي يعمل خارج إطار الشعب والحكومة، ويضم بين طياته المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما كما يخضع أفرادها لقواعد قانونية سنوها لأنفسهم وتفرض أحكاما باللغة القسوة على من يخرج عن نظام الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها وبجنون من ورائها الأموال الطائلة.[4]

الجريمة المنظمة ليست وليدة التقدم والسهولة وإن كانت استفادت منه فالجريمة المنظمة وبسبب تقدم وسائل الإتصال والتكنولوجيا أصبحت غير محدودة لا بقيود الزمن ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع كبير وأصبحت لا تحددها الحدود الجغرافيا،

---

[1] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان 2009، ص138.

[2] محمد علي العريان، الجرائم المعلوماتية ، كلية الحقوق جامعة الاسكندرية ، دار الجامعة الجديدة للنشر، الإسكندرية، مصؤ 2004، ص123.

[3] ربيعي حسن ، المرجع السابق، ص76.

[4] نهلا عبد القادر المومني، المرجع السابق، ص87.

كما اشتعلت عصابات الجريمة المنظمة الإمكانات المتاحة لوسائل الأنترنت في تخطيط وتمرير وتوجيه المخططات وتنفيذ العمليات الإجرامية بسير وسهولة.[1]

ثانيا: الإرهاب.

يتم بث ثقافة الإرهاب عبر الأنترنت عن طريق تأسيس مواقع افتراضية تتمثل في المنظمات وهي مواقع أخذت في الإزدياد مع زيادة المنظمات الإرهابية حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت أو بيانات تنفي أو تعلق على الأخبار الصادرة عن المنظمات أو جهات دولية أخرى **ثالثا: جريمة التجسس.**

ينتج عن الإستخدام المتزايد للحاسبات الألية في العديد من المجالات تجميع المعلومات بدرجة كبيرة في موضوع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها وعلى المعطيات المخزنة فيها بمختلف درجات سريتها.

ويقصد بالتجسس في هذا الموضوع هو الإطلاع على المعلومات خاصة بالغير مؤمنة في جهاز أخر ، وليس مسموحا لغير المخولين الإطلاع عليها.[2]

اعتبر المشرع الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي من المؤسسات الرسمية بمثابة ظرف تشديد وهذا ما يستخلص من المادة 394 مكرر 3 بقولها أن:" تضاعف العقوبات المنصوص عليها في هذا القسم ، إذا استهدفت الجريمة الدفاع الوطني أو المؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".[3]

[1] سمية مزغيش، المرجع السابق، ص 33-34.

[2] سمية مزغيش، المرجع السابق، ص35.

[3] زبيخة زيدان ، المرجع السابق، ص 99-100.

إن الجريمة المعلوماتية بإعتبارها مستحدثة أثارت ضجة بخصوص تحديد الأفعال الإجرائية التي تدخل في نطاقها، لذلك إرتأينا دراسة أركانها بالتفصيل وذلك بالتعرض لجميع الجرائم وتتمثل في جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة التلاعب بمعطيات الحاسب الآلي وأخيرا جريمة التعامل في معطيات غير مشروعة وذلك بالمقارنة مع مختلف التشريعات التي أكست نظام المعالجة الآلية للحماية الجزائية على غرار المشرع الجزائري واتفاقية بوداست، وهذا ما سنتعرض له في المبحث الأول، أما المبحث الثاني فتناولنا فيه الجزاءات المقررة في القانون 15/04 المعدل والمتمم لقانون العقوبات وذلك من خلال المواد من 394 مكرر إلى غاية المادة 394 مكرر05.

المبحث الأول: أركان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

متى ثبت توافر الشرط الأول لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة الألية للمعطيات أمكن الإنتقال إلى المرحلة التالية وهي البحث في توافر أركان أية جريمة من الجرائم المعلوماتية.

المطلب الأول: جريمة الدخول واللقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

لعل جريمة الدخول والبقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات من أهم جرائم المعطيات والجرائم المعلوماتية عموما، ذلك أن أغلب جرائم المعطيات لا يمكن إرتكابها إلا بعد الدخول للنظام، ولهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرى، لذلك أولت لها التشريعات إهتماما كبيرا وهناك من التشريعات من يجعلها الجريمة الأساسية وما بقى من الجرائم إلا نتائج لها.[1]

وقد حرص المشرع الجزائري على تجريم فعل الدخول غير المصرح به، ونتيجة تتمثل في تشديد المشرع للعقاب إذا ترتب على هذا الفعل حدوث أضرار بالمعلومات ونظم معالجتها فضلا البقاء على

[1] محمد خليفة الحماية الجنائية لمعطيات الحاسب الألي، في القانون الجزائري المقارن، دار الجامعة الجديدة الأسكندرية، 2008، ص131.

الإتصال أو الدخول الذي تم بطريقة الخطأ، وهو ما سيتفاذ من المادة 394 مكرر من قانون العقوبات الجزائري وإلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي تناول هو بدوره تجريم السلوك وهذا بموجب المادة 1/323[1] من قانون العقوبات الفرنسي كما يلي:" كل من دخل أو بقى بنفس في كل أو جزء من نظام المعالجة الآلية يعاقب بـ...وإذا ترتب على الأفعال المذكورة حذف أو تعديل لمعطيات النظام أو تخريب اشتغال هذا النظام تكون العقوبة...".

كما نصت اتفاقية بودابست على هذه الجريمة في المادة 02 منها تحت عنوان " الدخول غير القانوني ".... " على أنه " يجب على كل طرف أن تتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية أو لجزء من جهاز الحاسب دون حق كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب أو بنية أخرى إجرامية أو أن تكون الجريمة في حاسب ألي يكون متصلا عن بعد حاسب أخر".

الفرع الأول: الركن المادي لجريمتي الدخول أو البقاء غير المصرح بهما.

إنطلاقا من نص المادة 394 مكرر من قانون العقوبات الجزائري والنصوص القانونية السابقة المادة 1/323 من قانون العقوبات الفرنسي والمادة 02 اتفاقية بودابست فإن تحقق الركن المادي لجريمة الدخول أو البقاء يغش أو في المصرح به يتم بسلوك إجرامي يرتكبه الجاني قد يتخذ صورة الدخل المنطقي وذلك بغرض فتح باب يؤدي إلى نظام المعالجة الآلية بمكوناته المختلفة وأحيانا يتخذ صورة البقاء إذا حرص المشرع على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات.

[1] *"Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 € d'amende.* Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 € d'amende

من النظام وبصرف النظر عن العادة التي يرنو إليها الجاني، من خلال إرتكابه للجريمة وكذلك بصرف النظر كما إذا كان النظام محميا بجهاز للأمان أو لا، فالمشرع إذا أراد أن يقفل الباب أمام كل وجود غير مصرح له داخل النظام، دخولا أو بقاءا في كل أو في جزء من النظام بقصد خاص أم دونه وسواء كان محميا فنيا أو غير محمي. وتتحقق الجريمة سواءا أدى هذا التواجد إلى نتائج معينة أم لم يؤدي لكن إذا نجم عن هذا التواجد غير المشروع داخل لنظام تخريب الأخير أو محو أو تعديل لمعطياته فإن العقوبة تشدد.[1]

وتقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أو لا علاقة بالحاسب الآلي وسواء كانت لديه المقدرة الفنية على الإستفادة من النظام أم لا، إنما فقط يكفي ألا يكون من أولئك الذين لهم حق الدخول إلى هذا النظام.ويلجأ أصحاب الأنظمة المعلوماتية كثيرا إلى مثل الأساليب وغيرها لتأمين الحماية لمعلومات التي تحتويها أنظمتهم، والسؤال الذي طرح في هذا الشأن هل أن الأنظمة المحمية بأجهزة أمان هي وحدها التي نحظى بحماية قانون العقوبات أو أن كل الأنظمة تحظى بتلك الحماية؟

لقد إختلف الفقه في الإجابة على هذا التساؤول بين هل الأنظمة المحمية بأجهزة أمان هي وحدها التي تحظى بحماية وتطبيق قانون العقوبات أم أن كل الأنظمة تحظى بتلك الحماية أي إلى أي مدى اعتبار الحماية الفنية عنصرا في الركن المادي؟.

أشار المشرع الجزائري لا من قريب أو بعيد إلى ذلك وكذلك فعل المشرع الفرنسي، ومع ذلك نبدأ أن الفقه الجزائي قد اختلف في الإجابة على هذا السؤال بين موسع للحماية وبين حصرها في تلك المحمية فقط بأجهزة أمان.[2]

[1] محمد خليفة، المرجع السابق، ص132.

[2] رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة في التشريع الجزائري ، دار هومه ، الطبعة الأولى 2008.، ص165.

1 -الإتجاه المقيد للحماية المدنية.

