رقم القيد :

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de L'enseignement Supérieur et de La Recherche Scientifique

جامعة عين تموشنت بلحاج بوشعيب

UniversiteAin Témouchent-Belhadj Bouchaib

كلية:الحقوق والعلوم السياسية
قسم:الحقوق
مخبر:الأسواق، التشغيل، التشريع والمحاكاة في الدول المغاربية

أطـروحــة

مقدمة من أجل نيل شهــادة الــدكتــوراه

ميدان: الحقوق والعلوم السياسية

شعبة:الحقوق

تخصص:قانون أعمال

من إعداد :خليفي فتيحة

العنوان

الجرائم الالكترونية المرتبطة بشركات المساهمة

ناقش علنا، بتاريخ 27 جوان 2024 أمام أعضاء لجنة المناقشة المكون من :

الإسم واللقب	الرتبة	الصفة	مؤسسة الإنتماء
أ.د.سويقي حورية	أستاذة	رئيسا	جامعة عين تيموشنت
أ.د.مهداوي محمد صالح	أستاذ	مقررا	جامعة عين تيموشنت
أ.د.زعزوعة فاطمة	أستاذة	مقررا ثانيا	جامعة عين تيموشنت
أ.د.هاملي محمد	أستاذ	ممتحنا	المركز الجامعي مغنية
أ.د.حاج علي بدر الدين	أستاذة	ممتحنا	المركز الجامعي مغنية
د.عبد اللاوي خديجة	أستاذة محاضرة أ	ممتحنا	جامعة عين تيموشنت

السنة الجامعية :2024/2023


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد الله حمدا طيبا مباركا فيه كما ينبغي لجلال وجهه وعظيم سلطانه.

الحمد الله الذي ما تم جهدٌ إلا بعونهِ وما خُتم سعيٌ إلا بفضلهِ.

فالحمد الله الذي أعانني على إتمام هذا العمل وألهمني الصبر ووفقني لمواصلة الدرب.

فلك الحمدُ ولك الشكرُ.

وعملا بقوله صلى الله عليه وسلم "لَا يَشْكُرُ اللهَ مَنْ لَايَشْكُرُ النَّاسَ"

أتوجه بخالص الشكر والتقدير والإمتنان للدكتور "**مهداوي محمد صالح**" الذي تفضل بالإشراف على هذه الرسالة والذي لم يبخل علي بنصائحه وتوجيهاته من أجل إثراء هذا العمل وتصويبه، فكان عوناً صادقًا ومرشدًا أمينًا فجزاك الله عني كل خير أستاذي الفاضل.

شكرا لكل من قدم لي يد العون ولو بالكلمة الطيبة.

إهداء

إلى الوالدين حفظهما الله.

إلى سندي، إخوتي

إلى أصدقائي الصغار، مريم، حنين، يقين، سجى، فادي، أمير.

وإلى الغائبة الحاضرة "**فدوى**" رحمها الله.

إلى كل من يحملهم قلبي ولا يكتبهم قلمي

قائمة المختصرات

أولا: باللغة العربية.

ج: جزء.

ج.ر: جريدة رسمية.

د.س.ن: دون سنة نشر.

د.ت.ص: دون تاريخ صدور.

د.ب.ن: دون بلد نشر.

ص: صفحة.

ط: طبعة.

ع: عدد.

مج: مجلد.

ثانيا: باللغة الأجنبية.

ART: Article.
ED: Edétion.
J.O.R.F: Journal official république francais.
J.H.S: Journal of humane sciences.
N^0: Numéro.
OP. CIT: Ouvrage précédemment cité.
P: Page.
R.I.D.C: Revue internationale de droit comparé.
R.D.E.J: Revue diaa des études juridique.
VOL: Volume.

مقدمة

مقدمة:

يعد التحول الرقمي من أبرز السمات والملامح التي يتميز بها العالم اليوم، وذلك على جميع الأصعدة وخاصة الصعيد الاقتصادي الذي إنتقل من الاقتصاد التقليدي إلى الاقتصاد الرقمي والذي يمكن تعريفه على أنه، ذلك الاقتصاد الذي يقوم على أساس إستخدام تكنولوجيا المعلومات والإتصال والتي تسهل عملية تدفق كل من المعلومات والسلع والخدمات وحركة رؤوس الأموال من و إلى أية نقطة في العالم وذلك في أي وقت[1].

