الجمهورية الجزائريــة الديمقـراطية الشعبيــة

وزارة التعليم العالي و البحث العلمي

جامعة د. الطاهر مولاي – سعيدة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

جريمة الغش المعلوماتي في التشريع الجزائري

" الجوانب الموضوعية والقواعد الإجرائية "

مذكرة لنيل شهادة الماستر

التخصص: القانون الجنائي والعلوم الجنائية .

من إعداد الطالبة : **تحت إشراف الأستاذة:**

عليوان نادية . **مولاي ملياني دلال .**

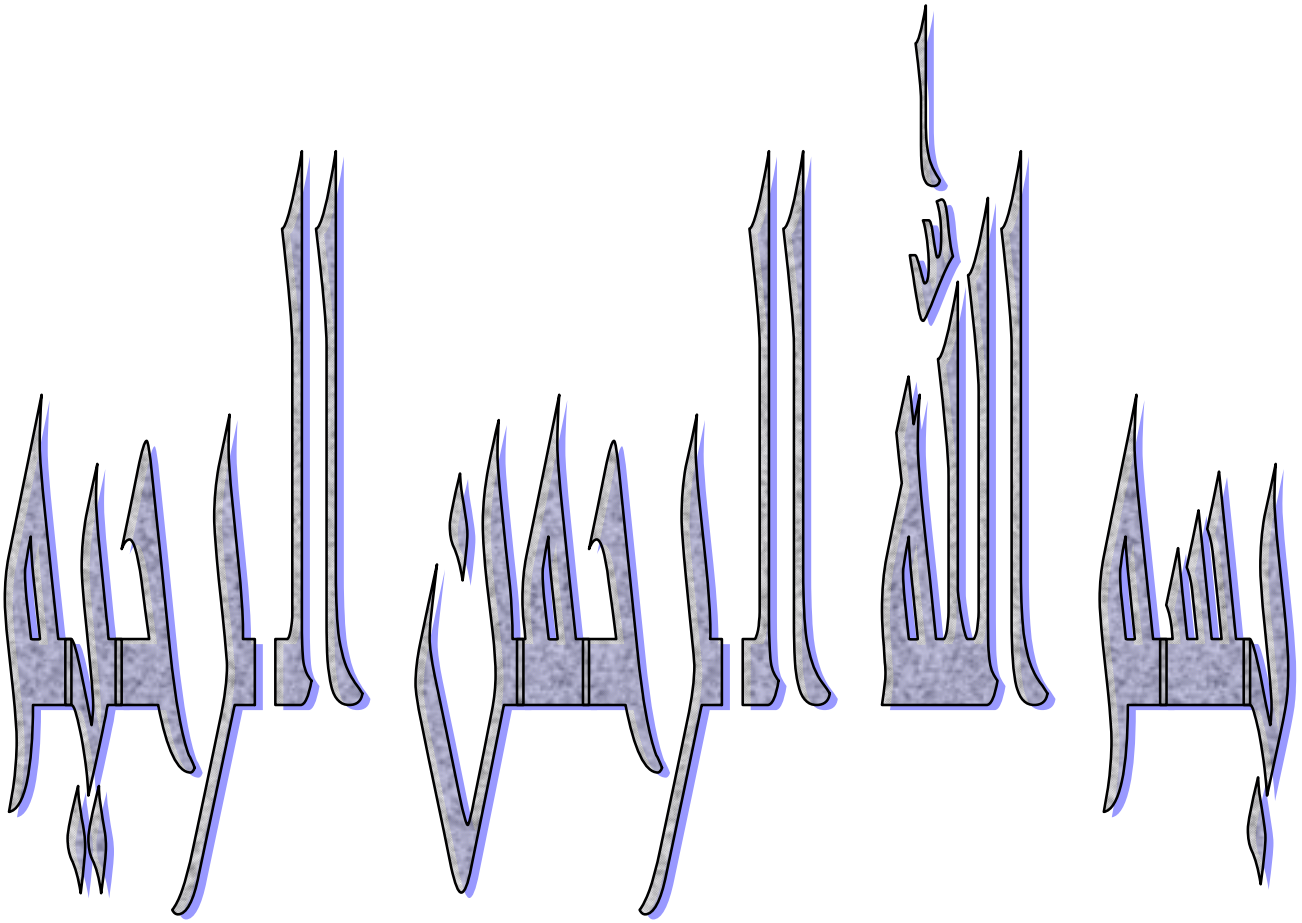
لجنة المناقشة

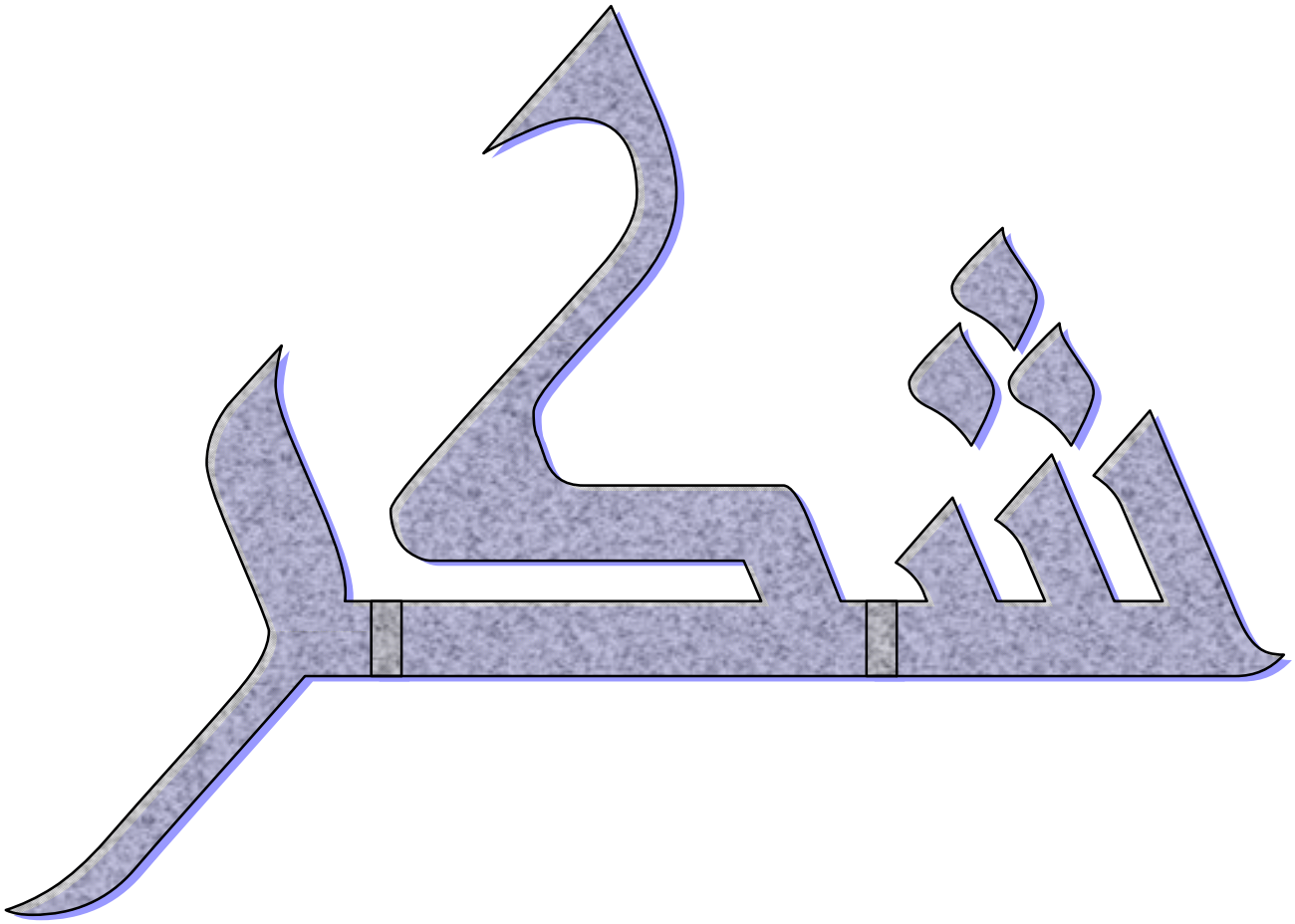
الأستاذة : مراح نعيمة ..... رئيسا .

الأستاذة : مولاي ملياني دلال ..... مشرفا ومقررا .

الأستاذة : سويلم فضيلة ..... عضوا مناقشا .

السنة الجامعية 2015/2014


بسم الله الرحمن الرحيم


شکر

كلمة شكر وتقدير

اللّهم إني أعوذ بك من علم لا ينفع وقلب لا يخشع ودعاء لا يسمع ، اللّهم صلي وسلّم على سيّدنا محمد رحمتك المهداة للعالمين ، خاتم رسلك نبيك وحبيبك وعلى آله وصحبه ، ومن دعى بدعواته وإهتدى بسنته إلى يوم الدين وبعد :

- أبدأ بشكر من هو أهل لكل شكر وثناء ، من بنعمته تتم الصالحات ، من خلقنا وهدانا وأنعم علينا بنعمة العقل وأنار دربنا بالعلم ، خالقنا وحبيبنا الله سبحانه وتعالى .
- كما أتقدم بالشكر الجزيل إلى اللجنة الموقرة التي قبلت مناقشة هذا العمل المتواضع .
- وإلى كل أساتذة جامعة الدكتور مولاي الطاهر ، وعلى رأسهم من كان لها الفضل في إنجاز هذه المذكرة الأستاذة الموقرة مولاي ملياني دلال ، التي أسأل الله أن يعينها في مسارها المهني ، ويوفقها في إنجاز رسالة الدكتوراه .
- إلى جميع عمّال المكتبة خاصة سمية هرباحي والأخ ناصر .
- إلى كل من غرس بذرة العلم في ذاتي من بداية مشواري الدراسي إلى يومنا هذا .

إلى كل من ساهم من قريب أو بعيد في إنجاز هذه المذكرة ، وأسأل الله التوفيق لكل من يحمل شعلة العلم .

إهداء

إهداء

أهدي هذا العمل المتواضع إلى :

الوالدين الكريمين أطال الله في عمّرهما .

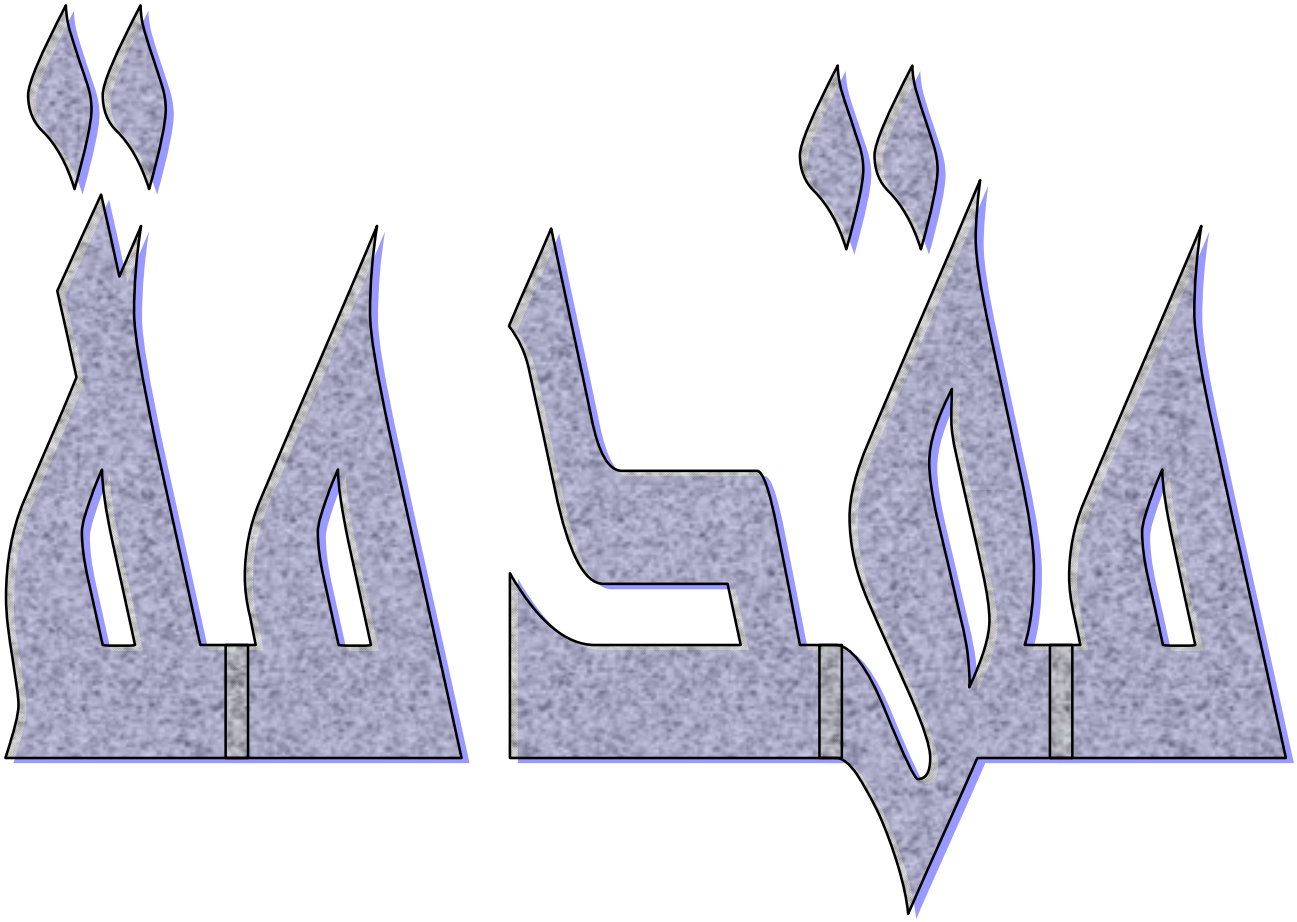
إخوتي وأخواتي .

إلى الكتكوتة ملاك .

إلى صديقاتي قادة حورية ، طرطار مريم .

إلى جميع عمّال متوسطة جلولي الجيلالي وأخص بالذكر من أحمل لهما الكثير من المحبة والإحترام والتقدير السيدين بودية عمر ، مرابط علي .

كما أهدي هذا العمل المتواضع إلى الأخ أبو مصبح أحمد وعائلته الكريمة وإلى كافة الشعب الفلسطيني .


مقدمة

إن كل من الفكر القانوني والإجتهاد الفقهي يعيش حاليا مرحلة إنتقالية ، إتجاه ظاهرة إجرامية عالمية حديثة حيث عرف العالم مند منتصف القرن العشرين ثورة جديدة أصطلح على تسميتها بالثورة المعلوماتية ، حيث كان للتطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والإتصالات والإندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه الثورة المعلوماتية ، إذ يعد الحاسب الآلي والأنترنت ؛ حجر الزاوية في مجال التقّنية الحديثة التي هدفت لخدمة البشرية في مجالّات عدّة ، وتركت آثارا إيجابية وشكلت قفزة نوعية في حياة الأفراد والدول ، حيث تعتمد القطاعات المختلفة في الوقت الحاضر على إستخدام الأنظمة المعلوماتية نظرا لمّا تتميز به من عنصري السرعة والدّقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها بين الأفراد والجهات .

فمنذ أول ظهور للأنترنت [1] ،كان لها أثر كبير في إنتقال المعلومات وتداولها والإستفادة منها في وقت قياسي في أي مكان ، غير أن الجانب الإيجابي لعصر المعلوماتية وبالرغم من المزايا التي تحققت وتتحقق كل يوم بفضل ثورة تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة ، فإن هذه الثورة التقنية المتنامية صاحبتها في المقابل جملة من الإنعكاسات السلبية الخطيرة جراء سوء إستخدام هذه التقنية المتطورة والإنحراف عن الأغراض المتّوخاة منها [2] ، تّبدت في تفشي طائفة من الجرائم المستحدثة أصطلح على تسميتها بالجرائم المعلوماتية التي تعتبر جريمة الغش المعلوماتي إحدى أنواعها.

فظهور هذا النوع من الجرائم كان عاملا حاسما لتدّخل المشرع الجزائي في مختلف العديد من الدول بوضع نصوص لإكساء الأفعال الإجرامية المّاسّة بنظم المعالجة الآلية الصّبغة التجريمية ، كون هذا الشكل من الجرائم أصبح يثير العديد من المشاكل والصعوبات التي تواجه متابعتها وضبط مرتكبيها إذ أصبحت النصوص القانونية التقليدية في شقيها الموضوعي والإجرائي لا تفي بمواجهتها ولا تتناسب مع التّكييف القانوني لها [3] .

وبما أن دولة الجزائر ليست بمنأى عن هذا التّحول المعلوماتي ، فهي وإن لم تبلغ مصاف الدول المتّقدمة ، فإنها قد تأثرت بهذه الثورة المعلوماتية سلبا وإيجابا فلقد تأثرت بما جرّته هذه الثورة من ألوان جديدة لم تشهدها البشرية من قبل وإرتبطت إرتباطا وثيقا بالحاسب الآلي ، لذلك نجد أن المشرع الجزائري قد واكب هذا التطور ، وأصدر نصوص قانونية جديدة ، إذ بادر إلى تعديل قانون العقوبات ، وإستحدث جريمة الغش المعلوماتي ضمن الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات ، ولم يقتصر على هذا التعديل فقط،بل عدّل قانون الإجراءات الجزائية وأصدر قانونا مستقلا يتلاءم وطبيعة هذا النوع من الإجرام الحديث .

وعليه فإن هذه الدراسة المتواضعة ستعني بتسليط الضوء على جريمة الغش المعلوماتي ، بإعتبارها جريمة خاصة ، فهذا السبب يعتبر من بين الأسباب التي دفعت بنا

---

(1) : أنظر الملحق رقم 01 .

(2) : رشيدة بوكر ، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن ، الطبعة الأولى ، منشورات حلبي الحقوقية ، لبنان ، 2012 ، ص. 14 .

(3) : فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني ، رسالة دكتوراه ، قسم الحقوق ، جامعة الجزائر 01 ، 2009 – 2010 ، ص. 03 .

إلى الوقوف على هذا النوع من الجرائم وذلك لبيان ماهيتها ، ومن الأسباب أيضا محاولة معرفة مدى كفاية الحماية القانونية التي أتى بها المشرع الجزائري لمواجهة الإنتهاكات الواقعة بواسطة الحاسب الآلي .

هذا وتبدو أهمية هذا البحث في بيان الإطار القانوني لجريمة الغش المعلوماتي خاصة إذا كان المشرع الوطني قد تطرّق لها في إطار ما يسمى بالجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات ، أما بخصوص الهدف الذي ترمي له هذه الدراسة فهو بيان الجانب الموضوعي وكذا أهم الجوانب الإجرائية لجريمة الغش المعلوماتي ، وذلك من خلال الإجابة عن الإشكالية التالية :

كيف عالج المشرع الجزائري جريمة الغش المعلوماتي من الناحية الموضوعية وما هي أهم الإجراءات الكفيلة بمواجهتها ؟

وقد إعتمدت في هذه المذكرة على المنهج التحليلي ، وذلك من خلال تحليل المواد القانونية ذات العلاقة بموضوع الغش المعلوماتي ، بالإضافة إلى المنهج الوصفي عند بيان مفهوم هذه الجريمة وخصائصها وسّماتها ، أما المنهج المقارن فقد تّم توظيفه عند مقارنة النص الوطني بنظيره الأجنبي خاصة الفرنسي والمصري الذي له علاقة بالموضوع محل الدراسة .

ومن الصعوبات التي إعترضت سبيل إعداد هذه المذكرة ندرة المراجع المتخصصة ذات المصدر الجزائري ، التي وإن وجدّت فهي لا تتناول الغش المعلوماتي بشكل مباشر، إلى جانب الصّعوبة التي تعلقت بالمصطلحات الفنية ذات العلاقة بالمدلول القانوني في جريمة الغش المعلوماتي .

هذا وسيتم التطرق لموضوع الغش المعلوماتي تحديداً في إطار قانون العقوبات بشقيه الموضوعي والإجرائي حيث أنه ومن خلال الفصل الأول ، نبين الجوانب الموضوعية لهذه الجريمة ، بتحديد أركانها وبيان سّماتها وخصائص مرتكبيها ، ثم التطرق للمسؤولية الجزائية عن الغش المعلوماتي .

أما الفصل الثاني فنتطرق من خلاله إلى أهم القواعد الإجرائية الكفيلة بمواجهة جريمة الغش المعلوماتي ، وذلك من خلال قواعد قانون الإجرائية الجزائية التي إستحدثها المشرع وكذا القواعد القانونية المتعلقة بتكنولوجيات الإعلام والإتصال .

الفصل الأول

الجوانب المرضوعية

لجريمة الغش المعلوماتي

إن دراسة جريمة الغش المعلوماتي من الناحية الموضوعية تعد من الموضوعات البالغة التعقيد ، وذلك لإرتباطها بالحاسب الآلي وإستخدامه إلى جانب تعدد صّور هذه الجريمة مما جعل التداخل حاصل بين صورها خاصة في ركنها المادي ، كما أن هذه الجريمة مثلها مثل باقي الجرائم يتطلب القانون لقيامها الركن المعنوي فيها ؛ هذا ويذهب الفقه إلى القول بأن مرتكب جريمة الغش المعلوماتي هو شخص يتميز بصفات وسّمات خاصة ، على أنه مهما كانت هذه الصفات والسّمات فإنه يسأل جنائيا

متى توافرت أركان الجريمة وثبت بالأدلة بأنه الفاعل لها ، وعليه سنحاول معالجة هذه الأفكار بمزيد من التفصيل في المبحثين التاليين ؛ المبحث الأول نتطرق فيه لأركان جريمة الغش المعلوماتي أما المبحث الثاني فنخصصه للمسؤولية الجنائية في جريمة الغش المعلوماتي .

المبحث الأول : أركان جريمة الغش المعلوماتي

لبيان أركان هذه الجريمة وجب الإعتماد على تعريفها الفقهي وتنظيمها القانوني ، فمن الناحية الفقهية وجدت عدّة تعاريف فقد عرفها البعض على أنها حث الحاسب الآلي على تغيير بعض الحقائق بأي وسيلة كانت بهدف الحصول على ربح غير مشروع على حساب شخص آخر ، فوظيفة الحاسب الآلي من خلال هذا التعريف تكمن في مساعدة الجاني على إتمام فعل الإحتيال ، في حين عرفها آخرون على أنها الإستعمال الغير مصرح به لنظام الحاسب الآلي بنّية الحصول على ممتلكات أو خدمات عن طريق الإحتيال [1] .

أما من الناحية القانونية فقد تناولت التشريعات الوطنية والدولية جريمة الغش المعلوماتي ، فمن الناحية الدولية نجد إتفاقية بودابست لمكافحة الإجرام المعلوماتي المؤرخة في 23 نوفمبر 2001 قد نصت على جريمة الغش المعلوماتي في إطار نص المادة الثامنة منها [2] ، أما بالنسبة للتشريعات الوطنية نجد أن المشرع الجزائري قد نص عليها على إثر تعديل قانون العقوبات بموجب القانون رقم 04 – 15 وذلك في إطار المواد 394 مكرر- 394 مكرر 1 [3] ، وللإشارة فإن هذه المواد تقابلها المادة 323 – 1 – 3 من ق ع ف [4] ، فهذه النصوص القانونية الوطنية والدولية تمثل الركن الشرعي لجريمة الغش المعلوماتي كون كل فعل أو إمتناع لا يجرم ولا يعاقب عليه إلا بوجود نص قانوني وإلا أعتبر ما يخالف ذلك إخلالا بمبدأ الشرعية الجنائية .

---

(1) : نائلة محمد فريدة ، جرائم الحاسب الآلي الاقتصادية ، دراسة نظرية وتطبيقية ، بدون طبعة ، منشورات حلبي الحقوقية ، مصر ، بدون سنة نشر ، ص. 425 .

(2) : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

(3) : المادتين 394 مكررو 394 مكرر01 من القانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الآمر رقم 66 – 156 المؤرخ في 08 جويلية 1966 ، المتضمن قانون العقوبات ، ج ر: العدد 71 الصادرة في 10 نوفمبر 2004 ، ص. 11 ، 12 .

(4) : http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719

بناءً على ما سبق نتطرق لدراسة الركن المادي لجريمة الغش المعلوماتي في المطلب الأول ، والركن المعنوي في المطلب الثاني ، أما تفصيل أهم خصائص جريمة الغش المعلوماتي فسيكون من خلال المطلب الثالث .

المطلب الأول : الركن المادي لجريمة الغش المعلوماتي

لا يعاقب قانون العقوبات على الأفكار والنوايا رغم قباحتها ولا على النوايا السيئة ما لم تظهر إلى الوجود الخارجي بفعل أو عمل ، ويشكل الفعل أو العمل الخارجي الذي يعبر عن النية الجنائية أو خطأ الجزائي ما يسمى بالركن المادي للجريمة [1] ، ويتمثل هذا الأخير في جريمة الغش المعلوماتي وبإستقراء نص المادة 394 مكرر من القانون رقم 04 – 15 السالف الذكر في فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ، علما أن المشرع قد ضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، وكذلك في حالة تخريب نظام إشتغال المنظومة ، وما ورد في إطار نص هذه المادة يصطلح عليه بتسمية الدخول في المنظومة المعلوماتية.

هذا ويتجسد الركن المادي في جريمة الغش المعلوماتي من خلال نص المادة 394 مكرر01 من القانون رقم 04 – 15 السالف الذكر في عملية إدخال وبطريقة الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريقة الغش المعطيات التي يتضمنها ، ومضمون هذه المادة يصطلح عليه بتسمية المساس بالمنظومة المعلوماتية ، من خلال هذا العرض نستنتج أن جملة الأفعال المادية الواردة في إطار نص هاتين المادتين تشكل صور الغش المعلوماتي وهي صورة الدخول في المنظومة المعلوماتية ، وصورة المساس بالمنظومة المعلوماتية ، هذا ومن خلال دراسة الركن المادي للغش المعلوماتي لا بد من توضيح مسألة إن كانت هذه الجريمة وقتية أم مستمرة ، وكيفية حدوث الشروع فيها ، وعليه سنحاول من خلال الفرع الأول التطرق لصّور الغش المعلوماتي والفرع الثاني سيتم فيه معالجة الإحتيال المعلوماتي في ضوء تقسيم الجرائم المستند إلى إعتبارات متصلة بالركن المادي ، ويتم تخصيص الفرع الثالث للشروع في جريمة الغش المعلوماتي .

(1) - أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة التاسعة ، دار الهومة للطباعة والنشر والتوزيع ، الجزائر ، 2009 ، ص.97 .

الفرع الأول : صّور الغش المعلوماتي

يأخذ الغش المعلوماتي كما سبق القول في ق ع ج صورتين أساسيتين هما : الدخول في المنظومة المعلوماتية ، والمساس بالمنظومة المعلوماتية [1] ، فبالنسبة للصورة الأولى والتي يصطلح عليها أيضا بجريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات المنصوص عليها في المادة 394 مكرر من القانون رقم 04 – 15 السالف الذكر والتي تقابلها المادة 323 – 1 من ق ع ف ، تعتبر من أهم صّور الغش المعلوماتي عموما ذلك أن أغلب جرائم المعطيات لا يمكن إرتكابها إلا بعد الدخول للنظام ولهذا كانت جريمة الدخول هي الحد الفاصل بين الجاني وبين إرتكابه لمختلف جرائم المعطيات الأخرى لذلك أولت لها التشريعات إهتماما كبيرا وهناك من التشريعات من يجعلها الجريمة الأساسية وما باقي الجرائم إلا نتائج لها ، وقد حرص المشرع الجزائري على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات ، فجرم الدخول غير المصرح به ، كما جرم البقاء فيها بغير تصريح وهو الذي قد يحصل بعد دخول مشروع ، وهذا التجريم يشمل الدخول وكذا البقاء في كل أو جزء من النظام وبصرف النظر عن الغاية التي يرنو إليها الجاني من خلال إرتكابه للجريمة ، وكذلك بصرف النظر عما إذا كان النظام محميا ببرنامج الأمان أم لا ، فالمشرع إذا أراد أن يقفل الباب أمام كل وجود غير مصرح به داخل النظام دخولا أو بقاءً ، في كل أو جزء من النظام بقصد خاص أم بدونه وسواء كان محمي فنيا أم غير محمي ، وتتحقق هذه الجريمة سواء أدّى هذا التواجد إلى نتائج معينة أم لم يؤد [2] .

أما بالنسبة للصورة الثانية من صّور الغش المعلوماتي ، التي وردت في إطار نص المادة 394 مكرر 01 ، التي يقابلها من التشريع الفرنسي نص المادة 323 – 03 من ق ع ف ، فإنه يصطلح عليها كذلك بجريمة التلاعب بالمعطيات ، وهي الجريمة الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول والبقاء غير المصرح بهما أما قانون العقوبات الفرنسي فينص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات والمشرع الجزائري لم ينص على هذه الأخيرة نظرا للتشابه الكبير بينها وبين جريمة التلاعب بالمعطيات ، بحيث يصعب في الكثير من الأحيان التمييز بينهما وبالرجوع لنص المادة 394 مكرر 1 التي ورد فيها " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500 ألف إلى مليونين كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها " ، فالملاحظ على هذا النص أنه جاء شاملا لكل أنواع المعطيات ولم يشترط شروطا معينة فيها كأن تكون من طبيعة ما أو تكون تابعة لجهة معينة ، كما أنه جاء شاملا لكل وسائل التلاعب بالمعطيات ولم تقتصر على وسيلة معينة

(1) : أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول ، الطبعة الرابعة عشر ، دار الهومة ، الجزائر ، 2012 ، ص. 453 .

(2) : محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن ، بدون طبعة ، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص. 63 .

وبالتالي يدخل في نطاق هذه المادة إستخدام البرامج الخبيثة مهما كانت وسيلة إدخالها إلى الحاسب ، كما أنه لا يشترط لقيام هذه الجريمة أن يكون التلاعب قد تّم بعد عملية الدخول غير مشروع إلى نظام الحاسب الآلي ، إذ يستوي أن يكون الدخول مشروعا أو غير مشروع [1] .

بناءً على ما سبق وإنطلاقا من أهمية هاتين الصورتين من صور الغش المعلوماتي نتناول فيما يلي بالتفصيل الدخول في المنظومة المعلوماتية والمساس بها ، وقبل ذلك نشير إلى أن المشرع الجزائري قد عرف المنظومة المعلوماتية في إطار نص المادة 02 الفقرة ب من القانون 09 – 04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بالقول أنها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين " [2] .

البند الأول : الدخول في المنظومة المعلوماتية

لقد ثار جدل بين الفقهاء بين مؤيد ومعارض لتجريم الدخول الغير المشروع إلى أنظمة الحاسب الآلي حيث ذهب أنصار الإتجاه الأول وهو المعارض لفكرة التجريم إلى أنه لا يوجد ما يدعو لتجريم هذا الفعل نظرا لعدم وجود حاجة ملحة تستدعي ذلك ، حيث لم تبين الدراسات والإحصائيات المختلفة هذه الضرورة ، بالإضافة إلى أن إرتكاب هذا الفعل دون أن يكون لدى صاحبه نية إرتكاب جريمة كالإعتداء على البيانات والمعلومات التي في النظام لا يعدو أن يكون مجرد إستعراض لبعض الملكات الذهنية والفنية ، إلى جانب أن حالات الدخول الغير المشروع والذي لا يترتب عليه إتلاف للمعلومات والبيانات لا يمكن الكشف عنها من حيث أنه لا دليل على إرتكابها بالإضافة إلى الصعوبات الفنية التي قد تصادف الجهات المختصة بالتحقيق لإثبات التهمة على الجاني [3] ، أما الإتجاه الثاني فهو يذهب إلى ضرورة تجريم فعل الدخول لما له من آثار سلبية ومخاطر عديدة سواء على الأنظمة ذاتها أو على المعطيات المخزنة بداخلها والخسائر المادية التي تترتب على فعل الدخول ذاته أو التي تترتب على محاولة وقفه [4] .

ومن التشريعات المقارنة التي أخذت بهذا الإتجاه نجد من الغربية التشريع الفرنسي في نص المادة 323 – 1 من ق ع ف ، والمادة الأولى من قانون إساءة إستخدام الحاسبات الآلية

---

(1) : محمد خليفة ، المرجع السابق ، ص. 177 ، 178 .