يرى البعض من الفقهاء ضرورة وجود نظام أمني على إعتبار أن القانون يجرم الإعتداء على نظم الأمن المتضمنة في نظام المعالجة الآلية ، إن المنطق السليم والعدالة يقتضيان قصرا الحماية الجنائية على الأنظمة المحمية بأنظمة أمان فحسب ذلك لأن القانون الجنائي لا يساعد إلا الأشخاص المجتهدين، ومن غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أية إجراءات تكفل لها الحماية، ولا ينبغي حماية حق لن يتحوط له صاحبه، هذا يجعل الأشخاص لا يلجئون إلى القانون الجنائي إلا عندما تعجز تلك التدابير الوقائية عن حماية أنظمتهم.[1]

وقد قاس أصحاب الرأي جريمة الدخول عير المصرح به على جريمة إنتهاك المسكن حيث أن هذه الأخيرة لا تقوم بمجرد دخول المسكن بغير رضا صاحبه، وإنما يجب لقيامها أن يصحب ذلك الدخول استعمال وسائل تدل على عدم الرضا صاحب المسكن كالتهريب أو الإحتيال.[2]

إن قانون المعلوماتية والحريات الفرنسي الصادر في 1978/01/06 يعتبر سابقة تشريعية مهمة في هذا الشأن يفرض هذا القانون على مالك النظام أو المسؤول عنه بتأمين هذا النظام (المادة 29) وكذلك المادة 226 فقرة 17، من قانون العقوبات تعاقب على إجراء أو معالجة آلية لمعلومات اسمية دون اتخاذ الإجراءات اللازمة لتأمين هذه المعلومات ولا ينبغي حصر هذا الأمر في المعطيات الشخصية ، وإنما يجب أن تشمل كل المعطيات بما فيها تلك التي تحميها المادة 1/323 من قانون العقوبات الفرنسي، فلا تحظى بالحماية منها إلا تلك المعطيات المحمية منها بأجهزة أمان.

[1] رشيد بوبكر، المرجع السابق، ص165.

[2] د/ نائلة قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية تطبيقية ن منشورات الحلبي الحقوقية 2005، ص341.

2 الاتجاه الموسع للحماية الجنائية.

رغم قوة المنادين بتضييق الحماية الجنائية وحصرها في الأنظمة المحمية فقط، فإن هناك اتجاها أخر يرى بأن أنظمة الحسابات الآلية وما تحويه من معطيات لابد أن تحظى بالحماية بغض النظر على الإتجاه السابق بالحجج الآتية:

- أن تمنع المال المسروق بحماية صاحبه أو عدم تمتعه لا يؤثر في قيام جريمة السرقة، كما يؤثر فيها مقدار الصعوبة التي واجهها الجاني في إرتكابه لجريمته.
- أن اشترط وجود أجهزة أمان شأنه أن يضيق كثيرا مجال تطبيق النص.
- هذا الشرط يتجلهل الحالات التي يتم فيها الدخول إلى النظام نتيجة خطأ قام به المبرمجون أو المسؤولون عن أمن النظام.
- أن تطلب المادة 01/323 ق.ع.فرنسي لضرورة حصول الدخول عن طريق الغش هو أمر يتصل بالركن المعنوي للجريمة وليس بالركن المادي، حيث يشير إلى تطلب القصد الجنائي العام لقيامها.[1]
- أن سكوت القانون يدل على عدم اشتراطه لهذا الأمر، ومن المعروف أن المبادئ العامة في تفسير القانون الجنائي تقضي عدم إضافة شرط لم ينص عليه القانون.
- فالنص جاء عاما ولم يفرق بين نظام محمي وأخر غير محمي[2].
- الوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي إذا لم تنشر المادة 394 مكرر إلى ضرورة أن يكون نظام المعالجة الآلية للمعطيات محميا بجهاز أمان

[1] محمد خليفة، المرجع السابق، ص136.

[2] علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، جامعة الإمارات، ماي 2000.، ص45.

وإنما حاء النص عاما، وعليه فإن جميع الأنظمة سواءا كانت محمية أو غير محمية تحظى بحماية هذا القانون.

– وبناءا على ذلك لا يدخل نظام الحماية الفنية عنصرا في جرائم المعطيات، فهذه الأخيرة تقوم بالإعتماد على نظام المعالجة الألية للمعطيات سواء كان محميا لنظام للأمان أو لم يكن محميا، فالحماية الجنائية إذا عامة على كل الأنظمة.

وسنتناول فيما يلي السلوك الإجرامي لهذه الجريمة في كلتا الصورتين.

1 – الدخول نصت عليه المادة 394 مكرر على تجريم سلوكين اثنين هما الدخول والبقاء غير المصرح بهما إلى نظام المعالجة الألية للمعطيات.

فالدخول غير المصرح به هو الولوج إلى المعلومات والمعطيات المخزنة داخل نظلم الحاسب الآلي دون رضا المسؤول هن هذا النظام أو هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعطيات.[1] أو قد عرف أيضا بأنه:[2]" عملية ولوج غير شرعي إلى نظام التشغيل في الحاسب من قبل أشخاص لا يملكون صلاحيات الدخول وذلك بهدف القيام بأعمال غير قانونية مثل التجسس أو السرقة يملكون صلاحيات الدخول وذلك بهدف القيام بأعمال غير قانونية مثل التجسس أو السرقة أو التخريب، مع الأخذ بعين الإعتبار قدر هؤولاء الأشخاص على نقل ومسح أو إضافة ملفات وبرامج أو القدرة على التحكم بنظام التشغيل وإصدار الأوامر" أو أنه عملية دخول غير مصرح.

ويتحقق الدخول غير المصرح به إلى أنظمة المعالجة الألية للمعطيات بأحد الأمرين:

[1] د/ خالد ممدوح ابراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الاسكندرية، 2008.

[2] محمد خليفة ، المرجع السابق، ص145.

– أولهما: ألا يكون هناك تصريح بالدخول بتاتا لدى من تقوم بالدخول وهي الحالة التي لا تكون فيها للشخص الذي يدخل النظام أي علاقة بهذا الأخير، وذلك كونه من العاملين لدى الجهة التي يتبعها النظام أو رغم كونه من العاملين له بالنظام ولا تخوله وظيفته الإتصال فيه وفي كلتا الحالتين لا يجوز لهذا الشخص ترخيصا بالدخول للنظام، سواءا كان الترخيص بالدخول يتوقف على سداد مبلغ معين، أو يتوقف على العضوية في جهة معينة أو على غير ذلك من الشروط أو كان الدخول إلى النظام ممنوعا على الإطلاق.

– ثانيهما: المصرح له يقوم بتجاوز الحدد التي رسمت له في هذا التصريح.

– يثير تجاوز التصريح في الدخول إلى أنظمة الحسابات مشاكل عملية عديدة، لاسيما في إثبات القصد الجنائي لدى فاعله الذي يتمتع بتصريح محدود، لأن هناك حالات كل عامل بدقة، ولا سيما كذلك وأن أنظمة الحسابات تمتاز بأن مناطقها مفتوح بعضها على البعض، وتمتاز بتشعب نوافذها كما يؤدي إلى مناطق المختلفة لهذا يجب التأكد من توافر القصد الجنائي لدى الفاعل في تجاوز التصرح الممنوح له، وأخيرا جريمة الدخول غير المصرح به لا تتحقق الغرض الممنوح من أجله الترخيص أو التصريح لأن المادة 394 مكرر من القانون الجزائري إذ نصت على :" دخول عن طريق الغش وليس ما يحصل بعد هذا الدخول من الزام بحدود التصريح أو تجاوزه" فصيغة الغش إل تتصرف إلى عملية الدخول وليس إلى حدود التصريح بهذا الدخول ومن المعروف أن مبادئ التفسير في القانون الجنائي لا تسمح بهذا التوسع أو القياس.

2) فعل البقاء.[1]

قد يتخذ النشاط الإجرامي الذي يتككون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الألية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام، وقد يجتمعان، يكون البقاء معاقبا عليها استقلال حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك أذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقى رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي.

وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة. من له الحق في السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الإجتماعي المادي للجرائم.[2] وإن كان الدخول –في نظر هذا الرأي– يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل، وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام وتنتهي بإنتهاء حالة البقاء.

الفرع الثاني: الركن المعنوي لجريمتي الدخول والبقاء غير المصرح بهما.

إن الركن المعنوي لجريمتي الدخول والبقاء غير المصرح بهما يتخذ صورة القصد الجنائي من علم إدارة وإدارة باعتبارها من الجرائم العمدية، ولقد عبر نص المادة 394 مكرر من ق.ع.ج. عن القصد الجنائي العام الذي يتطلب أن يكون الدخول والبقاء " عن طريق الغش" فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع وهو نفس ما عبر

[1] د/ نائلة قورة، مرجع سابق، ص346.

[2] علي عبد القادر القهوجي، المرجع السابق، ص22.

المشرع الفرنسي في نص المادة 1/323 ق.ع.ج بعبارة frauduleusment أي أن القصد الجنائي لا يكفي إنما يجب توافر قصد جنائي وهو " الغش " ليس القصود به نية الغاضرار وإلا يكون هناك تناقض بين الركن المادي الذي يتطلب النتيجة والركن المعنوي.

مفهوم الغش الذي اعتمده الفقه والقضاء بالنسبة لهذه الجريمة هو مفهوم مستعار من الغش في جريمة السرقة وقد عرفه القضاء كالتالي: il y a accés ou maintenir frauduleux lorsque l'agent a su qu'il agissait sans droit .qu'il n'était pas autorisé ou encore qu'il agissait contre le gré du naitre du systéme[1]

عادة يبدو طابع الغش الذي تتم به الدخول من خلال الجهاز الرقابي الذي يحمي النظام، أما بالنسبة للبقاء فيستنتج من العمليات التي تمن داخل النظام.