وبالتالي من خلال من خلال هذا الاقتصاد يمكن تحقيق الفروقات الخمسة والمتمثلة في كل من الوقت، التكلفة، الوفرة، الجودة والجهد، والتي كان من الصعب تحقيقها مجتمعة كاملة في ظل الاقتصاد التقليدي الذي كان يتطلب وقتا أطول وتكلفة أكبر، إذ أنه بظهور الاقتصاد الرقمي ظهر ما يعرف بالسلع والخدمات الرقمية وذلك على إختلاف أنواعها وأشكالها والتي بطبيعة الحال لها قيمة إقتصادية كبيرة في تحقيق نمو الدول، الشيئ الذي ينجم عنه تقليص الفجوة بين الدول التي تشهد إقتصادا رقميا محتشما وتلك التي تشهد إقتصادا رقميا متسارعا ومتطورا.

وفي الوقت الذي زاد فيه إنتشار الاقتصاد الرقمي إنتشارا مذهلا شاع ما يعرف بالتجارة الإلكترونية والتي يعتمد عليها الاقتصاد الرقمي، والتي تعود نشأتها إلى الستينيات من القرع العشرين حيث كانت تعرف باسم التبادل الإلكتروني وكانت قد إقتصرت في البداية على تبادل البيانات المتعلقة بعملية البيع والشراء وذلك بين بعض المؤسسات الكبيرة عبر الشبكات الإلكترونية خاصة، أما بالنسبة للمصارف فقد إستعملت ما يعرف بنظام تحويل الأموال الإلكترونية وذلك بغية تحسين خدماتها المالية، ومع نهاية القرن العشرين عوضت الأنترنت شيئا فشيئا

[1] خالد رجم، خولة واصل، الويزة سعادة، (واقع الاقتصاد الرقمي في الجزائر دراسة تحليلية لقطاع تكنولوجيا المعلومات والإتصال)Journal of economic Growthand entrepreneurshp، ع 1، مج 1، الصادر في 2019/12/25، ص 44.

نظام التبادل الإلكتروني للبيانات المستعملة من طرف المؤسسة لتتطور بعد ذلك التجارة الإلكترونية إلى أن وصلت إلى ما هي عليه الآن.[1]

وما ينبغي الإشارة إليه هو أن ممارسة النشاط التجاري لا يقتصر على الأفراد فقط كونه مجالا متسعا ومتنوعا، الأمر الذي ينجم عنه وقوف هؤلاء الأفراد عاجزين عن النهوض بالمجال التجاري وتلبية كافة الحاجيات المتعلقة به، الأمر الذي إستلزم بروز كيانات قانونية تكون لها القدرة الكافية على إدارة المشروعات الضخمة والتي تتطلب أموالا طائلة ومجهودات كبيرة، لتظهر بذلك ما يعرف بالشركات التجارية والتي تعتبر من أهم ظواهر الحياة الاقتصادية فهي تعد من أقدم العقود في التاريخ، والتي عرفتها الحضارات القديمة من أجل سد ثغرات أكتنفت تلك الحياة ولا أدل على ذلك من شريعة حمورابي والتي تعد من أقدم الوثائق القانونية التي عرفت إلى غاية اليوم، فقد تم رصد ثماني مواد من المادة 100 إلى غاية المادة 107 في التنظيم القانوني للشركة وذلك من أصل 44 مادة خصصت للعقود، إذ مازال بعضها شاخصا إلى غاية اليوم تأخذ بأحكامها معظم التشريعات الحديثة.[2]

وبمرور الزمن نمت وتطورت هذه الشركات حتى أصبحت هي المسيطرة على المجال التجاري وذات سلطان لا يعلو عليه غير سلطان الدولة، وهذه الشركات تنقسم من الناحية القانونية إلى قسمين، شركات أشخاص وشركات أموال والتي يُعد نموذجها البارز شركات المساهمة نظرا لقُدوراتِها الضخمة التي تتمبز بها.

ونظرًا لجملة التطورات التكنولوجية التي شهدها العالم بسبب إستخدام تكنولوجيا المعلومات والإتصال والتي شهد على إثرها ما يعرف بالإقتصاد الرقمي والتجارة الإلكترونية كما سبقت الإشارة إلى ذلك وهذا نتيجة المزاوجة بين مختلف الشبكات والتقنيات التي تتميز بها أجهزة الحاسوب.

فنجد بأن المعلومات أصبح يتم تداولها عبر مختلف الشبكات العالمية المفتوحة وكذا المحلية بعيدًا تمامًا عن الطرق التقليدية الكلاسيكية، الأمر الذي نجم عنه حدوث تغييرات

[1] بوعافية رشيد، يدو محمد، (التجارة الإلكترونية والإستثمار عبر شبكة الأنترنت الإطار النظري والتطبيقي)، مجلة الاقتصاد الجديد، ع 18، مج 1، الصادر في 2018، ص 154.