(2) : المادة 02 من القانون رقم 09 – 04 المؤرخ في 5 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، ج ر : العدد 47 الصادرة في 16 أوت 2009 ، ص. 05 .

(3) : حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الأنترنت ، دراسة مقارنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، 2009 ، ص. 346 .

(4) : نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، الأردن ، 2008 ، ص. 157 .

والمادة 1030 (A) من القانون الفيدرالي الأمريكي ، ومن التشريعات العربية نجد التشريع الجزائري في نص المادة 394 مكرر كما سبقت الإشارة والمادة 276 من ق ع العمّاني والمادة 371 من ق ع القطري [1] .

وعليه وإنطلاقا من قاعدة أنه " لا جريمة بغير سلوك " نجد أن جريمة الدخول والبقاء الغير المصرح بهما ، تتحقق بوجود نوعين من السلوك أولها سلوك إيجابي وهو الذي يتمثل في فعل الدخول ، وثانيهما سلوك سلبي أو ما يصطلح عليه بالإمتناع وهو الذي يتمثل في البقاء فالسلوك الإيجابي عبارة عن حركة إرادية من شأنها أن تحدث تغيير في العالم الخارجي، وهذا التغيير يكون ملموسا في العالم المعلوماتي بالنسبة لجريمة الدخول ، أما السلوك السلبي أو الإمتناع فهو إحجام الشخص إراديا عن إتخاذ سلوك إيجابي كان يتعين إتخاذه وهو يتمثل في هذه الصورة من صور الغش المعلوماتي – الدخول في المنظومة المعلوماتية – في الإمتناع عن الخروج من النظام والبقاء فيه في الوقت الذي كان يجب فيه مغادرة النظام [2] ، وعليه سيتم فيما يلي التطرق للسلوك الإجرامي بالنسبة لصورة الدخول في المنظومة المعلوماتية كما يلي :

أولا : تعريف الدخول وطبيعته

يقصد بالدخول في المنظومة المعلوماتية الإتصال بنظام الكمبيوتر بأي طريقة كانت حيث يمكن تصور الدخول في النظام ، بأن يقوم المستخدم بالدخول في النظام دون أن يكون مسموحا له بذلك ، وسواء قام في ذلك المتداخل بعمل توصيله مع النظام أو تدخل إليه عن طريق شبكة الأنترنت [3] ، ومن التعريفات أيضا " الولوج غير المشروع لنظام المعالجة الآلية أو مجموعة نظم عن طريق إنتهاك الإجراءات الأمنية [4] ، وبهذا يكون فعل الدخول الذي يشكل الركن المادي في جريمة الغش المعلوماتي لا يقصد به الدخول إلى المكان الذي يتواجد به الحاسوب ونظامه ، بل يقصد به الدخول بإستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي [5] ، ومن هنا إعتبر الفقه أن الدخول إلى النظام المعلوماتي يمكن أن يتشابه مع الدخول في ذاكرة الإنسان ، حيث يعتبر هذا الفقه أن الدخول إلى النظام المعلوماتي يمكن أن يشتمل على جميع صور التعدي المباشرة أو غير المباشرة إلا أن هذا الدخول يكون غير مباشر أكثر منه مباشر لأنه ليس دخول إلى مكان في العالم المادي وإنما هو دخول في القدرة على تحقيق عمليات ذهنية وفكرية ، هذا ما يجعله غير مباشر ، فالدخول

(1) : حسين بن سعيد الغافري ، المرجع السابق ، ص. 347 .

(2) : محمد خليفة ، المرجع السابق ، ص. 138 .

(3) : شيماء عبد الغني محمد عطا الله ، الحماية الجنائية للتعاملات الإلكترونية ، بدون طبعة ، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص. 99 .

(4) : زينات طلعت شحادة ، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية ، بدون طبعة ، المنشورات الحقوقية صادر ، لبنان ، بدون سنة نشر ، ص. 43 .

(5) : نهلا عبد القادر المومني ، المرجع السابق ، ص. 158 .

إذا له طبيعة معنوية وليست مادية ، ذلك أن المعايير التي تحكم العالم المادي لا يمكن تطبيقها على العالم الإفتراضي [1] .

هذا وتجدر الإشارة إلى أن أغلب تشريعات الأنترنت والحاسب الآلي ، لم تتعرض لمفهوم الدخول ومنها التشريع الجزائري الذي لم يقدم تعريف للدخول إذ نص على هذه الكلمة مجردة دون إعطاء معنى لها ، هذا ولا يشترط في الدخول أن يتم بطريقة معينة فالمادة 394 مكرر جاءت شاملة لكل طرق الدخول ولم تحدد طريقة بعينها ، وعليه فالدخول يتحقق بكل وسيلة تصلح لذلك سواء كانت عن طريق كلمة السّر أو شفرة أو برنامج بمعنى أن جريمة الدخول غير محددة الوسيلة [2] .

وللإشارة فإن تشريعات الدول قد إختلفت في تحديد محل الدخول غير المصرح به وهي لا تخرج عن ثلاث إتجاهات :

1- **الإتجاه الأول :** وهو الذي يجمع بين المعلومات وأنظمة الكمبيوتر وشبكات المعلومات ويعتبر القانون الفرنسي مثالا يحتذى به في هذا الإتجاه .

2- **الإتجاه الثاني :** وهو الذي يستبعد شبكات المعلومات من نطاق التجريم ، ويعتبر القانون الإنجليزي بشأن إساءة إستخدام الكمبيوتر لسنة 1995 من أبرز الأمثلة على هذا الإتجاه ، حيث تعاقب المادة الأولى منه على الدخول الغير المصرح به إلى البرامج والمعلومات التي يحتوي عليها أي كمبيوتر .

3- **الإتجاه الثالث :** يجرم الدخول غير المصرح به إلى أنظمة الكمبيوتر عبر شبكات المعلومات فوفق القانون السويسري تّم إدراج جريمة جديدة تضمنتها المادة 143 مكرر من قانون العقوبات تعاقب على الدخول الغير المشروع إلى أنظمة الكمبيوتر بواسطة جهاز لنقل المعلومات [3] .

هذا وبالنسبة لموقف المشرع الجزائري فقد تبنى الرأي الأول الذي يجرم الدخول الغير المصرح به إلى أنظمة الكمبيوتر والمعلومات وشبكات المعلومات ، وهذا ما يتجلى من خلال النصوص القانونية الواردة في إطار الغش المعلوماتي – 394 مكرر – 394 مكرر 1 – التي عاقبت على هذا الفعل إذا إستهدف منظومة للمعالجة الآلية للمعطيات ، وبالرجوع لمصطلح

(1) و(3) : محمد خليفة ، المرجع السابق ، ص. 139 – 141 .

(3) : خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، بدون طبعة ، الدار الجامعية ، الإسكندرية ، 2008 ، ص. 88 .

المعطيات المعلوماتية نجد أن المشرع قد عرفها من خلال نص المادة الثانية الفقرة جـ من القانون 04 – 09 السالف الذكر بقوله " أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية،بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ".

كما أثير تساؤل بشأن وجوب أن يكون النظام محميا ضد الإعتداءات عليه بأجهزة أو وسائل أمنية وبهذا الخصوص إختلف الفقه في الإجابة عن هذا السؤال بين من يرى ضرورة قصر الحماية الجزائية على تلك الأنظمة التي وفر لها أصحابها حماية فنية ، ويستند هذا الرأي في تبرير موقفه إلى القول بأن إقامة الدليل على قيام الركن المادي للجريمة والتحقق من توافر القصد الجنائي لدى فاعلها يتطلب وجود أنظمة الأمان [1] ، أما الرأي الثاني وهو موقف الفقه الفرنسي فقد ذهب إلى عدم إشتراط وجود نظام حماية لنظم المعالجة الآلية مدعما موقفه بالقول بأن سكوت القانون يدل على عدم إشتراطه لهذا الأمر ، ومن المعروف أن المبادئ العامة في تفسير القانون الجنائي تقتضي عدم إضافة شرط لم ينص عليه القانون [2] ، كما أن المشرع الجزائري في نص المادة الثانية من القانون 09 – 04 السالف الذكر لم يشترط في الفقرة ب المتضمنة تعريف المنظومة المعلوماتية أن تكون هذه المنظومة محاطة بحماية فنية حتى يتم تجريم الإعتداء عليها [3] .

ومن بين الخلافات الفقهية التي ثارت بشأن جريمة الدخول غير المصرح به إلى جانب الخلافات التي سبقت الإشارة إليها ، أثير تساؤل بصدد هذه الجريمة في غاية الأهمية يتمثل فيما يلي : من يصرح بالدخول ، وماذا عن حالات عدم التصريح ؟

من يصرح بالدخول

لا تقوم جريمة الدخول إلا إذا كانت بدون تصريح وبالتالي وجب أن نعلم المسؤول عن إعطاء هذا التصريح لأن تحديد الشخص أو الهيئة التي تصرح بالدخول أمر بالغ الأهمية ، إذ تتوقف الجريمة على إرادة ذلك الشخص أو تلك الهيئة ، ويسمي الفقه الفرنسي هذا الشخص بصاحب السلطة أو السيطرة على النظام ، وقد عرفته المادة الثانية الإتفاقية الخاصة بحماية الأفراد في مواجهة نظام المعالجة الآلية للمعلومات ذات الطابع الشخصي " بأنه كل شخص طبيعي أو معنوي ، أو كل سلطة عامة أو كل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونة أو محتواه وكيفية تنظيمه والهدف منه " .

فإذا كان الأصل أنه لا يكون للنظام أكثر من مسؤول له سلطة التصرف فيه ، فإن التساؤل يثار حول إمكانية أن يكون للنظام الواحد أكثر من مسؤول ففي هذه الحالة يكون

(1) : محمد خليفة ، المرجع السابق ، ص. 135 .

(2) : زينات طلعت شحادة ، المرجع السابق ، ص. 34 .

(3) : طعباش أمين ، الحماية الجنائية للمعاملات الإلكترونية ، مذكرة ماجستير ، قسم الحقوق ، جامعة الحاج لخضر ، باتنة ، 2012 – 2013 ، ص. 31 .

للجميع سلطة التصريح بدخول هذا النظام هذا من الناحية النظرية أما من الناحية العملية فإن سلطة تقرير مضمون النظام وسلطة تنظيمه متداخلان ويصعب الفصل بينهما ، وللإشارة فإن حالة التعدد هذه تثور في حالة الأنظمة المشتركة أو الأنظمة الناتجة عن أكثر من نظام ففي هذه الحالة لا بد من تحديد المسؤول عن النظام المشترك وإذا لم يحدد هذا المسؤول فإن الجميع سيكون مسؤولا عن هذا النظام إضافة إلى مسؤولية كل واحد عن نظامه ويترتب على هذا أن التصريح بالدخول الذي يصدر من أحد هؤلاء يلزم الباقين ويعتبر كأنه صادر منهم جميعا [1].

حالات عدم التصريح : وهناك حالتين هما .

1- حالة عدم وجود تصريح إطلاقا :

وهي الحالة التي لا يكون فيها للشخص الذي يدخل النظام أي علاقة بهذا الأخير ، كون هذه الجريمة تقع من أي إنسان أيا كانت صّفته [2] ، ففي هذه الحالة لا يملك الشخص ترخيص بالدخول للنظام سواء كان هذا الترخيص 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 [3] .

وبالرجوع لنص المادة 394 مكرر من القانون 04 – 15 السالف الذكر نلاحظ أن هذا الأخير جاء عاما ومطلقا لكل حالات الدخول إلى أنظمة الحاسب الآلي عن طريق الغش .

2- حالة تجاوز التصريح :

إن الفاعل في هذه الحالة يكون مصرحا له بالدخول نظام الحاسب الآلي في حدود معين ولكنه يتجاوز هذه الحدود ، التي هي تجاوز في المكان لا في الزمان ، أي تجاوز الفاعل للمناطق والمجال المكاني المصرح به إلى غيره من المجالات غير المصرح له بدخولها [4] ، ومثال ذلك عندما يكون مسموح للشخص بالدخول إلى جزء معين في النظام ولا يحق له الدخول إلى جزء آخر ، فدخوله إلى الجزء الغير المسموح له بالنظام يعتبر دخول بدون حق يستحق القمع وبالتالي لا تتحقق الجريمة ولا تكون هناك عقوبة في حالة ما إذا كان

---

(1) : محمد خليفة ، المرجع السابق ، ص. 145 ، 146 .

(2) : زينات طلعت شحادة ، المرجع السابق ، ص. 49 .

(3) : محمد خليفة ، المرجع السابق ، ص. 147 .

(4) : محمد خليفة ، المرجع السابق نفسه ، ص. 150 .

الولوج بحق ، وذلك في حالة الولوج المصرح به من مالك النظام أو مالك جزء منه أو صاحب الحق فيه [1] .

أما بخصوص حالة تجاوز الغرض الذي منح من أجله الترخيص ، إن كان يعد من قبيل تجاوز التصريح أم لا ؟ .

فإن موقف القضاء قد إختلف ، فالقضاء الإنجليزي يرى بأن الدخول في هذه الحالة يكون مشروعا حيث رفض تطبيق المادة الأولى من قانون إساءة إستخدام الكمبيوتر والمتعلقة بالدخول غير المصرح به في حالات تجاوز الغرض الذي منح من أجله التصريح ، أما القضاء الأمريكي فهو يرى بأن الدخول غير المصرح به يتحقق في حالة إستخدام العامل للحاسب الآلي لأسباب تتعارض مع مصلحة رب العمل ، والباعث هو الذي يحدد ما إذا كان الدخول مصرحا به أو غير مصرح ، وتسمى هذه الحالات في الفقه الأمريكي بحالات سوء إدارة العاملين ، وبالرجوع للقانون الجزائري فإنه يمكن القول بأن المادة 394 مكرر التي نصت على الدخول عن طريق الغش بمعنى أن الدخول في حد ذاته يجب أن يكون عن طريق الغش وبالتالي فهو لا يتحقق بتجاوز الغرض الذي منح من أجله الترخيص أو التصريح،فصفة الغش تنصرف إلى عملية الدخول وليس إلى حدود التصريح بهذا ، ومن المعروف أن مبادئ القانون الجنائي لا تسمح بهذا التوسع أو القياس [2] .

ثانيا : تعريف البقاء وطبيعته :

إن السلوك الثاني الذي نصت عليه المادة 394 مكرر من ق ع ج ، هو سلوك البقاء داخل نظام المعالجة الآلية للمعطيات ، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام [3] ، ومن ثم فإن بقاء المتهم داخل نظام الكمبيوتر قد يكون بعد دخوله إليه بطريق الخطأ ، ففي هذه الحالة يعاقب على البقاء ولا يعاقب على الدخول كونه وقع على وجه مشروع ، كما قد يدخل المتهم النظام بطريق مشروع ولكنه يستمر بعد الوقت المحدد لبقائه فيه ، وكثير ما يحدث ذلك إذا كان إستعمال النظام محددا بوقت معين نظير أجر مالي ، فيتخطى المتهم هذا الوقت [4] ، وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وقد يجتمعا ويكون البقاء معاقبا عليه إستقلالا حيث يكون الدخول إلى النظام مشروعا كأن يكون الدخول إلى النظام عن طريق الصدفة أو السّهو إذ كان يتوجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا ، فإذا بقى رغم ذلك فإنه يعد مرتكبا لجريمة البقاء غير المشروع

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 189 .

(2) : محمد خليفة ، المرجع السابق ، ص. 152 ، 153 .

(3) : محمد خليفة ، المرجع السابق نفسه ، ص. 154 .

(4) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 121 .

فالمجرم هنا لم يسعى إلى التوصل بل ضبط وهو يتجول داخل النظام بطريق المصادفة ويعني ذلك أنه إستمر بداخله بدون حق [1] .

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له السيطرة عليه ثم يبقى داخل النظام بعد ذلك ، في هذا الفرض يتحقق الإجتماع المادي بين الجريمتين وهنا يطرح التساؤل التالي متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء ؟

لم يستقر الفقه على رأي موّحد بل ظهرت عدّة آراء في هذا المجال .

الرأي الأول : يرى بأن جريمة الدخول تتحقق من اللحظة التي يتم الدخول فيها فعلا إلى النظام والبقاء فيه فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل وبعد ذلك تبدأ جريمة البقاء داخل النظام وتنتهي بإنتهاء حالة البقاء [2] .

الرأي الثاني :ويحدد أصحابه تلك اللحظة من الوقت الذي يعلم فيه المتدخل أن البقاء داخل النظام غير مشروع .

الرأي الثالث : يرى بأن جريمة البقاء داخل النظام تبدأ من اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع أو أصبح غير مشروع ، فإذا لم ينسحب من تلك اللحظة يرتكب جريمة البقاء داخل النظام [3] .

البند الثاني : صورة المساس بالمنظومة المعلوماتية

نصت المادة 394 مكرر 01 على هذه الصورة بقولها " يعاقب ... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها " ، وتقابلها من التشريع الفرنسي المادة 323 – 03 من ق ع ف ، وما يلاحظ في هذا الشأن أن المشرع لا يحمي البيانات من الناحية المادية أو البرامج أو التطبيقات ، ولكنه يوفر الحماية للمعلومات الموجودة داخل النظام ذاته ، وذلك ضد أي نشاط إجرامي علما أن هدف الجاني من هذه الجريمة هو أن يحقق النظام المعلوماتي نتائج أو معطيات غير تلك التي كان يجب أن يحققها والنشاط الإجرامي في هذه الصورة يتمثل في أفعال الإدخال والمحو والتعديل ، ويكفي توافر إحداها لقيام الجريمة ، فلا يشترط إجتماعها معا حتى يتوافر النشاط الإجرامي فيها ، لكن القاسم المشترك في هذه الأفعال جميعها هو إنطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو

---

(1) : محمد خليفة ، المرجع السابق نفسه ، ص. 155 .

(2) : زينات طلعت شحادة ، المرجع السابق ، ص. 53 ، 54 .

(3) : طعباش أمين ، المرجع السابق ، ص. 39 .

تعديل أخرى قائمة ، وعلى ذلك فإن موضوع السلوك الإجرامي في هذه الصورة محدد ، وهو الإعتداء على معطيات في نظم المعالجة أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز أو إشارات تمثل تلك المعلومة أي بيانات تمت معالجتها ، فالجريمة في هذه الحالة تقع على المعطيات أي البيانات المعالجة دون المعلومة ذاتها ولذلك تخرج من نطاق هذه الجريمة المعلومات التي لم تعالج ، ولم تدخل إلى نظام معالجة البيانات وكذلك البيانات التي أدخلت إلى النظام ، لكن لم تبدأ بعد أي خطوة في معالجتها ، وكذلك المعلومات التي إنفصلت عن النظام وسجلت على شريط ممغنط أو قرص مدمج ، وذلك لأنها خارج النظام والنص يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بأن إتخذت خطوة أو أكثر في مراحل معالجتها [1] .

وبناءً على ما سبق وإستنادا إلى المادة 394 مكرر 01 فإن النشاط الإجرامي في هذه الصورة - التلاعب بالمعطيات - من صور الغش المعلوماتي ، يتمثل فيما يلي:

أولا : الإدخال :

فعل الإدخال هو العمل الذي بدأت به المادة 394 مكرر 1 من ق ع ج وكذلك المادة 323 - 2 من ق ع ف ويشمل هذا الفعل إدخال خصائص ممغنطة جديدة في الدعامة الموجودة سواء كانت فارغة أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال[2] .

ومن الصور العملية للإدخال إدخال معلومات مصطنعة بقيام المسؤول المعلوماتي في منشأ بضم مستخدمين غير موجودين بالفعل أو قيامه بالإبقاء على مستخدمين تركوا الوظيفة بالفعل ، ومن صّورها أيضا إختلاس النقود وعن طريق الغش المعلوماتي ، كذلك يتحقق فعل الإدخال في الفرض الذي يتمكن فيه الحامل الشرعي لبطاقات الممغنطة والتي تسحب النقود من البنوك وتحديدا من أجهزة السحب الآلي ، وذلك حين يستخدم رقمه الخاص للدخول كي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه ، وكذلك عند إدخال برنامج غريب مثل فيروس حصان طروادة أو أي قنبلة معلوماتية تؤدي إلى إضافة معطيات جديدة [3] .

ثانيا : الإزالة :

(1) : عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ، دراسة قانونية معمقة في القانون المعلوماتي ، الطبعة الأولى ، دار الفكر الجامعي الإسكندرية ، 2006 ، ص. 376 ، 377 .

(2) : محمد خليفة ، المرجع السابق ، ص.179.

(3) : عبد الفتاح بيومي حجازي ، المرجع السابق ، ص.180.

نصت المادة 394 مكرر01 من ق ع ج على فعل الإزالة ونصت عليه المادة 323-03 من ق ع الفرنسي وأيضا المادة الرابعة من إتفاقية بودابست عند تجريمها لمختلف إشكال العدوان على سلامة المعطيات [1] .

ويقصد بهذا السلوك الإجرامي إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنظومة الخاصة بالذاكرة [2] .

وللإشارة فان عملية إزالة المعطيات هي مرحلة لاحقة على عملية إدخال المعطيات فالإزالة تفترض الوجود السابق لعملية الإدخال.

ثالثا : التعديل :

نصا المادة 394 مكرر01 ق ع ج والمادة 323 - 03 ق ع ف على تجريم فعل تعديل معطيات الحاسب الآلي بطريق الغش ، وكذلك نص عليه القرار الصادر عن مجلس أوربا في 24 فبراير 2005 والمتعلق بالهجمات الموّجهة للأنظمة المعلوماتية وذلك في المادة الرابعة منه ولم تتناول المادة الرابعة من إتفاقية بودابست سلوك التعديل بالتجريم وإنما تناولت الإضرار بالمعطيات عموما وهو ما يتضمن التعديل المؤدي إلى ضرر ، إضافة إلى المحو والتعطيل والإتلاف وطمس المعطيات ، ويقصد بالتعديل تغيير المعطيات الموجودة داخل النظام وإستبداله بمعطيات أخرى وقد يتم التلاعب عن طريق التلاعب في البرنامج وذلك بإمداده بمعطيات مغايرة تؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها [3] .

إن الأفعال السابقة ، سواء كانت الإدخال أو المحو أو التعديل قد وردت على سبيل الحصر ، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها ، حتى لو تضمن إعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات [4] .

الفرع الثاني : الإحتيال المعلوماتي في ضوء تقسيم الجرائم المستند إلى إعتبارات متصلة بالركن المادي

يتجسد النشاط الإجرامي في جريمة الغش المعلوماتي في الصّور التي تم ذكرها والمتمثلة في الدخول والبقاء الغير المصرح بهما والتلاعب بالمعطيات فهذه الصّور تمثل

---

(1) : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

(2) : عبد الفتاح بيومي حجازي ، المرجع السابق نفسه ، ص.383.

(3) : محمد خليفة ، المرجع السابق ، ص.182.

(4) : عبد الفتاح بيومي حجازي ، المرجع السابق ، ص.388 ، 389 .

ماديات جريمة الغش المعلوماتي التي أثيرت بشأنها إشكاليتين أساسيتين هما : الأولى تتعلق بصورة الدخول الغير المصرح به إلى أنظمة الحاسبات الآلية ، فهذه الصورة هل تعد من الجرائم المادية أم من الجرائم الشكلية ؟ وأما الإشكالية الثانية فهي تتعلق بصور الغش المعلوماتي بصفة عامة ومفادها هل يعد الغش المعلوماتي جريمة وقتية أم جريمة مستمرة ؟

فبالنسبة للإشكالية الأولى ، يقسم الفقه الجرائم إلى نوعين مادية وهي جرائم النتيجة وجرائم شكلية وهي ذات السلوك والنشاط البحث ، وفي الإجابة عن التساؤل الذي طرح بشأن الدخول الغير المشروع عما إذا كان يعتبر من الجرائم المادية ذات النتيجة التي تتطلب أن يكون هذا الدخول الغير المشروع منتج لأثر ما أي يؤدي إلى نتيجة إجرامية محددة كالوصول إلى المعطيات المختلفة التي يحتويها هذا النظام ، أم أنه جريمة شكلية تتم بمجرد الدخول ؟

إن أغلب التشريعات التي تناولت الدخول غير المشروع تأخذ بالدخول المجرد إلى النظام المعلوماتي حيث أن الجريمة تقوم بمجرد الولوج إلى النظام حتى وإن لم يترتب على فعل الدخول ضرر أو فائدة ، طالما أن ذلك الدخول كان بدون وجه حق ، ومن أمثلة هذه التشريعات القانون الفرنسي في المادة 323 - 01 ق ع والتشريع الجزائري في المادة 394 مكرر والتشريع القطري في المادتين 371 ، 372 قانون العقوبات [1] .

في حين أن البعض الآخر من التشريعات يشترط تحقق نتيجة معينة كما هو الحال في التشريع الفيدرالي الأمريكي لجرائم الحاسب الآلي في المادة 1030 (A) - 1 والمادة 1030 (A) - 2 اللتان تعاقبان على الدخول الغير المصرح به متى أعقبه الحصول على بعض المعلومات [2] .

أما بخصوص الإشكالية الثانية والتي تتعلق بالإحتيال المعلوماتي إن كان جريمة وقتية أم جريمة مستمرة ؟ فإن طبيعة الفعل الذي يعاقب عليه القانون هو الذي يجب الرجوع إليها لتمييز بين الجريمة الوقتية والجريمة المستمرة ، فإذا كان هذا الفعل ممّا يقع وينتهي بمجرد إرتكابه كانت جريمة وقتية أما إذا كان حالة مستمرة فترة من الزمن فتكون الجريمة مستمرة طوال هذه الفترة ، فلا صعوبة تثار في الحالة التي يتم فيها إستعمال شفرة غير صحيحة للدخول إلى النظام ، ففي هذه الحالة لا تستغرق الجريمة غير برهة يسيرة ولا يتحقق ذلك في حالة التلاعب في البيانات أو البرامج أو في المكونات المادية للحاسب فعناصر الجريمة في هذه الحالة قد تمتد في الغالب خلال وقت طويل نسبيا.

(1) : حسين بن سعيد الغافري ، المرجع السابق ، ص. 352 .

(2) : حسين بن سعيد الغافري ، المرجع السابق نفسه ، ص. 353 .

ونخلص من ذلك إلى أن الإحتيال المعلوماتي قد يشكل في بعض الأحيان جريمة وقتية وفي البعض الآخر جريمة مستمرة ، فتقسيم الجرائم إلى وقتية ومستمرة ليس تقسيما مطلقا فالعبرة بالزمن الذي يستغرقه تحقق عناصر الجريمة [1] .

هذا وفي إطار ما سبق بيانه تثار إشكالية أخرى تتعلق بالشروع في الغش المعلوماتي إن كان معاقب عليه في هذه الجريمة أم لا ؟ وما هو موقف المشرع الجزائري من ذلك ، وهو ما سيتم التطرق له في الفرع التالي.

الفرع الثالث : الشروع في جريمة الغش المعلوماتي

الأصل في القانون الجزائري أن الشروع معاقب عليه ، فالجريمة قبل تمامها تمر بثلاث مراحل ، منها مرحلة التفكير والعزم وهذه لا يعاقب الفاعل فيها على ما يأتيه من أفعال ولو إعترف بذلك وتوجد أيضا مرحلة التحضير للجريمة وهي الأخرى الأصل فيها عدم العقاب إلا ما أورده المشرع الجزائري بشأنها بنص قانوني يعاقب عليها ، ثم تأتي مرحلة الشروع وهي المرحلة التي تنصرف فيها إرادة الجاني إلى تنفيذ الجريمة فعلا فيبدأ في تنفيذ الركن المادي ولكنها لا تتم لأسباب لا دخل لإرادته فيها [2] .

فالشروع معاقب عليه في التشريع العقابي الجزائري بنص المادتين 30 و 31 ق ع وبإعتبار جريمة الغش المعلوماتي من الجرائم التي إعتبرها المشرع الجزائري جنح فإن نص المادة 31 هو الذي يهمنا في هذا الإطار ، حيث ورد فيها " المحاولة في الجنحة لا يعاقب عليها إلا بناءً على نص قانوني صريح في القانون ، والمحاولة في المخالفة لا يعاقب عليها إطلاقا " [3] . وبالرجوع إلى حالة تجريم الغش المعلوماتي ، فإن هناك من الفقه من يرى ضرورة أن تتجه التشريعات إلى العقاب على الشروع فيه بإعتبار أن الأفعال التي يقوم عليها تمثل خطر على الحق الذي يحميه المشرع [4] ، وهذا ما إتجهت إليه إرادة المشرع في نص المادة 394 مكرر السالفة الذكر بقولها " يعاقب ... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك " وبهذا يكون المشرع الجزائري قد عاقب على الشروع في الغش المعلوماتي في صورة الدخول والبقاء الغير

---

(1) : نائلة عادل محمد فريدة ، المرجع السابق ، ص.473 ، 474 .

(2) : أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص. 107.

(3) : المادتين 30 و 31 من الأمر رقم 66 - 156 ، المؤرخ في 08 جولية 1966 ، المتضمن قانون العقوبات ، المعدل والمتمم ، ج ر : العدد 49 ، الصادر بتاريخ 11 جويلية 1966 ، ص. 704 .

(4) : نائلة عادل محمد فريدة ، المرجع السابق ، ص.479.

مصرح بهما ، هذا وبتطبيق نص المادة 31 من ق ع السالفة الذكر كأصل عام ونص المادة 394 مكرر 7 من القانون 04 – 15 السالف الذكر بإعتبارها نص خاص التي ورد فيها " يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها " نجد أن المشرع الجزائري قد عاقب على الشروع في إرتكاب أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي من بينها الغش المعلوماتي.

ومن أمثلة الشروع في الغش المعلوماتي ، الحالة التي يبدأ فيها الجاني بالتلاعب بالبيانات ثم إنقطع التيار الكهربائي ، حيث لم يستكمل الفاعل كل الأفعال اللازمة لتنفيذ الجريمة ، فنشاط الجاني في هذا المثال توقف بسبب لا دخل لإرادة الجاني فيه [1].

إن الشروع في الغش المعلوماتي يستلزم التمييز بينه وبين الأعمال التحضيرية من جهة وبين الجريمة التامة من جهة أخرى.

البند الأول : تمييز البدء في تنفيذ الغش المعلوماتي عن العمل التحضيري له

لقد سبق الإشارة إلى أن النشاط الإجرامي يمر بعدة مراحل منها مرحلة العمل التحضيري ، الذي يتجرد من الأهمية القانونية إذ لا ينطوي على خطر يهدد حقا أو مصلحة ذلك لأنه من ناحية ليس قاطعا في دلالته على إرادة الفاعل ومن ناحية أخرى إحتمال عدول الفاعل عن البدء في تنفيذ الجريمة على الرغم من الإعداد لها.

وفيما يتعلق بالغش المعلوماتي فإنه يعد عمل تحضيري كل نشاط يأتيه الجاني قبل إستعمال وسائل الإحتيال ، أي كل نشاط يأتيه قبل البدء في تنفيذ وسيلة الإحتيال ، كالتلاعب في البيانات أو في البرامج ، ويعني ذلك أن مرحلة الأعمال التحضيرية تقف عند اللحظة التي يبدأ الفاعل فيها إتصاله بالحاسب الآلي ، فبمجرد السعي إلى الإتصال بالحاسب الآلي يدخل في عداد الأعمال التحضيرية أما إذا إقترن بإستخدام أحد وسائل الاحتيال فيعد عندئذ بدء في التنفيذ.

وعليه إذا وقف نشاط الجاني عند حد العمل التحضيري فالأصل أنه لا يعاقب عليه إذ لا يعد شروعا في الجريمة ، إلا أن القانون قد يعتبر هذا النشاط جريمة متميزة عن الجريمة محل التحضير ، حيث ينطوي العمل التحضيري على خطر يهدد أو يكشف على نحو واضح عن خطورة مرتكبة ؛ وهذا ما يقتضي أن يجعل منه جريمة متميزة عن الجريمة محل التحضير وهو يتجلى في حالة وقوف النشاط الإجرامي عند حد الإتصال غير المشروع بالحاسب الآلي فإتصال الفاعل بالحاسب الآلي على نحو غير مشروع في أكثر الحالات إمّا على دخول غير مصرح به لنظام الحاسب متى توفرت الشروط اللازمة لتحقيق ذلك ، فإن كان النظام على

(1) : نائلة عادل محمد فريد فورة ، المرجع السابق نفسه ، ص. 480 .