المطلب الثاني: جريمة التلاعب بمعطيات الحاسب الألي.

جريمة التلاعب بالمعطيات هي جريمة الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول والبقاؤ غير المصرح بها، أما قانون العقوبات الفرنسي في نص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات وقد أثر المشرع الجزائري عدم النص على هذه الأخير نظرا للتشابه الكبير بينهما وبين جريمة التلاعب بالمعطيات، بحيث يصعب في الكثير من الأحيان نظرا للتشابه الكبير بينها وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده، وقد إكتفى المشرع الجزائري نتيجة إفساد النظام كطرف مشدد فقط لجريمة الدخول واستبعادها كجريمة قائمة بذاتها.[2] والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والمحو والتعديل، ويكفي توافر أحدها لقيام الجريمة، فلا يشترط إجتماعها معا حتى تتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن

[1] Vivant ; informatique et droit penal, les biens informatiques objets d'une fraude lamy informatique 1991.p1511.N°3443.

[2] محمد خليفة، المرجع السابق، ص175.

المادي للجريمة لكن القاسم المشتري في هذه الأفعال جميعا هو إنطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[1]

وعلى ذلك فإن موضوع السلوك الإجرامي في هذه الجريمة محدد، وهو الإعتداء على معطيات في نظم المعالجة أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز أو إشارات تمثل المعلومات، أي بيانات تمت معالجته.

فالجريمة في هذه الحالة تقع على معطيات البيانات المعالجة دون المعلومة ذاتها، وذلك يخرج من نطاق هذه الجريمة المعلومات التي تعالج بع، ولم تدخل إلى نظام معالجة البيانات وكذلك البيانات التي أدخلت إلى النظام، لكن لم تبدأ بعد أي خطوة في معالجتها، وكذلك المعلومات التي انفصلت عن النظام وسجلت على شريط ممغنط أو قرص مدمج، ذلك لأنها أصبحت خارج النظام والنص يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بأن اتخذت خطوة أو أكثر في مراحل معالجتها.

وترتيب على ذلك يمكن القول بأن الحماية الجنائية في هذه الجريمة قائما طالما أن المعلومة المعالجة داخل النظام أو في طريقها للمعالجة حسب التحديد السابق أو المعلومات المعالجة داخل النظام أو النظام أو في طريقها للمعالجة حسب التحديد السابق أو المعلومات المعالجة التي انفصلت ثم إعيد إدخال فيه، أما المعلومات غير المعالجة لم تدخل إلى النظام أو دخلت ولم تبدأ مراحل معالجتها فقط، أو عولجت وانفصلت عن النظام، فهي خارج نطاق الحماية المشمولة بهذا النص، وإن كان يجوز حمايتها وفقا لنصوص جنائية أخرى.[2]

[1] د/ محمد نجيب حسني، الموجز في شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 2003، ص253.

[2] علي عبد القادر القهوجي، المرجع السابق، ص58.

الفرع الأول: الركن المادي لجريمة التلاعب بمعطيات الحاسب الآلي.

الركن المادي لجريمة التلاعب بمعطيات الحاسب الآلي، يقوم الركن المادي لجريمة التلاعب في المعطيات على السلوك الإجرامي الذي يتكون من ثلاثة أفعال هي الإدخال غير المصرح به للمعطيات على السلوك الإجرامي الذي يتكون من ثلاثة أفعال هي الإدخال غير المصرح به للمعطيات داخل نظام المعالجة الآلية للمعطيات أو إزالة هذه المعطيات أو تقديمها بغيار تصريح، وهذه الأفعال تؤدي كلها إلى التغيير من الحالة التي توجد عليها المعطيات محل الإعتداء أي تؤدي إلى المساس بسلامتها وتكاملها.[1]

أولا: الإدخال غير المشروع للمعلومات.

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت خالية أوم كان يوجد فيها معطيات من قبل، والإدخال غير المشروع للمعلومات أو البرامج قد يترتب عليه فضلا عن التعديل يطرأ على ذاكرة الحاسب الآلي تذلل لمعلومات ذاتها أو تدميرها كما في حالة إدخال برامج خبيثة إلى نظام الحاسب الآلي.[2]

ثانيا: الإزالة غير المشروعة للمعلومات (تدمير المعلومات).

نصت المادة 394 مكرر 1. من ق.ع.ج على فعل الإزالة ويتم ذلك بإزالة المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة وتخزين المعطيات إلى المنظمة الخاصة بالذاكرة.

ولقد إستخدمت جميع القوانين التي جرمت الإتلاف المعلوماتي بقصد إخفاء المعلومات ومحوها، للتعبير عن تدمير المعلومات بإعتبار صورة متميزة من صورة الإتلاف.[3]

---

[1] محمد خليفة، المرجع السابق، ص179.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الطبعة الأولى ، 2008، ص122.

[3] أسامة محمد لمناعسة، جرائم الحاسب الألي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، عمان 2009، ص 73.

ويرى البعض أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تميزا لها ومؤدى ذلك أن إخفاء الملفات على سبيل المثال: لا يترتب على محو المعلومات التي يحتوي عليها ذاكرة الحاسب الألي وإنما يؤدي إلى تعديل في قائمة الملفات فهو لا تعديل ولا تدمير.[1]

ثالثا: التعديل غير المشروع للمعطيات.

ويقصد بتدمير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويتحقق ببرامج غريبة تتلاعب في المعطيات سواءا بمحوها كليا أو جزئيا أو بتعديلها وذلك بإستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرامج المحاماة، أو برامج الفيروسات بصفة عامة هذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل أخر غيرها.[2]

الفرع الثاني: الركن المعنوي لجريمة التلاعب بالمعطيات.

جريمة الإعتداء العمدي على المعطيات أو ما تعرف بجريمة التلاعب بالمعطيات جريمة عمدية يتخذها فيها الركن المعنوي صورة القصد الجنائي بقيصرية العلم والإرادة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بأنه نشاط الجرمي يترتب عليه التلاعب في المعطيات ويعلم أيضا أن ليس له الحق بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته.

كما يشترط التوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام بنية الغش لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركناها بمجرد الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه.

[1] نائلة محمد فريد قورة، المرجع السابق، ص 218.

[2] أمال قارة ، المرجع السابق، ص122.

تلك المعطيات دون موافقته ولا يتطلب نص المادة 394 مكرر 01 قصدا جنائيا خاصا إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التشريعات المقارنة التي اشترطت قصدا خاصا إلى جانب القصد العام، يتمثل في اتجاه نية المتهم إلى الأضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، وهو ما كان عليه النص الفرنسي القديم قبل تعديله، ويبرز ذلك في عبارة " إرتكاب الفعل دون مراعاة حقوق الأخرين" وقد انتقدت هذه المادة قبل تعديلها بشدة لتطلبها القصد الجنائي الخاص، كون أن اشترط هذا القصد الخاص سوف يؤدي إلى اللاعقاب في الحالات التي تتجه فيها نية الفاعل إلى تحقيق الربح، على الرغم من أهمية المعلومات التي قد يتم إتلافها، مثل اتلاف معلومات علمية.[1]

المبحث الثاني: الجزاءات والعقوبات المقررة لجرائم الإعتداءات الماسة بالأنظمة المعلوماتية.

لقد نصت المادة 13 من الإتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبات المقررة نتيجة إرتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية، كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ له مساءلة الشخص المعنوي الوارد في المادة 12 من نفس الإتفاقية.

المطلب الأول: العقوبات المطبقة على الشخص الطبيعي.

الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات.

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذا نجد سلم خطورة يتضمن ثلاثة درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى، وبعدها الدرجة

[1] أحمد خليفة الملط، جرائم المعوماتية دار الفكر الجامعي الاسكندرية ، 2006، ط02، ص181.

الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة، فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.[1]

أولا: جريمة الدخول والبقاء.

أ) الدخول وإلقاء بالغش (الجريمة البسيطة) العقوبة المقررة هي 03 أشهر على السنة حبس و50.000دج إلى 100.000 دج غرامة (المادة 394 مكرر).

ب) الدخول والبقاء بالغش الجريمة المشددة) تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات العقوبة من 06 أشهر إلى سنتين وغرامة 50.000 دج على 150.000 دج إذا ترتب عن الدخول أو البقاء غير المشروع لنظام اشتغال المنظومة (المادة 394 مكرر 03، 02).

ثانيا: جريمة التلاعب بالمعطيات.

نصت عليها المادة 394 مكرر 1 ، ق.ع.ج بالحبس من 6 أشهر إلى 03 سنوات وعقوبة الغرامة التي تتراوح من 500.00 إلى 200.00 دج.

والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواءا كانت هذه الأخيرة في صورتها البسيطة والمشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالحتها وحتى في صورتها المشددة، وإن أردت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها الصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة.[2]

[1] أمال قارة، مرجع سابق، ص127.

[2] د/ نادلة عادلة محمد فريد قورة، المرجع السابق، ص228.