[2] أحمد عبد الرحمان بن سالم، (التحول الإلزامي للشركة التجارية دراسة مقارنة)، مجلة الحقوق والعلوم الإنسانية ، ع 1، مج 15، الصادر في 2022، ص 406.

جذرية في كافة أساليب وطرق العمل نتيجة للدور الواضح والفعال الذي أثبتته هذه التطورات التكنولوجية.

وعلى إثر ذلك سارعت جلّ القطاعات بما فيها القطاع التجاري إلى إعتماد هذه التكنولوجيا والتي ظهرت آثارها الإيجابية من خلال القفزة النوعية والتقدم الواضح الذي شهِدته تلك القطاعات، وفي خضّم هذا التسارع نحو هذه التكنولوجيا نجد بأن شركات المساهمة وباعتبارها النموذج الأمثل لشركات الأموال والممثلة للقطاع التجاري، لم تبق بمعزل عن هذه التطورات التكنولوجية بل سارعت هي الأخرى إلى إعتمادها لتبلغ بذلك ذروة التقدم والتطور.

إذ أصبح لا مجال للإستغناء عن إستعمال هذه التكنولوجيا من أجل القيام بالأعمال والأنشطة التجارية الخاصة بشركات المساهمة، فجلّ أعمالها يتم تنفيذها بطريقة إلكترونية سواء كانت تلك الأعمال بينها وبين العملاء أو بينها وبين غيرها من الشركات، من خلال إستخدام الأنظمة المعلوماتية والتي أضّحت تعد الأداة الأساسية في معالجة وتخزين ونقل البيانات والمعلومات بل ومستودعا لأسرارها التجارية.

لكن من جهة أخرى، فإن إستخدام شركات المساهمة للتقنيات التي أفرزتها التطورات التكنولوجية لم يكن له فقط ذلك الجانب المشرق والإيجابي، وإنما كانت له إنعكاسات سلبية على درجة كبيرة من الخطورة، فهناك من عمِل بمكرٍ ودهاءٍ على إساءة إستخدام هذه التقنيات من أجل الإعتداءعلى هذه الشركات واستهداف أنظمتها المعلوماتية، بل أنه كلما زاد إستخدامها لتقنيات متطورة أكثر كلما تضاعف تعرضها للإعتداء بشكل أكبر، وذلك نظرا لظهور نوع جديد من الجرائم التي لم تكن معروفة من قبل تسمى بالجرائم الإلكترونية، ذات الصلة الوثيقة بمدى إعتماد شركات المساهمة على الوسائل التقنية في إنجاز أعمالها لتكون بذلك خطرا يهدد أمنها المعلوماتي.

ولا مجال للجدال والشك بأن الجرائم الإلكترونية من أخطر أنواع الجرائم وأكثرها تعقيدا، فبعد ما كان الجناة يعتدون على شركات المساهمة بطرق تقليدية محدثين بذلك صخبا بسبب إستهدافها في أموالها المادية، مخلفيّن وراءهم مسرحا شاهدا على ما إرتكبوه من سلوكات

إجرامية فإن الأمر الآن مختلف تماما في ظل الجرائم الإلكترونية التي إتخذ جناتها من البيئة الإفتراضية مسرحا لها، معتمدين في إرتكابها على وسائل تكنولوجية في غاية الدقة والتطور تسمح لهم بتنفيذ اعتدائهم دون أن يُحدث ذلك أي ضجيج أو عنف وفي أسرع وقت ممكن وبأقل جهد.

كما أن إعتداء الجناة على شركات المساهمة في ظل الجريمة الإلكترونية لم يعد يستهدف الأموال المادية لها فقط، بل أن معلوماتها وأسرارها التجارية أصبحت أكثر إستهدافا وذلك نظرا لما تمثله من أهمية، بل أنها تعد رأسمال لهذه الشركات وأن المساس بها يؤدي إلى إزاحتها من الساحة التجارية، فإذا كان بعض الجناة يحصلون عليها إرضاءً لغرورهم وإثباتا لذكائهم وقدرتهم على الإختراق فإن البعض الآخر يحصلون عليها من أجل إبتزاز هذه الشركات أو المتجارة فيها مع غيرها من الشركات المنافسة، ورغم أن هؤلاء الجناة قد يكونوا من داخل الشركة أو من خارجها غير أن هدفهم واحد وهو الإعتداء على هذه الشركات.