سبيل المثال غير مصرح بالدخول إليه وكان قصد الفاعل التحضير للتلاعب في أحد البيانات كوسيلة من وسائل الإحتيال المعلوماتي ، إلا أن نشاطه أوقف عند حد هذا الدخول وهو ما يعد عمل تحضيري للغش ، فإن هذا النشاط يشكل جريمة تامة متميزة عن الجريمة التي يستهدف الفاعل التحضير لها ألا وهي الدخول غير المصرح به إلى نظام الحاسب الآلي [1] .

البند الثاني : التمييز بين الشروع في الغش المعلوماتي والجريمة التامة

إن الجريمة التامة هي تلك التي تتحقق فيها النتيجة الإجرامية ، وللتمييز بينها وبين الشروع في الغش المعلوماتي ، لا بد من الرجوع إلى نص المادتين 394 مكرر - 394 مكرر01 فمن خلال هذين النصين يلاحظ بأن المشرع الجزائري قد إعتبر الغش المعلوماتي من الجرائم الشكلية ، حيث لا يتطلب فيها ضرورة تحقق أثر معين عن الغش ، وبالتالي فإن مجرد قيام الجاني بالنشاط الإجرامي سواء كان دخول أو بقاء غير مصرح بهما في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك وسواء كان إدخال أو إزالة أو تعديل للمعطيات في النظام ، يكون ذلك كافي لمساءلة الجاني بغض النظر عن النتيجة الإجرامية التي قد تتحقق [2] .

إن الجريمة لا تكتمل ولا تتم بمجرد إتيان مادياتها الظاهرة ، وإنما يجب بالإضافة إلى ذلك أن تتعاصر هذه الماديات مع إرادة إجرامية ، هذه الأخيرة التي يعبر عنها بالركن المعنوي لجريمة وهو ما سيتم بيانه في إطار جريمة الغش المعلوماتي في المطلب التالي .

المطلب الثاني : الركن المعنوي لجريمة الغش المعلوماتي

إن التشريعات الجزائية التي من بينها التشريع الجزائري لم تعرف الركن المعنوي في مختلف الجرائم الأمر الذي أدى بالفقه إلى تعريفه وبيان أنواعه ، فقد عرف الفقه الجنائي الركن المعنوي على أنه " إنصراف إرادة الجاني إلى إرتكاب الجريمة مع العلم بأركانها كما يتطلبها القانون " [3] ، أما بالنسبة لتقسيماته وأنواعه فقد وجد بصدد بيانها عدة أنواع منها القصد الجنائي العام والخاص وهما ما يهم في إطار توضيح معنويات جريمة الغش المعلوماتي في مختلف صورها.

فبالرجوع لنص المادتين 394 مكرر،394 مكرر01 سالفتي الذكر والتي تقابلهما من التشريع الفرنسي 323 - 1 - 3 ق ع ف نلاحظ بأن المشرع الجزائري وكذا نظيره الفرنسي قد إعتبرا الأفعال الواردة بهذه المواد جرائم مقصودة ، يتطلب القصد العام فيها أن يعلم الجاني أنه يقوم بإحدى السلوكيات التي أوردها النص القانوني كعلمه مثلا بأنه ليس له الحق في

(1) : نائلة عادل محمد فريدة ، المرجع السابق ، ص.481 .

(2) : نائلة عادل محمد فريدة ، المرجع السابق نفسه ، ص. 482 .

(3) : أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص.121.

الدخول أو البقاء في نظام المعالجة الآلية أو علمه بأنه يقوم بإدخال أو إزالة أو تعديل غير مصرح به على معلومات نظام المعالجة وأن من شأن أفعاله أن تؤدي إلى نتيجة هي تغيير حالة المعلومات وأن تتجه إرادته إلى إرتكاب هذه الأفعال وإلى تحقيق هذه النتيجة [1].

وعليه فإذا كان الإشكال لا يثار من خلال ما سيتم إيضاحه أكثر بالنسبة للقصد الجنائي العام في جريمة الغش المعلوماتي ، فماذا عن القصد الجنائي الخاص في هذه الجريمة ؟ هذا ما سيتم توضيحه من خلال الفرع الأول الذي تمت عنونته بالقصد الجنائي العام في جريمة الغش المعلوماتي أمّا القصد الجنائي الخاص في إطار هذه الجريمة نتطرق له في الفرع الثاني .

الفرع الأول : القصد الجنائي العام في جريمة الغش المعلوماتي

يستشف من خلال نص المادة 394 مكرر السالفة الذكر أن القصد الجنائي العام في صورة الدخول والبقاء الغير المصرح بهما ، يتحقق من خلال علم الجاني بأنه يدخل بصورة غير مشروعة إلى نظام معالجة آلية يخص الغير أو إلى جزء منه ، وأنه ليس له الحق في الدخول إلى هذا النظام ، أي معرفته بأنه دخل في نظام المعالجة الآلية ضد رغبة صاحب النظام أيا كان الدافع إلى ذلك ، سواء كان على سبيل الفضول أو إثبات القدرة الإنتصار على النظام أو اللعب أو اللهو ، مع إنصراف إرادته إلى إرتكاب ذلك الفعل الإجرامي إذ يكفي أن تكون نية الجاني قد إتجهت إلى الدخول الغير المشروع إلى نظام المعالجة الآلية دون إشتراط أن تتجه هذه النية إلى تحقيق ضرر [2] .

وتبعا لذلك فإن الغش المعلوماتي في هذه الصورة لا يتحقق بالخطأ ، كما لو توّصل أحدهم مصادفة أو عن طريق الخطأ إلى أحد الأنظمة بشرط خروجه فورا بعد علمه بذلك لأن الشخص الذي توصل بطريق الخطأ مع النظام وإستمر بالبقاء داخله مع علمه وإتجاه إرادته لذلك تقوم في مواجهته المسؤولية عن جرم البقاء الغير المشروع فهذا الأخير يعتبر هو الآخر من سلوكيات العمدية ، فالجاني يجب أن يعلم بعدم مشروعية أفعاله ، أي تواجده داخل النظام هو خلاف لإرادة صاحب النظام مع إتجاه إرادته للبقاء ، وكجرم الدخول غير المشروع فإنه لا يعتد بالباعث على إرتكابها ، فالغش المعلوماتي في صورة البقاء الغير المشروع يعتبر جريمة شكلية تكتمل بمجرد الإنتهاء من السلوك المكون لها دون إشتراط حصول أي نتيجة إجرامية [3] .

هذا ويتطلب الغش المعلوماتي في صورة التلاعب بمعلومات نظام المعالجة قصدا جنائيا عاما وذلك بحسب ما ورد في المادة 394 مكرر01 ، شأنه في ذلك شأن ما سبق ذكره

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 269 .

(2) : زينات طلعت شحادة ، المرجع السابق ، ص.51.

(3) : زينات طلعت شحادة ، المرجع السابق نفسه ، ص.55 .

بصدد الدخول والبقاء غير المصرح بهما ، إلا أن ما يلاحظ بشأن هذه الصورة أن المشرع الجزائري لا يتطلب بشأنها قصدا محددا ، إذ تقوم الجريمة سواء حدد القصد بمعلومات معينة أو لم يحدد فلا فرق في التشريع الجزائري بين إتجاه إرادة الجاني إلى معلومات دون أخرى فيعد مرتكب للجريمة من سعى للتلاعب بمعلومات ما فإعتدى على أخرى [1] .

الفرع الثاني : القصد الجنائي الخاص في جريمة الغش المعلوماتي

يذهب جانب من الفقه إلى القول بأن جريمة الغش المعلوماتي ، لا تتطلب قصدا جنائيا خاصا مثل قصد الإضرار أو نية الإضرار بالغير ، فهذا الجانب يعتبرها من جرائم الخطر وليست من جرائم الضرر بمعنى أن المشرع يستشعر خطورة الجاني من السلوك المجرد الذي يقوم به ولا يرتب حصول نتيجة معينة حتى يتم عقابه أي ليست من جرائم الضرر [2] ، إلا أن جانب آخر خاصة في ظل الفقه الفرنسي يذهب إلى إشتراط توافر القصد الخاص في الدخول والبقاء غير المصرح بهما ، والذي يتمثل في الغش ويستندون بالقول أن المشرع الفرنسي قد إستعمل لفظ "عن طريق الغش " وهذا اللفظ يختلف عن مصطلحي عمدا وإراديا.

هذا ويتفق جميع الشراح أن الغش هنا ليس مقصودا منه نية الإضرار ، وإلا يكون هناك تناقض بين الركن المادي الذي لا يتطلب النتيجة والركن المعنوي ، ومفهوم الغش الذي إعتمده الفقه والقضاء بالنسبة لهذه الجريمة هو مفهوم مستعار من الغش في جريمة السرقة ، إذ يرون أن الدخول والبقاء غير المصرح بهما يتحققان عندما يكونان بدون رضا صاحب النظام ، وقد إستند هذا الرأي إلى القرار المشهور الذي أصدرته محكمة باريس في 05 أفريل 1994 ، الذي قضت فيه بأن الدخول والبقاء يكون بدون وجه حق ومع معرفة السبب ، وعليه يخلص هذا الرأي إلى أن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في نظم المعالجة الآلية ، وهذا ما يستشف من خلال نص المادة 394 مكرر ق ع ج التي تقابلها المادة 323-01 ق ع ف ، حيث نجد أن كل ما يتطلبه المشرع في هذه الصورة هو توافر القصد الجنائي العام [3] ، هذا وبالرجوع للمادة 394 مكرر01 والتي تقابلها المادة 323-03 ق ع ف، نجد أن المشرع لم يستخدم فيها من العبارات الدالة على القصد الخاص في صورة التلاعب بالمعلومات ، وهو الأمر الذي يستفاد منه أن هذه الجريمة تقوم بمجرد توافر القصد العام ، أما لفظ الغش الذي أقر المشرع إستخدامه فإنه لا يدل على هذا المعنى ، وإنما يدل على أن الجريمة مقصودة ليس إلا [4] .

وفي ختام هذا الفرع نشير إلى أن إتفاقية بودابست لمكافحة الإجرام المعلوماتي وبالرجوع إلى نص المادة الثامنة منها وكذا المذكرة التفسيرية لها في الفقرة 90 منها نجد أن

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 269 .

(2) : عبد الفتاح بيومي حجازي ، المرجع السابق ، ص.391.

(3) : رشيدة بوكر ، المرجع السابق نفسه ، ص. 237 ، 238 .

(4) : رشيدة بوكر ، المرجع السابق نفسه ، ص. 270 .

جريمة الغش المعلوماتي تتطلب قصدا جنائيا خاصا [1] بجانب القصد العام ، يتمثل في نية الغش أو أي نية سيئة أخرى من أجل الحصول على مكسب إقتصادي وغيره للنفس أو للغير وهذا ما يبدو واضحا من خلال الفقرة ب من المادة السالفة الذكر في قولها " كل أشكال الإعتداء على وظيفة الحاسب الآلي ، بنية الغش أو أي نية إجرامية مشابهة للغش ، من أجل الحصول بدون وجه حق على منفعة إقتصادية لمرتكب الفعل أو الغير " [2] .

بعد أن تم بيان الركن المادي والمعنوي لجريمة الغش المعلوماتي في المطلبين السابقين سيتم التطرق فيما يلي إلى بيان خصائص هذه الجريمة.

المطلب الثالث : خصائص جريمة الغش المعلوماتي

تتميز جريمة الغش المعلوماتي بطبيعة خاصة ، تميزها عن غيرها من الجرائم التقليدية ، وذلك نتيجة إرتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية ، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السّمات والحقائق ، والتي إنعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميّزه عن المجرم التقليدي [3] .

وسوف نحاول فيما يلي التطرق إلى بعض السّمات الخاصة بالغش المعلوماتي في الفرع الأول ، إلى جانب أهم السّمات التي تميز المجرم المعلوماتي في الفرع الثاني .

الفرع الأول : السمات الخاصة بجريمة الغش المعلوماتي

تتميز جريمة الغش المعلوماتي بجملة من الخصائص من أهمها : أنها جريمة لا حدود جغرافية أو زمنية لها ، كذلك تتسم بالخطورة البالغة ، مما أدى إلى صعوبة التحقيق والتحري فيها ، وذلك لإرتباطها بنظام المعالجة الآلية للبيانات فهذه السّمات جعلت منها جريمة صعبة للإثبات ، وعليه سنحاول فيما يلي توضيح هذه الخصائص والسّمات كما يلي .

البند الأول : جريمة الغش المعلوماتي جريمة بالغة الخطورة

فهي جريمة تتسم بالخطورة من عدّة نواحي : الأولى نجد أن الخسائر المادية الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال ، ومن ناحية ثانية نجدها ترتكب من فئات متّعددة تجعل من التنبؤ بالمشتبه فيه أمرا صعبا ، ومن ناحية ثالثة تنطوي على

(1) : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

(2) : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

(3) : سوير سفيان ، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير ، قسم الحقوق ، جامعة أبوبكر بلقايد ، تلمسان ، 2010 – 2011 ، ص. 17 .

سلوكيات غير مألوفة ، وهذا ما حدى بمكتب التحقيقات الفيدرالية الأمريكية FBI أن يطلق عليها وصف الوباء [1] .

البند الثاني : جريمة الغش المعلوماتي ذات طابع عالمي

تتسم جريمة الغش المعلوماتي بالطابع العالمي نتيجة إرتكابها في إطار مجتمع معلوماتي لا يعترف بالحدود الجغرافية ، كونه مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود [2] ، فعالمية الشبكات التي من بينها شبكة الأنترنت على سبيل المثال تعتبر أساس المجتمع المعلوماتي ، قد جعلت من دول العالم في حالة إتصال دائم تسهل إرتكاب جريمة الغش المعلوماتي من دولة إلى أخرى ، فهذا النوع الجديد من الجرائم لا يعترف بالحدود بين الدول والقارات ، ولذلك يمكن القول بأنها جريمة عابرة للقارات ، فهي تعتبر شكل جديد من الأشكال العابرة للحدود الإقليمية بين دول العالم كافة إذ يمكن من خلال النظام المعلوماتي إرتكاب العديد من الجرائم [3] .

البند الثالث : وقوع جريمة الغش المعلوماتي أثناء المعالجة الآلية للبيانات

فمن خصائصها أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالحاسب الآلي ، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة المعلوماتية أو الغش المعلوماتي بالتعدي على نظام معالجة البيانات ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية [4] .

البند الرابع : صعوبة إثبات جريمة الغش المعلوماتي

إن إثبات جريمة الغش المعلوماتي أمر تحيط به الكثير من الصّعاب ، نجملها في كون هذه الجريمة لا تترك أثر ويصعب فنيا الإحتفاظ بآثارها إن تركت أثر ، كذلك يصعب في هذا النوع من الجرائم على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية ، وذلك لإعتمادها على الذكاء من جهة والخداع والتظليل في التعرف على مرتكبها من جهة أخرى [5] .

---

(1) : حسين بن سعيد الغافري ، المرجع السابق ، ص. 53 .

(2) : نهلا عبد القادر المومني ، المرجع السابق ، ص. 50 .

(3) : حسين بن سعيد الغافري ، المرجع السابق نفسه ، ص. 54 .

(4) : خالد ممدوح إبراهيم ، المرجع السابق ، ص. 49 .

(5) : بن عقون حمزة ، السلوك الإجرامي للمجرم المعلوماتي ، مذكرة ماجستير ، قسم الحقوق ، جامعة الحاج لخظر ، باتنة ، 2011 - 2012 ، ص. 24 .

الفرع الثاني : سّمات المجرم المعلوماتي

إن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف ، فالمجرم المعلوماتي يتميز بمهارات تقنية عالية والإلمام بتكنولوجيا نظم المعلومات فهذا النوع الجديد من المجرمين لم تتضح الصورة جليا في تحديد صّفاتهم وإستظهار سّماتهم وضبط دوافعهم نظرا لقلة الدراسات الخاصة بهذه الظاهرة من جهة ولصعوبة الإلمام بمداها الحقيقي من جهة ثانية ، والتغيّر السريع الحاصل في نطاقها والمرتبط أساسا بالتسارع الرهيب في ميدان الحاسب الآلي من جهة ثالثة ، فالمزيد من الوسائل والمخترعات يعني المزيد من التغير في أنماط الجريمة ووسائل الاعتداء وهذا بدوره يساهم في إحداث تغير على السّمات التي يتصف بها مجرمي المعلوماتية [1] .

فهناك دراسات قامت بوضع تصنيف لهؤلاء المجرمين ، بحسب ما توصلت إليه الدراسة في ميدان علم الإجرام ، ونتطرق فيما يلي إلى أهم هذه التقسيمات ثم بعدها نبرز أهم السّمات التي يتميزون بها.

أولا : تصنيفات المجرم المعلوماتي

هناك العديد من الأنماط لهؤلاء المجرمين ، فهناك فئة المخترقون أو القراصنة وهؤلاء يمكن تصنيفهم إلى صنفين هما : الهاكرز والكراركرز ، فبالنسبة للصّنف الأول فهم متّطفلون يتحدون إجراءات أمن النظم والشبكات لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات،وتتألف هذه الطائفة أساسا من مراهقين وشباب. أما الصنف الثاني - الكراركرز - فهم أشخاص يقومون بالتسلسل إلى النظم المعالجة الآلية للإطلاع على المعلومات المخزنة فيها لإلحاق الضرر أو العبث بها أو سرقتها وذلك بدافع التحدي الإبداعي [2] .

وهناك أيضا فئة المحترفون وتعد هذه الفئة الأخطر من بين مجرمي المعلوماتية أو التّقنية ، حيث تهدف إعتداءاتهم بالأساس إلى تحقيق الكسب المادي سواء لهم أو للجهات التي سّخرتهم لإرتكاب هذا النوع من الجرائم-الغش المعلوماتي - فضلا عن تحقيق أغراض سّياسية والتعبير عن موقف فكري أو فلسفي ، أما بالنسبة لفئة الحاقدين فهي فئة لا تسعى إلى تحقيق مكاسب مادية أو سياسية بل هدفهم هو الإنتقام سواء كأثر لتّصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم ، كما نشير إلى طائفة صّغار السّن وهم الذين لم يبلغوا بعد سّن الأهلية مفتونين كثيرا بالتقنيات الرقمية [3] .

ثانيا :أهم سّمات المجرم المعلوماتي

(1) : خالد ممدوح إبراهيم ، المرجع السابق ، ص. 45 – 47 .

(2) : بن عقون حمزة ، المرجع السابق نفسه ، ص. 36 – 40 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 96 ، 97 .

إن الخبرة الكبيرة والدّراية الفائقة بكل ما يتعلق بالحاسب الآلي هي ما تميّز مرتكب الغش المعلوماتي بشكل عام ، حيث يعتبر المجرم المعلوماتي من النّوابغ ، كما أنه من سّماته أنه شخص متكيف إجتماعيا ، وعليه سيتم التطرق فيما يلي لبعض السّمات التي يتميّز بها المجرم المعلوماتي كما يلي .

أ- المجرم المعلوماتي من النوابغ

إن المجرم المعلوماتي ليس مجرما عاديا ، فهو يقترب من حيث سّماته من المجرمين ذوي الياقات البيضاء ذلك أن كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة المسّتوى ، ومن ذوي الكفاءات العالية ، ولهم القدرة على التكّيف الإجتماعي ، ولا يعني ذلك التقليل من شأنه بل أن خطورته الإجرامية قد تزداد إذا زاد تكّيفه الإجتماعي مع توافر الشخصية الإجرامية لديه ، كما يتمتع هذا المجرم بقدر لا يستهان به من المهارة والمعرفة بالوسائل الإلكترونية المستحدثة في التحكم في المعلومات بما في ذلك الحاسوب والإنترنت [1] .

ب- المجرم المعلوماتي إجتماعي

إن المجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به ، بل أنه إنسان متكيف إجتماعيا ، ذلك أنه أصلا مرتفع الذكاء ويساعده على ذلك عملية التكّيف ، وما الذكاء في رأي الكثير سوى القدرة على التكّيف [2] .

هذا ويذكر بأن الإجرام المعلوماتي قد تمّخض عن عوامل مستحدثة في أذهان مرتكبيه حيث يلجأ العديد منهم إلى إرتكاب هذه الجرائم بدافع اللّهو أو لمجرد إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن نظم المعلوماتية ، ونشير في هذا المجال إلى مثال شهير مستمد من إعترافات متهم يبلغ من العمر 17 سنة أمام القضاء الجنائي الألماني حيث نسب إليه دخوله بطريقة الغش في نظام الفيديو تكس الخاص ب Bunds post والمعروف بمصطلح BTX ودافع المتهم عن نفسه قائلا : " تملكني إحساس قوّي بأن أكون مفيدا في كشف عيوب نظام BTX ولذلك أرسلت في الحال إلى مجموعة عمل BTX كل العناصر التي إكتشفتها بالصّدفة والتي أظهرت تشكلها فيما يخص حماية البيانات ، لاسيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء مما أتاح الأمر إلى تلاشي هذه العيوب " [3] .

---

(1) : رشيدة بوكر ، المرجع السابق نفسه ، ص 94 .

(2) : بن عقون حمزة ، المرجع السابق ، ص. 30 .

(3) : عبد الفتاح بيومي حجازي ، المرجع السابق ، ص.86 .

بعد أن تم التطرق في هذا المبحث إلى بيان أركان جريمة الغش المعلوماتي وخصوصياتها نتطرق في المبحث الثاني إلى بيان المسؤولية الجنائية في حال إرتكاب هذه الجريمة ، ذلك أن الشخص الفاعل يسأل جنائيا متى ثبت إرتكابه لفعل من أفعال المعاقب عليها في قانون العقوبات ، وهذا ما سيتم بيانه فيما يلي:

المبحث الثاني : المسؤولية الجنائية عن جريمة الغش المعلوماتي

يتناول هذا المبحث بحث العلاقة بين دولة القانون وبين مرتكب الواقعة الإجرامية وهي علاقة قانونية لها سّند من الشرعية الجنائية ، بحيث لا يسأل من قبل دولة العقاب سوى من إرتكب جرما معاقبا عليه بمقتضى نص جنائي صريح ، هذه العلاقة القانونية يطلق عليها المسؤولية ، وإليها يعود الفضل في إمكانية تدخل الدولة لمكافحة الإجرام بطريقة الردع بنوعيه الخاص والعام [1] .

ويمكن تعريف المسؤولية الجنائية بأنها تحمّل الشخص نتائج فعله الإجرامي ، ومن ثم فإن المسؤولية الجزائية ليست ركنا من أركان الجريمة وإنما هي أثرها ونتيجتها القانونية[2]، فمن المبادئ الأساسية المسّتقر عليها في التشريعات الجنائية أن المسؤولية الجنائية هي مسؤولية شخصية بمعنى عدم تقرير المسؤولية الجنائية إلا بالنسبة للشخص الذي تتوافر لديه صّفة الفاعل الأصلي أو الشريك ، ومع ذلك ونظرا لوجود مسّتجدات في أنماط إرتكاب الجرائم فقد خرج المشرع الجنائي عن هذا الأصل بتقرير المسؤولية الجنائية للأشخاص المعنوية [3] ، وبناء على ما سبق سنحاول توضيح المسؤولية الجنائية للشخص الطبيعي عن جريمة الغش المعلوماتي ، بحيث تقتصر الدراسة على مسؤولية كل من مقدمو الخدمات وكذا المستخدم العادي ، أما بالنسبة لمسؤولية الشخص المعنوي ، فإنه سيتم توضيح مسؤولية كل من الشخص العام والخاص ، ذلك أنه وفي إطار إرتكاب جرائم الغش المعلوماتي أصبح للأشخاص المعنوية دور في المجال المعلوماتي لا يستهان به ، مما يجعل أمر إرتكابها للغش المعلوماتي مسألة ممكنة بل وخطيرة نظرا للخسائر المترتبة عن ذلك .

وعليه نتطرق للمسؤولية الجنائية عن الغش المعلوماتي للشخص الطبيعي في المطلب الأول والشخص المعنوي في المطلب الثاني .

المطلب الأول : المسؤولية الجنائية للشخص الطبيعي عن الغش المعلوماتي

إن الإتيان على جريمة ماديا لا يؤدي حتما إلى تطبيق العقوبة المقررة قانونا لمرتكبها فلا يعاقب هذا الأخير إلا إذا أثبت القاضي مسؤوليته الجزائية ، وهذه الأخيرة تتمثل في إلتزام

(1) : عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الأنترنت ، الأحكام الموضوعية والجوانب الإجرائية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ،2004 ، ص.695 .

(2) : أحسن بو سقيعه ، الوجيز في القانون الجنائي العام ، المرجع السابق ، ص.207 .

(3) : رشدى محمد علي محمد عيد ، الحماية الجنائية الموضوعية للمعلومات عبر الأنترنت ، دراسة مقارنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، بدون سنة نشر ، ص.351 .

الشخص بتحمل نتائج فعله الإجرامي [1] ، وفيما يخص المسؤولية الجنائية الشخصية التي تترتب على إثبات جريمة الغش المعلوماتي وجدت عدّة مساءل كانت محل نقاش من قبل الفقهاء ، نّجد من بّينها ما يتعلق بسّن الجاني الذي إرتكب الجريمة ، حيث أن الواقع العملي كشف أن معظم مرتكبي هذا النوع من الجرائم هم من طوائف الشباب صّغار السّن الذين لا ينطبق عليهم السّن المقررة في قانون العقوبات بشأن الأهلية الجنائية لمرتكبي هذه الجريمة حيث أن هذا التّطور من شأنه أن يؤدي إلى إحداث ثورة في القانون الجنائي بشأن إعادة النظر في توصيف الأهلية الجنائية المتعلقة بأهلية الإدراك وسّن الجاني [2] ، هذا وقد أثير بشأن هذا النوع من الجرائم مسألة أخرى تتعلق بموانع المسؤولية الجنائية في إطار إرتكاب هذا النوع من الجرائم ، حيث يرى البعض أن الإعاقة العضوية والمعنوية لا تشكل عائقا حال إرتكاب جرائم الغش المعلوماتي نظرا لأن المعاقين عضويا تتوافر لهم مقومات الزّمن والجّهد مما يجعلهم يملكون القوة لكي يصبحوا هكرة حقيقيين ، فحسب هذا الرأي إذا كانت قواعد القانون الجنائي التقليدي في مجال الإعاقة العضوية لم تميز بين بني البشر ، فهذا يمكن أن يؤدي إلى أن يأتي اليوم الذي تكون فيه الإعاقة ككل محل إعادة نظر في قانون العقوبات وهذا الرأي رغم وجاهته إلا أنه محل نظر من قبل العديد من الفقهاء ذلك أن الإعاقة سواء كانت عضوية أو نفسية تؤثر في الإرادة ، وكل سبب يؤثر في هذه الإرادة يؤدي إلى إمتناع المسؤولية الجنائية عن إرتكاب الجريمة ، لأن الأساس الذي بنيت عليه هذه المسؤولية هو الإرادة الحرّة فالشخص الذي يقوم بالدخول إلى أحد المواقع وأصاب عارض من عوارض الأهلية ، كأن يكرهه شخص آخر على ذلك ، فهنا يجب أخذ ذلك بعين الإعتبار وإلا كان ذلك إخلال بالمبادئ الرئيسية في القانون الجنائي وبمبادئ العدالة الجنائية [3] .

وبعد هذا العرض لأهم الآراء الفقهية التي أثيرت بشأن المسؤولية الجنائية الشّخصية في جريمة الغش المعلوماتي سيتم فيما يلي التطرق لبيان المسؤولية الجنائية لكل من المستّخدم في الفرع الأول ومقدمي الخدمات في الفرع الثاني .

الفرع الأول : المسؤولية الجنائية للمستخدم عن الغش المعلوماتي

إن المستخدمين هم الأطراف الأكثر أهمية في شبكة الأنترنت لأن هذه الشبكة أولا وأخيرا هي شبكة من المستخدمين ، ويقصد بالمستّخدم العادي في شبكة الأنترنت من يتصل بواسطة موّرد خدمة الإتصالات بالإنترنت إما للحصول على معلومات أو لإرسال المعلومات [4] .

---

(1) : أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص. 201 .

(2) : رشدي محمد علي محمد عيد ، المرجع السابق ، ص. 357 .

(3) : رشدي محمد علي محمد عيد ، المرجع السابق ، ص. 360 – 362 .

(4) : حسين بن سعيد الغافري ، المرجع السابق ، ص. 21 .

وبشأن تحديد المسؤولية الجنائية للمسّتخدم عن جريمة الغش المعلوماتي ، فإن أهم صعوبة يمكن الإشارة إليها في هذا الإطار هي وجود الوسيط المادي الذي هو الحاسوب حيث أن ما يتم رصّده هو الحاسوب الآلي الذي إرتكبت من خلاله الجريمة ، خاصة إذا كان الفاعل قد دخل النظام المعلوماتي بإسم مستعار أو إستخدم تقنيات إخفاء الهوية التي تمنع الوصول إلى أي معلومات عن هذا الشخص مرتكب الجريمة [1] ، وكذلك في الحالة التي يقوم فيها المجرم بنشاطه الإجرامي من بلد غير البلد الذي يوجد فيه الكمبيوتر الذي بدأ إنطلاق نشاطه منه بحيث يتم تحديد نقطة الإنطلاق من قبل أجهزة التحري في دولة معينة إلا أن الحقيقة قد تبدو خلاف ذلك فقد يقوم المجرم بالتسّلل إلى ذلك الجهاز بهدف إخفاء مكان التواجد الحقيقي لمكانه من خلال نقطة إنطلاق وهمية [2] ، فمثل هذا الأمر يجعل موضوع المسؤولية في شكلها الأصلي محلا للعديد من التساؤلات ، وفي هذا الشأن هناك من يرى ضرورة التمييز بين مالك الحاسوب وبين المستخدم فإذا كان مستخدم الحاسوب موظف في مؤسسة تملك هي جهاز الحاسوب ، وقام بإرتكاب صورة من صور الغش المعلوماتي كالتلاعب بالمعطيات ، فمثل هذا الوضع هو محل إستفسار أدى بالبعض إلى القول بأن الإعتراف فقط هو من له المصداقية، إلا أن هذا الأمر في الحقيقة ، وحسب رأي آخر سيبقى من المشكلات القائمة ، طالما أن هناك حرية إقتصادية في مسألة إقتناء الحاسوب ، بل حتى محاولات بعض الدول في إقرار إجراءات إدارية تتناول في مجملها تسجيل أجهزة الحاسوب التي يتم إقتناؤها لدى الجهات الأمنية هي محاولات فاشلة إذا أدركنا أن مالكي الحواسيب قد يمكنهم نفي قيامهم إرتكاب الجريمة في الوقت الذي لا يمكن أن يتخذ مجرد التعرف على هوية الحاسوب دليلا على إرتكاب مالك الحاسوب لها ، إذ من الممكن أن يكون المالك مؤجرا لهذا الحاسوب ، كما يمكن أن يكون قد منحه لعدّة أشخاص على سبيل العارية وإنطلاقا مما سبق إتجه القضاء المقارن إلى الإقرار بإعتبار مصطلح المسّتخدم عائد إلى الحاسوب وليس إلى غيره ، بحيث يفهم من هذا أن البشري العامل على الحاسوب هو الوسيط وليس الحاسوب ذاته [3].

وللإشارة فإن المشرع الجزائري قد حسّم هذا الخلاف الفقهي بنّص في المادة 11 التي وردت في إطار الفصل الرابع بعنوان إلتزامات مقدمي الخدمات من القانون رقم 04 – 09 السالف الذكر ، حيث نصّت على أنه " مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمات بحفظ : أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة ... " [4] ، فبهذا الإلتزام الذي ألزم به المشرع مقدمو الخدمات يمكن التعرف على المستخدم ومن ثّم إمكانية مساءلته جنائيا إن كان قد إرتكب إحدى صور الغش المعلوماتي .

---

(1) : رشدى محمد علي محمد عيد ، المرجع السابق نفسه ، ص. 357 .

(2) : فايز محمد راجح غلاب ، المرج السابق ، ص. 283 .

(3) : عمر محمد بن يونس ، المرجع السابق ، ص. 700 .

(4) : المادة 11 من القانون 04 – 09 السالف الذكر ، ص. 07 .