ثالثا: جريمة التعامل في معطيات غير مشروعة.

تعاقب المادة 394 مكرر 2 من ق.ع.ج على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبالغرامة المالية من 1.000.000 دج إلى 5.000.000 دج بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواءا في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات (غير أن حدها الأدنى يقل عن كلتا الجريمتين).

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتها (سنة أو سنتين) وستساوي مع الأحد الأقصى لجريمة التلاعب بالمعطيات (03 سنوات).

غير أن حدها الأدنى يقل عن الجريمتين معا، لأنه في جريمة الدخول أو البقاء البسيطة 3 أشهر وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب في 6 أشهر.[1]

الفرع الثاني: العقوبات التكميلية.

نصت المادة 394 مكرر 6 من ق.ع.ج على العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فيها مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا من الجرائم المعاقب عليها في هذا القسم، علاوة على إغلاق المحل أو مكان الإستعمال إذا كانت الجريمة قد ارتكبت بعلم مالكها ويستخلص من نص هذه المادة العقوبات التكميلية التالي:

أولا: مصادرة الأجهزة والوسائل والبرامج المستخدمة : وذلك مع الإحتفاظ بحقوق الغير حسن النية، وتجدر الإشارة إلى أن المشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط. وأغفل مصادرة الوسائل الموجهة لإرتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المرسلة عن طريق

[1] محمد خليفة، المرجع السابق، ص219.

منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 قانون عقوبات جزائري، حيث أن عبارة " المستخدمة" الواردة في نص المادة 394 مكرر 6 الخاصة بالعقوبات التكميلية تقيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر 6 من قانون عقوبات جزائري التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجها للقيام.

ثانيا: إغلاق المواقع التي تكون محلا للجريمة من جرائم الإعتداءات الماسة بأنظمة المعالجة الألية للمعطيات.[1]

ثالثا: إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها وأضاف المشرع شرط علم المالك إذا كان على سبيل المثال الجاني مستأجر للمحل المالك المؤجر له، ويعلم خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الأنترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالأفعال الخطيرة التي يقوم بها زبونه، ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الإستغلال، مما يطرح مشكلا في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل أو أماكن كعقوبة تكميلية للشخص الطبيعي المسؤول جزائيا، ومن جهة أخرى لا يمكننا الرجوع إلى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى المدة، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي فيوجد حسب رأينا في توقيع الجزاء الجزاء، حيث تم توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي.

إن العقوبة التكميلية الواردة في المادة 394 مكرر 06، ق.ع.ج غير كافية في مواجهة الحالات العديدة التي يمكن أن يرتكبها الشخص الطبيعي فمثلا تنص المادة على العقوبة التكميلية الخاصة بالموظف العمومي المصرح له بالدخول على نظام الألية للمعطيات لكنه يبتعد ذلك إلى ارتكاب جرائم

[1] د/ أحسن بوسيقة، المرجع السابق، ص448.

أخرى متعلقة بالمنظومة المعالجة أليا، وكذلك الشيء بالنسبة للوظيفة المهنية فيما يخص المحامين أو الأطباء مثلا، وكذلك الوظيفة الإجتماعية إذا ارتكبت الجريمة عند تأدية الوظيفة أو بمناسبتها وهذا ماجءت به أحكام المادة 323-05 من قانون العقوبات الفرنسي والتي نصت على تكميلية أخرى، ندعوا المشرع الجزائري إلى الأخذ بها وهي كما يلي:

- المنع لمدة أقصاها 5 سنوات من الحقوق المدنية والسياسية.
- المنع لمدة أقصاها 5 سنوات من ممارسة الوظيفة العمومية أو النشاط المهني أو الإجتماعي إذا ارتكبت الجريمة أثناء تأدية الوظيفة أو بمناسبتها.
- مصادرة الشيء الذي استخدم أو الموجه لإرتكاب الجريمة أو الشيء محل الجريمة الغلق لمدة أقصاها 5 سنوات للمؤسسات، أو لحد أو عدة مؤسسات المقاولة التي استعملت في ارتكابها الأفعال المجرمة.
- الحرمان لمدة أقصاها 5 سنوات من الصفقات العمومية.
- المنع لمدة أقصاها خمس سنوات في اصدار الشيكات، بما فيها التي تسمح سحب الأموال من طرف الساحب لدى المسحوب له أو المرخص أو المرخص لهم بذلك، تقليل أو نشر الحكم أو القرار الصادر.[1]

الفرع الثالث: الظروف المشددة.

نصت المادة 394 مكرر 2-03 على ظروف التشديد بع عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا لظروف عندما ينتج عن الدخول أو القاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

[1] د/ أحسن بوسقيعة، المرجع السابق، ص449.

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة الحبس ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج.

هذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافر.

نصت المادة 394 مكرر 3، على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.[1]

المطلب الثاني: العقوبات المطبقة على الشخص المعنوي.

لقد كانت العقوبة إحدى أهم الحجج التي استند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي حيث رأو أنه لا يمكن تطبيقها عل هذا الأخير خاصة تلك العقوبات السالبة والمقيدة للحرية، لكن وبعد اتساع تطبيق عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي لم لهذا الإعتراض محل، ولقد تضمنت المادة 18 مكرر من قانون العقوبات الجزائري بعد تعديله سنة 2004، أنواع العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح، وأول هذه العقوبات هي الغرامة التي تساوي من مرة إلى خمس مرات الحد أو جبن الأخذ بالحد الأقصى لهذه العقوبات، وهو خمس مرات فيما يتعلق بجرائم المعطيات وفيما يخص القانون الفرنسي فقد نصت المادة 323-06 من قانون العقوبات بأن الأشخاص المعنوية يمكن أن يحكم عليها بالمسؤولية الجنائية وفقا للشروط التي حددتها المادة 121-2 وأن العقوبات المقررة عليها هي:[2]

- الغرامة وفق ما تنص عليه المادة 131-38.
- العقوبات المحددة في المادة 131-39.

[1] أنظر نص المادة 394 مكرر5 من قانون العقوبات الجزائري.

[2] أنظر نص المادة 121 وما يليها من قانون العقوبات الجزائري.

– العقوبات المحددة في المادة 131–39 فقرة 2 بالنسبة للنشط المهني الذي تقصت بمناسبة الجريمة.

وتنقسم العقوبات المقررة على الشخص في قانون العقوبات الجزائري وكذا الفرنسي بالنظر إلى طبيعة الحق الذي تمس أنواع:

– العقوبات الماسة بوجود الشخص المعنوي أو حياته وتتمث في الحل.

– العقوبات الماسة بالذمة المالية للشخص المعنوي وتتمثل في الغارمة والمصادرة .

– العقوبات الماسة بالنشاط المهني للشخص المعنوي وتتمثل في إغلاق أو المؤسسة وكذا التمتع من ممارسة النشاط المهني أو الإجتماعي.

– العقوبات الماسة بالسمعة وتتمثل في نشر الحكم وتعليقه.

– العقوبات الماسة بحق الشخص المعنوي في التعامل بحرية لتحقيق أهداف التي أنشء من أجلها، وتتمثل في الحراسة القضائية والإقصاء من الصفقات العمومية ويضيف القانون الفرنسي المنع حتى الدعوى العام للإدخار وكذلك منع إصدار الشيكات.

– وهذه العقوبات في القوانين الجزائري والفرنسي ليست خاصة بجرائم المعطيات وإنما يمكن أن توقع على الجرائم التي يرتكبها الشخص المعنوي وليس هناك ما يميز جرائم المعطيات إلا عقوبة الغارمة المشددة.

المبحث الثالث: خصوصية جرائم المعطيات من حيث الإجرام

بعد تطرف لأركان أنظمة المعالجة الآليات للمعطيات و الجزاءات المقررة لها ،سوف نعالج في هذا الفصل الآليات القانونية في مفهوم أصول التحقيق الجنائي في الجرائم الالكترونية بما فيها جمع الأدلة و التفتيش و جمع الاستدلالات ، وطرق متابعاتها بما فيها الانتقال و المعاينة . وذلك تماشيا مع مواد القانون رقم 09–04 المتضمن القواعد الخاصة

للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي يسمح باستعمال وسائل قانونية جديدة تتلاءم وخصوصية هذا النوع من الجرائم إضافة إلى الأشخاص المخولين قانونا لكيفية إثبات الجريمة (ضباط الشرطة القضائية) والأقطاب الجزائية المتخصصة .

بحيث نتناول فيها :

.

مطلب الأول: خصوصية جرائم المعطيات من حيث إجراءات و التحقيق .

يقوم ضباط الشرطة القضائية و النيابة العامة بإجراءات المتابعة فور تلقي بلاغ أو دعوى عن وقوع جريمة معلوماتية مع التحقيق في هذه الجرائم و كل لهم صلة بالموضوع محل البلاغ ، بجمع الاستدلالات من خلال الانتقال و المعاينة ، التفتيش وتلقي المراسلات .... ،و هذا ما سيتم عرضه في المطلبين التاليين :

خصوصيتها من حيث إجراءات المتابعة

إن لضباط الشرطة القضائية دور فعال من ضبط أدلة الجرائم و مرتكبيها وكشف كل ما يتعلق بها حال وقوعها .