وقد تعددت وتنوعت أنماط الجرائم الإلكترونية التي أصبحت تستهدف شركات المساهمة، فمنها ما يرتكب ضد نظامها المعلوماتي من خلال الولوج إليه والإعتداء على وظائفه ومعطياته، ولم يتوقف الأمر عند هذا الحد بل عمد مرتكبي هذه الجرائم إلى التطوير من الأساليب الإجرامية ليتمكنوا بذلك من الإعتداء على هذه الشركات من خلال الجرائم التقليدية ولكن بطريقة إلكترونية، لتصبح البيئة الإفتراضية مجالا خصبا لجرائم التجسس، التزوير، خيانة الأمانة، السرقة، الإحتيال وغسل الأموال.

وأمام هذا التنوع من الجرائم الإلكترونية التي باتت شركات المساهمة عرضة لها، ونظرا للطابع المعقد الذي تتسم به أساليب إرتكابها فإن إكتشافها لم يكن أبدا بالأمر البسيط أو الهين من قبل هذه الشركات بل أن العديد منها تم إكتشافها بمحض الصدفة، الأمر الذي إستلزم إتباع أساليب خاصة من أجل القيام بإجراءات التحري والتحقيق حتى تتناسب والبيئة الإفتراضية لهذه الجرائم، فهذه البيئة لا مجال للإعتراف أمامها بالحدود الإقليمية، فجناة الجرائم الإلكترونية وشركات المساهمة لا يشترط أن يكونوا ضمن حيز جغرافي واحد مثلما يحدث في الجرائم التقليدية التي تتعرض لها.

ومن المؤكد بأن الجرائم الإلكترونية أول ما ظهرت كانت تستهدف بشكل أوسع الأفراد في سمعتهم وشرفهم واعتبارهم وحياتهم الخاصة، غير أن الأمر تغير فيما بعد لتتجه نحو شركات المساهمة حيث تضاعفت الإعتداءات الموجهة ضدها وهي في تزايد مستمر.

وعلى ضوء ما سلف طرحه تتجلى أهمية هذه الدراسة في أن الجرائم الإلكترونية رغم حداثتها غير أنها تشهدا تطورات مذهلة بشكل يومي في أساليب إرتكابها فهي متعددة ومتجددة باستمرار، خاصة وأنها أصبحت تستهدف أكبر الشركات –شركات المساهمة– التي تمثل ركائز الإقتصاد بالنسبة للدول وأن المساس بها يعني المساس بالإقتصاد وزعزعته، والنتيجة المترتبة على ذلك هي إنعدام الأمن الاقتصادي.

إلى جانب ذلك تبرز أهمية هذه الدراسة في أن شركات المساهمة إتجهت إلى إستخدام أجهزة الحاسوب وشبكات الأنترنت ومختلف التقنيات من أجل ممارسة أعمالها التجارية، الأمر الذي زاد من إحتمال تعرضها للجرائم الإلكترونية، فحسب الإحصائيات المتعلقة بالجريمة الإلكترونية فقد تم الكشف عن أرقام مرعبة تدل أنها فعلا تشكل خطرا محدقا يهدد هذه الشركات، حيث كلفت خروقات بيانات الشركات في المتوسط 4،35 مليون دولار عام 2022 وكانت قد أفادت 39% من الشركات البريطانية أنها تعرضت لهجوم إلكتروني في عام 2022 والتي كلفتها 4200 جنيه إسترليني في نفس العام، هذا وقد كان للغزو الروسي على أوكرانيا تأثيرا هائلا على مشهد التهديدات الإلكترونية منذ بداية الحرب فقد زادت هجمات التصيد التي تتخذ من روسيا مقرا لها ضد عناوين البريد الإلكتروني للشركات التي تتخذ من أوروبا والولايات المتحدة الأمريكية مقرا لها 8 أضعاف.

كما شهدت تكلفة إختراق بيانات الشركات إرتفاعا بشكل مطرد وصلت في المتوسط إلى 4،35 مليون دولار في عام 2022 بعد أن كانت 4،24 في عام 2021 وذلك بسبب التغييرات في مكان العمل وكذا أساليب الإختراق الأكثر تقدما مما شجع مجرمي الأنترنت على ذلك .[1]

[1] عبد الرحمن عايش، أحدث إحصائيات الجرائم الإلكترونية لعام 2023، مقال منشور على صفحة تكنولوجيا اليوم بتاريخ 2023/05/19، تاريخ الدخول: 2024/06/29، متاح على الرابط: https://today-tech.net.