الفرع الثاني : المسؤولية الجنائية لمقدمي الخدمات عن الغش المعلوماتي

يقصد بمقدمي خدمات الإتصال بالإنترنت من يقدمون للمشتركين خدمة الإتصال بشبكة الأنترنت بموجب عقود إشتراك ، ولهم بالإضافة إلى ذلك وظائف تقنية إضافية مكملة لخدمة الوصول للشبكة أبرزها تخزين الرسائل الإلكترونية ، إيواء أو إستضافة مواقع الويب لفائدة المشتركين داخل ملقمات خاصة لديهم كذلك وصل المشتركين مع منتديات المناقشة وغيرها [1] ، من خلال هذا التعريف نلاحظ أن خدمة الأنترنت لكي تصل إلى المسّتخدم تمر بأكثر من وسيط يتعاونون فيما بينهم ، هؤلاء الوسطاء هم : مزود الخدمات وهو من يقدم للجمهور خدمة الإتصال بشبكة الأنترنت أمّا متّعهد الإيواء فهو من يقدم خدمات للجمهور تتمثل في تسكينهم على مواقع الشبكة ، ومن هنا يمكن القول بأن متّعهد الإيواء هو شخص طبيعي أو معنوي يعرض تسكين مواقع صفحات الويب على أجهزته الخادمة مقابل أجر، أما متعهد الوصول فهو شخص طبيعي أو معنوي يقوم بتوصيل المسّتخدم إلى شبكة الأنترنت [2] .

هذا وبالنسبة للمشرع الجزائري فقد عرّف مقدمو الخدمات من خلال نص المادة 02 الفقرة د من القانون رقم 09 – 04 السالف الذكر بقوله : " أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام للإتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعملها " ، كما حدد إلتزاماتهم في إطار الفصل الرابع تحت عنوان إلتزامات مقدمي الخدمات في ذات القانون وحصرها في مساعدة السلطات وحفظ المعطيات المتعلقة بحركة السّير وكذا الإلتزامات الخاصة بمقدمي خدمة الأنترنت وذلك في المواد 10 ، 11 ، 12 على التوالي [3] .

أما بخصوص المسؤولية الجنائية لمقدمي الخدمات فإن أهم صعوبة يمكن أن تعترض سبيل تطبيق هذه المسؤولية ما يتعلق بتحديد هوية مرتكب الجريمة ، حيث أنه إذا أمكن بواسطة الوسائل التقنية الحديثة في الجرائم المعلوماتية بصفة عامة والغش المعلوماتي بصفة خاصة تحديد الأسلوب الذي أرتكب من خلال الجريمة وذلك من خلال بروتوكول الأنترنت IP [4] ، الذي يحدد الطريقة التي أرتكبت من خلالها الجريمة إلا أن معرفة المتهم قد لا تكون بالأمر السّهل وذلك عندما يتم إرتكاب الجريمة من خلال محل للأنترنت أو أي مكان

---

(1) : حسين بن سعيد الغافري ، المرجع السابق ، ص. 20 ، 21 .

(2) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 164 .

(3) : المواد 10 ، 11 ، 12 من القانون 04 – 09 السالف الذكر ، ص. 7 ، 8 .

(4) : بروتوكول الانترنت (IP) : أنظر الملحق رقم 01 .

جماعي نظرا لإستخدام الأنترنت بشكل جماعي أو من قبل فئات معينة وكذلك في الحالة التي لا يكون فيها للشخص رقم IP الخاص به،هذه التقنية التي نجدها فقط في الدول المتقدمة أما الدول النامية ، فإنها تفتقد لهذا النظام [1] ، وبالتالي فإن مشكلة تحديد هوية مرتكب جريمة الغش المعلوماتي ستظل قائمة ، ومن ثم فإن مسألة تحديد الشخص المسؤول في حالة إرتكاب هذا النوع من الجرائم ستظل أيضا قائمة ، وفي هذا الصدد وجدت عدّة آراء فقهية ، بشأن تحديد هذه المسؤولية حيث ذهب جانب من الفقه إلى القول بالمسؤولية الجنائية المفترضة لمقدمي الخدمات ، حيث قيل بأنه إذا كان الأصل هو أن المسؤولية الجزائية شخصية لا يسأل عنها إلا من إرتكب الجريمة أو شارك فيها [2] ، فإن بعض التشريعات قد عرفت هذا النوع من أنواع المسؤولية الإستثنائية ، إذ إتجه المشرع المقارن إلى الأخذ بهذه الحيلة القانونية وإعتبر هذا النوع من المسؤولية المفترضة يفترضها القانون مسبقا لذلك يضفي عليها المشروعية ، ومن مظاهر هذه المسؤولية ما سنحاول إسقاطه على جريمة الغش المعلوماتي من خلال ما يلي .

البند الأول : المسؤولية الجنائية لمقدمي الخدمات عن فعل الغير

يقصد بالمسؤولية الجنائية المفترضة أن يتحّمل من هو غير الجاني المسؤولية عن الفعل الإجرامي الذي أرتكب وذلك بسبب وجود صّلة تتعلق بشخص الجاني أو الواقعة المرتكبة ويجب لإعمال هذا النوع من المسؤولية أن يكون هناك نص قانوني يحكم هذه المسألة ، بحيث يوضح النموذج القانوني للجريمة وعلى ضوء ذلك تتحدد الجريمة التي إرتكبها الغير ، وأن يحدد ما هية وطبيعة الإلتزام الذي يقع على عاتق الشخص الذي تبعه هذا الفعل ، فالمسؤولية عن فعل الغير في حقيقتها مسؤولية شخصية عن فعل الغير [3] ، هذا ولقد حدثت خلافات فقهية بين مؤيد ومعارض بشأن تقرير مسؤولية مقدمي الخدمات عن جرائم الغير لم يرتكبوها حيث إنقسم الفقه إلى من يرفض فكرة تحّمل مقدمي خدمات الأنترنت تبعة الجريمة تأسيسا على عدم معرفة الجاني أو الجهالة به ، نظرا لأنه لا يمكن مساءلة شخص عن جريمة لم يرتكبها لمجرد أنه يملك أدوات الإتصال بين شبكة الأنترنت والمستخدمين ، كما أن ذلك يتعارض مع مبدأ شخصية الجريمة ومبدأ التفسير الضيق لنصوص التجريم والعقاب وقرينة البراءة ، أما الرأي الآخر فإنه يرى تقرير مسؤولية مقدم الخدمات وتحميله بنصيب من المسؤولية عن فعل الغير طالما أنه له دورا في الإتصال بالشبكة والتفاعل مع عالمها ، وإن كان هذا الرأي يميل إلى التخفيف من هذه المسؤولية وذلك عن طريق الفصل بين مسؤولية مقدمي الخدمات وبين مسؤولية مرتكب الواقعة غير المشروعة ، بحيث يمكن أن تتقرر مسؤولية مورد الخدمة في الوقت الذي يتم فيه التعرف على مرتكب الواقعة الأصلي ، وقد أنتقد هذا الإتجاه بالقول أن أساس المسؤولية الجنائية عن فعل الغير ينبع أساسا من عدم تحديد هوية الجاني مرتكب الواقعة في الجريمة المعلوماتية[4].

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 283 ، 284 .

(2) : أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص. 216 .

(3) : رشدى محمد علي محمد عيد ، المرجع السابق ، ص. 366 .

(4) : رشدى محمد علي محمد عيد ، المرجع السابق نفسه ، ص. 367 – 369 .

البند الثاني : المسؤولية الجنائية التتابعية لمقدمي الخدمات

المسؤولية الجنائية بالتتابع هي نظام إستتنائي من القواعد العامة من المسؤولية الجنائية لأن المسؤولية فيها مفترضة ، ويمكن أساس هذا النوع من المسؤولية في أن المساهم في إرتكاب الجريمة لا يعرف على وجه الدّقة موقعه من أحداث الواقعة الإجرامية هذا ويرى البعض أن هذا النظام الإستتنائي يخالف مبدأ الشرعية الجنائية فيما هو مقرر بشأن مبدأ شخصية العقوبة ، وفيما يتعلق بالمساهمة الجنائية ، لأن القانون يفترض وجود مسؤولية جنائية تمت إقامتها على أساس وهمي مصدره القانون ، ومن ثمت كان يتعين وفقا للعدالة تطبيق القواعد العامة في المسؤولية بشأنه ، فالقانون في هذا النظام الإستتنائي يفترض وجود من هو مسؤول عمّا أرتكب من جرائم [1] .

بناءً على ما سبق وبالرجوع للتشريع الجزائري خاصة إلتزامات مقدمي الخدمات التي حددها المشرع الجزائري في ظل القانون 04 – 09 السالف الذكر ، خاصة الإلتزام المتعلق بحفظ المعطيات المتعلقة بحركة السّير التي عرفها بأنها معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة بإعتبارها جزءا في حلقة إتصالات توضح مصدر الإتصال ونوع الخدمة ، حيث أنه من خلال هذا الإجراء يمكن التعرف على الشخص الذي إرتكب جريمة الغش المعلوماتي وبالتالي إمكانية مساءلته جنائيا ، خاصة إذا ما علمنا أن المشرع الجزائري قد وضع على عاتق مقدمي الخدمات إلتزام آخر يتعلق بجعل مدّة الحفظ سنة بهدف تقديمها للسلطة المختصة في وقت الطلب ، هذا وبالرجوع للفقرة الأخيرة من المادة 11 من القانون 04 - 09 السالف الذكر [2] ، يمكن القول أنه في حالة الإخلال من قبل مقدمي الخدمات بالإلتزامات الواقعة على عاتقهم وأدّى ذلك إلى عرقلة حسن سير التحريات القضائية تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين ، وبهذا يمكن القول بأن هذه المسؤولية قائمة على أساس الإخلال بأحد الإلتزامات وهي مستقلة عن مسؤولية الشخص الذي يرتكب جريمة الغش المعلوماتي .

لقد سبق الإشارة إلي القول بأن المسؤولية الجنائية لم تعد تقتصر على الشخص الطبيعي فقط ، بل أن التشريعات الحديثة أقرت أيضا بمسؤولية الشخص المعنوي ، فماذا عن مسؤولية هذا الأخير في ظل جريمة الغش المعلوماتي ؟

هذا ما سنحاول الإجابة عنه في المطلب الآتي.

المطلب الثاني : المسؤولية الجنائية للشخص المعنوي عن الغش المعلوماتي

يقصد بالشخص المعنوي مجموعة أشخاص وأموال تتمتع بالشخصية القانونية [3] ، وبخصوص إقرار المسؤولية الجزائية للأشخاص المعنوية فإن أغلب التشريعات المقارنة قد

---

(1) : رشدى محمد علي محمد عيد ، المرجع السابق نفسه ، ص. 370 .

(2) : نصت المادة 11 الفقرة الأخيرة من القانون 09 – 04 السالف الذكر على أنه " دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في هذه المادة ، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ، ويعاقب الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50 ألف إلى 500 ألف دج ، ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات " .

(3) : عمر محمد بن يونس ، المرجع السابق ، ص.731 .

إنتهت بعد الصراع الذي دار بين الفقهاء بشأن إقرار هذه المسؤولية من عدمه إلى ضرورة تبنّي القول الذي أخذ بمسؤولية الشخص المعنوي ومن بين هذه التشريعات نجد التشريع الفرنسي في نص المادة 121-2 ق ع ف التي جاء فيها " فيما عدا الدولة ، تسأل الأشخاص المعنوية جنائيا عن الجرائم التي ترتكب لحسابها بواسطة أجهزتها أو ممثليها ، وفقا للقواعد الواردة في المواد 121-4-7 وذلك في الحالات المنصوص عليها في القانون أو اللائحة ومع ذلك فإن المحليات لا تسأل جنائيا إلا عن الجرائم التي ترتكب أثناء مزاولة الأنشطة التي يمكن أن تكون محلا للتفويض في إدارة المرفق العام عن طريق الإتفاق والمسؤولية الجنائية للأشخاص المعنوية لا تستبعد معاقبة الأشخاص الطبيعيين الفاعلين أو الشركاء عن نفس الأفعال " [1] .

أما المشرع الجزائري فقط كرّس المسؤولية الجنائية للشخص المعنوي على إثر تعديل قانون العقوبات بالقانون رقم 04-15 المؤرخ في 10-11-2004 وذلك في نص المادة 51 مكرر منه التي نصت على أنه " باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام ، يكون الشخص المعنوي مسؤول جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك . إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال " [2] .

بناءً على ما سبق يمكن القول بأنه لا يمكن إنكار مساءلة الأشخاص المعنوية عن جرائم الحاسوب التي من بينها الغش المعلوماتي ، ذلك أن تقنية الحاسوب هي تقنية مكلفة وتحتاج إلى رؤوس أموال ضخمة ومثل هذا الأمر لا يمكن القيام به من قبل شخص طبيعي واحد ودون أن يكون هناك تجمع إقتصادي لرؤوس الأموال هذه ، فهو يحتاج بالضرورة إلى صيغة إقتصادية جماعية ليؤدي دوره ممثلة في وجود شخص معنوي لتستمر صناعة هذه التقنية التي بهرت العالم المعاصر ونقلته إلى ثورة المعلومات ومن ثم فإن هذه الأشخاص المعنوية ، في كافة صورها التي عددها القانون مقررا الإعتراف بها ، يمكن أن تلجأ إلى جريمة من الجرائم كالغش المعلوماتي ، تحقيقا لمطامعها وأغراضها ، مشروعة كانت أم غير مشروعة ، لذا وجب اللجوء إلى مساءلتها والعمل على كبح أنشطتها غير المشروعة والإجرامية التي تهدد الكيانات والنظم الإقتصادية للدول والجماعات [3] ، وهذا ما نصت عليه معظم التشريعات حيث نصت المادة 323-6 ق ع فرنسي المتعلقة بالعدوان على نظم المعالجة الآلية للمعطيات على أنه " يمكن إعلان مسؤولية الأشخاص المعنوية جنائيا بالشروط والأوضاع المقررة في المادة 121-2 عن الجرائم المقررة في هذا الفصل " [4] ، أما المشرع الجزائري فهو الآخر وتطبيقا للمسؤولية الجنائية التي أقرها في حق الشخص المعنوي ، نص في القانون رقم 04 - 15 السالف الذكر في إطار المادتين 394 مكرر 4 ، 394 مكرر 6 ، على العقوبات

(1) : http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417204&cidTexte=LEGITEXT000006070719

(2) : المادة 51 مكرر من القانون رقم 04-15 السالف الذكر .

(3) : عمر محمد بن يونس، المرجع السابق ، ص.732 .

(4) : http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417204&cidTexte=LEGITEXT000006070719

المطبقة في حالة إرتكابه جريمة من الجرائم المذكورة في القسم السابع بعنوان المساس بأنظمة المعالجة الآلية للمعطيات .

هذا ولقد نصت المادة 12 من إتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي على مسؤولية الشخص المعنوي عن الجرائم المشار إليها في الإتفاقية والتي من بينها جريمة الغش المعلوماتي بقولها " **1-** يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل إعتبار الأشخاص المعنوية مسؤولة عن الجرائم المشار إليها في الإتفاقية الحالية ، إذا إرتكبت لمصلحتها عن طريق أي شخص طبيعي يتصرف بشكل فردي أو بصفته عضوا في مؤسسة الشخص المعنوي ويمارس سلطة القيادة في داخله وفقا لما يلي : ممارسة سلطة تمثيل الشخص المعنوي ، ممارسة سلطة إتخاذ القرارات بإسم الشخص المعنوي ، ممارسة سلطة الضبط داخل الشخص المعنوي .

2- بالإضافة إلى الحالات المشار إليها في الفقرة 1 ، يجب على كل طرف أن يتخذ الإجراءات الضرورية والهامة من أجل تأكيد مسؤولية الشخص المعنوي في حالة تخلف الإشراف أو الرقابة أو التحكم في الموظف أو المستخدم لدى الشخص الإعتباري ، لأن الفشل في عملية الإشراف يسهل إرتكاب الموظف أو المستخدم لإحدى الجرائم المنصوص عليها في هذه الاتفاقية.

3- مسؤولية الشخص المعنوي يمكن أن تكون مسؤولية جنائية أو مدنية أو إدارية وفقا لقوانين الدول أطراف الإتفاقية .

4- هذه المسؤولية المقررة بالنسبة للشخص المعنوي يجب أن تكون بدون إضرار بالمسؤولية الجنائية للأشخاص الطبيعيين الذين إرتكبوا الجريمة " .

بناءً على ما سبق ذكره فإن البحث في المسؤولية الجزائية للشخص المعنوي سيكون حسب التقسيم التقليدي لهذا الأخير حسبما أرساه الفقه وأقره التشريع ، إلى أشخاص القانون العام وأشخاص القانون الخاص ، فيما يتعلق بمسؤوليتها الجنائية عن جريمة الغش المعلوماتي ، وعليه سيتم التطرق في الفرع الأول لمسؤولية الشخص المعنوي العام عن الغش المعلوماتي ، وفي الفرع الثاني لمسؤولية الشخص المعنوي الخاص عن الغش المعلوماتي .

الفرع الأول : مسؤولية الشخص المعنوي العام عن الغش المعلوماتي

لقد ورد في نص المادة 121 – 1 ق ع فرنسي " فيما عدا الدولة ، تسأل الأشخاص المعنوية جنائيا عن الجرائم التي ترتكب لحسابها ... ومع ذلك فإن المحليات وتجمعاتها لا تسأل جنائيا إلا عن الجرائم التي ترتكب أثناء مزاولة الأنشطة التي يمكن أن تكون محل تفويض في إدارة مرفق عام عن طريق الإتفاق ... " ونصت المادة 51 مكرر ق ع جزائري السالفة الذكر " بإستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام يكون الشخص المعنوي مسؤولا جزئيا " .

من خلال هذه النصوص نلاحظ بأن أشخاص القانون العام في كلا من التشرعين الجزائري والفرنسي لم يتم إخضاعها للمسؤولية الجزائية ، وقد أيّد بعض الفقه وجهة نظر المشرعين في هذا الصدد ، وذلك بعدم إخضاع الدولة للقانون الجنائي وسلطة العقاب وبالتالي المسؤولية الجزائية ككل ، لأنها في نظرهم قائمة على تنظيم شعبها وحماية إقليمها وتحقيق مصالحها ، أما البعض الآخر فيرى أن إستثناء الدولة من قاعدة المسؤولية الجنائية ، لا يمكن قبوله على الإطلاق ، حيث قالوا بأن الدولة تخضع لمساءلة القانون الجنائي في بعض أعمالها [1] ، فإذا كان مرتكب جريمة الغش المعلوماتي موظف حكوميا من أصحاب القرار في مؤسسة وظيفية ذات شخصية معنوية مثل الهيئة والوزارة ، فإنه من غير المنطق في هذه الحالة محاسبة الشخص الطبيعي عن الجريمة التي إرتكبها بإسم الشخص المعنوي ولحسابه ولا يحاسب الشخص المعنوي أو المؤسسة العامة التي إتخذ فيها قرار إرتكاب الجريمة من المسؤول وظيفيا عنها ، وقد دعم هذا الإتجاه موقفه أيضا بالقول أنه في ظل التطور التكنولوجي الحالي لا مانع من أن تسأل الدولة جنائيا على نفس النهج القانوني المقرر بشأن مسؤوليتها الإدارية والمدنية والعقوبة لا تشمل الدولة كسيادة ولكنها تشمل الهيئات أو المؤسسات التي ترتكب الجريمة بإسمها ولحسابها ، هذا ونشير إلى أن هذا النوع من المسؤولية في كلا من القانونين الجزائري والفرنسي لا يستبعد مسؤولية الأشخاص الطبيعيين الفاعلين أو الشركاء ، لأن المشرع لم يرد إعفاء الشخص الطبيعي من تحمل مسؤوليته عن إرتكاب الجريمة وإنّما أراد أن تتعدد بينه وبين الشخص الإعتباري ، كما تعتبر هذه المسؤولية مشروطة [2] ، ومن ثمت فإن الدخول الغير المصرح به أو البقاء بدون وجه مشروع في النظام المعلوماتي من جانب أحد العاملين في إحدى المؤسسات الحكومية أو التلاعب بالبيانات يجب لمساءلة الشخص المعنوي عنه وفقا للمادة 51 مكرر ق ع ج ، والمادتين 394 مكرر 4 394 مكرر 6 السالفتي الذكر ، أن ترتكب الجريمة لحساب الشخص المعنوي وبواسطة أجهزته وممثليه .

الفرع الثاني:مسؤولية الشخص المعنوي الخاص عن الغش المعلوماتي

بجانب الأشخاص المعنوية العامة - التي سبق الحديث عنها - يوجد الأشخاص الإعتباريين الخاصين الذين تسري عليهم أحكام القانون الخاص ، فرغم أن هؤلاء الأشخاص المعنويين يحققون فوائد كبيرة للمجتمع والأفراد على حد سواء. فإن بعضهم يمكن أن يسبب أضرار كبيرة تفوق الأضرار التي يحدثها الإنسان العادي عند إرتكاب الجريمة .

ولقد تبين أن معاقبة الشخص الطبيعي الذي يرتكب الجريمة لحساب الشخص المعنوي وحده دون معاقبة الشخص المعنوي على الجريمة لا يحقق الردع ، مما دفع الكثير من التشريعات المقارنة الحديثة إلى إقرار المسؤولية الجنائية للأشخاص المعنوية الخاصة ، حيث أنه لا يوجد خلاف بشأن هذه المسؤولية ، خصوصا في التشريعات التي أقرت مبدأ المسؤولية الجنائية للأشخاص المعنوية ، إذ أن إدخال تلك المسؤولية في التشريع الجنائي يكون مقرر أصلا للشخص الإعتباري الخاص فهذا الأخير على خلاف الشخص الإعتباري العام ، ليس

(1) : عمر محمد بن يونس ، المرجع السابق ، ص. 736

(2) : رشدي محمد علي عيد ، المرجع السابق ، ص. 390 – 392 .

من أغراضه تحقيق خدمة أو مصلحة عامة ، بل أن هدفه تحقيق المصالح الخاصة به وبالأشخاص الطبيعيين أصحابه [1] .

إنطلاقا مما سبق فإن الشخص الإعتباري الخاص في التشريع الجزائري يخضع للمسؤولية الجزائية بموجب المادة 51 مكرر السالفة الذكر ، أيا كان هدفه سواء كان يهدف إلى كسب الربح ، أو خيريا ، فمثلا تسأل جزائيا الشركات التجارية والتجمعات ذات المصلحة الإقتصادية ، سواء كانت تابعة للقطاع العام ، كالمؤسسات العمومية الإقتصادية . أو تابعة للقطاع الخاص ، كما تسأل الشركات المدنية والجمعيات ذات الطابع السياسي كالأحزاب السياسية أو ذات الطابع الاجتماعي أو الثقافي أو الرياضي [2] .

بناءً على ما سبق فالشخص المعنوي الخاص في حالة إرتكابه لصورة من صّور الغش المعلوماتي المنصوص عليها في التشريع الجزائري ، كتّلاعب إحدى الشركات التجارية ببيانات ومعطيات داخل نظام معلوماتي لشركة تجارية أخرى منافسة مثلا أيا كان القصد من وراء ذلك ، يسمح بمساءلة هذه الشركة جزائيا باعتبارها شخص معنوي خاص ومن ثم توقيع العقوبات الواردة في إطار المساس بأنظمة المعالجة الآلية للمعطيات ، التي سيأتي الحديث عنها في المطلب الآتي .

المطلب الثالث : الجزاء الجنائي لجريمة الغش المعلوماتي

من أهم التوصيات التي أسفرت عنها الدراسات التي ناقشت جرائم الإعتداء على نظم المعالجة الآلية للمعطيات التي من بينها الغش المعلوماتي هي ضرورة وجود جزاء قانوني رادع يتم تعميمه على كل من يشارك في إرتكاب هذا النوع من الجرائم ، وتنبع أهمية العقوبة من كونها تشكل الإطار التنظيمي الوقائي الرادع [3] ، فتكريس عقوبات رادعة يجعل التفكير في إرتكاب صورة من صّور الغش المعلوماتي أمر في غاية الصعوبة ولهذا أشارت المذكرة التفسيرية لإتفاقية بودابست على ضرورة أن يكون كل فعل مجرّم تم النص عليه في هذه الإتفاقية مستحق لجزاءات جزائية التي يجب أن تكون فعالة وملائمة ورادعة ، وذلك للحيلولة دون حدوث نتائج خطيرة وهو ما أقرته بموجب المادة 13 بعنوان الجزاءات والإجراءات وإدراكا لأهمية هذه المسألة فضلا عن إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام ألحق المشرع الجزائري تعديلا على القسم السابع مكرر من قانون العقوبات المتضمن المساس بنظم المعالجة الآلية للمعطيات وذلك بموجب القانون رقم 06 - 23 المؤرخ في 20 ديسمبر 2006 ومسّ به تشديد عقوبة الغرامة دون المساس

(1) : رشدي محمد علي عيد ، المرجع السابق نفسه ، ص. 393 ، 394 .

(2) : أحسن بوسفيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص. 273 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 314 .

بالنصوص التجريمية الواردة في هذا القسم .

وإلى جانب المشرع الجزائري نجد المشرع الفرنسي هو الآخر قام بتعديل قانون العقوبات وذلك بموجب القانون رقم 2004 - 575 المؤرخ في 21 جوان 2004 والمتعلقة بالثقة بالإقتصاد الرقمي حيث مسّ هذا التعديل القسم الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، وذلك بتشديد عقوبة الحبس والغرامة المقررة لهذه الأفعال وذلك بموجب المادة 45 الفصل الثاني منه [1] .

ومن هنا نخلص إلى أن العقوبة تمثل آلية قانونية ردعية إعتمدها المشرع الجزائري وغيره من التشريعات الجزائية المقارنة في سبيل الحماية من وقوع جرائم لو وقعت لسبّبت خسائر إقتصادية فادحة [2] .

وهذه العقوبات المقررة في حق الجاني الذي يرتكب جريمة الغش المعلوماتي هي عقوبات أصلية وتكميلية كما أنها مقررة في حق الشخص الطبيعي والشخص المعنوي وعليه سيتم التطرق في الفرع الأول للعقوبات المقررة للشخص الطبيعي ، وفي الفرع الثاني للعقوبات المقررة للشخص المعنوي .

الفرع الأول : العقوبات المطبقة على الشخص الطبيعي

تنص المادة 394 مكرر على أنه : " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50,000 إلى 100,000 كل من يدخل أو يبقى عن طريق الغش.... وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة ، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50,000 إلى 150,000 دج " .

أما المادة 394 مكرر 1 فقد نصت على ما يلي " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500,000 إلى 2,000,000 دج كل من أدخل بطريق الغش معطيات في نظام . " ، من خلال هذه النصوص نلاحظ أن المشرع الجزائري قد وضع تدرج فيما يتعلق بالعقوبات الأصلية ، إذ أن هذا التدرج يعكس الخطورة الإجرامية لهذا النوع من الجرائم وبهذا يكون المشرع قد وضع سلم يتضمن ثلاث درجات نجد في الدرجة الأولى صورة الدخول أو البقاء بالغش وهذه قرر لها المشرع عقوبة الحبس كما هو الوارد في المادة

(1) : JORF n°138 du 16 juin 2004 page 10719

أنظر الموقع : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000617671&dateTexte=&categorieLien=id

(2) : رشيدة بوكر ، المرجع السابق ، ص. 314 ، 315 .

من ثلاثة أشهر إلى سنة وغرامة من 50 ألف إلى 100 ألف ، وفي الدرجة الثانية نجد الدخول والبقاء في صورتها المشددة حيث قرر لها عقوبة مشددة إذا ترتب عن هذه الأفعال حذف أو تغير لمعطيات المنظومة ونص على عقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50 ألف إلى 150 ألف دج إذا ترتب على الدخول أو البقاء تخريب لنظام إشتغال المنظومة ، وفي الدرجة الأخيرة نجد العقوبة الخاصة بجريمة التلاعب بالمعطيات ، وقرر لها عقوبة الحبس من ستة أشهر إلى ثلاث سنوات [1] .

وأما عن العقوبات التكميلية المطبقة على الشخص الطبيعي فقد تضمنتها المادة 394 مكرر 6 بقولها " مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها " [2] .

فمن خلال هذا النص يتضح أن المشرع قد قرر عقوبتين تطبق في حال إرتكاب إحدى صور الغش المعلوماتي وهما المصادرة والغلق ، وفيما يلي توضيح لكلا العقوبتين :

البند الأول : المصادرة

عرفتها المادة 15 المعدلة بالقانون رقم 06 - 23 على أنها " الأيلولة النهائية إلى الدولة لمال أو مجموعة من أموال معينة أو ما يعادل قيمتها عند الاقتضاء " [3] ، وبالرجوع إلى نص المادة 394 مكرر 6 السالفة الذكر يلاحظ أن المصادرة إنّما هي عقوبة وجوبية لأنها لم تترك الخيار للقاضي بين الحكم بها كما في العقوبات الأصلية والمشددة للجريمة وكذلك لأن الهدف من هذه العقوبة هو الحد من تلك الجرائم ، فأصحاب الأجهزة والوسائل عندما يعلمون مسبقا بأنه سوف تتم المصادرة لكل الأجهزة والوسائل التي ترتكب بها الجريمة بالإضافة إلى العقوبات الأصلية التي ستوقع عليهم ، فإن ذلك سيكون مانع من الإقدام على إرتكاب الجرائم ولتطبيق عقوبة المصادرة فإنه يتطلب توافر بعض الشروط منها :

- يجب أن تكون عقوبة المصادرة تابعة لعقوبة أصلية من العقوبات المنصوص عليها في القانون وهي الحبس أو الغرامة .
- أن تتم مصادرة الأجهزة والوسائل التي إستخدمت في إرتكاب الجريمة مهما كانت تلك الوسائل تقليدية أو معلوماتية ، ولا يشترط أن تكون الوسائل والأجهزة التي يتم

---

(1) : سوير سفيان ، المرجع السابق ، ص. 98 .

(2) : المادة 394 مكرر 6 من القانون رقم 04 – 15 ، السالف الذكر .

(3) : المادة 15 من القانون رقم 06 – 23، المؤرخ في 20 ديسمبر 2006 ، المتضمن قانون العقوبات المعدل والمتمم، ج ر: العدد 84،الصادرة في 24 ديسمبر 2006،ص. 16 .

مصادرتها كعقوبة تكميلية محددة على سبيل الحصر وإنما تطبق العقوبة على أية وسيلة كانت ويجب أن تكون الأشياء التي يحكم بمصادرتها قد تم ضبطها من قبل الجهات المختصة .

- يجب أن لا تمدد عقوبة المصادرة إلى حقوق الغير الحسن النية ، وهذا القيد نابع من طبيعة العقوبة كونها عقوبة شخصية يجب أن لا تطال الغير الحسن النية [1] .

البند الثاني : عقوبة الغلق

نصت المادة 394 مكرر 6 على عقوبة الغلق إلى جانب عقوبة المصادرة كعقوبتين تكميليتين ، يعاقب بهما كل من إرتكب جريمة من جرائم المساس بالأنظمة المنصوص عليها في القانون ، وتشمل غلق المواقع التي إستخدمت في إرتكاب جريمة من جرائم المعلوماتية المنصوص عليها في القسم السابع مكرر ق ع ج ، وكذلك غلق المحلات أو أماكن الإستغلال التي إرتكبت فيها تلك الجرائم ، إذا إرتكبت بعلم مالكها ، وعليه إذا إنتفى علم مالك المحل أو مكان الإستغلال فلا تطبق العقوبة ، وعقوبة الغلق مثلها مثل عقوبة المصادرة لا تقع في مواجهة الغير حسن النية [2] .

الفرع الثاني : العقوبات المطبقة على الشخص المعنوي

لقد سبقت الإشارة إلى أن المشرع الجزائري قد أقر بالمسؤولية الجزائية للشخص المعنوي ، وقد عنّون الباب المخصص لها بالعقوبات المطبقة على الأشخاص المعنوية [3] ، حيث عددت المادة 18 مكرر ق ع ج مجموعة العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح وإلى جانب هذه العقوبات نجد العقوبات المطبقة عليه في مجال الغش المعلوماتي بموجب المادة 394 مكرر 4 .