أما بالنسبة للجرائم المستحدثة فإنها تلقى المزيد من الأعباء على عائق هذه السلطة وكذلك المر بالنسبة للسلطات القضائية ،و ذلك نظرا ضعف خبرة كلا منهما في مواجهة هذه الجرائم .فمن المتصور أن يجد ضباط الشرطة القضائية أنفسهم غير قادرين على لتعامل بالوسائل الاستدلالية و الإجراءات غير التقليدية مع هذه النوعية من الجرائم ، و قد يفشل جهاز الضبط القضائي في تقدير أهمية الجريمة نظرا لنقص الخبرة و التدريب و لهذه الأسباب كانت من أولويات السياسة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال تكوين و تأهيل سلك ضباط الشرطة القضائية و أعوانهم.[1]

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص232.

فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، فبموجب هذا العمل فإن الكثير من إطارات الدرك الوطني استفادوا من تكوين خاص في جامعات سويسرا و أمريكا ،كندا ، سواء في المجال التقني لإعلام الألي (أو القانوني) الجرائم المتصلة المعلوماتية (و كذلك تم التكوين في مؤسسات وطنية مثل مركز الدراسات الذي عرض تكوينا في الأمن المعلوماتي في إطار التكوين كل سنة cerist و البحوث في الإعلام العلمي و التقني هذا البرنامج التكويني يهدف إلى تطوير كفاءات سلك الدرك الوطني ،حتى تكونن أكثر عملية في مجال مكافحة الجرائم المعلوماتية [1] كما أن إطارات الدرك الوطني تساهم في عدة ملتقيات وطنية و دولية تنصب موضوعاتها في إطار الجرائم كما أن إطارات الدرك الوطني تساهم في عدة ملتقيات وطنية و دولية تنصب موضوعاتها في إطار الجرائم المتصلة بالمعلوماتية بينما مصالح الأمن الوطني هي غائبة عن مجالات تكريس مكافحة هذه الجرائم ما عدا ما يتم تنظيمه من معارض و ملتقيات تتعلق بالموضوع،و كذلك المشارك و المساهمة في ملتقيات و مؤتمرات وطنية و دولية تتناول بالخصوص حقوق المؤلف في البيئة الرقمية كما أن الدرك الوطني الفرنسي أنشأ منذ سنة 1998 إدارة مكافحة الجرائم المعلوماتية ضمن المصلحة التقنية للأبحاث القانونية والوثائقية، كل هذه الترسانة من الهيئات و المؤسسات لمكافحة الجرائم المعلوماتية بمختلف أشكالها ما هي إلا دليل على خطورة و تشعب هذا النوع الجديد من الإجرام ، وهو ما يجب على السياسة الجنائية الجزائرية أن تتبعه ، لأنه يلاحظ تباطؤ كبير في مجالات هذه الجرائم ، وإفلات الكثير من المجرمين من العقاب خاصة فيما يتعلق بالاعتداءات على الأشخاص والأموال التي تتم بواسطة شبكة الأنترنت وكذلك ما وصلنا إليه من تبادل للصور عبر التي

[1] Hadjira bouder.orientatiot de la politique pénale de prevention et de lutte contre la criminalité liees au tic en amlgerie.centre de recherche sur l'information scentifique et tchnique cerist03 , www.alexalaw.com ,01/05/2014,22h.43.

تحمل في طياتها خدش للحياة العام، وصور لأشخاص أبرياء التقطت لهم تلك الهواتف المحمولة عبر الصور بعلم منهم أو بدون عملهم ،و لكن وظفت تلك الصور لتكون أفعال إجرامية يعاقب عليها القانون ، ولأنه لا توجد سياسية وقائية تحسيسية فإن فاعلي هذه الجرائم يتمادون في ارتكاب جرائهم لهذا فإن التدريب الجيد العناصر الأمن و الدرك الوطنيين والحملات التحسيسية للمواطنين ستحد من انتشار هذه الجرائم ، و في حالة وقوعها فغن المجرمين ينالون عقابهم لإمكانية الوصول إليهم عبر إجراءات قانوني تتسم بالشرعية [1].

إن النيابة العامة في قضايا الجرائم المتصلة بالجريمة المعلوماتية ، و لاسيما بعد اللجوء الواسع و المتزايد إلى الشبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية و قانونية لمعالجة هذه القضايا ، وعلى هذا فإن حتمية المعرفة و لو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي .

ومنذ سنة 2003 و في إطار إصلاح العدالة ، قانت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة ، ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم اجراء أول دمج مادة الجريمة المعلوماتية في برنامج تكوين طلبة المدرسة الوطنية للقضاة على شكل ملتقيات ينشطها خبراء العديد من دورات التكوين في مختلف مجلات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصلح القضاة.

الفرع الثاني :خصوصيتها من التحقيق

من الصعب التحقيق في الجرائم المعلوماتية بسبب تعقيداته مما يستوجب الإلمام بأمور تقنية بحثة ، تختلف عن طرق العادية في مجال التحقيق و توجيها للأسئلة الاستفسارات بحيث يجب أن تكون مقنعة و ذات مصداقية و هذا ما يجعلها ذات طبيعة خاصة ، و هذا ما سنتناوله في يلي:

[1] Hadjira bouder.opcit , www.alexalaw.com ,02/05/2014,22h.43

أولا : الانتقال والمعاينة

من خصائص الجريمة المعلوماتية أنها قلما تخلف أثار مادية إضافة إلى لزوم وقت طويل نسبيا لاكتشافها ما يعطي الفرصة لمرتكبي هذه الجرائم أن يضروا أو يتلفوا أو يبعثوا بالآثار المادية للجريمة إن وجدت و هو الأمر الذي يولد الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية .

وفي كل الأحوال فإنه عند تلقي البلاغ عن وقوع إحدى الجرائم المعلوماتية و بعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة المعلوماتية و تعيين مراعاة ما يلي: [1]

1/ ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها و شبكاتها .

2/ وجود خريطة توضح الموقع الذي ستتم معاينته و تفاصل المبنى أو الطابق موضوع البلاغ ، عدد الأجهزة و الخزائن و الملفات و يحدد ذلك من خلال مصادر سرية لجهات الأمن .

3/ تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة .

4/ تأمين الأجهزة و المعدات التي سيتم الإستعانة بها في عملية سواء كانت أجهزة أو برامج .

5/ إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء و رجال الضبط و الأمن .

6/ تحديد البيانات و المهام و الاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدى ، و ذلك حتى لا تتداخل الإختصاصات .

[1] [1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية ، جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، 2006، ص317.

7/ إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل .

8/أن تتم هذه العملية وفق مبدأ المشروعية و في إطار ما تنص عليه القوانين الجنائية .تأمين عدم إنقطاع التيار الكهربائي لأن معاينة الأجهزة و ما بها من برامج وشبكات و أنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي .

وعند معاينة مسرح الجريمة يرى الفقه الجنائي ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية و هذه الضوابط هي :

- تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة و تحديد مواقعها بأسرع فرصة ممكنة ، وفي حالة وجود و ذلك لأج تعطيل الاتصالات لمنع تخريب الأداة الموجودة serveur شبكة اتصالات وجوب البحث عن خادم الملفأ ومحوها ويراعي تصوير الأجهزة الموجودة خاصة الأجهزة الخلية منها .

ضرورة وضع حراسة كافية على مكان المعاينة ،ومراقبة التحركات داخل بل ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول أجهزة الهاتف النقال التي قد تساعد عن طريق تقنية معينة في تدمير أدلة الجريمة المعلوماتية متى تم توصيلها بالأجهزة محل المعاينة .

*ملاحظة الطريقة المعد بها النظام ألمعلوماتي و الآثار التي يخلفها ومعرفة السجلات الإلكترونية التي تزود بها شبكة المعلومات لمعرفة موقع الاتصال ورع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار وبروتوكولات الاتصال عبر الانترنت وهو ما يعرف اختصارا ip[1].

كما يتعين كذلك ملاحظة وإثبات حالة التوصيلات والكبلات المتصلة بكل مكونات النظام حتى يمكن تحليل البيانات ومقارنتها والوصول منها إلى الدليل .

[1]يعؤف ال ipهو اختصار لكلمة internet protocol أنه وسيلة لنقل البيانات من كومبيوتر مربوط بشبكة الأنترنت إلى كومبيوتر أخر على نفس الشبكة.

عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للكمبيوتر من مجالات القوى المغناطيسية التي قد تسبب في محو البيانات و لن يأتي ذلك إلا عن طريق خبراء الكمبيوتر .

*التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة و غير سليمة أو محطمة و رفع البصمات التي قد تكون عليها ، وكذلك التحفظ على مستندات الإدخال و الأوراق المطبوعة لجهاز الكمبيوتر و التي قد تكون ذات صلة بالجريمة .

*ضرورة قصر المعاينة على الباحثين و المحققين الذين لديهم كفاءة علمية و خبرة فنية في مجال المعلوماتية و استرجاع البيانات .

ثانيا : التفتيش و ضبط الأشياء [1].