وبهذا يمكن القول بأن العقوبات التي تطبق على الشخص المعنوي نوعان ، منها العقوبات التي وردت في قانون العقوبات بشكل عام ، ومنها عقوبات وردت في قانون العقوبات بنصوص خاصة بجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي [4] ، ومما سبق سيتم التطرق في البنود التالية إلى ما يلي :

البند الأول : عقوبات الجرائم المرتكبة من الشخص المعنوي بشكل عام

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 172 .

(2) : فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 173 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 336 .

(4) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 99 .

تضمنت هذه العقوبات المادة 18 مكرر السالفة الذكر ، وهي تتعلق بالعقوبات المطبقة على الشخص المعنوي في حالة إرتكابه جناية أو جنحة منصوص عليها في القانون وهي تتمثل في:

- العقوبة الأصلية : وتشمل عقوبة الغرامة من مرّة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة .

- العقوبات التكميلية : ومنها على سبيل المثال حل الشخص المعنوي ، نشر الحكم وتعليقه الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات [1] .

البند الثاني : عقوبة الشخص المعنوي في مجال الغش المعلوماتي

إن العقوبة التي نصت عليها المادة 394 مكرر 4 هي عقوبة الغرامة والتي حددها المشرع بحد واحد فلم يترك للقاضي الحق في تفريد العقوبة بين حد أدنى وحدا أقصى كما جاء في المادة 18 مكرر ق ع ج . بل أن القاضي مقيد بتطبيق حد واحد للغرامة وهي تساوي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وبذلك تكون عقوبات الشخص المعنوي في مجال الغش المعلوماتي كما يلي:

أولا : عقوبة الدخول أو البقاء في صورتها العادية

تكون عقوبة جريمة الدخول والبقاء المرتكبة من قبل الشخص المعنوي هي الغرامة خمسة أضعاف عقوبة الجريمة المرتكبة من قبل الشخص الطبيعي فتكون من (250,000=5*50,000) ، مائتين وخمسين ألف دينار ، إلى (100,000 * 5 = 500,000) خمسمائة ألف دينار جزائري.

ثانيا : عقوبة الدخول أو البقاء في صورتها المشددة

تختلف في هذه الحالة بحسب النتيجة المترتبة على الدخول والبقاء ، إذا نتج عن الدخول أو البقاء حذف أو تغير لمعطيات النظام تكون العقوبة من (500,000=5*2*50,000) خمسمائة ألف إلى (1,000,000=5*2*100,000) أي مليون دج ، أما إذا نتج عن الدخول أو

(1) : المادة 18 مكرر من القانون رقم 06 – 23 ، السالف الذكر .

البقاء تخريب نظام إشتغال النظام ففي هذه الحالة تكون العقوبة من (50,000*5=250,000) مائتان وخمسين ألف إلى (150,000*5=750,000) سبعمائة وخمسين ألف دج .

ثالثا : عقوبة التلاعب بالمعطيات

تكون عقوبة التّلاعب بالمعطيات سواء بإدخال معطيات عن طريق الغش إلى نظام المعالجة الآلية للمعطيات ، أم بالحذف أم التعديل للمعطيات التي يتضمنها النظام من (500,000*5=2,500,000) مليونين ونصف إلى (2,000,000*5=10,000,000) عشرة ملايين [1] .

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 100 .

الفصل الثاني

القواعد الإجرائية

لجريمة الغش المعلوماتي

إن البعد الإجرائي لجرائم الكمبيوتر أو جرائم الإعتداء على نظم المعالجة الآلية للمعطيات التي من بينها جريمة الغش المعلوماتي تنطوي على تحديات ومشكلات جمّة ، نبعت من طبيعة هذه الجرائم المتعلقة بعناصرها ووسائل إرتكابها ، التي دفعت بالمشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرائية ذلك أن طبيعة هذا النوع من الإجرام جعل أو بالكاد قانون الإجراءات الجزائية في صورته المعاصرة أو المعروفة في مأزق حقيقي .

فمن هذا المنطلق لجأ المشرع الجزائري إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 [1] ، حيث إستحدث إجراءات جديدة تتلاءم وطبيعة الجرائم المستحدثة ، ولعل أهم هذه الإجراءات التي تهمّنا في الجريمة محل الدراسة ، إجراء التسرب وإجراء إعتراض المراسلات السلكية واللاسلكية .

هذا ولم يكتفي المشرع الجزائري بإجراء هذا التعديل على قانون الإجراءات الجزائية لمعالجة هذا النوع الحديث من الإجرام ، وإنما قام بإصدار قانون مستقل هو القانون رقم 09 – 04 السالف الذكر ، إذ ألحت الحاجة إلى تكريس إطار قانوني أكثر ملائمة وإنسجاما مع خصوصية وخطورة جرائم الإعتداء على نظم المعالجة بصفة عامة وجريمة الغش المعلوماتي بصفة خاصة ، حيث يتضمن القواعد الوقائية التي تسمح بالرصد المبكر للإعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها [2] ، ولعل أهم هذه القواعد مراقبة الإتصالات الإلكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية.

إن جملة هذه الأفكار ستتم معالجتها من خلال المبحثين التاليين ، الأول نتطرق فيه لإجراءات مواجهة جريمة الغش المعلوماتي في قانون الإجراءات الجزائية والثاني نتناول فيه إجراءات مواجهة جريمة الغش المعلوماتي في ظل القانون رقم 09 – 04 .

المبحث الأول : إجراءات مواجهة جريمة الغش المعلوماتي في قانون الإجراءات الجزائية

(1) : القانون رقم 06 – 22 المؤرخ في 20 ديسمبر 2006 ، يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 جويلية 1966 ، المتضمن قانون الاجراءات الجزائية ، ج ر : العدد 84 ، الصادرة بتاريخ 24 ديسمبر 2006.

(2) : رشيدة بوكر ، المرجع السابق ، ص. 366 .

لقد أجمع مشرعي القانون الوضعي في مختلف دول العالم على جسامة جريمة الغش المعلوماتي والتهديدات التي يمكن أن تنشأ عن إستخدام الحاسب الآلي ، فدفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما أثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الجانب الإجرائي [1] .

والمشرع الجزائري كما سبقت الإشارة بادر إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06 – 22 السالف الذكر ، ومن أهم الإجراءات المستحدثة ضمن هذا القانون لمواجهة جريمة الغش المعلوماتي ، إجراء التسرب الذي نتطرق له في المطلب الأول وإجراء إعتراض المراسلات السلكية واللاسلكية الذي نعالجه من خلال المطلب الثاني .

المطلب الأول : إجراء التسرب في جريمة الغش المعلوماتي

يعتبر التسرب من بين المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته لمكافحة الجرائم المستحدثة ، من بينها جرائم الإعتداء على نظم المعالجة الآلية التي من بينها جريمة الغش المعلوماتي [2] . وقد كان ذلك بموجب الفصل الخامس بعنوان – في التسرب – من القانون رقم 06 – 22 السالف الذكر ، حيث تم تنظيم هذا الإجراء وفق ثمانية مواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 [3] ، فمن خلال التعديل الذي أجراه المشرع الجزائري نلاحظ بأن هذه التعديلات قد منحت لقاضي التحقيق صلاحيات جديدة لم يكن يتمتع بها من قبل وذلك لمواجهة هذا النوع من الجرائم نظرا لخطورتها ولطبيعتها الخاصة ، كذلك وّسع المشرع بموجب هذا التعديل من إختصاص ضباط الشرطة القضائية في حالة ما إذا كان التحقيق التمهيدي الذي يتم إجراءه يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، حيث أصبح ضباط الشرطة القضائية يتمتع بإختصاصات أوسع في سبيل تسهيل إجراءات البحث والتحري عن هذه الجريمة وكشف مرتكبيها وجمع الإستدلالات عنها . بما يمكنه من مجابهة الصّعاب التي قد تعترضه إعتبارا لخطورة هذه الجريمة [4] . ونظرا لكون التسرب إجراء مستحدث في مجال التحريات والتحقيقات ونظرا لما يكتسيه من خطورة على حريات وحقوق الإنسان فإن المشرع الجزائري قد وضع له ضوابط تجعله يقع ضمن الأطر القانونية المرسومة له [5] ، وعليه سنحاول من خلال الفروع الآتية بيان كيفية تطبيق هذا الإجراء في جريمة الغش المعلوماتي ، وذلك بالإعتماد على النصوص القانونية الواردة في هذا الإطار ، حيث سيتم توضيح مفهوم التسرب في الفرع الأول ، وشروط صحة عملية التسرب في الفرع الثاني ، وآثار التسرب في الفرع الثالث .

---

(1) : أسامة سمير حسين ، الاحتيال الالكتروني ، الوجه القبيح للتكنولوجيا ، الطبعة الأولى ، الجنادرية للنشر والتوزيع ، 2011 ، ص. 105 .

(2) : رشيدة بوكر ، المرجع السابق ، ص. 433 .

(3) : الفصل الخامس بعنوان في التسرب المواد من 65 مكرر 11 إلى المادة 65 مكرر 18 من القانون 06 ، 22 السالف الذكر ، ص. 9 ، 10 .

(4) : محمد حزيط ، مذكرات في قانون الاجراءات الجزائية الجزائري ، الطبعة السادسة ، دار الهومة ، الجزائر ، 2012 ، ص. 132 .

(5) : زيبحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، بدون طبعة ، دار الهدى للطباعة والنشر والتوزيع ، الجزائر ، 2011 ، ص. 169 .

الفرع الأول : تعريف التسّرب

لقد عرفت المادة 65 مكرر 12 من القانون 06 – 22 السالف الذكر ، التسّرب على أنه " قيام ضابط عون الشرطة القضائية ، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف .

يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض ، هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على إرتكاب الجرائم " .

فمن خلال هذا التعريف يلاحظ بأن عملية التسّرب هي في الغالب عملية معقّدة تتطلب أن يدخل العون المكلف بالعملية في إتصال بالأشخاص المعنيين ويربط معهم علاقات ضيقة ويحافظ على السّر المهني لغاية تحقيق الهدف النهائي من العملية ، وهي تتطلب على الخصوص المشاركة المباشرة في نشاط الخلية التي تسرب إليها والذي يكون أحيانا ضرورة لقبوله [1] .

كما نلاحظ من خلال التعريف السابق بأن المشرع الجزائري قد أتاح لمأموري الضبط إستخدام الإسم الوهمي أو المستّعار تحت مسمّى التسّرب متى إستدعت ضرورة التّحري والتحقيق ذلك في جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ما دامت من بين الجرائم التي وردت في إطار نص المادة 65 مكرر 5 التي نصت على أنه " إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الجرائم المتعلقة بالصّرف وكذا جرائم الفساد ... " .

وبهذا يكون المقصود من التسّرب هو مراقبة الأشخاص المشتبه بإرتكابهم جريمة الغش المعلوماتي ، بحيث يسمح لمن يقوم بالمراقبة ضابط الشرطة القضائية أو عون يعمل تحت رقابته إتخاذ إسم وهمي أو مغاير بغرض ضبط الجريمة وفي هذه الحالة يكون التخفي تحت إسم وهمي أو مستعار عملا مشروعا بموجب القانون [2] .

ويمكن تصّور عملية التسّرب في نطاق جرائم الإعتداء على نظم المعالجة الآلية بصفة عامة وجريمة الغش المعلوماتي بصفة خاصة ، من خلال دخول ضابط أو عون الشرطة القضائية إلى العالم الإفتراضي ، وإشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والإتصال المباشر في كيفية قيام أحدهم بإختراق شبكات أو بث الفيروسات مستخدما في ذلك

---

(1): رشيدة بوكر ، المرجع السابق ، ص. 434 .

(2) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 262 .

أسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سّعيا منه للإستفادة منهم حول كيفية إقتحام الهاكر مثلا لموقع ما [1] ، فعملية التسرب يمكن أن تتم من خلال الأنترنت وللإشارة فإن عملية التسرب تتم بعد إرتكاب الجريمة [2] .

بعد أن تم بيان تعريف التسرب ، وجب التطرق إلى شروط صحته وذلك حتى يكون هذا الإجراء واقع ضمن الإطار الشرعي والقانوني الذي حدّده المشرع وهو ما ستتم معالجته في الفرع الثاني .

الفرع الثاني : شروط صحة عملية التسرب

لقد نص المشرع على جملة من الشروط يمكن إستخلاصها من المواد القانونية المنظمة لإجراء التسّرب ، وذلك ضمانا لصحة عملية التسرب ، فهذا الأخير ممارسته غير مألوفة لضباط أو عون الشرطة القضائية كما أنه من أخطر الإجراءات إنتهاكا لحرمة الحياة الخاصة للمتهم ، لذلك نجد أن المشرع قد أحاطه بجملة من الضمانات يتعين مراعاتها [3] ، عندما تقتضي ضرورات التحقيق أو التحري ذلك في جريمة الغش المعلوماتي ، والشروط التي أتى بها المشرع الجزائري هي على نوعين يمكن إيجازها وتوضيحها فيما يلي :

البند الأول : الشروط الشكلية

تطبيقا لمبدأ الشرعية الجنائية وضمانا لحقوق وحريات المتهم ، نجد جملة من الشروط الشكلية التي أوردها القانون لضمان صحة عملية التسّرب هي :

أولا : صدوره بإذن قضائي : وهذا ما نصت عليه المادة 65 مكرر 11 ق إ ج بقولها " ... يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب .... " [4] ، ومن ثم فإن عملية التسرب لا يجوز قانونا مباشرتها إلا بموجب إذن قضائي من وكيل الجمهورية أو من قاضي التحقيق بعد إخطار وكيل الجمهورية وذلك تحت طائلة البطلان [5] ، وذلك حماية للحقوق الأساسية المكرسة دستوريا ، وعليه لا يمكن بأي حال من الأحوال أن يقوم ضابط الشرطة القضائية بالعملية بمفرده دون المرور على الجهاز القضائي [6].

---

(1) و (3) : رشيدة بوكر ، المرجع السابق ، ص. 435 .

(4) : فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 291 .

(4) : المادة 65 مكرر 11 من القانون رقم 06 – 22 السالف الذكر .

(5) : محمد حزيط ، المرجع السابق ، ص. 72 .

(6) : رشيدة بوكر ، المرجع السابق ، ص. 435 .

ثانيا : أن يكون مكتوبا : حيث نصت المادة 65 مكرر 15 على أنه " يجب أن يكون الإذن المسلّم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان " [1] ، ذلك أن الأصل في العمل الإجرائي الكتابة والتدوين وإذا صدر في إطار الإنابة القضائية ينبغي مراعاة الشروط الشكلية والموضوعية للإنابة القضائية التي نصت عليها المادتين 138 ، 139 ق إ ج [2] .

هذا ولقد نصت المادة 65 مكرر 15 السالفة الذكر على ضرورة أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهي في محل الدراسة جريمة الغش المعلوماتي كما يجب ذكر هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته .

ثالثا : المدة المطلوبة لعملية التسّرب : ولقد تضمنتها المادة 65 مكرر 3/15 ق إ ج بقولها " ... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر ، ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل إنقضاء المدة المحددة " .

رابعا : إبقاء الإذن بالتسّرب خارج ملف الإجراءات إلي غاية الإنتهاء من العملية : وذلك حفاظا على السرّية المطلوبة التي حصرها المشرع بين القاضي الآمر بها - وكيل الجمهورية وقاضي التحقيق - وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب .

خامسا : وجود تقرير مسبق محرر من طرف الضابط عن الجريمة : بشكل مفصل لإطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها [3] ، وهذا ما نصت عليه المادة 65 مكرر 13 بقولها " يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم ..." [4] ، وتطبيقا لذلك يكون ضابط الشرطة القضائية في في جريمة الغش المعلوماتي ملزما بأن يحرر تقرير يتضمن كافة العناصر الضرورية لمعاينة هذه الجريمة .

البند الثاني : الشروط الموضوعية

يمكن إيجاز الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري في شرطين أساسيين : الأول يتمثل في تحديد نوع الجريمة والتي يجب ألا تخرج

---

(1) : المادة 65 مكرر 15 من القانون رقم 06 – 22 السالف الذكر .

(2) : المادتين 138 ، 139 من الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 ، المتضمن قانون الإجراءات الجزائية ، المعدل والمتمم ، ج ر : 48 ، ص. 238 .

(3) : رشيدة بوكر ، المرجع السابق نفسه ، ص. 436 .

(4) : المادة 65 مكرر 13 من القانون 06 – 22 السالف الذكر .

عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 5 وهي جرائم المخدرات الجريمة المنظمة العابرة للحدود الوطنية ، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، جرائم تبيض الأموال أو الإرهاب ، الجرائم المتعلقة بالتشريع الخاص بالصّرف جرائم الفساد ، وبهذا يكون المشرع الجزائري قد جعل من جريمة الغش المعلوماتي التي هي جزء من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، إحدى أهم الأسباب الموضوعية التي تبرر اللجوء لعملية التسرب .

أما الشرط الموضوعي الثاني فهو أن يكون الإذن بالتسرب مسّببا ، فمن خلال التسبيب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للّجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن لذلك فكان لزاما عند إصدار الإذن بالتسّرب سواء من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية [1] .

الفرع الثالث : آثار التسرب

بعد صدور الإذن بالتسرب من طرف القضاء وفقا لما نص عليه المشرع قانونا يباشر العون المتسرب عمله حسب المقتضيات المطلوبة منه ومن ثم هناك آثار ستترتب على ذلك يمكن إجمالها في النقاط التالية :

البند الأول : تسخير الوسائل المادية والقانونية

وهذا الأثر نصت عليه المادة 65 مكرر 14 [2] ، وبالتالي يمكن للعون المتسرب إستعمال الأموال المتحصل عليها من إرتكاب جريمة الغش المعلوماتي ، كون هذه الجريمة تدخل في إطار الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي أشارت لها المادة 65 مكرر 5 ، ومن ثم يمكن للمتسرب تسخير الوسائل المادية لفائدة الخلية الإجرامية ، أما بخصوص الوسائل القانونية فإن معناها ينصرف إلى توفير الوثائق الرسمية إن كان هناك ضرورة لذلك كإستخراج بطاقة تعريف ، أو رخصة السياقة وبالتالي يحتاج إلى جهاز خاص لتزويد الوثائق الرسمية دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة .

---

(1) : سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، قسم الحقوق ، جامعة الحاج لخضر ،باتنة ، 2012 – 2013 ،ص. 176 .

(2) : نصت المادة 65 مكرر 14 من القانون 06 ، 22 السالف الذكر على أنه " يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض ، دون أن يكونوا مسؤولين جزائيا ، القيام بما يأتي :

- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في إرتكابها .
- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني والمالي وكذا وسائل النقل أو التخزين أو الايواء أو الحفظ أو الاتصال " .

البند الثاني : الإعفاء من المسؤولية

وهي نتيجة للأثر السابق ، كون قيام بالأفعال المشار إليها في نص المادة 65 مكرر 14 تستوجب من القائمين بها مشاركة إيجابية كحيازة متحصلات الجريمة أو وسائل إرتكابها وهذا الصنف من الأفعال يوجب المسؤولية الجزائية [1] ، وإدراكا من المشرع لهذا الوضع قام بإعفائهم صراحة من هذه المسؤولية ، وقد مدد نطاق هذا الإعفاء لظروف أمنية للمتسرب حتى بعد إنقضاء المهلة المحددة في رخصة التسرب ، وفي حالة عدم تمديدها أو في حالة تقرير وقف العملية ، بشرط ألا يتجاوز ذلك مدة أربعة أشهر سواء من تاريخ إنقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخص بإجرائها وهذا ما نصت عليه المادة 65 مكرر 17 ق إ ج [2] .

البند الثالث : إحاطة عملية التسّرب بالسّرية التامة

وذلك لتحقيق الأهداف المتوخاة منها من جهة ، ولحماية العون من جهة أخرى ، هذه الحماية التي لم تقتصر على شخصه فقط بل مددها المشرع الجزائري ، إلى أفراد عائلته كزوجه أو أبناءه أو أصوله المباشرين ، وبصفة عامة يمكن في هذا الإطار الإشارة إلى نص المادة 65 مكرر 16 التي نصت على أنه " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات ، يعاقب كل من يكشف هوية ضابط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50,000 دج إلى 200,000 دج .

وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 200,000 دج إلى 500,000 دج " ، هذا ولم يكتفي المشرع بنص المادة 65 مكرر 16 ، بل نص أيضا في المادة 65 مكرر 18 ق إ ج على أنه " يجوز سماع ضابط الشرطة القضائية الذي تجرى عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية " . وبهذا يمنع سماع الضابط المتسرب ويجوز سماع الضابط المشرف على العملية بوصفه شاهدا [3] .

إن المشرع الجزائري لم يكتفي بموجب التعديل الذي أجراه على قانون الإجراءات الجزائية بالنص على إجراء التسرب كما تم التطرق إليه في المطلب السابق ، وإنما نص كذلك

---

(1) : المادة 65 مكرر 17 من القانون 06 – 22 السالف الذكر .

(2) : رشيدة بوكر ، المرجع السابق ، ص. 437 ، 438 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 440 .

على إجراء آخر هو إعتراض المراسلات السلكية واللاسلكية الذي سيتم الحديث عنه في المطلب الآتي.

المطلب الثاني : إجراء إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي

من بين الإجراءات التي نص عليها القانون رقم 06 -22 السالف الذكر إجراء إعتراض المراسلات السلكية واللاسلكية ، حيث خصص المشرع الجزائري لهذا الإجراء الفصل الرابع تحت عنوان – في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور – وقد ضمنه ستة مواد من المادة 65 مكرر 5 إلى المادة 65 مكرر 10 [1] .

فبالرجوع لنص المادة 65 مكرر 5 نجد أن القانون الجزائري قد تميز بأنه أتاح لضابط الشرطة القضائية الحق في إعتراض وتسجيل المحادثات وإلتقاط الصّور ، وذلك في حالة ما إذا إقتضت ضرورة التحري ذلك في إحدى الجرائم الواردة بهذه المادة التي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي نجد من ضمنها جريمة الغش المعلوماتي [2] .

وبهذا يكون المشرع الجزائري من خلال هذا التعديل يهدف إلى تحقيق التوازن بين حق الفرد في الخصوصية والسرّية وحق المجتمع في التصّدي للجريمة لتحقيق الأمن والسلامة لهذا الإنسان ، والمشرع الجزائري في هذا الإطار لم يكن منفردا بهذا المنحنى بل سبقته التشريعات الأكثر تطوّرا ومنها التشريع الفرنسي ، فقد نصت المواد 80 ، 81 ق إ ج ف [3] على أنه لقاضي التحقيق إتخاذ الإجراءات التي يرى منها فائدة في الوصول إلى الحقيقة ولفائدة التحقيق وكرس القانون الفرنسي الصادر سنة 1991 فكرة إعتراض المراسلات والإتصالات بما فيها الممتدة عن طريق الشبكة المعلوماتية [4] .

بناءً على ما سبق وبالإعتماد على النصوص القانونية المنظمة لإجراء إعتراض المراسلات السلكية واللاسلكية ، سيتم فيما يلي التطرق إلى بيان المقصود بهذا الإجراء في الفرع الأول وكذا ما مدى مراعاة السّرية في إعتراض المراسلات السلكية واللاسلكية في الفرع الثاني ، إلى جانب الضمانات المقررة للقيام بهذا الإجراء في الفرع الثالث .

---

(1) : رشيدة بوكر ، المرجع السابق نفسه ، ص. 441 .

(2) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 295 .

(3) : أنظر الموقع :

http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575441&dateTexte&categorieLien=cid

(4) : زيبحة زيدان ، المرجع السابق ، ص. 158 .

الفرع الأول : مفهوم إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي

من خلال نص المادة 65 مكرر 5 ق السالفة الذكر يمكن القول بأن المقصود بإعتراض المراسلات إعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والإستقبال والعرض ، كما تم تعريف المراسلات في إجتماع لجنة الخبراء للبرلمان الأوربي بستراسبورغ بتاريخ 6 / 10 / 2006 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية على أنها " عملية مراقبة سّرية للمراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في إرتكاب الجرائم " [1] .

وللإشارة فقد عرف القانون الجنائي الفيدرالي الأمريكي الإتصالات السلكية في المادة (Title 18 , Part 1 , Chapter 119 , sec 2510) بأنها " نقل للكلمات المنطوقة بصفة كلية أو بصفة جزئية من خلال إستعمال معدات لنقل الإتصالات عن طريق أسلاك أو كوابل أو أي وسيلة أخرى مشابهة بين نقطة الإتصال الأصلية ونقطة الإستقبال بما فيها إستعمال هذه الوسائل في محطة تحويل الإتصالات والتي يتم تقديمها أو تشغيلها من جانب شخص يعمل في تقديم أو تشغيل هذه المعدات لنقل هذه الإتصالات بين الولايات أو مع الخارج أو يقدم خدمة الإتصالات التي تؤثر في التجارة داخل الدولة أو التجارة الخارجية ، وهذا ما أكدت عليه المحاكم الأمريكية حيث قضت بأن الأصل في الإتصال أن يكون إتصالا إلكترونيا إذا لم يكن محمولا بواسطة الموجات الصوتية ولا يتضمن إتصالات إنسانيا ومن هنا يمكن القول بأن كل إتصالات الأنترنت بما فيها البريد الإلكتروني تعتبر إتصالات إلكترونية [2] .

وقد عرف القانون الأمريكي الإعتراض بقوله أن كلمة " يعترض " تعني الحصول على محتوى الإتصال السلكي أو الإلكتروني أو الشفوي وذلك بإستعمال أي وسيلة إلكترونية أو ميكانيكية أو أي وسيلة أخرى [3] .

هذا ويعتبر البريد الإلكتروني من أهم الوسائل الحديثة للإتصال في مجال الأنترنت وهو الأكثر إستخداما في هذا المجال نظرا لما يتسم به من سرعة ويسر في الإستخدام ، بل ويمكن القول بأن البريد الإلكتروني أضحى مجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة ودون عائق ، وهو ما فتئ يشكل طبقة من المواطنين المنتمين لمختلف دول العالم ، يتميزون بظهور وعي سياسي جديد يتجاوز المجالات البلاغية المستهلكة ، وعلى هذا الأساس

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 441 ، 442 .

(2) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 247 ، 248 .

(3) : شيماء عبد الغني محمد عطا الله ، المرجع السابق نفسه ، ص. 251 .

فإن أهمية البريد الإلكتروني تجعله عرضة لأعمال القرصنة وإصطياد كلمة المرور وإعتراض محتواه من قبل المنحرفين ومجرمي المعلوماتية ، فالبريد الإلكتروني والذي هو بمثابة نظام للتراسل بإستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم،ولا يمكن الدخول إليه إلا عن طريق كلمة المرور ومن ثم فهو يتمتع بالحماية القانونية [1] ، كون أن صاحب البريد الإلكتروني يتمتع بالحق في الحياة الخاصة بالنسبة للمعلومات المتواجدة داخل البريد الإلكتروني بجهاز الكمبيوتر الخاص به ، حيث إتجه القضاء في هذا الصدد إلى إقامة التماثل بين مراسلات البريد الإلكتروني والمراسلات التي تتم عن طريق البريد العادي ، وبناءً عليه لا يجوز التدخل للإطلاع على البريد الإلكتروني دون إذن صاحبه ما لم يصدر إذن قضائي بذلك تطبيقا لذلك قضي بعدم مشروعية الدليل في قضية MAXWELL في الولايات المتحدة الأمريكية بالنسبة للمتهم MAXWELL الذي كان يحوز صورا فادحة خاصة بالأطفال الأمر الذي يعاقب عليه القانون الأمريكي لأن رجال الضبط القضائي لجأوا إلى مزود الخدمات الخاص بهذا المتهم لكي يساعدهم على الدخول إلى بريده الإلكتروني والتعرف على ما يحوزه من تلك الصور ومعرفة من يتعامل معهم في هذه الصّور وذلك دون سبق الحصول على إذن قضائي بذلك [2] .

الفرع الثاني : السّرية في إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي

إن العمليات المنصوص عليها في المادة 65 مكرر 5 والتي تتمثل في إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية ، وضع الترتيبات التقّنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وتسجيل الكلام المتفوه به بصفة خاصة أو سّرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو إلتقاط صّور لشخص أو عدة أشخاص يتواجدون في مكان خاص ؛ تتطلب عدم المساس بالسّر المهني المنصوص عليه في المادة 45 ق إ ج التي نصت على أنه " ... غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم بكتمان السّر المهني أن تتخذ جميع التدابير اللازمة لضمان إحترام ذلك السّر ... " ، وهذا ما جاء به نص المادة 65 مكرر 6 ق إ ج التي نصت على أنه " تتم العمليات المحددة في المادة 65 مكرر 5 أعلاه دون المساس بالسّر المهني المنصوص عليه في المادة 45 من هذا

(1) : زيحة زيدان ، المرجع السابق ، ص. 159 .

(2) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 261 .

القانون ..." [1] ، ومن ثم وجب إتخاذ التدابير اللازمة لضمان إحترام ذلك السّر حتى ولو تعلق الأمر بجريمة الغش المعلوماتي.

ذلك أنه في التشريع الجزائري وبشأن إعتراض المراسلات لا توجد نصوص قانونية في التشريع الجزائي تشير إلى الأماكن والأشخاص الذين لا يجوز إتخاذ هذه الإجراءات في شأنهم ، فمن الأماكن على سبيل المثال التي يشغلها أشخاص ملزمون بكتمان السّر المهني مكتب المحامي وذلك بموجب المادة 80 من القانون رقم 91 – 04 المتعلق بتنظيم مهنة المحاماة [2] ، وبالنسبة للأشخاص فإنه لا يوجد أشخاص مستثنون لكن نظرا لصّفاتهم فإن القيام بهذه العمليات التقّنية تتطلب إجراءات خاصة مثل أعضاء الحكومة وقضاة المحكمة العليا الوّلاة ومنه فإن تلك الأماكن وهؤلاء الأشخاص غير مستثنين من الإجراءات الخاصة للتحري وإنما يقتضي الأمر وجوب مراعاة طابع السّر وتعامل خاص مع تلك الأماكن وهؤلاء الأشخاص [3].

الفرع الثالث : الضمانات المقررة لإعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي

مما لا شك فيه أن أسلوب إعتراض المراسلات السّلكية واللاّسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بنظام المعالجة الآلية التي من بينها الغش المعلوماتي ، فهو من جانب آخر يمثل إنتهاكا لحرمة الحياة الخاصة للأفراد وإعتداء على سّرية مراسلاتهم وإتصالاتهم التي كفلتها الدساتير والتشريعات العقابية [2] ، فمن المسّتقر عليه أنه لا يجوز دخول المساكن بغير سبق الحصول على إذن بذلك من سلطة التحقيق ، ويقترب الأمر في ذلك بالنسبة للدخول إلى البيانات الموجودة في داخل النظام ، غير أن مفهوم الدخول إلى النظام يختلف عن الدخول إلى المساكن ، فالدخول إلى النظّام يتم عن طريق تشغيل الجهاز عن قرب أو بعد أو الدخول إلى البيانات الموجودة في جهاز يعمل بالفعل وذلك بإستعمال برنامج خاص بذلك ، وتطبيقا لذلك قضي في الولايات المتحدة الأمريكية بأن التعديل الرابع للدستور الأمريكي الذي يحمي الحق في الخصّوصية يحمي البيانات المعالجة آليا من التداخل إليها عن بعد ، مقيما التماثل بين الإقتحام المادي للمنازل والإقتحام المعنوي للمعلومات ، هذا وينسحب التعديل الرابع للدستور الأمريكي على البريد الإلكتروني ويشمله بالحماية [3] .

---

(1) : المادة 65 مكرر 5 والمادة 45 والمادة 65 مكرر 6 من القانون رقم 06 . 22 السالف الذكر .

(2) : المادة 80 من القانون رقم 91 / 04 المؤرخ في 8 جانفي 1991 ، المتضمن تنظيم مهنة المحاماة ، ج ر : العدد 02 الصادرة بتاريخ 9 جانفي 1991 ، ص. 29 .

(3) و (2) : رشيدة بوكر ، المرجع السابق ، ص. 443 .

(3) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 241 .

(4) : شيماء عبد الغني محمد عطا الله ، المرجع السابق نفسه ، ص. 242 .

ولقد عنيت الإتفاقية الأوربية في مجال جرائم الأنترنت بالنّص على ضرورة إحترام حقوق الإنسان في مجال الإجراءات الجنائية التي تتخذ عند وقوع جريمة من جرائم الأنترنت فقد نصت على ذلك صراحة المادة 15 منها وقد أشارت هذه الإتفاقية إلى أنه من بين الضمانات ، الضمانة القضائية أو السلطة المحايدة وإلى وجود أسباب معقولة تبرر الإجراءات الجنائية الماسّة بالحقوق الفردية وإلى ضرورة تحديد محل تلك الإجراءات وتحديد المدة ومضمون تلك الإجراءات [4] .

والمشرع الجزائري على غرار باقي تشريعات العالم يسّعى إلى وضع الضمانات القانونية اللاّزمة التي تبيح ممارسة إجراء إعتراض المراسلات السّلكية واللاّسلكية ، ضمن الأطر القانونية التي تبيح مباشرته في إطار مكافحة جريمة الغش المعلوماتي كإجراء مشروع وتمنع تعسّف السلطات العامة وتصّون الحرية الفردية.

هذه الضمانات يمكن تصنيفها إلى ضمانات موضوعية وأخرى شكلية نتطرق لها فيما يلي :

أولا : الضمانات الموضوعية

ويمكن حصّرها في ضمانتين الأولى تتعلق بالجرائم التي يجوز فيها الإعتراض وهي بموجب المادة 65 مكرر 5 السّالفة الذكر سبعة جرائم ، من بينها الجرائم الماسة بأنظمة المعالجة الآلية ، التي من بينها جريمة الغش المعلوماتي ، حيث نجد أن المشرع الجزائري قد أدرك عدم كفاية الوسائل التقليدية لجمع الدليل التقّني نظرا لما تتمتع به هذه الجريمة المستحدثة من خصوصية .

أما بالنسبة للضمانة الثانية فهي تتعلق بفائدة الإعتراض في إظهار الحقيقة ، ذلك أن التشريعات المعاصرة تقرر بأن ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السّند الشرعي المبرر للإعتراض ، كون هذا الإجراء يتضمن إعتداء جسيم كما سبقت الإشارة على حرمة الحياة الخاصة وسّرية الإتصالات ، فيباح إستثناء في حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة [1] .

ثانيا : الضمانات الشكلية

وهي الأخرى يمكن إجمالها في ضمانتين الأولى تتعلق بترخيص السلطة القضائية ومراقبتها والثانية تتعلق بتحديد طبيعة المراسلة ومدة الإعتراض ، فبالنسبة للأولى يمكن القول

(1) : رشيدة بوكر ، المرجع السابق ، ص. 444

بأن ترخيص السلطة القضائية ومراقبتها أمر ضروري ولازم لمشروعية إعتراض المراسلات السلكية واللاسلكية في القانون الجزائري ، وطبقا للمادة 65 مكرر 5 السالفة الذكر ، لا يمكن لضباط الشرطة القضائية اللّجوء إلى هذا الإجراء إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي ، وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الترخيص أو الإذن تقدير فائدة الإجراء وجدّيته وملاءمته لسّير الدعوى بعد الإطلاع على معطيات التّحريات التي قامت بها مصالح الضبطية القضائية مسبقا [1] .

وللإشارة فإن القانون الأمريكي ألزم هو الآخر بضرورة أن يصدر إذن من القاضي المختص بناءً على طلب أحد أعضاء النيابة ممّن حددهم القانون الأمريكي بالموافقة على طلب تسجيل المحادثات الإلكترونية الذي يقدمه رجال الضبط القضائي وقد حدد القانون الأمريكي الجرائم التي يجوز فيها إستصدار إذن بتسجيل الإتصالات ، ومن أهمها الجرائم المعاقب عليها بالإعدام أو الحبس لمدة تزيد عن سنة واحدة .

وبهذا نصل إلى أن أغلب التشريعات المقارنة تقر مشروعية إعتراض المراسلات السّلكية واللاّسلكية بناءً على إذن من السلطة المختصة لتجميع الأدلة عن جريمة معينة متى كان ذلك ضروريا لظهور الحقيقة ، والجدير بالذكر أن المحكمة الأوربية لحقوق الإنسان أجازت هذا الإجراء تطبيقا للمادة 08 من الاتفاقية الأوربية لحقوق الإنسان بإعتبار أن له ما يبرره في مجتمع ديمقراطي وما دام أنه محاط بالضمانات القانونية اللاّزمة [2] ، وقد نصت المادة 65 مكرر 9 على أن عملية تنفيذ إجراء إعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف قاضي التحقيق المختّص بإعداد محضرا عن كل عملية إعتراض للمراسلات وكذا عن عمليات وضع التّرتيبات التّقنية لهذا الغرض ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والإنتهاء منها [3] .

أما بالنسبة للضمانة الثانية والتي تتعلق بتّحديد طبيعة المراسلة ومدة الإعتراض ، فهي ضمانة يمكن إستنتاجها من خلال ما ورد ذكره صراحة في نص المادة 65 مكرر 7 [4]، التي نصّت على أنه يجب أن يتّضمن الإذن بإعتراض المراسلات كل العناصر التي تسّمح بالتّعرف على الإتصالات أو المراسلات المطلوب إعتراضها ، كما أن المشرع الجزائري قد إستوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السّلطة مصدرة

---

(1): رشيدة بوكر ، المرجع السابق ، ص. 445 .

(2) : شيماء عبد الغني محمد عطا الله ، المرجع السابق ، ص. 252 – 255 .

(3) و (4): المادتين 65 مكرر 9 و 65 مكرر 7 من القانون 06 – 22 السالف الذكر .

الإذن وفقا لمقتّضيات التّحري والتحقيق وهي نفس المدة التي حددها المشرع الفرنسي في المادة 100 ق إ ج فرنسي [1] .

المبحث الثاني : القواعد الإجرائية لجريمة الغش المعلوماتي في ظل القانون رقم 09 – 04

إن إصدار المشرع الجزائري للقانون رقم 09 – 04 قد أرسّى قواعد إجرائية جديدة تخضع لها السّلطة القضائية وأعوانها تطبيقا لمبدأ الشّرعية الذي يّعد حجر الزاوية في الإجراءات القانونية لتحقيق في الجرائم المرتكبة ومتّابعة فاعليها وتوقيع العقوبة المناسبة لهم هذه الإجراءات الجديدة التي يستطيع رجال الضبط القضائي من خلالها ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية والتي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية التي أرساها قانون الإجراءات الجزائية [2] .

وعليه سنحاول من خلال هذا المبحث التطرق إلى أهم الإجراءات التي جاء بها هذا القانون ، حيث سيتم التطرق إلى إجراء المراقبة الإلكترونية في المطلب الأول وكذا التفتيش المعلوماتي أو تفتيش المنظومة المعلوماتية في المطلب الثاني إلى جانب إجراء الضبط أو حجز المعطيات المعلوماتية في المطلب الثالث .

المطلب الأول :مراقبة الإتّصالات الإلكترونية في جريمة الغش المعلوماتي.

لقد سبق القول أن جرائم الإعتداء على نظم المعالجة بصّفة عامة وجريمة الغّش المعلوماتي بصفة خاصة ، تتسم بالغموض حيث يصعب إثباتها فالتّحري عنها والتحقيق فيها ينطوي على العديد من المشكلات والتحدّيات الإدارية والقانونية والتي ابتداءً من عملية ملاّحقة الجّناة فإن تحققت مكنة الملاحقة أصبحت الإدانة صّعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصّعوبة الوصول إلى الأدلة أو لغياب الإعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة [3] .

ومن هنا ظهرت الحاجة إلى تكريس إطار قانوني أكثر ملائمة وإنسجاما مع خصوصية وخطورة جرائم الإعتداء على النّظم ، ينظم القواعد الوقائية التي تسمح بالرّصد المبكر

---

(1) : سعيداني نعيم ، المرجع السابق ، ص. 181 .

(2) : أحمد مسعود مريم ، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون 09 – 04 ، مذكرة لنيل شهادة الماجستير ، قسم الحقوق ، جامعة قاصدي مرجاح ، ورقلة ، ص. 66 .

(3) : رشدى محمد علي محمد عيد ، المرجع السابق ، ص. 55 .

للإعتداءات المحتّملة والتدّخل السّريع لتحديد مصدرها والتّعرف على مرتكبيها [1] ، حيث إستحدث المشرع بموجب القانون رقم 09 – 04 السالف الذكر ، إجراء المراقبة الإلكتّرونية بموجب المادة الثالثة منه حين أجاز تّبعا لمستلزمات التّحريات والتّحقيقات القضائية الجارية في إطار هذا النوع من الجرائم اللّجوء إلى وضع تّرتيبات تّقنية لمراقبة الإتصالات الإلكترونية وتّجميع وتّسجيل محتواها [2] ، وقد شملت على نوعين من الرقابة الأولى وقائية غرضها الوقاية من الجرائم الخطرة المتعلقة بتّكنولوجيا الإعلام والإتصال ، والثانية غرضها ضبطي وقضائي وتشمل حالتين : الأولى لمقتضيات التّحريات والتّحقيقات القضائية عندما يكون من الصّعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تلك المراقبة والثانية في إطار طلبات المساعدة القضائية الدولية المتبادلة [3] .

ولمزيد من التفصيل بشأن المراقبة الإلكترونية ، نتطرق في الفرع الأول إلى بيان المقصود منها وفي الفرع الثاني نتناول مشروعية مراقبة الإتصالات الإلكترونية ، وفي الفرع الثالث نبين مدى حظر مراقبة الإتصالات الإلكترونية الخاصة .

الفرع الأول : المقصود بمراقبة الإتّصالات الإلكترونية

إن المراقبة الإلكترونية جملة مركبة من كلمة المراقبة ، والتي تعني مراقبة أنشطة الأشخاص أو مجموعة الأمكنة وعلى كل حال فإن التكنولوجيا الحديثة للمعلوماتية قدمت نطاقا جديدا لتطبيق الرقابة ، أما الإتّصالات الإلكترونية فقد عرفها المشرع الجزائري بأنها " تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صّور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية " وهذا حسب المادة الثانية من القانون 09 – 04 السالف الذكر.

أمّا بالنسبة لمراقبة الإتصالات الإلكترونية كإجراء فإن المشرع الجزائري لم يعرفها وهذا على غرار العديد من المشرعين ولكن بعض التّشريعات عرفته مثل التشريع الأمريكي والكندي ، فقد عرفها المشرع الأمريكي بأنها " عملية الإستماع لمحتويات أسلاك أو أي إتصالات شّفوية عن طريق إستخدام جهاز إلكتروني أو أي جهاز آخر " ، بحسب ما جاءت به المادة 2510 – 4 من القانون الفيدرالي الأمريكي لسنة 1968 [4] ، أمّا من النّاحية الفقهية فقد تصّدى الفقه إلى هذه المهمّة حيث أوجد عدّة تعريفات بشأنها ، حيث عرفت على أنها " إجراء تحقيق يباشر خلسة ، وينتهك سّرية الأحاديث الخاصة تأمر به الشرطة القضائية في الشّكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ، ويتضمن

(1) : رشيدة بوكر ، المرجع السابق ، ص. 366 .

(2) : سعيداني نعيم ، المرجع السابق ، ص. 183 .

(3) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 360 ، 361 .

(4) : أحمد مسعود مريم ، المرجع السابق ، ص. 79 .

من ناحية إستراق السّمع إلى الحديث ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك " ، وعرفت أيضا على أنها " إجراء خاص يتم بإشراف قضائي بحسب الحالات " [1] .

ومن التعريفات الفقهية التي تبين لنا وسائل وطرق المراقبة الإلكترونية ، نجد أنها قد عرفت على أنها " تّقنية تقوم على تّدخل وسطي لتحويل مسار في خط مشترك بواسطة ممغنطة ، من أجل تسجيل المحادثة وهي تمثل فائدة أكيدة لفعّالية المتّابعة الجزائية " ، وعرفت أيضا على أنها " العمل الذي يقوم به المراقب بإستخدام التّقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر " ، فالملاحظ من خلال هذه التعريفات أن التّقنية المسّتخدمة في هذه المراقبة هي التّقنية الإلكترونية [2] ، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيّانات الدّاخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة [3] .

الفرع الثاني : مشروعية مراقبة الإتّصالات الإلكترونية

يعتبر تكريس المشرع الجزائري لإجراء المراقبة الإلكترونية خطوة جريئة منه ، على إعتبار أن هذا الإجراء يّعد من أخطر الإجراءات في إطار النّظام الإجرائي عبر العالم الإفتراضي يّمس مباشرة بخصوصيات الإنسان ، وذلك بالرغم من أن البعض من الفّقه يرى بأن المراقبة لا تزال محل نظر في القانون من حيث ضرورة الإلتزام بما هو مقرر في القوانين والضّمانات الدستورية للحق في الخصوصيّة [4] ، لذلك نجده قد أحاط هذه المراقبة ببعض الضمّانات القانونية الفعّالة التي تّعد أمر ضروري لحماية الحّرية الفردية ولحماية حق الإنسان في سّرية إتصالاته ، هذه الضمانات التي سيتم التطرق لها من خلال ما يلي :

البند الأول : شروط اللّجوء للمراقبة الإلكترونية

نذكر من هذه الشّروط أن يتّم تّنفيذ هذا الإجراء تحت سّلطة القضاء وبإذن من قبله وخلاله وبعده وهو ما كرسته المادة 04 من القانون 09 – 04 السّالف الذكر بقولها " لا يجوز إجراء عمليات المراقبة ... إلا بإذن مكتوب من السّلطة القضائية المختّصة " ، كذلك هناك شرط آخر مفاده أن تكون هناك ضرورة تّتطلب هذا الإجراء وتّتحقق هذه الضرورة عندما يكون من الصّعب الوصول إلى نتّيجة تّهم مجريّات التّحريات أو التّحقيق دون اللّجوء إلى المراقبة الإلكترونية وهو ما أكد عليه المشرع الجزائري في الفقرة جـ من نفس المادة [5] ،

---

(1) : أحمد مسعود مريم ، المرجع السابق ، ص. 81 .

(2) : نص المشرع الجزائري على وضع الترتيبات التقنية لمراقبة الإتصالات الإلكترونية من خلال نص المادة 03 من القانون 09 – 04 السالف الذكر .

(3) : سعيداني نعيم ، المرجع السابق ، ص. 183 .

(4) : سعيداني نعيم ، المرجع السابق نفسه ، ص. 184 .

(5) : سعيداني نعيم ، المرجع السابق ، ص. 185 .

فمن خلال هذه الشروط نلاحظ أن المشرع الجزائري قد نظم مراقبة الإتّصالات الإلكترونية بقانون واضح يشمل جميع الضّمانات التي تمنع تعسّف القائمين عليها ، مما يترتب عليه القول بأن عدم المحافظة على هذه الضمانات من قبل السّلطات والهيئات التي تباشر إجراء المراقبة يعرض عملها لجزاء البطلان ومن ثّم إستبعاد الدليل المستّمد من هذا الإجراء [1] ، أضّف إلى ذلك أن إستخدام المعطّيات المتّحصل عليها جراء هذه المراقبة خارج الحدود الضرورية للتّحريات يعرض صاحبها للمسؤولية الجزائية وفقا لما جاء في المادة 09 من القانون 09 – 04 السّالف الذكر التي نصّت على أنه " تّحت طائلة العقوبات المنصوص عليها في التّشريع المعمول به ، لا يجوز إستعمال المعلومات المتّحصل عليها عن طريق عمّليات المراقبة المنصوص عليها في هذا القانون ، إلاّ في الحدود الضرورية للتّحريات أو التّحقيقات القضائية " .

البند الثاني : الهيئات أو السلطات التي تباشر المراقبة الإلكترونية .

لقد طرح تساؤل عمّا إذا كانت الجرائم المعلوماتية بصّفة عامة وجريمة الغش المعلوماتي بصّفة خاصّة تّتطلب سلطات أو هيئات أو أشخاص يتّمتعون بقدر كاف من المعرفة التّكنولوجية لوسائل الإعلام والإتّصال أم أنه يمكن للسّلطات الحالية متّابعة مجرمي المعلوماتّية ومساءلتهم بما لديهم من أساليب تّقليدية في البحث والتّحري وتقديم أدلة تثبت إدانتهم ؟

إجابة عن هذا السؤال يمكن القول بأن إرتباط الجريمة المعلوماتية بتطور تكنولوجيا الإعلام والإتصال يستدعي إمكانيات وخبرات تقنية لا يمكن مواكبتها إلا بإنشاء هيئات ومراكز متخصصة لمكافحة الجرائم المتصلة بها ، وبتجنيد العاملين في قطاع العدالة عن طريق التكوين المتخصص الذي يهدف إلى توسيع معارفهم بتلك التكنولوجيات [2] .

هذا وبالرجوع للتشريع الجزائري نجد أن المشرع الوطني قد نص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته ، حيث خصص لها في إطار القانون 09 – 04 السالف الذكر مادتين ، الأولى رقم 13 التي نصت على أنه " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته ، تحدد تشكيلة الهيئة وتنظيمها وكيفيات تسيرها عن طريق التنظيم " أما الثانية فهي رقم 14 التي حددت مهام هذه الهيئة [3] .

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 377 .

(2) : أحمد مسعود مريم ، المرجع السابق ، ص. 44 .

(3) : تنص المادة 14 من القانون 09 – 04 السالف الذكر على أنه " تتولى الهيئة المذكورة في المادة 13 أعلاه ، خصوصا المهام الآتية :

أ- تنشيط وتنسيق عمليات الوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته .

ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز

هذه الهيئة التي نص عليها المشرع لم تجسد على أرض الواقع بعد ، مما أدى بالسياسة الوطنية إلى إنشاء على مستوى جهاز الشرطة المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر ومخبرين جهويّن بكل من قسنطينة ووهران ، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي ، كما يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية بالتنسيق مع هذه المخابر ، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية بالإضافة إلى مركز الوقاية من جرائم الإعلام والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني الذي هو قيّد الإنشاء [1] .

بناءً على ما سبق يمكن القول أنه بالإضافة إلى السّعي السياسة الوطنية إلى تطوير تأهيل جهاز الضبط القضائي لجعل مهامه يتلاءم وطبيعة جريمة الغش المعلوماتي ، نص المشرع الجزائري على أنه من بين مهام الهيئة الوطنية لمكافحة الجرائم الإعلام والإتصال ومكافحته مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذا النوع من الجرائم ، وهذا ما أشارت إليه الفقرة ب من المادة 04 السالفة الذكر،مما يدل دلالة واضحة على أن الأشخاص الذين لهم الحق في القيام بعملية المراقبة هم ضباط الشرطة القضائية إلى جانب الضباط المنتمون للهيئة في إنتظار تنصيبها .

الفرع الثالث : حظر مراقبة الإتصالات الإلكترونية الخاصة

إن مراقبة الأحاديث والإتصالات الخاصة تمس بحق الإنسان في الخصوصية ، هذا الحق الذي حظى بحماية دستورية في مختلف التشريعات الدستورية والقانونية ، من بين هذه التشريعات الدستور الجزائري الذي كفل حماية الحقوق والحريات الفردية في الفصل الرابع في المواد 35 ، 36 ، 39 ، 40 [2] ، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا ، والحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة ، أضحى في الوقت الحالي تحت تهديد وسائل تنصت حديثة هذه الوسائل التي لم تعد تقتصر على وسائل التنصت على الإتصالات السلكية أو اللاسلكية فحسب ، بل إمتدت بقدرتها الفائقة إلى إلتقاط الإتصالات التي تتم بطريق الأنترنت مما أفقد الإنسان أكثر حريته وخصوصيته .

وهو ما أيقض الدافع لدى المشرع بسن نصوص قانونية تعمل على توفير قدر كبير من الحماية الجزائية على سرية الإتصالات الخاصة للأفراد ، حيث عاقب على إعتراض

الخبرات القضائية .

ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم " .

(1) : سعيداني نعيم ، المرجع السابق ، ص. 107 .

(2) : المرسوم الرئاسي رقم 96– 438 المؤرخ في 07 ديسمبر 1996،المتعلق بإصدار نص تعديل الدستور، المصادق عليه في إستفتاء 28 نوفمبر 1996،ج ر:العدد 76، ص.11.

الإتصالات دون إذن بذلك بموجب المادة 303 مكرر من القانون رقم 06 – 23 السالف الذكر [1] .

وبخصوص هذه المادة يرى بعض الفقهاء أنها تخص المحادثات الخاصة أو التي تتم في مكان خاص والتي تتم عن طريق خط تلفوني ، دون المحادثات التي تتم عن طريق الوسائل الإلكترونية والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية ، إلا أن هذا الرأي مهما كانت مبرراته التي يقوم عليها ، قيل بأنه لا يمكن القبول به ، بسبب أن المشرع لم يحدد وسيلة نقل المحادثات أو تسجيلها إن كانت بخط تلفوني ، أو كانت وفق البريد الإلكتروني أو غرف الدردشة ، بل إستخدم مصطلحات عامة ومرنة تشمل صور الإعتداء على الحياة الخاصة بمختلف التقنيات [2] .

هذا ولم يقتصر المشرع الجزائري في إطار مسايرته للإجرام الحديث الذي من بينه الغش المعلوماتي على إجراء المراقبة الإلكترونية ، بل إستحدث أيضا إجراء التفتيش المعلوماتي لمسايرة هذا التطور على الرغم من أن هذا الإجراء له قواعده ضمن قانون الإجراءات الجزائية في إطار ما يصطلح عليه بالجرائم التقليدية .

المطلب الثاني : التفتيش في جريمة الغش المعلوماتي

يعرف التفتيش بوجه عام بأنه عبارة عن " إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة " وعرفه البعض الآخر بأنه " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون " [3] .

وذهب آخرون إلى إعتباره " إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجريمة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه " ، فمن خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة ، حيث أن طبيعة الإجراءات المتخذة بشأنه مادية تتمثل في الإنتقال والدخول إلى المكان المراد تفتيشه .

---

(1) : نصت المادة 303 مكرر على انه " يعاقب بالحبس من 6 أشهر إلى ثلاث سنوات وبغرامة من 50,000 إلى 300,000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك :

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

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

(2) : رشيدة بوكر ، المرجع السابق ، ص. 372 - 373 .

(3) : خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، الاسكندرية ، 2009 ، ص. 182 .

ومن هنا ذهب جانب من الفقه إلى القول بأنه إذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش ، أما إذا كانت الجريمة واقعة على برامج الكمبيوتر وبياناته ، فإن الصعوبات تبرز ، وبالرجوع للجريمة محل الدراسة – الغش المعلوماتي – والتي تستلزم أن يقع التفتيش على المكونات المادية والمعنوية للحاسب الآلي ، لضبط أدلتها وبالتالي إدانة مرتكبها فإن المشرع الجزائري قد ساير تطور هذه الجريمة المستحدثة وذلك عندما نص على إجراءات التفتيش التي تتناسب وطبيعتها وذلك في القانون رقم 09 -04 السالف الذكر [1] .

وقبل التطرق إلى مدى خضوع المكونات المادية واللآمادية لنظام المعالجة الآلية للتفتيش ، وإلى تفتيش المنظومة المعلوماتية عن بعد أو ما يصطلح عليه بالتفتيش عن بعد نشير أولا إلى أهم الصعوبات التي تعترض التفتيش في البيئة الإفتراضية ، ذلك أن الأمر في الكثير من الأحيان يتطلب الولوج في البيئة الإفتراضية بحثا عن الدليل وكشف مرتكب هذه الجريمة وتعقبه ، حيث ذهب البعض من الفقه إلى القول بأن التفتيش في هذه البيئة يكون في كثير من الأحيان غير مجدي لما يكتنفه من صعوبات أثناء تنفيذه خاصة إذا ما كان محل البحث هو الشبكة المعلوماتية ، ونجمل هذه الصعوبات التي تواجه خاصة الدول النامية في النقاط التالية :

- إن القضاء في الدول النامية لا يكترث بالدليل الرقمي ، ولا يعول عليه كثيرا لإفتقاره إلى المصداقية التي تجعله جدير بالثقة ، ولعل السبب في ذلك يرجع لعدم تطور هذه الدول في المجال المعلوماتي والتكنولوجي [2] .
- كما يثير تفتيش الشبكة المعلوماتية أمر في غاية الصعوبة يتعلق بسيادة الدول ، كون التفتيش في البيئة الإفتراضية يمكن أن يقع خارج حدود الدول وبالتالي لا بد من الحصول على إذن مسبق بذلك من سلطاتها .
- تواجه أجهزة البحث والتحري في البيئة المعلوماتية في الدول النامية مشكل نقص الدورات التدريبية ، بشأن إستراتجية التحقيق والإستدلال عن هذا النوع من الجرائم ، وما يزيد هذا المشكل تعقيدا إحجام المجني عليهم عن الإبلاغ عنها [3] .

كان هذا العرض لأهم الصعوبات في مجال العالم الإفتراضي بخصوص التفتيش الأمر الذي يتضح من خلاله أن جريمة الغش المعلوماتي وعلى غرار باقي جرائم المعلوماتية، يمكن أن تصادف هذه الصعوبات ، على إعتبار أن إجراء التفتيش بشأنها سوف ينصب على مكونات الحاسب الآلي المادية واللآمادية وكذا شبكاته المعلوماتية ، وعليه سنحاول من خلال الفرع

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 307 .

(2) : موسى مسعود أرحومة ، " الإشكاليات التي تثيرها الجريمة المعلوماتية عبر الوطنية " ، المؤتمر المغاربي الأول حول المعلوماتية والقانون ، جامعة قاريونس ، طرابلس ، يومي 28 ، 29 أكتوبر 2009 ، ص. 05 .

(3) : موسي مسعود أرحومة ، المرجع السابق ، ص. 06 .

الأول بيان نطاق تفتيش مكونات الحاسب الآلي في جريمة الغش المعلوماتي ، وفي الفرع الثاني نتطرق لتفتيش المنظومة المعلوماتية عن بعد في هذه الجريمة ، أما الفرع الثالث فستتم فيه معالجة شروط وضمانات التفتيش في جريمة الغش المعلوماتي .

الفرع الأول : نطاق تفتيش مكونات الحاسب الآلي في جريمة الغش المعلوماتي

يتكون الحاسب الآلي من مكونات مادية وغير مادية أي معنوية ، فبالنسبة للنوع الأول من هذه المكونات يمكن القول بأنها جميع المكونات المادية الملموسة ، اللازمة لعمله وإشتغاله بوجه يحقق وظيفته ويؤدي الغرض المطلوب منه ، ومن حيث الأصل يؤدي نظام المعالجة الآلية ثلاثة عمليات رئيسية هي : الإدخال ، المعالجة والتخزين ، والإخراج ، وتبعا لهذه العمليات تنقسم أجزاء نظام المعالجة الآلية إلى ثلاث أقسام رئيسية كما يلي [1] :

- **وحدات الإدخال :** وهي مجموعة الوحدات المسؤولة عن إيصال البيانات للحاسوب فتقوم بإستقبال البيانات المدخلة إلى الحاسوب وتمريرها داخل الجهاز إلى وحدة الذاكرة للتخزين ، ومن أجهزة الإدخال لوحة المفاتيح ، الفأرة ، مشغل الأقراص [2] .
- **وحدة المعالجة المركزية :** وتعتبر بمثابة العقل المفكر والمسيطر على باقي الوحدات المكونة لنظام المعالجة الآلية بحيث تعمل هذه الوحدة على تنفيذ جميع العمليات الخاصة بالتشغيل وعمليات المقارنة المنطقية والعمليات الحسابية الموجودة في البرنامج تنفيذه من وإلى الوحدات المساعدة مع ضمان تحرك المعلومات من وإلى الذاكرة الرئيسية [3] ، ومن أهم مكونات هذه الوحدة الذاكرة ووحدة الحساب والمنطق ووحدة التحكم .
- **وحدة الإخراج :** وهي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات ومن أهم هذه الوسائل الشاشة والطابعة .... [4] .

أما بالنسبة للنوع الثاني من مكونات الحاسب الآلي أو نظام المعالجة الآلية ، فهي تلك المكونات الغير المادية أو كما يصطلح على تسميتها بالبرامج أو البرمجيات أو الكيان المنطقي والتي تعرف على أنها مجموعة البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات وبهذا يكون يشمل الكيان المنطقي على جميع العناصر الغير المادية اللازمة لتشغيل الكيان المادي [5] .

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 58 .

(2) : على جبار الحسيناوي ، جرائم الحاسوب والأنترنت ، دار اليازوري العلمية للنشر والتوزيع ، الطبعة العربية ، عمان ، 2009 ، ص. 03 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 59 .

(4) : خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، المرجع السابق ، ص. 21 .

(5) : على جبار الحسيناوي ، المرجع السابق ، ص. 25 .

فهذه الصورة الموجزة عن المكونات المادية والغير المادية للحاسب الآلي تساعد على إعطاء فكرة واضحة عن طريقة التفتيش في هذه المكونات ، وإن كان تفتيش النوع الأول من هذه المكونات لا يثير أي مشكلات تعيق القيام به ، مثلها مثل أي مكونات مادية أخرى يتم تفتيشها بالطرق التقليدية وبموجب النصوص الإجرائية التقليدية ، بخلاف النوع الثاني الذي يثير تفتيشه مشكلات نظرا لطبيعتها المنطقية وكذلك طبيعة إجراءات التفتيش التي هي من نفس الطبيعة المعنوية [1] ، وعليه فسيتم التطرق فيما يلي إلى :

البند الأول : تفتيش مكونات الحاسب الآلي المادية

ليس هناك خلاف حول تفتيش المكونات المادية للكمبيوتر بحثا عن شيء يتصل بجريمة وقعت كالغش المعلوماتي محل الدراسة ، يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش،بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات ، هل هو من الأماكن العامة أو من الأماكن الخاصة ؟ ، حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش ، فإذا كانت موجودة في مكان خاص كمسكن المتهم وأحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا،أما لو وجد شخص يحمل مكونات الكمبيوتر المادية أو كان مسيطرا عليها أو حائز لها في مكان ما من الأماكن العامة سواء كانت بطبيعتها أو كانت عامة بالتخصيص فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال [2] .

فمن التشريعات الوطنية التي تجيز تطبيق القواعد التقليدية على تفتيش مكونات الحاسوب المادية ، القانون الجزائري ، حيث تضمن هذا الأخير نصوص قانونية – سواء تعلقت بالتحري أم التحقيق أم المحاكمة – تنطبق من حيث الأصل على تفتيش المكونات المادية للحاسوب بهدف كشف الجريمة وتجميع الأدلة ، ومن أمثلة هذه النصوص القانونية المادة 44 ق إ ج حيث تضمنت هذه المادة تفتيش الحاسوب الآلي بصورة صريحة من خلال النص على خضوع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لإجراءات التحري والتحقيق في حالة التلبس وإن تطلبت شرط الإذن بذلك من وكيل الجمهورية أو قاضي التحقيق [3] ، حيث جاء في نص المادة ما يلي " لا يجوز لضابط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهروا أنهم ساهموا في جناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بأذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب إستظهار هذا الإذن قبل الدخول إلى المنزل أو

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 307 .

(2) : خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، المرجع السابق ، ص. 195 ، 196 .

(3) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 309 .

الشروع في التفتيش ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادة 37 و 40 من هذا القانون " .

كما يمكن في هذا الإطار الإشارة إلى نص المادة 42 ق إ ج التي أوجبت على ضابط الشرطة القضائية في حالة الإبلاغ بجناية في حالة تلبس ضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة ففي مثل هذه الحالة يجوز تفتيش حاسوب المتهم إذا كان في ذلك التفتيش فائدة في كشف الجريمة ، وللإشارة فإن أجهزة العدالة المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو إستثنائية يمكنها القيام بتفتيش المكونات المادية للحاسوب في جريمة الغش المعلوماتي ، دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية مثلها مثل غيرها من المكونات المادية الأخرى .

وبناءً على ما سبق فإن تفتيش الأدوات المادية لجهاز الكمبيوتر مثل لوحة المفاتيح أو الفأرة أو الشاشة وغيرها من الأشياء المادية الملموسة وكذلك البصمات الموجودة عليها لا تدخل ضمن المشاكل الإجرائية التي تعيق إجراء التفتيش إذ بالإمكان تطبيق النصوص التقليدية وبهذا فإن أجهزة الكمبيوتر التي يراد تفتيشها تخضع للقواعد التي تخضع لها الأدوات المادية الأخرى ، فإن كانت في مسكن كما في المثال السابق فإنه ينطبق عليها ما ينطبق على تفتيش المساكن والتي من بينها مراعاة وقت التفتيش والإذن بالتفتيش والأشخاص القائمين على التفتيش والأشخاص المطلوب حضورهم ومراعاة الإختصاص المكاني [1] ، ومن النصوص القانونية التي يمكن تطبيقها في هذا المجال نص المادة 64 ق إ ج والمواد من 44 إلى 47 ق إ ج [2] .