فيما يخص احراءات التفتيش و الحجز فتناولنا المادة 47 المعدلة في فقرتها 3 و 4 من قانون الإجراءات الجزائية ،و التي تكون في محل سمني و في كل ساعة من ساعات الليل أو النهار بناء على إذن مسبق من وكيل الجمهورية ،و يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد الإقليم الوطني ،أو يأمر ضباط الشرطة القضائية المختصين بذلك أو القاضي المنتدب لذلك و إذا وجدت اثناء التحري في جريمة متلبس بها أو تحقيق في هذه الاعتداءات أن كان هذا الشخص موقوفا للنظر أو محبوسا لسبب أخر يمكن أن يجري التفتيش دون حضوره و دون الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق و بحضور شاهدين مسخرين أو ممثل يعينه صاحب المسكن و هذا لدواعي المحافظة على النظام العام . و قد نصت المادة 5 من قانون 09-04 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها عن حالات اللجوء للتفتيش نظم المعلوماتية و هما الحالتين المتعلقتين بالوقاية من الفعال

[1] د/ مصطفى محمد موسى ، المرجع السابق، ص205.

الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ،و كذلك حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع ت الوطني أو مؤسسات الدولة أو الاقتصاد الوطني . فالتفتيش هنا و خلافا للتفتيش التقليدي عن الأدلة التي تثبت وقوع الجريمة و نسبتها إلى المتهم ، إنما هي حالة إجراء تفتيش وقائي قد تسفر عنه أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به ارتكاب جرائم ذات خطورة على الأمن الداخلي للدولة ،و كما نعلم فإن الحكام العامة للتفتيش تقضي بأنه الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة جناية أو جنحة واقعة بالفعل و ترجح نسبتها إلى متهم معين و أن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو حرمته الشخصية [1] . و كذلك الأمر في حالة التحري في الجنحة المتلبس بها (المادة 44 من قانون الإجراءات الجزائية).

كما نصت المادة 64 من ق.ا.ج. التي تحيل أحكام المواد من 44 إلى 47 ق.ا.جح . فيما يخص التحريات الأولية التي يجريها ضباط الشرطة القضائية كما أن الدستور نص على وجوب أن يتم التفتيش مكتوب صادر عن السلطات القضائية المختصة المادة 40 من دستور 1996 .

كما نصت أيضا المادة 5 والمادة 2 على إمكانية الدخول إلى منظومة معلوماتية موجودة على جهاز أخر متصل بالجهاز الأول لكن في مكان أخر مختلف تماما عنه داخل الدولة و متصلان فيها بينهما بشبكة اتصالات أين كانت، يمكن الدخول إلى هذه المنظومة سواء كان الجهاز الثني ملك للمتهم أو لشخص أخر فلا فرق، مادامت هناك دلائل على إمكانية وجود المعطيات المبحوث عنها في ذلك النظام، وعليه فإن التفتيش في هذه الفرضية:

[1] أحمد مسعود مريم، رسالة ماجستر، اليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون 09-04 قاصدي مرباح ، ورقلة، 2013/2012، ص90.

1 وجود دلائل أو أسباب تدعوا للإعتقاد بأن الكشف عن المعطيات يكون بالبحث في المنظومة الثانية.

2 إعلام السلطة القضائية لم يفرض المشرع إذن ثاني يسمح بهذا التفتيش وإنما مجرد اعلام السلطة القضائية التي تولت أمر هذا التفتيش (وكيل الجمهورية، قاضي التحقيق بحسب الحالة).

إجراءات إعتراض المراسلات وتسجيل الأصوات والتقاط الصور: المواد من 65 مكرر 5 إلى 65 مكرر 10 يجوز لوكيل الجمهور المختص أو قاضي التحقيق أن يأذن كتابيا في أجل 4 أشهر قابلة للتجديد بـ: اعتراض المراسلات التي تتم عن طريق وسائا لالإتصال السلكية ولالسلكية، مع امكانية تسخير عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية مكلفة بالموصلات السلكية واللاسلكية للتكفل بالجوانب التقنية مع ضرررورة تحرير محضر عن كل عملية.

وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط صور في أماكن خاص، ويسمح هذا الإذن بالدخول للمحلات السكنية أو غيرها في أي وقت ودون علم رضا صاحب المسكن ويجب أن يتضمن كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها، والأماكن المقصودة بالجريمة التي تبرر اللجوء لهذه التدابير ومدتها، وإذا ما اكتشفت جرائم أخرى غير التي وردت في الإذن فأن ذلك لا يكون سببا في بطلان الإجراءات العارضة كما يصف أو ينسخ ضابط الشرطة القضائية المأذون له المراسلات أو الصور أو المحادثة المسجلة أو المقفيدة في إظهار الحقيقة في محضر يودع الملف[1].

[1] أحمد مسعود مريم، رسالة ماجستر، نفس المرجع، ص92.

رابعا: إجراءات التسرب [1] المواد 65 مكرر 11 إلى 65 مكرر 18 قانون إجراءات الجزائية.

عندما تقتضي ضرورة التحري والتحقيق في الإعتداءات الماسة بأنظمة المعالجة الآلية لأنظمة المعلومات يوم الضابط أو عون الشرطة الفضائي تحت مسؤولية ضابط الشرطة القضائية المكلفة بتنسيق العملية وبموجب إذن مكتوب ومسبب من وكيل الجمهورية أو قاضي التحقيق بعد أخطار وكيل الجمهورية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بايهامهم أنه فاعل معهم أو شريك لهم خاف، مع إمكانية استعمال هوية مستعارة وارتكاب الأفعال التالية دون اعتبار تحريضا على ارتكاب الاعتداءات.

اقتناء أو حيازة أو نقل أو تسليم، أو اعطاء أو مواد أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الاعتداءات، ويجب أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته، ويحدد كذلك مدة عملية التسرب التي لا يمكن أن تتجاوز 4 أشهر إلا في حالة التمديد من طرف القاضي الذي رخص بها.

المطلب الثاني: خصوصيتها من حيث المحاكمة. [2]

إن علوم الإثبات الرقمي هي استعمال المناهج العلمية لحماية، أو جمع ، أو صلاحية ، أو تعريق، أو تحليل وترجمة الوثائق، وتقديم الحجج المادية المتحصل عليها من المصادر الإلكترونية، بهدف تسهيل إعادة تركيب الأحداث، أو توقع المحاولات الإجرامية.

والحجة الإلكترونية هي الآثار المتحصل عليها من منظومة الكترونية عندما تستعمل لإتمام عمليات نوعية، مثل إرسال الكتروني أو تسجيل حدث ما، والنتيجة من هذه الأنشطة هي المعطيات المتحصل عليها من النظام نفسه، والتي يمكن أن تعطي نظرة عامة أو جزئية

[1] أنظر نص المواد 65 مكرر 11 إلى 65 مكرر 18 قانون الإجراءات الجزائية.

[2] فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، 2010.

عن الحدث. فبعد إكتشاف الأفعال الإجرامية من طرف مصالح الضبطية القضائية ، تبدأ عملية البحث والتحري من خلال تنقل الفرق المختصة إلى مسرح الجريمة لمعاينة محل الجريمة، وجمع وحفظ الأدلة، وإرسالها إلى المخبر العلمي لترجمة التحاليل، بغرض تهيأة المحضر وتقديم وتتبع هذه المصالح قواعد مرتبطة بحماية الأدلة من خلال:

-حفظها باستعمال نسخ خلال مرحلة التحليل المخبري.

-إعداد تقرير عن كل عملية تمت بالتدقيق حتى نهاية التحليل.

-تنصيب سلسة التوضيح، وهي تثبيت الموجودات التي أفضى عنها التحليل في كل مرحلة للوصول إلى الدليل.

كما تتبع أيضا قواعد مرتبطة بصلاحية الطريقة المستعملة لإرتكاب الجريمة من خلال:

- بحث إن كانت هذه التقنية قد جربت من قبل، وهل يمكن تجريبها مرة أخرى.

-البحث في ما إذا كانت التقنية قد نشرت، أو أخضعت للتقييم من طرف مخابر مختصة.

والذي يمكنه أن يأمر في أي وقت بوقفها قبل انقضاء المحددة، وقد أقر ق.أ.ج عقوبات صارمة ضد من يكشف هوية ضابط أو عون الشرطة القضائية المتسرب في أي مرحلة من مراحل الإجراءات طبقا للمادة 65 مكرر 16 من ق.أ.ج.

البحث عن نسبة الخطأ الذي يمكنه أن تتضمنه التقنية، وكذلك مختلف أشكال الرقابة الضرورية الملائمة.

الفرع الأول: من حيث الإختصاص المحلي

تنص المادة[1] 2/37 من قانون الإجراءات الجزائية، على أنه يجوز تمديد الإتصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الألية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

كما أن المشرع الجزائري أراد أن يواكب سياسة التخصص ونظرا لوجود جرائم تحتاج إلى أقطاب قضائية لمعالجة جرائم معينة من بينها الجرائم الماسة بنظام المعالجة الألية للمعطيات.

ولقد صدر المرسوم التنفيذي [2] رقم 06-348 المؤرخ في 12 رمضان عام 1425هـ الموافق لـ 05 أكتوبر 2006، وقد أجاز المشرع تمديد الإختصاص بإصداره لهذا الموسم الذي يعالج الأقطاب القضائية في هذه الجرائم الذي يمتد الإختصاص المحلي بها، ولقد نصت المادة 1 على تطبيق الأحكام مواد 37و40 و329 من الأمر 66-155 المتضمن ق.أ.ج.

بحيث يهدف إلى تمديد الإختصاص المحلي لبعض المحاكم وبغض وكلاء الجمهورية وقضاء التحقيق إلى دوائر اختصاص محاكم أخرى كما هو محدد في المواد 1 و2 أدناه في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عب الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وجرائم المتعلقة بالتشريع الخاص بالصرف. يتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، حيث حددت المواد 2-3-4-5 من ق.أ.ج اختصاص محاكم كما يلي:

---

[1] أنظر نص المادة 37-40 و329 من الأمر 66-156 المؤرخ في 18 صفؤ 1386هـ، الموافق لـ1966/06/08 المتضمن قانون الإجراءات الجزائية.

[2] أنظر المرسوم التنفيذي رقم 06-340، المؤرخ في 2006/10/05، المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة وقضاة التحقيق

" سيدي محمد"، قسنطينة"، "وهران"، " ورقلة" إلى محاكم أخرى، سنتطرق لها بالتفصيل فيما بعد، ومدد إختصاص وكلاء الجمهورية لهذه المحاكم الأربعة كذلك، بما فيها قضاة التحقيق وبالتالي يختص وكلاء الجمهورية لهذه المحاكم "سيدي محمد"، قسنطينة"، "وهران"، " ورقلة" بتحريك الدعوى العمومية ومباشرتها فيما يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

الفرع الثاني: من حيث الإختصاص النوعي.

ولقد تم تعديل قانون الإجراءات الجزائية بموجب القانون 06-23 الصادر في 2006/12/20 وجاء بإجراءات خص بها ضباط الشرطة القضائية وأعوانهم في مرحلة البحث والتحري تحت إشراف وكيل الجمهورية المختص.

وهذا تماشيا مع الإجراءات الخاصة بالإختصاص النوعي والمحلي لوكيل الجمهورية، أو قاضي التحقيق عندما يتعلق الأمر بالإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وذلك كما يلي:

أصبح اختصاص أعوان وضباط الشرطة القضائية يمتد إلى كامل الإقليم الوطني بموجب التعديل الأخير لقانون الإجراءات الجزائية من خلال المادة 07/16، أما فيما يخص عمليات مراقبة الأشخاص الذين يوجد ضدهم مقبول أو أكثر يحمل على اشتباه فيهم ارتكاب الاعتداءات الماسة بأنظمة المعالجة الالية للمعطيات، وكذلك مراقبة وجهة أو نقل الأشياء أو الأموال أو المتحصلات من إرتكاب هذه الإعتداءات أو التي قد تستعمل في إرتكابها، وبعد إخبار وكيل الجمهورية المختص إقليميا وإن لم يعترض، يتم تمديد الإختصاص لكافة الإقليم الوطني لضباط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية. [2] ويخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل ونسختين من إجراءات التحقيق الإبتدائي، ويرسل هذا الأخير فورا النسخة الثانية إلى

[1] أنظر المرسوم التنفيذي رقم 06-348، المؤرخ في 2006/10/05، نفس المرسوم.

[2] أنظر المرسوم التنفيذي رقم 06-348، المؤرخ في 2006/10/05 نفس المرسوم.

النائب العام لدى المجلس القضائي التابعة له المحكمة التي مدد اختصاصها، وهذا ما نصت عليه المادة 40 مكرر 1 من قانون الإجراءات الجزائية.[1]

كما يتلقى ضباط الشرطة القضائية العاملين بدائرة اختصاص المحكمة التعليمات من وكيل الجمهورية لدى هذه المحكمة عند تمديد إختصاصاصهم الوطني وفقا للمادة 40 مكرر2، أين يطالب النائب العام بالإجراءات فوؤا إذا اعتبر أن الجريمة تدخل اختصاص المحكمة المذكورة في المادة 40 مكرر، والذي يمكنه كذلك المطالبة بها في جميع مراحل الدعوى طبقا للمادة 40 مكرر3.

[1] أنظر المادة 40 من قانون الإجراءات الجزائية الجزائري.

بعد هذا العرض المتواضع لموضوع أنظمة المعالجة الآليات للمعطيات لاحظنا تشعب في موضوع و صعوبته و خصوصا ما يتعلق منه بخصوصية جرائم المعطيات من حيث الإجراءات ثم أن هذه الأخيرة من الجرائم الحديثة نسبيا التي تستلزم دراسات مستقبلية محاولة لوضع المبادئ العامة بكل ما يتعلق من جرائم ترتبط بالتطور الالكتروني والمعلوماتي ووسائل الاتصال الحديثة، وهذا ما يتطلب تدخلا تشريعيا من أجل وضع حماية قانونية متكاملة وسد جميع الثغرات قانون العقوبات والتي تعد صالحة لمواكب نظم المعلومات ولعل أبرز المشكلات التي أفرزتها هذه الجريمة تتمثل في:

-من أبرز المشكلات التي أترثها الجريمة المعلوماتية أن التحديات الإجرائية في ميدان التحري والتحقيق والمحاكمة من حيث الاختصاص والقانون الواجب التطبيق خاصة وأن الجريمة المعلوماتية كما سبق وأن وضحنا هي جريمة عالمية لا تعترف بالحدود الدولية والإقليمية.

وأنه رغم توفر النصوص القانونية الموضوعية فإن مكافحة جرائم المعلوماتية رهين بالمعيقات الإجرائية التي أفرزتها هذه الجرائم، فبالنسبة لمرحلة التحري والتحقيق فإن أول معوق يواجه حسن سيرها هو غياب القدرات التأهيلية والوسائل الفنية التي تتيح سرعة إدراك ما حصل وأن غياب التأهيل قد يؤدي إلى إتلاف الدليل على الجريمة .

فيكون الأثر هو إفلات مرتكبي هذه الجرائم من العقاب هذا إضافة إلى قصور النصوص الإجرائية التقليدية للضبط والتفتيش لتلاءم الجرائم المعلوماتية التي تتميز بسهولة إخفاء الدليل.

وإلى حين انتهاء التحقيق تبدأ مشكلات المحاكمة وأولها هو الاختصاص، المتعلق بمكان وقوع الجريمة أو بناء على معيار إلحاق الضرر. إضافة إلى القانون واجب التطبيق باعتبار أن الجريمة المعلوماتية جريمة عالمية عابرة للحدود.

لهذا يكون من الضروري الإسراع بسن قواعد إجرائية تتلاءم مع طبيعة الجريمة المعلوماتية حتى تكون القواعد الموضوعية المجرمة لها أكثر فعالية هذا من جهة، ومن جهة أخرى فإنه لا بد من تكاثف الجهود الدولية والإقليمية في حقل جرائم المعلوماتية لتخطي العقبات التي تطرحها هذه الجرائم.

بعد الاقتراحات :

-ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين من الادعاء العام (النيابة) والقضاء على كيفية التعامل مع هذا النوع من الإجرام وتحقيق التعاون مع التقنيين من أصحاب الخبرة، وذلك بعقد دورات تدريبية بشكل دررري ودائم للاستفادة من خبراتهم وإرشاداتهم ابتدءا من مرحلة الاستدلال وجمع الأدلة، و انتهاء بقرارات المحاكم.

-تدريس مواد الأنظمة المعلوماتية والجرائم التي تنشأ منها في كليات الحقوق والمعاهد القضائية.

-تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية و المخاطر المرتبة عن الاستخدام الغير الآمن لشبكة الانترنت.

-التطور المستمر للتشريعات القائمة بما يحقق مرونتها ومواكبته ا للتطورات المتسارعة في مجال تكنولوجيا المعلومات.

-ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الإلكترونية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني في حال وقوعها، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم المعلوماتية، وهذا ما يجب أن يحدث بالنسبة للجزائر وضرورة انضمامها لاتفاقية بوادبست 2001 لمكافحة الجريمة المعلوماتية.

أولا: باللغة العربية:

1 الكتب

1. أحسن بوسقيفة، الوجيز في القانون الجزائي العام، الطبعة الثالثة عشر، دار هومه، الجزائر، 2013.
2. أحمد خليفة ملط، الجرائم المعلوماتية، الطبعة 02، دار الفكر الجامعي الاسكندرية، 2006.
3. أسامة محمد لمناعسة، جرائم الحاسب الألي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، عمان 2009.
4. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الطبعة الأولى ، 2008.
5. حنان ريحان مبارك المضاحكي، الجرائم المعلوماتية ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
6. خالد ممدوح إبراهيم ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية 2009.
7. خالد داودي ، الجريمة المعلوماتية، الطبعة الأولى، دار الإعصار العلمي، عمان، 2018.
8. د/ خالد ممدوح ابراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الاسكندرية، 2008.
9. د/ محمد نجيب حسني، الموجز في شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 2003.
10. د/ نائلة قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية تطبيقية ن منشورات الحلبي الحقوقية 2005.

11. رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة في التشريع الجزائري ، دار هومه ، الطبعة الأولى 2008.

12. زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار النهضة للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011.