البند الثاني : تفتيش مكونات الحاسب الآلي اللامادية

قد يرد التفتيش وما في حكمه على الجانب الغير المادي لمكونات الحاسب الآلي المتمثل في المعلومات المعالجة إلكترونيا ، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات الذي يعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الإعتداء على نظم المعالجة الآلية [3] ، مثل الدخول الغير المشروع إلى نظم الغير الذي يمثل إحدى صور الركن المادي لجريمة الغش المعلوماتي ، فوجود برمجيات غير مصنفة تعمل في بيئة الإختراق أو تساعد عليه كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة يمكن أن يشكل منطقة إستفهام ودلالة كافية أيضا على إرتكاب الشخص لجريمة الدخول الغير المشروع لنظام المعالجة الآلية إذا إستتبع ذلك إعترافا شفويا بإرتكاب الجريمة ومن هنا فإن التفتيش في مكونات الحاسب الآلي المعنوية ، يشكل إحدى أهم المشاكل التي تعيق إجراءات

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 309 .

(2) : المادة 64 والمواد من 44 إلى 47 من القانون رقم 06 – 22 السالف الذكر .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 397 .

التحقيق ، حيث أثارت هذه الصورة خلافا كبيرا في الفقه المقارن لأن هذا النوع من التفتيش ينصب على بيانات وبرامج الحاسب الآلي التي تغيب فيها الطبيعة المادية فليس لها أي أثر مادي محسوس في العالم الخارجي [1] .

فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط " أي شيء " فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة .

بينما ذهب رأي آخر إلى عدم إنطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير ملموسة ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أحكام خاصة تكون أكثر ملائمة لهذه المعلومات اللامحسوسة [2] .

وهذا ما تبناه المشرع الجزائري حيث أنه وإستجابة لهذه التغيرات أجاز تفتيش المعطيات المعلوماتية وذلك بموجب المادة 05 من القانون رقم 09 -04 السالف الذكر ، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من نفس القانون ، التي من بينها توافر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الإقتصاد الوطني وللوقاية من الجرائم الماسة بأمن الدولة ، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية [3] ، وإلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي قدر هذه التغيرات إذ قام بتعديل نصوص التفتيش حيت قام بإضافة عبارة المعطيات المعلوماتية في المادة 94 ق إ ج وذلك بموجب المادة 42 من القانون رقم 545–2004 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي ، لتصبح المادة على النحو التالي " يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات يكون كشفها مفيدا في إظهار الحقيقة " [4] .

الفرع الثاني : تفتيش المنظومة المعلوماتية عن بعد في جريمة الغش المعلوماتي

بالإضافة إلى كون تفتيش نظام الحاسب الآلي تعد ضمن الإشكاليات التي تعيق سير التحقيق فإن تفتيش شبكات الحاسب الآلي تثير مشكلة قد تكون أشد خطورة من تفتيش نظام

---

(1) : فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 311 .

(2) : خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الإلكترونية ، المرجع السابق ، ص. 197 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 348 ، 349 .

(4) : JORF n°138 du 16 juin 2004 page 10719

أنظر الموقع : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000617671&dateTexte=&categorieLien=id

الحاسب الآلي حينما يكون مرتبط بشبكة إتصال ، وتثار هذه المشكلة عندما يتعلق الأمر بنهاية طرفية موجودة في منزل المتهم ومتصلة بجهاز يقع خارج منزل المتهم في نفس الدولة ومملوك لغير المتهم ، كما تثار الإشكالية بصورة أكبر عندما يكون النظام المراد تفتيشه واقعا خارج الدولة وتعد شبكة الأنترنت هي الشبكة الأهم التي تشكل عائقا في مجال التفتيش الجنائي من بين الشبكات المختلفة بسبب الإنتشار الواسع لها والعدد الهائل من البشر الذين يستخدمونها والخدمات التي تقدمها في مجال الحياة المختلفة والكم الهائل من البيانات والمواقع التي تتضمنها [1] ، فالجانب السلبي للتكنولوجيا الرقمية طرح عدة تساؤلات تمثلت في : هل يمتد تفتيش حاسوب معين إلى الأجهزة المرتبطة به سواء كانت موجودة داخل الدولة أو خارجها ؟، كما يثار تساؤل آخر حول أثر تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر إختصاص مختلفة ، في هذه الصورة وإجابة عن هذه التساؤلات يمكن التفرقة بين الفرضين التاليين :

البند الأول : حالة جهاز متصل بجهاز المتهم داخل الدولة

تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم ويقع داخل الدولة وتكمن المشكلة في تجاوز الإختصاص المكاني لسلطة التحقيق من ناحية والإعتداء على خصوصيات الغير من ناحية أخرى .

وقد عالجت بعض التشريعات هذه المسألة حيث نصت على إمكانية إمتداد تفتيش المسكن إلى تفتيش نظام آلي موجود في مكان آخر ، بغرض التوصل إلى بيانات تفيد في كشف الحقيقة وبالتالي يجوز للقائم بالتفتيش أن يسجل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق من قاضي التحقيق غير أن هذه السلطة مقيدة بقيدين هما :

الأول : ألا تكون النهاية الطرفية التي يرتبط بها الحاسب الآلي موجودة ضمن نطاق إقليم دولة أخرى .

الثاني : أن تحتوي النهاية الطرفية المرتبط بها الحاسب على بيانات تؤدي إلى كشف الحقيقة وبالنسبة للتشريع الجزائري فقد تضمن نصوص قانونية إجرائية ضمن التعديل الأخير لقانون الإجراءات الجزائية وسعت بعض الصلاحيات التي يمكن القيام بها من قبل سلطة التحقيق ، ومن ذلك إمكانية قيام قاضي التحقيق بالتفتيش أو الحجز في أي وقت وفي أي مكان على إمتداد كامل التراب الوطني أو يأمر ضابط الشرطة القضائية المختص للقيام بذلك وبالتالي القيام بإجراءات التحقيق في مجال الجرائم المعلوماتية التي من بينها الغش المعلوماتي في أي مكان داخل الإقليم الوطني للدولة .

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 312 .

ونظرا لوجود قصور في نصوص قانون الإجراءات الجزائية في تعديله الأخير لسنة 2006 ، حيث لم يتضمن التفتيش عن بعد الكيانات المنطقية في نظام المعالجة الآلية للبيانات [1] ، فقد تلافى ذلك القصور بأن سمح للسلطات القضائية المختصة لمقتضيات التحريات والتحقيقات القضائية تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني وهذا ما نصت عليه الفقرة الثانية من المادة 05 من القانون رقم 09 – 04 السالف الذكر .

وإلي جانب المشرع الجزائري نجد المشرع الفرنسي قد حسم هذه المسألة أيضا ، وذلك بمناسبة تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 2003 – 239 بشأن الأمر الداخلي الصادر في 18 مارس 2003 حيث أضاف المادة 57 – 1 ق إ ج وذلك بموجب المادة 17 – 1 منه التي أجازت لرجال الضبط القضائي الدخول من الجهاز الرئيسي على المعلومات التي تهم عملية البحث والتحري فتنص المادة 17-1 منه على أنه " يجوز لضباط الشرطة القضائية أو تحت مسؤولياتهم أعوان الشرطة القضائية ، وفي إطار التفتيش المنصوص عليه ، الدخول عن طريق الأنظمة المعلوماتية التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر بها ، أن هذه المعطيات يتم الدخول إليها أو تكون متاحة انطلاقا من النظام الرئيسي " [2] .

البند الثاني : حالة جهاز متصل بجهاز المتهم خارج الدولة

في هذه الحالة فإن الإشكالية تثار بصورة أكبر ، في حالة أن يكون الجهاز المطلوب تفتيشه والمربوط بجهاز المتهم بنهاية طرفية يقع خارج الدولة ، ففي الغالب يعّمد مرتكبي جرائم المعلوماتية وعلى سبيل المثال جريمة الغش المعلوماتي إلى تخزين البيانات الخاصة بهم والتي تعد أدلة لإدانتهم في جرائم تم إرتكابها من قبلهم خارج الدولة التي يقيمون بها،عن طريق شبكة الإتصالات البعيدة بهدف عرقلة التحقيقات .

والتفتيش عن بعد أصبح مشكلة تواجه النظام الإجرائي ككل ، حيث يتم إجراؤه من خلال الحاسوب ذاته وتزداد خطورة الأمر حينما يتم إستخدام برامج تمتلكها دول معينة متقدمة في مجال التكنولوجيا الرقمية ، للتفتيش على أنظمة دول أخرى ، لكونه لا يستند إلى مبرر قانوني ويشكل إعتداء على الخصوصية ، فضلا عن كونه يجعل الدولة عرضة للإعتداء في إطار جريمة التجسس عليها .

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 314 .

(2) : JORF n°66 du 19 mars 2003 page 4761

أنظر الموقع :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199&fastPos=17&fastReqId=32016638&categorieLine=id

وإذا كانت بعض التشريعات قد وسعت من صلاحيات سلطة التحقيق للقيام بتفتيش النظم خارج الإقليم وقرنت ذلك بحالة الضرورة ، وإذا كان هذا الإجراء يفيد في كشف الحقيقة إلا أن ذلك التوجه قد تم معارضته من قبل الفقه والقضاء في تلك الدول بإعتبار أن فيه مساس بسيادة الدول ويجب التنسيق للقيام بذلك الإجراء [1] .

وبالنسبة للقانون الجزائري فقد تلافى مشكلة التفتيش عن بعد خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة 5 من القانون رقم 09 – 04 السالف الذكر التي نصت على أنه " إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل " ، فبخصوص هذه الفقرة قيل بأنه لا يمكن تفتيش تلك المنظومة وإنما يجب الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ، فبالرغم من إمكانية تفتيشها من الناحية الفنية داخل النطاق الإقليمي إلا أن ذلك لا يتم إلا بعد موافقة الطرف الأجنبي وهو أمر متعلق بسيادة الدول على أراضيها وهذا يؤكد على أهمية التعاون الدولي في هذا المجال [2] .

وبالنسبة للمشرع الفرنسي فقد أجاز هو الآخر بموجب الفقرة الثانية من المادة 57 – 1 من قانون الإجراءات الجزائية المضافة بموجب المادة 17 / 2 من قانون الأمن الداخلي السالف الذكر لضباط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم فنصت " إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني ، وأنه يمكن الدخول إليها أو أنها متاحة إنطلاقا من النظام الرئيسي ، فإنه يمكن الحصول عليها من طرف ضابط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية [3] .

بعد أن تم التطرق إلى بيان كيفية إجراء التفتيش في مكونات الحاسب الآلي المادية واللآمادية وكذا التفتيش عن بعد في إطار جريمة الغش المعلوماتي ، نتناول فيما يلي الشروط الواجب توافرها للقيام بإجراء التفتيش حتى يكون محاطا بالضمانات القانونية الكافية .

الفرع الثالث : شروط وضمانات التفتيش في جريمة الغش المعلوماتي

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 315 .

(2) : أحمد مسعود مريم ، المرجع السابق ، ص. 92 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 403 .

مما سبق يتضح بأن جريمة الغش المعلوماتي يمكن أن تخضع لإجراء التفتيش طبقا للقواعد التقليدية أو المستحدثة ، هذا الإجراء الذي وجد أثناء مباشرته أنه يتضمن تقييد للحرية الفردية وإعتداء على حرمة الحياة الخاصة [1] ، لهذا نجد أن القوانين الإجرائية قد حرصت على إحاطة إجراء التفتيش بشروط وضمانات أساسية وهدف ذلك تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم ، ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي [2] ، وهو ما سيتم التطرق له فيما يلي :

البند الأول : الشروط الموضوعية للتفتيش في جريمة الغش المعلوماتي

تتمثل الشروط الموضوعية التي يلزم تحققها لإجراء التفتيش في : سبب التفتيش الذي يتمثل في وقوع الجريمة وهو في هذه الحالة وقوع الغش المعلوماتي ، ونسبة إرتكابها إلى متهم إضافة إلى ضرورة أن ينصب التفتيش على محل يحتمل العثور فيه على أدلة الجريمة وأخيرا يفترض لكي يكون التفتيش صحيحا أن يكون له غاية تتمثل في أن يكون التفتيش بغرض العثور على الآثار والأشياء التي يمكن أن تفيد في كشف الجريمة ، وجملة هذه الشروط أو الضمانات سنحاول تفصيلها فيما يلي :

أولا : وجود سبب لتفتيش النظام المعلوماتي

الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة واقعة بالفعل ، وترجحت نسبتها إلى متهم معين ، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية [3] ، وذلك عملا بقاعدة المشروعية " لا جريمة إلا بنص " وبالتالي لا يجوز التفتيش من أجل فعل لا يشكل جريمة وفي حالة عدم توافر الدلائل الكافية بإقترافها ونسبتها إلى شخص أو أشخاص ، فسبب التفتيش بحثا عن أدلة الجريمة يعد ضمانة بالنسبة للجرائم المنصوص عليها في القوانين إذ بدون السّبب المتمثل في الجريمة ، وبدون توجيه الإتهام لشخص أو أشخاص محددين فإن القيام بالتفتيش يعد إجراءً باطلا ، ولا يكفي لقيام سبب التفتيش ، وقوع جريمة منصوص عليها في القانون كجريمة الغش المعلوماتي التي تناولها المشرع الجزائري بنصوص قانونية تضفي وصف التجريم على الأفعال المكونة لها ، بل لا بد من توافر أمارات قوية على وجود أشياء تفيد في كشف هذه الجريمة .

فتفتيش مكونات الحاسوب المادية في القانون الجزائري يتطلب توافر سبب للقيام به مثل أي مكونات مادية أخرى ، ويتمثل السبب في وقوع الجريمة وقيام قرائن كافية على وجود

---

(1) : رشيدة بوكر ، المرجع السابق نفسه ، ص. 405 .

(2) : سعيداني نعيم ، المرجع السابق ، ص. 152 .

(3) : خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الإلكترونية ، المرجع السابق ، ص. 209 .

الدليل أو الأدلة محل البحث والتي تفيد في كشف الحقيقة لدى شخص معين أو في مسكنه،حيث تطرق المشرع الجزائري لسبب التفتيش في أكثر من نص ومن تلك النصوص المادة 44 ق إ ج التي سبقت الإشارة إليها ، وفي هذه المسألة فإن المشكلة التي يمكن أن تثار بسبب الحاسب الآلي والشبكة المعلوماتية بالنسبة للجرائم المعلوماتية عامة تكون في دول لم تواجد فيها حتى الآن نصوص قانونية تنظم مسألة تجريم تلك الجرائم وعقاب مقترفيها لكون إجراء التفتيش لا بد أن يبنى على سبب يتمثل بوقوع الجريمة [1] .

وقد تلافى المشرع الجزائري ما يخص بعض الجوانب الإجرائية المتعلقة بجريمة الغش المعلوماتي ومنها التفتيش بحيث يمكن القول بتوافر سبب التفتيش ، في جرائم المعلوماتية المستحدثة والتقليدية وعدم الإقتصار على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المشار إليها في القسم السابع مكرر من قانون العقوبات ، وإنما تعدى ذلك إلى كافة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها حيث عرفها المشرع بموجب المادة 02 / أ من القانون رقم 09 – 04 السالف الذكر بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية [2] ، ومن هنا نجد أن المشرع الجزائري قد حدد سبب التفتيش في الجرائم المعلوماتية التي من بينها جريمة الغش المعلوماتي من خلال هذا التعريف .

ثانيا : محل التفتيش

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سّره والسّر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة [3] ، ومحل التفتيش قد يكون منزلا وقد يكون شخصا وقد يكون محله رسائل [4] .

هذا ومحل التفتيش في إطار جرائم الإعتداء على نظم المعالجة أو الجرائم المعلوماتية التي من بينها جريمة الغش المعلوماتي هو نظام المعالجة بكل مكوناته المادية والمعنوية وشبكات الإتصال كما سبق بيانه وفي هذا المجال لا داعي لتكرار مدى قابلية هذه المكونات المادية والمعنوية فضلا عن شبكات الإتصال للتفتيش .

ثالثا : الغاية من التفتيش

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 319 .

(2) : فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 320 .

(3) : رشيدة بوكر ، المرجع السابق ، ص. 408 .

(4) : فايز محمد راجح غلاب ، المرجع السابق نفسه ، ص. 321 .

نظرا لخطورة إجراء التفتيش على الحياة الخاصة للأفراد بإعتباره إجراء من إجراءات التحقيق فلا بد أن يكون له غاية إذ بدونها ، وكذلك في حالة تجاوزها فإن الإجراء سيكون باطلا وبهذا الخصوص نصت المادة 81 ق إ ج على أن يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة ، وفي مجال المعلوماتية بصفة عامة نجد أن المشرع الجزائري وبخصوص الغرض من التفتيش قد أحال تفصيل ذلك إلى قواعد قانون الإجراءات الجزائية حيث نص على أنه : " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة الرابعة أعلاه ، الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها .
- منظومة تخزين معلوماتية. " [1] .

وبالتالي فإنه إذا تحققت الغاية من التفتيش وفقا لنصوص قانون الإجراءات الجزائية فيحق للسلطات المختصة بالتحقيق الدخول إلى النظام المعلوماتي أو جزء منه ، بغرض التفتيش على ذلك النظام أو المعطيات المخزنة به ، كما يجوز الدخول إلى نظام معلوماتي آخر داخل الإقليم الوطني أيضا بغرض التفتيش إذا ما تحققت الغاية منه وذلك في حالة وجود أسباب تدعو للإعتقاد بأن المعطيات محل البحث مخزنة في ذلك النظام [2] .

البند الثاني : الشروط الشكلية للتفتيش في جريمة الغش المعلوماتي

بالإضافة إلى الضوابط الموضوعية للتفتيش ، توجد ضوابط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء وذلك صونا للحريات الفردية من التعسف أو الإنحراف في إستخدام السلطة [3] ، ومن أهم هذه الضوابط أو الشروط ما يلي :

أولا : تحديد أوقات التفتيش

تذهب أغلب التشريعات الجزائية إلى تحديد وقت معين يتم فيه إجراء التفتيش ، وذلك حرصا منها على تضيق نطاق الإعتداء على الحرية الفردية وحرمة المسكن ، حيث ذهب المشرع الجزائري ونظيره الفرنسي ، إلى حظر تفتيش المنازل وما في حكمها في وقت معين فنجد ميقات التفتيش في التشريع الجزائري قد حدد من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وذلك من خلال المادة 47 ق إ ج ، أما بالرجوع إلى القانون الفرنسي فنجده يحدد ميقات التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساءا وذلك من خلال نص

(1) : المادة 05 من القانون 09 – 04 السالف الذكر .

(2) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 327 .

(3) : خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الإلكترونية ، المرجع السابق ، ص. 220 .

المادة 59 ق إ ج [1] ، وبذلك نجد أن هذه النصوص قد هدفت إلى حماية حرمة الأفراد ليلا ، حيث يعد المسكن ملجأ حصين لهم ، لا يجوز إنتهاكه ليلا حفاظا على خصوصياتهم .

ومع أن إشتراط تفتيش المنازل بوقت معين يعد ضمانة للمحافظة على خصوصيات الآخرين ، فإن ذلك الشرط لا يؤخذ به على إطلاقه ، حيث ورد العديد من الإستثناءات على تلك القاعدة تضمنت الخروج على الميقات الزمني في التفتيش بالنسبة لبعض الجرائم وكذلك في بعض الحالات مثل حالة الضرورة ، من ذلك وفي نطاق التفتيش المتعلق بجرائم المعلوماتية ، فإن الإستثناء الوارد بالمادة 47 / 3 ق إ ج والمتعلق بجواز إجراء ضابط الشرطة القضائية التفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم ، فقد شمل هذا الإستثناء جريمة الغش المعلوماتي بإعتبارها من الجرائم المعلوماتية حيث جاء فيها " عندما يتعلق الأمر .... والجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات .... فإنه يجوز إجراء التفتيش " [2] .

وفي هذه النقطة أيدت وجهة نظر المشرع الجزائري ذلك أن تطبيق القيد السابق على هذا النوع من الجرائم ، قد يكون سببا في إخفاء الأدلة ومن ثمت عرقلة سير التحقيق لكون أدلة هذه الجرائم هي عبارة عن كيانات غير مادية يمكن إخفاء أدلتها بسرعة غير متوقعة،إذا علم الجاني مسبقا بالوقت الذي سيتم تفتيش أنظمته فيه [3] .

ثانيا : الأشخاص المطلوب حضورهم للتفتيش

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية وذلك لضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط [4] ، حيث ذهب أغلب الفقهاء إلى ضرورة حضور المتهم التفتيش معتبرين ذلك من القواعد الأساسية التي يترتب على مخالفتها البطلان وقد نص المشرع الجزائري على هذا الضمان في المادة 45 و 83 ق إ ج.

وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى عدم التعسف في إستخدامها،إلا أنها قد تتحول إلى مشكلات تحول دون الوصول إلى النتائج المتوقعة من إجراء التفتيش في حالة أن يكون التفتيش يخص إحدى جرائم المعلوماتية ، على سبيل المثال جريمة الغش المعلوماتي محل الدراسة ، بسبب أن إشعار الأشخاص المطلوب حضورهم قد يتيح لهم التلاعب بالمعطيات والبرامج المراد تفتيشها ، وبالتالي إخفاء أدلة الجرائم أو التلاعب بها ومن ثم صعوبة التوصل إلى مرتكبها ، فقد يتم التلاعب بالأدلة وإخفاءها عن بعد في الوقت ما بين إجراءات إصدار الإذن بالتفتيش وموافقة المتهم بأن يتم التفتيش بحضوره ، وعليه فقد تنبه

---

(1) : رشيدة بوكر ، المرجع السابق ، ص. 416 ، 417 .

(2) : سعيداني نعيم ، المرجع السابق ، ص. 154 .

(3) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 329 – 330 .

(4) : رشيدة بوكر ، المرجع السابق ، ص. 413 .

المشرع الجزائري لمثل هذا الإجراء فلم يشترط في تفتيش عدد من الجرائم حضور المتهم أو صاحب المنزل المراد تفتيشه أو الشهود ومن تلك الجرائم ، الجرائم الماسة بأنظمة المعالجة الآلية [1] .

ثالثا : محضر التفتيش

بإعتبار التفتيش عملا من أعمال التحقيق فإنه ينبغي تحرير محضر به يثبت فيه كل ما تم من إجراءات ، وما أسفر عنه التفتيش من أدلة ، ولم يتطلب القانون شكلا خاصا لهذا المحضر ، مما ينبغي أنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما ، كأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره ، وأن يحوي في طياته كافة الإجراءات التي إتخذها بشأن الوقائع التي بينها ، حيث نصت المادة 68 / 2 ق إ ج ج " وتحرر نسخة من هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل " ، كما نصت المادة 79 ق إ ج ج على أنه " ... ويستعين قاضي التحقيق دائما بكاتب ويحرر محضرا بما يقوم به من إجراءات " .

وبالنسبة لمحضر تفتيش نظم الحاسب الآلي نتيجة إرتكاب جريمة الغش المعلوماتي فإنه لا بد بالإضافة إلى ما سبق ذكره من إحاطة قاضي التحقيق أو عضو النيابة العامة بتقنية المعلومات ، ومن جهة أخرى لا بد أن يرافقه شخصا متخصصا في الكمبيوتر للإستعانة به في المسائل الفنية الضرورية ، فوجود خبير سوف يساعد في صياغة مسوّدة محضر التحقيق بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش [2] .

إن الحديث عن أهم إجراءات بخصوص جريمة الغش المعلوماتي ، من إجراء مراقبة الإتصالات الإلكترونية وكذا إجراء التفتيش لا يكتمل إلا بالتعرض لإجراء الضبط أو حجز المعطيات المعلوماتية ، بإعتباره الوسيلة التي من خلالها يتم الوصول إلى الأدلة التي تثبت الحقيقة التي تبحث عنها الدعوى الجزائية ، وهذا ما سيتم التطرق له فيما يلي :

المطلب الثالث : قواعد حجز المعطيات المعلوماتية في جريمة الغش المعلوماتي

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 337 .

(2) : خالد ممدوح إبراهيم ، فن التحقيق في الجرائم الإلكترونية ، المرجع السابق ، ص. 225 .

ينتهي التفتيش بنتيجة طبيعية مفادها ضبط الأدلة التي يتم الحصول عليها أثناءه فالضبط هو غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه الإجراء ، ويكمن الأساس القانوني للضبط في العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق التي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه أو ما كان في مصلحته [1].

ويقصد بالضبط : " العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة " ، فمن خلال هذا التعريف نلاحظ بأن هناك إرتباط بين التفتيش والضبط ، مما يعني أنه لا يجوز أن يقع الضبط إلا على شيء وصفه دليل من أدلة الجريمة التي يجرى التفتيش بشأنها ، ولذلك فإنه يباشر من أجل الحقيقة المطلقة ، بمعنى أنه ما دام التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم البراءة ، لأن ما يضبط في الحالتين يحقق العدالة الجنائية [2] .

وبخصوص الضبط في مجال الجرائم المعلوماتية بصفة عامة وجريمة الغش المعلوماتي بصفة خاصة ، فإن محل الضبط إلى جانب كونه يقع على الأشياء المادية فإنه يشمل أيضا مكونات أخرى ذات طبيعة معنوية هذه الأخيرة التي أثارت جدلا فقهيا واختلافا تشريعيا حول إمكانية ضبطها ، خاصة وأن الضبط لا يرد إلا على الأشياء المادية .

هذا وينظم المشرع الجزائري إجراء الضبط بموجب قواعد قانون الإجراءات الجزائية كقاعدة عامة من حيث تحديد من يقع عليه الضبط ومن يقوم بالضبط ، بالإضافة إلى هذا التنظيم فإن المشرع الجزائري قد تدخل لإستكمال ما تبقى من فراغ في المنظومة التشريعية وذلك بموجب القانون 09 – 04 السالف الذكر ، حيث إستحدث المادة السادسة التي يمكن الإسترشاد بها في مجال جريمة الغش المعلوماتي التي جاء فيها " عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضرورة حجز كل المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز ، والوضع في أحراز وفق للقواعد المقررة في قانون الاجراءات الجزائية " ، فما يلاحظ من خلال هذا النص وغيره من النصوص المنظمة لضبط الأدلة الرقمية في القانون رقم 09 – 04 السالف الذكر أن المشرع الجزائري قد استعمل مصطلحا مغايرا لما إعتاد عليه في قانون الإجراءات الجزائية فإستبدل مصطلح الضبط بمصطلح الحجز [3] .

وإلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي قام بإدخال تعديل على قانون الإجراءات الجزائية الفرنسي لسّد الفراغ التشريعي ، وذلك بموجب قانون الأمن الداخلي رقم

---

(1) : سعيداني نعيم ، المرجع السابق ، ص. 158 .

(2) : أحمد مسعود مريم ، المرجع السابق ، ص. 94 .

(3) : أحمد مسعود مريم ، المرجع السابق ، ص. 94

239 لسنة 2003 السالف الذكر ، حيث إستحدث الفقرة الثالثة من المادة 57 – 1 التي تنص على أن " المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعامات التخزين المعلوماتية هذه يتعين تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون " [1] .

هذا ولقد نصت إتفاقية بودابست لسنة 2001 السالفة الذكر على إجراء الضبط في الفقرة الثالثة من المادة 19 من القسم الرابع منها على أن " على سلطة كل دولة طرف أن تتخذ الإجراءات التالية ، أن تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر ، وأن تحافظ على سلامة تلك المعلومات المخزنة " [2] .

يتبين من خلال هذا التدخل القانوني للمشرعين أن إجراء الضبط في مجال جريمة الغش المعلوماتي لا يثير أية صعوبات أو مشاكل بخصوص الأدلة المادية – المكونات المادية للحاسب الآلي – إذ بالإمكان تطبيق النصوص القانونية التقليدية المتعلقة بالضبط إلا أن الإشكال يثار بخصوص المكونات الغير المادية للحاسب الآلي أي المكونات المنطقية أو ذات الطبيعة المعنوية .

وعليه وبناءً على ما سبق سيتم التطرق من خلال ما يلي إلى أهم قواعد ضبط المكونات المادية للحاسب الآلي بإعتبارها أهم الأدلة التي يمكن أن تضبط على مسرح جريمة الغش المعلوماتي في الفرع الأول ، كما أنه سيتم التطرق إلى أهم القواعد التي تحكم ضبط المكونات الغير المادية وذلك بناءً على النصوص المستحدثة التي جاء بها المشرع الجزائري وغيره ، في المجال المعلوماتي بصفة عامة وذلك في الفرع الثاني ، هذا وسيتم بيان أهم إجراءات حجز المعطيات المعلوماتية من خلال الفرع الثالث .

الفرع الأول : قواعد ضبط المكونات المادية للحاسب الآلي في جريمة الغش المعلوماتي

لا يثير ضبط المكونات المادية للحاسب الآلي أية مشكلات تعيق إجراءات التحقيق وبالتالي لا يوجد خلاف بين فقهاء القانون في إمكانية ضبطها لأن الغاية من التفتيش في جريمة الغش المعلوماتي هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة ، وبالتالي لا مشكلة طالما أن المكونات التي سيتم تفتيشها وضبطها هي في حقيقتها مكونات مادية ، فلا

---

(1) : JORF n°66 du 19 mars 2003 page 4761

أنظر الموقع :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199&fastPos=17&fastReqId=32016638&categorieLine=id

(2) : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

توجد صعوبة في ضبط الدعامة المادية للبرنامج ، أو الوسائل المادية أو الوسائل المستخدمة في نسخه بطريقة غير مشروعة [1] .

أما بخصوص أهم القواعد المنصوص عليها في قانون الإجراءات الجزائية الجزائري والتي يمكن تطبيقها على المكونات المادية للحاسوب فهي : إن إجراءات الضبط هي من إجراءات التحقيق ، بحيث لا يجوز ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة ، وكذلك عدم جواز ضبط الأشياء التي تمس الأسرار الشخصية أو العائلية للشخص الحائز للمكان الجاري تفتيشه ، أو الأشخاص الآخرين ، وإحصاء الأشياء المضبوطة التي تفيد في كشف الحقيقة ووضعها في أحراز مختومة ، وعند فتحها فإنه يستوجب حضور المتهم مصحوبا بمحاميه [2] .

الفرع الثاني : ضبط المكونات الغير المادية للحاسب الآلي في جريمة الغش المعلوماتي

لقد سبقت الإشارة إلى أن التشريعات الإجرائية والإتجاهات الفقهية قد إختلفت حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية والتي لا تصلح بطبيعتها محلا لوضع اليد عليها ، وهي مجردة عن دعامتها المادية المثبتة عليها وإنقسمت في ذلك إلى إتجاهين :

الإتجاه الأول : يرى أصحابه أنه لا يمكن تصّور إجراء الضبط على الكيانات المنطقية للحاسوب لإنتفاء الكيان المادي عنها ، وبالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لإنتفاء الطابع المادي عن هذه البيانات في حال تجردها عن الدعامة المادية ومن التشريعات التي أخذت بهذا الإتجاه التشريع الألماني .

الإتجاه الثاني : يرى أصحابه أن المعطيات المخزنة آليا كونها مجردة عن الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليه بمقتضي النصوص التقليدية [3] .

وقد دعم كل من أنصار الفريقين رأيه بالحجج التي تقوي موقفه فبالنسبة للفريق الأول يرى بأن الحل يكون عن طريق التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط ، لتشمل البيانات وبرامج الحاسب الآلي بجانب الأشياء المادية وذلك بإضافة عبارة البيانات والبرامج المعالجة عن طريق الحاسب إلى النص القانوني الذي ينص على التفتيش والضبط . أما الفريق الثاني فيدعم موقفه بالقول بأن الغاية من التفتيش هي ضبط

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 342 .

(2) : المواد من 132 إلى 140 من الأمر رقم 66 – 155 ، السالف الذكر ، ص. 236 ، 237 .

(3) : سعيداني نعيم ، المرجع السابق ، ص. 159 .

الأدلة التي تفيد في كشف الحقيقة . وهذا المفهوم يمتد ليشمل البيانات الإلكترونية حيث أكد الفقه الكندي أن إجراء الضبط إذا نظر إليه من خلال تطوره التاريخي فإن الغرض منه في بادئ الأمر ضبط الأشياء المادية المحسوسة . أما الآن فالضبط لا يقتصر على هذا الغرض وإنما يمتد لأغراض أخرى على رأسها الحصول على المعلومات والأدلة التي تتيح ضبط الأشياء [1] .

الفرع الثالث : أساليب حجز المعطيات المعلوماتية في جريمة الغش المعلوماتي

إن جريمة الغش المعلوماتي تدخل ضمن الجرائم المعلوماتية التي إستحدث المشرع الجزائري بشأنها في مجال الضبط نصوص قانونية تلاءم طبيعتها الخاصة ، ذلك أنه يصعب إقامة الدليل على هذا النوع من الجرائم ، وذلك بسبب الطبيعة المعنوية للمحل لأن محل تلك الجرائم بصفة عامة وكما سبقت الإشارة هو الجوانب المعنوية التي تتعلق بالمعالجة الآلية للمعطيات والتي تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها وإدراكها إلا من خلال الحواسيب التي تحفظها ، لأجل ذلك فإن القواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه البيانات .

لذلك فإن طريقة ضبط المعلومات المعالجة آلية تختلف عما هي عليه عند ضبط المكونات المحسوسة ، هذا وبالرجوع للقانون رقم 09 – 04 السالف الذكر نجد أن المشرع الجزائري قد وضع أسلوبين لضبط الأدلة الرقمية في مجال الجرائم المعلوماتية بصفة عامة [2] ، واللذين يمكن الإستعانة وتطبيقهما في مجال جريمة الغش المعلوماتي ، فالأولى تكون عن طريق نسخ المعطيات الرقمية على جميع دعائم التخزين ، فيتم مثلا نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها ، وما يلاحظ أن أسلوب النسخ يصلح تماما أن ينتج عنه دليل رقمي مقبول أمام القضاء ، وقد نصت على هذا الأسلوب المادة السادسة السالفة الذكر في قولها : " ... يتم نسخ المعطيات محل البحث ... على دعامة تخزين إلكترونية " ، أما الأسلوب الثاني فهو الحجز عن طريق منع الوصول إلى المعطيات وهذا الأسلوب نصت عليه المادة السابعة من نفس القانون بقولها : " إذا إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (6) أعلاه لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية ، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة " ، فمن خلال ما ورد بهذه المادة نلاحظ أنها قد تضمنت طريقتين ضمن هذا الأسلوب الأولى تتضمن منع الوصول إلى المعطيات التي تحويها المنظومة المعلوماتية والثانية تتضمن منع نسخ تلك المعطيات [3] .

---

(1) : فايز محمد راجح غلاب ، المرجع السابق ، ص. 344 .

(2) : سعيداني نعيم ، المرجع السابق نفسه ، ص. 162 – 163 .

(3) : أحمد مسعود مريم ، المرجع السابق ، ص. 95 ، 96 .

هذا وإن كان الدليل الرقمي يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية عموما إلا أنه ونظرا إلى الطبيعة الخاصة له ، فإن عملية ضبطه وتحريزه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا والحفاظ عليه وصيانته من إمكانية العبث به ، وهو ما أشار إليه المشرع في المادة السادسة بقوله " ... ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش أو الحجز السّهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية ، غير أنه يجوز لها إستعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات ، قصد جعلها قابلة للإستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى هذه المعطيات " .

ومن هذه الإجراءات على سبيل المثال :

- ضبط الدعائم الأصلية للمعلومات وعدم الإقتصار على ضبط نسخها .

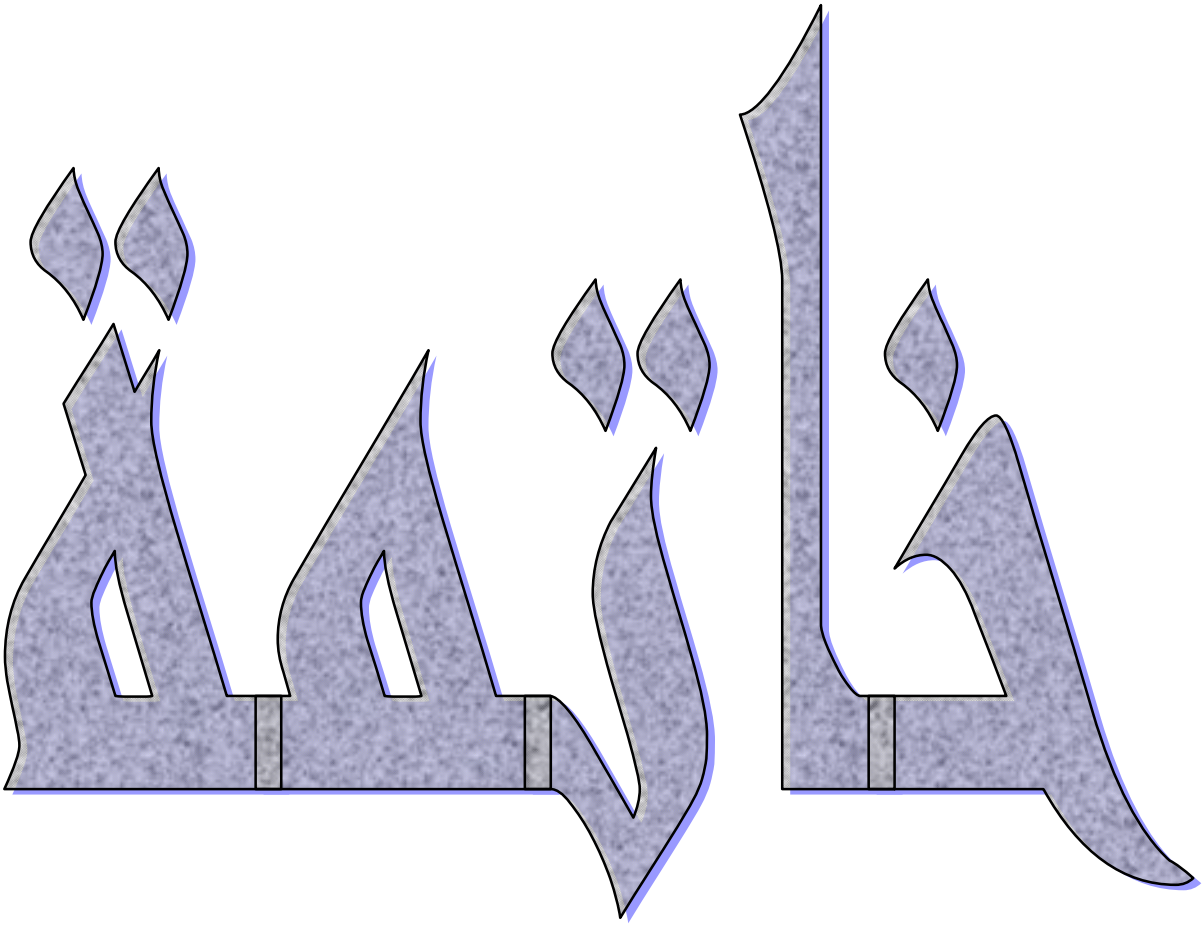
- عدم ثني القرص لأن ذلك يؤدي إلى تلف وفقدان المعلومات المسجلة عليه .

- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة [1].

وفي هذا الإطار نجد الهيئة الدولية لدليل الحاسب الآلي قد وضعت عدّة ضوابط لعملية ضبط الدليل الرقمي منها ألا تكون الإجراءات المتخذة في تحريز الدليل الرقمي سببا في تغير طبيعة هذا الدليل وأن تكون جميع الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها أو نقلها موثقة توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة وهو الأمر الذي أوردته كذلك الفقرة الثالثة من المادة 19 من الإتفاقية الأوربية للجريمة المعلوماتية [2] .

(1) : رشيدة بوكر ، المرجع السابق ، ص. 422 .

(2) : سعيداني نعيم ، المرجع السابق ، ص. 164 .


خاتمة

بعد أن فرغنا من دراسة موضوع جريمة الغش المعلوماتي ، وجدنا أن هذا الموضوع قد حظي بإهتمام الفكر القانوني ، فمن الناحية الفقهية وجد أن الفقه قد أولى لهذه الجريمة إهتمام كبير ، ويتجلى هذا من خلال حرصه على بيان مفهومها ، لكون هذا النوع من الإجرام الحديث ، لا يشكل فقط إنتهاكا لقاعدة قانونية ، بل يهدد حتى الحياة الخاصة للأفراد بأساليب وتقنيات جّد متطورة التي من بينها جهاز الحاسب الآلي الذي يعتبر عاملا أساسيا في إرتكاب جريمة الغش المعلوماتي ، أما من الناحية القانونية فمعظم التشريعات الوطنية والدولية إهتمت بتجريم الغش المعلوماتي وذلك من خلال بيان أركان هذه الجريمة وتقرير الجزاء المناسب لها ، حيث جاء هذا الإهتمام تجسيد لمبدأ الشرعية الجنائية ، إذ لا جريمة ولا عقوبة بغير نص قانوني .

هذا ولا نوّد أن نجعل من هذه الخاتمة تلخيصا لموضوع بحثنا ، وإنّما نحاول إستنتاج أو توضيح النتائج التي توّصلنا إليها من خلال دراستنا هذه والتي تتجلى فيما يلي :

- عند محاولتنا بيان أهم ما يميّز أركان جريمة الغش المعلوماتي ، وجدنا أن المشرع الجزائري قد جسّد الركن المادي فيها في فعلين هما : الدخول إلى المنظومة المعلوماتية وفعل المساس بها . حيث وجد بأن المشرع قد جعل من إفساد النظام ظرف مشدد لفعل الدخول عن طريق الغش وفي هذه النقطة خالف نظيره الفرنسي الذي جعل من إفساد النظام جريمة قائمة بذاتها .

- إن جريمة الغش المعلوماتي تعتبر من الجرائم الشكلية ، بحسب ما أخذت به معظم التشريعات إذ لا تتطلب أن يكون للدخول الغير المشروع نتيجة إجرامية محددة ، إلى جانب أن الغش المعلوماتي قد يكون جريمة مستمرة وقد يكون من الجرائم الوقتية ، وهذا يستلزم الرجوع إلى الفعل الذي يعاقب عليه القانون ، كما جرم المشرع الشروع في هذا النوع من الجرائم تطبيقا للقواعد العامة .

- أما بخصوص الركن المعنوي فإن أهم نتيجة توّصل إليها جميع الشراح هيّ ، إذا كان القصد الجنائي العام مطلوبا في الغش المعلوماتي ، فإن القصد الجنائي الخاص ليس مطلوبا كون الغش في هذه الحالة ليس مقصودا منه نيّة الإضرار .

- هذا ولقد ذهب الفقه إلى إعتبار جريمة الغش المعلوماتي ظاهرة إجرامية عالمية جديدة أهم ما يميزها أن فاعلها يختلف عن المجرم التقليدي لهذا إصطلح عليه بالمجرم المعلوماتي الذي يعتبر الذكاء عامل أساسي في نجاح مخططاته الإجرامية .

- إن المسؤولية الجزائية يتحملها المجرم سواء كان تقليديا أم معلوماتيا وسواء كان هذا الفاعل طبيعيا أو معنويا ، وبتقرير المسؤولية الجزائية فإن الجزاء الذي قرره المشرع يكون واجب التطبيق .

- هذا ولقد وصلنا من خلال هذه الدراسة المتواضعة إلى أن حداثة جريمة الغش المعلوماتي قد إضطرت المشرع الجزائري أن يراعي هذه الحداثة ، فقد أصدر تشريعات تواكب هذا التطور وبادر إلى تعديل قانون الإجراءات الجزائية ، فإستحدث إجراءات يمكن تطبيقها على جريمة الغش المعلوماتي التي من بينها كما أشرنا – التسرب وإعتراض المراسلات السلكية واللاسلكية – إذ تبين بتطبيق هاذين الإجرائين على الغش المعلوماتي ، أن المشرع الجزائري برّغم من حرصه على مواكبة التطورات الحاصلة في العالم إلا أنه حريص على أن تمارس هذه الإجراءات ضمن الإطار القانوني والشرعي الذي يكون كفيل بضمان حقوق وحرّيات الأفراد .

- ومن هنا نجد أن المشرع الجزائري وفي سبيل تدعيم مكافحته للسلوكيات السلبية الناتجة عن التطور التكنولوجي ، قد أدرك أن طبيعة جريمة الغش المعلوماتي تفرض عدم إمكانية التصدي لها بالأساليب التقليدية ، فبالرغم من تعديل قانون الإجراءات الجزائية ، أصدر قانونا مستقلا يتضمن نصوص تتلاءم وطرق مكافحة الغش المعلوماتي .

- بالنسبة لإجراء مراقبة الإتصالات الإلكترونية ، المشرع بالرغم من أنه أضفى عليه الصفة الوقائية ، إلا أنه أحاطه بضمانة قضائية تمثلت في ضرورة الحصول على إذن من السلطة القضائية المختصة .

ومن النتائج المتوصل إليها كذلك إن تفتيش المنظومة المعلوماتية في إطار إرتكاب جريمة الغش المعلوماتي وما يترتب عليه من حجز للمعطيات المعلوماتية يختلف عن التفتيش الذي يمارس في إطار إرتكاب إحدى الجرائم التقليدية ، إذ أن خصوصية هذه الجريمة من حيث الطبيعة التقنية لها فرضت هذه التفرقة .

- وبهذا نصل إلى نتيجة أن مجمل هذه القواعد التي أتى بها القانون رقم 09 – 04 ، يجوز تطبيقها على الغش المعلوماتي بإعتبارها إحدى جرائم المعلوماتية وهذه الأخيرة إصطلح المشرع الجزائري على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال .

وفي الأخير يمكن القول بأن هذه الترسانة القانونية التي واكب بها المشرع الجزائري التطور الحاصل في ميدان التكنولوجيا والمعلوماتية ، تحتاج إلى جهد كبير لتجسيدها على أرض الواقع ، فكل من الجهاز القضائي والأمني وحتى المجتمع بكامله بحاجة إلى هذا التطور وذلك لضمان السّرعة في الكشف عن الجرائم والقبض على مرتكبيها من جهة وللحفاظ على الأدّلة من جهة أخرى بإعتبارها إما دليل البراءة أو الإدانة .

بناءً على ما سبق ذكره نقترح جملة من التوصيات نوجزها فيما يلي :

- على مستوى قانون العقوبات ، يرجى من المشرع الجزائري إحداث نصوص قانونية أخرى واضحة ومحددة خاصة وأن الجرائم التقليدية التي يتضمنها قانون العقوبات أصبحت ترتكب بوسائل تقنية مستحدثة ، وذلك سّدا لذريعة الفراغ القانوني .

- على مستوى قانون الإجراءات الجزائية ، يستحسن تضمين التقنيات والأساليب المستجدة لمكافحة الإجرام ضمن نصوص قانونية حديثة ، تساعد الجهاز الأمني والقضائي في الكشف عن الجرائم وإدانة مرتكبيها ، وذلك تجسيدا لمبدأ الشرعية الجنائية الإجرائية .

- على المستوى الواقعي ، تنصيب الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ، وتزويدها بكامل الهياكل والموارد البشرية ذات الكفاءة للقيام بالدور المناط بها قانونا .

ملحق رقم

01

مصطلحات

المصطلح	دلالته
الحاسب الآلي	جهاز يسمح بإستعمال وتخزين المعلومات ومعالجتها وإخراج النتائج المطلوبة .
الأنترنت	شبكة الشبكات ، شبكة طرق المواصلات السريعة ، شبكة عالمية تربط عدّة آلات من الشبكات وملايين أجهزة الكمبيوتر المختلفة الأنواع والأحجام في العالم أما لغويا فالإنترنت معناها ترابط بين الشبكات ، وأول ظهور للأنترنت كان في 1969/01/12 على إثر تشكيل وزارة الدفاع الأمريكية فريق من العلماء للقيام بمشروع عن تشبيك الحاسبات .
خدمات الأنترنت	**خدمة البحث :** برنامج حاسوبي للمساعدة في العثور على مستندات مخزنة على شبكات الأنترنت أو على حاسوب شخصي . **البريد الإلكتروني :** أسلوب لكتابة وإستقبال الرسائل عبر نظم الإتصالات الإلكترونية . **خدمة الدخول عن بعد :** تسمح بإستخدام برامج وتطبيقات في الحاسب الآلي الآخر. **خدمة الأرشيف الإلكتروني :** تمكن من البحث عن ملفات معينة قد تكون مفقودة في البرامج المستخدمة . **خدمة الإستعلام الشخصي :** للإستعلام عن العنوان البريدي لأي شخص أو جهة تستخدم الأنترنت والمسجلين لديها . **خدمة المحادثات الشخصية :** بحيث يمكن التحدث مع أي طرف أخر صوتا وصورة وكتابة .
بروتوكول الأنترنت (ip)	عبارة عن رقم يتكون من أربعة أجزاء وكل جزء أقل من 256 ، يعرف الجزء الأول من الرقم بدءا من اليسار المنطقة الجغرافية والجزء الثاني يحدد المنظمة أو الحاسوب المزود والجزء الثالث يحدد مجموعة الحاسبات التي ينتمي إليها أما الجزء الرابع فهو يحدد الجهاز المستخدم ويمكن إعتبار هذا الرقم نوعا من الخرائط الخاصة بالإنترنت حيث يمكن الإتصال بأي حاسوب أو أي موقع من خلال نقطة معينة على هذه الخريطة .

المنظومة المعلوماتية	أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرامج معينة .
المعطيات المعلوماتية	أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها.
مقدمو الخدمات	أي كيان عام أو خاص يقدم لمستعملي خدماته ، القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام للإتصالات ، أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها .
المعطيات المتعلقة بحركة السير	أي المعطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة بإعتبارها جزءً في حلقة الإتصالات توضح مصدر الإتصال والوجه المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة .
الإتصالات الإلكترونية	أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.
الدليل الإلكتروني	هو المعلومات المخزنة في الأجهزة الحاسوب ولواحقها وغيرها من الوسائل التقنية الأخرى وكذا شبكات الإتصال والتي يتم تجميعها بإستخدام برامج وتطبيقات وتكنولوجيات خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها.

نظام المعالجة الآلية للمعطيات	يقصد بمنظومة الكمبيوتر أيّ جهاز أو مجموعة من الأجهزة المتّصلة ببعضها البعض أو ذات صلة بذلك ، ويقوم إحداهما أو أكثر من واحد منها ، تبعا للبرنامج بعمل معالجة آلية للبيانات.
بيانات الكمبيوتر	أيَّة عملية عرض للوقائع ، أو المعلومات أو المفاهيم في شكل مناسب لعمليّة المعالجة داخل منظومة الكمبيوتر ، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدِّي وظائفها ، أو غيرها من أجهز العرض كالهواتف النقالة الذكية واللوحات الرقمية وحتى ساعات اليد الذكية .
الشبكة المعلوماتية	هي مجموعة مكونة من أثنين أو أكثر من أجهزة الحاسوب والمتصلة ببعضها البعض إتصالا سلكيا أو لا سلكيا وتستوي أن تكون محلية أو موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف وتسميه بالشبكة بعيدة المدى.

ملحق رقم

02

الملحق رقم 01

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء .....

محكمة .....

نيابة .....

وكيل الجمهورية لدى محكمة .....

إلى السيد /

قائد فصيلة الأبحاث للدرك الوطني

إذن بالتسـرب

نحن وكيل الجمهورية لدى محكمة .....

بعد الإطلاع على الطلب المقدم من طرف .....

بتاريخ .....تحت رقم .....

بعد الإطلاع على المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية المعدل و المتمم.

نـأذن

..... ضابط الشرطة القضائية

..... بالتسرب

ضمن .....

تكون مدة التسرب لا تتجاوز أربعة أشهر تحدد طبقا للمعطيات الشكلية و القانونية المحددة بالمواد المذكورة أعلاه.

..... في : .....

وكيل الجمهورية

الملحق رقم 02

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

مجلس قضاء .....

محكمة .....

نيابة .....

وكيل الجمهورية لدى محكمة .....

إلى السيد /

قائد فصيلة الأبحاث للدرك الوطني

إذن بالتصنت

نحن وكيل الجمهورية لدى محكمة .....

بعد الإطلاع على الطلب المقدم من طرف .....

بتاريخ .....تحت رقم .....

بعد الإطلاع على المواد 65 مكرر 5 إلى 65 مكرر 9 من قانون الإجراءات الجزائية المعدل و المتمم.

نـأذن

..... ضابط الشرطة القضائية

..... بالتصنت

ضمن .....

تكون مدة التصنت لا تتجاوز أربعة أشهر تحدد طبقا للمعطيات الشكلية و القانونية المحددة بالمواد المذكورة أعلاه.

..... في :.....

وكيل الجمهورية

إحصائيات

قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم .

السنة	2005	2006	2007	2008	2009	2010	المجموع
عدد الجرائم	01	01	03	06	12	12	35
عدد الأشخاص	00	01	03	13	51	20	88

قضايا جريمة الغش المعلوماتي من سنة 2005 إلى 2010 .

نوع الجريمة	العدد	النسبة المئوية
الدخول الغير المشروع	11	% 29
الدخول الغير المشروع مع إتلاف المعطيات أو تعديلها	13	% 34

معلومات عن ضحايا جرائم المساس بأنظمة المعالجة الآلية للمعطيات .

الضحية	العدد	النسبة المئوية
إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري	21	% 60
شركات خاصة	07	% 20
شركات خاصة أجنبية	04	% 11
أشخاص طبيعيين	02	% 06
هيئات عمومية أجنبية	01	% 03
المجموع	35	% 100

الخبرات الرقمية المنجزة من طرف مخبر الشرطة العلمية للأمن الوطني .

السنوات	المخبر المركزي بالعاصمة	المخبر الجهوي بوهران	المخبر الجهوي بقسنطينة	المجموع
2008	21	44	08	73
2009	76	82	23	181
الثلاثي الأول 2010	23	40	09	72

المراجع

1/ المؤلفات العامة

- بوسقيعة احسن ، الوجيز في القانون الجزائي العام ،الطبعة التاسعة دار الهومة للطباعة و النشر و التوزيع .
- بوسقيعة أحسن ، الوجيز في القانون الجزائي الخاص ،الجزء الاول ، الطبعة الرابعة عشر ، دار الهومة للنشر والتوزيع ، الجزائر 2012 .
- محمد حزيط ، مذكرات في قانون الاجراءات الجزائية الجزائر ، الطبعة السادسة ، دار هومة للنشر والتوزيع ، الجزائر 2012 .

2/ المؤلفات الخاصة

- بوكر رشيدة ، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن ، الطبعة الأولى ، منشورات حلبي الحقوقية ، لبنان ، 2012 .
- حجازي عبد الفتاح بيومي ، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، دراسة قانونية معمقة في القانون المعلوماتي ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، 2006.
- حسين أسامة سمير ، الإحتيال الإلكتروني ، الوجه القبيح للتكنولوجيا ، الطبعة الأولى ، الجنادرية للنشر والتوزيع ، 2011 .
- الحسيناوي علي جبار ، جرائم الحاسوب والأنترنت ، دار اليازوري للنشر والتوزيع الطبعة العربية ، عمّان ، 2009 .
- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، بدون طبعة ، الدار الجامعية الإسكندرية ، 2008 .
- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، 2009 .
- خليفة محمد ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، بدون طبعة ، دار الجامعة الجديدة ، الإسكندرية ، 2007 .
- زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع ، الجزائر ، 2011 .

- شحادة زينات طلعت ، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية ، بدون طبعة ، المنشورات الحقوقية صادر ، لبنان ، بدون سنة نشر .
- عطا الله شيماء عبد الغني ، الحماية الجنائية للتعاملات الإلكترونية ، بدون طبعة ، دار الجامعة الجديدة ، الإسكندرية ، 2007 .
- عيد محمد علي رشدى ، الحماية الجنائية الموضوعية للمعلومات عبر الأنترنت دراسة مقارنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، بدون سنة نشر .
- الغافري حسين بن سعيد ، السياسة الجنائية في مواجهة جرائم الأنترنت ، دراسة مقارنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، 2009 .
- محمد نائلة فريدة ، جرائم الحاسب الآلي ، دراسة نظرية وتطبيقية ، بدون طبعة منشورات حلبي الحقوقية ، مصر ، بدون سنة نشر .
- المومني نهلا عبد القادر ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، الأردن ، 2008 .
- بن يونس عمر محمد ، الجرائم الناشئة عن إستخدام الأنترنت ، الأحكام الموضوعية والجوانب الإجرائية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2004 .

3/ الرسائل والمذكرات

- فايز محمد راجح غلاب ، الجرائم المعلوماتية في القانون الجزائري واليمني ، رسالة دكتوراه ، قسم الحقوق ، جامعة الجزائر 01 ، 2009 – 2010 .
- سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، قسم الحقوق ، جامعة الحاج لخضر ، باتنة ، 2012 – 2013 .
- سوير سفيان ، جرائم المعلوماتية ، مذكرة ماجستير ، قسم الحقوق ، جامعة أبو بكر بلقايد ، تلمسان ، 2010 - 2011 .
- طعباش أمين ، الحماية الجنائية للمعاملات الإلكترونية ، مذكرة ماجستير ، قسم الحقوق جامعة الحاج لخضر ، باتنة ، 2012 – 2013 .
- بن عقون حمزة ، السلوك الإجرامي للمجرم المعلوماتي ، مذكرة ماجستير ، قسم الحقوق ، جامعة الحاج لخضر ، باتنة ، 2011 – 2012 .

- مسعود أحمد مريم ، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون 09 – 04 مذكرة ماجستير ، قسم الحقوق ، جامعة قاصدي مرباح ، ورقلة ، 2012 – 2013 .

4/ المداخلات

- أرحومة مسعود موسى ، الإشكاليات التي تثيرها الجريمة المعلوماتية عبر الوطنية المؤتمر الوطني المغاربي الأول حول : المعلوماتية والقانون ، جامعة قاريونس طرابلس ، يومي 28 – 24 – أكتوبر 2009 .

5/ الوثائق والنصوص القانونية

- القانون رقم 06 . 23 ، المؤرخ في 20 ديسمبر 2006 ، المتضمن قانون العقوبات المعدل والمتمم ، ج ر : العدد 84 ، الصادرة بتاريخ 24 ديسمبر 2006 .
- القانون رقم 04 – 15 ، المؤرخ في 10 نوفمبر 2004 ، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جويلية 1966 ، المتضمن قانون العقوبات ، ج ر : العدد 71 ، الصادرة في 10 نوفمبر 2004 .
- القانون رقم 06 – 22 ، المؤرخ في 20 ديسمبر 2006 ، يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 جويلية 1966 ، المتضمن قانون الإجراءات الجزائية ، ج ر : العدد 84 ، الصادرة بتاريخ 24 ديسمبر 2006 .
- القانون رقم 09 – 04 ، المؤرخ في 5 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر:العدد 47 ، الصادرة بتاريخ 16 أوت 2009.
- القانون رقم 91 / 04 ، المؤرخ في 8 جانفي 1991 ، المتضمن تنظيم مهنة المحاماة ، ج ر : العدد 02 ، الصادرة بتاريخ 9 جانفي 1991 .
- المرسوم الرئاسي رقم 96 – 438 ، المؤرخ في 7 ديسمبر 1996 ، المتعلق بإصدار نص تعديل الدستور ، المصادق عليه في إستفتاء 28 نوفمبر 1996 ، ج ر : العدد 76.

- الأمر رقم 66 – 156 ، المؤرخ في 8 جويلية 1966 ، المعدل والمتمم ، المتضمن قانون العقوبات ، ج ر : 49 ، الصادرة بتاريخ 11 جويلية 1966 .

6/ المواقع الإلكترونية

http://conventions.coe.int/treaty/fr

http://www.legifrance.gouv.fr

الفهرس

المحتويات الصفحة

المقدمة 01

الفصل الأول : الجوانب الموضوعية لجريمة الغش المعلوماتي 04

المبحث الأول : أركان جريمة الغش المعلوماتي 04

المطلب الأول : الركن المادي لجريمة الغش المعلوماتي 05

الفرع الأول : صور الغش المعلوماتي 06

الفرع الثاني : الإحتيال المعلوماتي في ضوء تقسيم الجرائم المستند إلى إعتبارات متصلة بالركن المادي 16

الفرع الثالث : الشروع في جريمة الغش المعلوماتي 18

المطلب الثاني : الركن المعنوي لجريمة الغش المعلوماتي 20

الفرع الأول : القصد الجنائي العام في جريمة الغش المعلوماتي 21

الفرع الثاني : القصد الجنائي الخاص في جريمة الغش المعلوماتي 22

المطلب الثالث : خصائص جريمة الغش المعلوماتي 23

الفرع الأول : السّمات الخاصة بجريمة الغش المعلوماتي 23

الفرع الثاني : سّمات المجرم المعلوماتي 25

المبحث الثاني : المسؤولية الجنائية عن جريمة الغش المعلوماتي 27

المطلب الأول : المسؤولية الجنائية للشخص الطبيعي عن الغش المعلوماتي 28

الفرع الأول : المسؤولية الجنائية للمستخدم عن الغش المعلوماتي 29

الفرع الثاني : المسؤولية الجنائية لمقدمي الخدمات عن الغش المعلوماتي 30

المطلب الثاني : المسؤولية الجنائية للشخص المعنوي عن الغش المعلوماتي 33

الفرع الأول : مسؤولية الشخص المعنوي العام عن الغش المعلوماتي 35

الفرع الثاني : مسؤولية الشخص المعنوي الخاص عن الغش المعلوماتي 36

المطلب الثاني : الجزاء الجنائي لجريمة الغش المعلوماتي 37

الفرع الأول : العقوبات المطبقة على الشخص الطبيعي 38

الفرع الثاني : العقوبات المطبقة على الشخص المعنوي 40

الفصل الثاني : القواعد الإجرائية لجريمة الغش المعلوماتي 44

المبحث الأول : إجراءات مواجهة جريمة الغش المعلوماتي في قانون الإجراءات الجزائية 45

المطلب الأول : إجراء التسرب في جريمة الغش المعلوماتي 45

الفرع الأول : تعريف التسرب 46

الفرع الثاني : شروط صحة عملية التسرب 47

الفرع الثالث : آثار التسرب 49

المطلب الثاني : إجراء إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي 51

الفرع الأول : مفهوم إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي 52

الفرع الثاني : السّرية في إعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي 54

الفرع الثالث : الضمانات المقررة لإعتراض المراسلات السلكية واللاسلكية في جريمة الغش المعلوماتي 55
المبحث الثاني:القواعد الإجرائية لجريمة الغش المعلوماتي في ظل القانون رقم 09 – 04..... 58
المطلب الأول : مراقبة الإتصالات الإلكترونية في جريمة الغش المعلوماتي 58
الفرع الأول المقصود بمراقبة الإتصالات الإلكترونية 59
الفرع الثاني : مشروعية مراقبة الإتصالات الإلكترونية 60
الفرع الثالث : حظر مراقبة الإتصالات الإلكترونية 62
المطلب الثاني : التفتيش في جريمة الغش المعلوماتي 63
الفرع الأول : نطاق تفتيش مكونات الحاسب الآلي في جريمة الغش المعلوماتي 65
الفرع الثاني : تفتيش المنظومة المعلوماتية عن بعد في جريمة الغش المعلوماتي 69
الفرع الثالث : شروط وضمانات التفتيش في جريمة الغش المعلوماتي 72
المطلب الثالث : قواعد حجز المعطيات المعلوماتية في جريمة الغش المعلوماتي 78
الفرع الأول : قواعد ضبط المكونات المادية للحاسب الآلي في جريمة الغش المعلوماتي 80
الفرع الثاني : ضبط المكونات الغير المادية للحاسب الآلي في جريمة الغش المعلوماتي 80
الفرع الثالث : أساليب حجز المعطيات المعلوماتية في جريمة الغش المعلوماتي 81
الخاتمة 84
ملحق رقم 01..... 88
ملحق رقم 02..... 92
قائمة المراجع 97
الفهرس 102