13. عبد الفتاح بيومي حجازي، حول صياغة النظرية العامة في علم الجريمة والمجرم المعلوماتي، منشأة الإسكندرية سعد زغلول ، مصر 2008.

14. عبد الفتاح مراد، شرح جرائم الكومبيوتر والأنترنت، دار الكتب والوثائق المصرية مصر، 2005.

15. عبد الله أوهابية، شرح قانون العقوبات الجزائري القسم العام المؤسسة الوطنية للفنون المصنعة ، الجزائر، 2011.

16. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، جامعة الإمارات، ماي 2000

17. فتحي أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، 2010.

18. قارة أمال، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة 01، دار هومه 2006.

19. محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان 2009.

20. محمد خليفة الحماية الجنائية لمعطيات الحاسب الألي، في القانون الجزائري المقارن، دار الجامعة الجديدة الأسكندرية، 2008.

21. محمد زكي أبو عامر، قانون العقوبات القسم الخاص، دار الجامعة الجديدة، الإسكندرية، 2005.

22. محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، بدون سنة.

23. محمد علي العريان، الجرائم المعلوماتية ، كلية الحقوق جامعة الاسكندرية ، دار الجامعة الجديدة للنشر، الإسكندرية، مصر 2004.

24. نائلة قورة، جرائم الحاسب الإقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة 2003.

25. نهلا عبد القادر المومني، الجرائم المعلوماتية ، الطبعة 01، دار الثقافة للنشر والتوزيع عمان الأردن، 2008، ص58.

26. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتاقية العربية لمكافحة جرائم تقنية المعلومات– قانون العقوبات– قانون الاجراءات الجزائية– قوانين خاصة– دار الجامعة الجديدة الإسكندرية 2019.

2 المجلات:

1. براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، العدد 02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2016.

2. خالد أبو الفتوح، فيروس الكومبيوتر، مقال منشور في مجلة قضايا الدولة.

3. رابح وهيبة ، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد 04، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد ابن باديس، مستغانم، 12-2014.

4. ونوغي نبيل وزيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، المجلد الرابع، العدد الثالث، الجزائر، 2009/09/01.

3 **الأطروحات:**

1. ابتسام مهوب، جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري، مذكرة لنيل شهادة ماجستر كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي ، أم البواقي ، 2014.
2. أحمد مسعود مريم، رسالة ماجستر، اليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون 09-04 قاصدي مرباح ، ورقلة، 2013/2012، ص90.
3. أمال قارة، الجريمة المعلوماتية، مذكرة لنسل شهادة ماجستر، كلية الحقوق والعلوم السياسية، بن عكنون، 2002،
4. أيمان مسعود سالم، الجريمة المعلوماتية، مذكرة لنيل شهادة ماجستر كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين ، سطيف 2016.
5. ربيعي حسن، أليات البحث والتحقيق في الجرائم المعلوماتية ، رسالة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016.
6. سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة لنيل شهادة ماجستر في العلوم القانونية، تخصص علوم جنائية كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013.
7. سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة ماجستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2014.
8. نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع منها، مذكرة لنسل شهادة ماجستر، كلية بن يوسف بن خدة جامعة الجزائر، 01، 2017.

9. يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني " دراسة تحليلية مقارنة" رسالة لنيل شهادة الماجستر في القانون العام كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

4 القوانين والمراسيم:

1. الأمر 66-156 المؤرخ في 18 صفؤ 1386هـ، الموافق لـ 1966/06/08 المتضمن قانون الإجراءات الجزائية.

2. المرسوم التنفيذي رقم 06-340، المؤرخ في 2006/10/05، المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة وقضاة التحقيق

3. قانون رقم 09-04 المؤرخ في 05 أوت 2009، جريدة رسمية عدد 47، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها الصادرة في 16 أوت 2009.

5 المداخلات:

1. تمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، ورقة علمية في إطار أعمال المؤتمر الدولي الرابع الجرائم الإلكترونية طرابلس، لبنان، 25/24 2017/03.

2. فضيلة عاقلي، الجريمة الإلكترونية واجراءات مواجهتها من خلال التشريع جامعة باتنة 01 أعمال المؤتمر الدولي الرابع عش، طرابلس، لبنان، 24-2017/03/25.

3. لورنس السعيد الحوامدة، بحث بعنوان: الجرائم المعلوماتية أركانها وألية مكافحتها، " دراسة تحليلية مقارنة" ، كلية الحقوق جامعة طيبة، المملكة العربية السعودية، 2017.

ثانيا : باللغة الأجنبية.

1. Hadjira bouder.orientatiot de la politique pénale de prevention et de lutte contre la criminalité liees au tic en amlgerie.centre de recherche sur l'information scentifique et tchnique cerist03 , www.alexalaw.com ,01/05/2022,22h.43.
2. Vivant ; informatique et droit penal, les biens informatiques objets d'une fraude lamy informatique 1991.p1511.N°3443.

شكر

إهداء

مقدمة.....01

الفصل الأول: الجريمة المعلوماتية..... 06

المبحث الأول: الإطار ألمفاهيمي للنظام المعلوماتي والجريمة المعلوماتية 07

المطلب الأول: تعريف التشريعي الفقهي للنظام المعلوماتي.....07

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية.....07

الفرع الثاني: التعريف التشريعي للجريمة المعلوماتية.....10

المطلب الثاني: خصائص الجريمة المعلوماتية والجرم المعلوماتي.....12

الفرع الأول: خصائص الجريمة المعلوماتية.....12

الفرع الثاني: خصائص المجرم المعلوماتي.....13

المبحث الثاني:أركان وصور للجريمة المعلوماتية 20

المطلب الأول: أركان الجريمة المعلوماتية.....20

الفرع الأول: الركن الشرعي.....20

الفرع الثاني: الركن المادي.....21

الفرع الثالث: الركن المعنوي.....26

المطلب الثاني: صور الجريمة المعلوماتية.....27

الفرع الأول: الجرائم الواقعة على الكومبيوتر.....27

الفرع الثاني: الجرائم الواقعة على الأشخاص.....29

الفرع الثالث: الجرائم الواقعة على الأموال.....30

الفرع الرابع: الجرائم الواقعة على أمن الدولة.....31

الفصل الثاني: الجرائم الماسة بالنظم..... 33

المبحث الأول: أركان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجزاءات المقررة..... 33

المبحث الأول: أركان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....33

المطلب الأول: جريمة الدخول واللقاء غير المشروع في نظام المعالجة الآلية للمعطيات..... 33
الفرع الأول: الركن المادي لجريمتي الدخول أو البقاء غير المصرح بهما.....34
الفرع الثاني: الركن المعنوي لجريمتي الدخول والبقاء غير المصرح بهما.....40
المطلب الثاني: جريمة التلاعب بمعطيات الحاسب الألي..... 41
الفرع الأول: الركن المادي لجريمة التلاعب بمعطيات الحاسب الآلي.....42
الفرع الثاني: الركن المعنوي لجريمة التلاعب بالمعطيات..... 44
المبحث الثاني: الجزاءات والعقوبات المقررة لجرائم الإعتداءات الماسة بالأنظمة المعلوماتية..... 45
المطلب الأول: العقوبات المطبقة على الشخص الطبيعي..... 45
الفرع الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات..... 45
الفرع الثاني: العقوبات التكميلية..... 45
الفرع الثالث: الظروف المشددة..... 45
المطلب الثاني: العقوبات المطبقة على الشخص المعنوي..... 45
المبحث الثالث: خصوصية جرائم المعطيات من حيث الإجرام 51
المطلب الأول: خصوصية جرائم المعطيات من حيث إجراءات المتابعة والتحقيق.... 52
الفرع الثاني :خصوصيتها من التحقيق 55
المطلب الثاني: خصوصيتها من حيث المحاكمة..... 60
الفرع الأول: من حيث الإختصاص المحلي 62
الفرع الثاني: من حيث الإختصاص النوعي..... 63
الخاتمة..... 67
قائمة المراجع..... 73

مـلخص مذكرة

إن الأنترنت أكبر بوابة علمية تم إكتشافها حتى الآن، من خلاله يستطيع الفرد أن يقوم بالكثير من الأعمال والتصرفات التي كانت تحتاج سابقا إلى مجهود بدني، ولكن كلما ظهرت سبل التسيير على الأفراد من خلال إستعمال الأنترنت، ظهر من يفسد سهولة إستخدام هذه التقنية في أمن وأمان، وهذا ما يضعنا أمام أمرين، ظهور جرائم معلوماتية جديدة من جهة، وقيام ثورة تقنية لمكافحة هذه الجرائم من جهة أخرى.

الكلمات المفتاحية :1-الانترانت 2- الجريمة المعلوماتية-3الافراد4-الآليات5-الانترنات6-التسير

Note Summary

The Internet is the largest scientific portal that has been discovered so far, through which the individual can do a lot of actions and behaviors that previously required physical effort, but the more ways to manage individuals appear through the use of the Internet, the more it appears that spoils the ease of using this technology in safety and security And this puts us in front of two things: the emergence of new information crimes on the one hand, and the emergence of a technical revolution to combat these crimes on the other hand

Keywords: 1- Intranet 2- Information Crime 3- Individuals 4- Mechanisms 5- The Internet 6- Facilitation