وهناك بعض الدراسات (دراسة بن جدو بن علية، درار عياش) أشارت إلى أن الجرائم الإلكترونية تكلف الاقتصاد العالمي 0،8% كنسبة مئوية من الناتج المحلي الإجمالي وهناك توقعات قد أظهرت تسجيل ارتفاع صاروخي في الخسائر التي تتكبدها الدول جراء هاته الجرائم، إذ من المتوقع أن تقفز إلى 23،82 تريليون دولار بحلول عام 2027 مقابل 860 مليار دولار في عام 2018 أي أنها ستتضاعف بأكثر من 27 مرة، حيث أنه في نهاية عام 2019 كان هناك هجوم إلكتروني منظم على شركة "سولارويندز" الأمريكية وتم على إثره سرقة بيانات 18000عميل ولم يتم إكتشاف هذا الهجوم إلا في ديسمبر 2020 ولم تكتشف تفاصيله إلا في يناير 2012 ليصرح بعدها رئيس الشركة بأن هذا الهجوم يعد الأكبر والأكثر تعقيدا في تاريخ العالم كله.[1]

وانطلاقا من الأهمية التي تكتسيها هذه الدراسة فإن الهدف من ورائها هو تسليط الضوء على جملة أنوع الجرائم الإلكترونية التي قد تتعرض لها شركات المساهمة والطريقة التي يتم من خلالها إرتكابها وكذا التعرف على الثغرات التي تمكن الجناة من تحقيق إختراقهم لها.

وباعتبار أن الجرائم الإلكترونية التي تسهدف شركات المساهمة ذات طبيعة خاصة وفي غاية التعقد والغموض فإن هذه الدراسة تهدف أيضا إلى التعرف على الإجراءات المتعلقة بعملية التحري والتحقيق والجهة القضائية المختصة بالفصل فيها وكذا الدليل المناسب لإثباتها والآليات التقنية التي ينبغي على شركات المساهمة إتخاذها حتى تقي نفسها من خطر هاته الجرائم وبالتالي تحقيق أمنها المعلوماتي.

لذلك فإن الدواعي والأسباب التي كانت وراء إختيار دراسة الجرائم الإلكترونية المرتبطة بشركات المساهمة تعود إلى الطبيعة التقنية التي تتميز بها هذه الجرائم ، والتي تختلف جملة وتفصيلا عن تلك الجرائم التقليدية المألوفة التي كانت تتعرض لها شركات المساهمة وكذا التعرف على البيئة الرقمية التي تتخذ منها هذه الجرائم مسرحا لها.

[1] عوني الداوود، الجرائم الإلكترونية آثار مدمرة على إقتصادات الدول والشركات والبنوك والأفراد، مقال منشور على صفحة مركز الدستور للدراسات الاقتصادية، بتاريخ يوليو 2023، تاريخ الدخول 2024/06/29، متاح على الراط: https://www.addustour.com

بالإضافة إلى كونه موضوع متخصص أكثر، حيث أن جل الدراسات التي تناولت الجرائم الإلكترونية كانت ضمن إطار عام ومن أبرز تلك الدراسات نجد:

– دراسة الباحث يرمش مراد تحت عنوان: "خصوصية الجريمة الإلكترونية"[1]

– دراسة الباحثة هروال هبة نبيلة تحت عنوان: "جرائم الأنترت دراسة مقارنة"[2]

– دراسة الباحث فايز محمد راجح غلاب تحت عنوان: " الجرائم المعلوماتية في القانون الجزائري واليمني"[3]

– دراسة الباحثة عفاف خذيري تحت عنوان: " الحماية الجنائية للمعطيات الرقمية"[4]

فجل هذه الدراسات تطرقت إلى مختلف أنواع الجرائم الإلكترونية التي يمكن أن ترتكب دون التمييز بين الجهات التي تستهدفها وحصرها ضمن جهة معينة سواء كانت تتمثل في أشخاص طبيعية أو معنوية، بل أنه أحيانا تم التركيز بصورة أكثر على الزاوية المرتبطة بالأشخاص الطبيعية، لذلك فالجديد ضمن هذه الدراسة التي سنقوم بها هو أنها ستتناول موضوع الجرائم الإلكترونية بشكل حصري ضمن شركات المساهمة.

ومن أجل معالجة هذه الدراسة والوقوف على مختلف جوانبها نطرح الإشكالية التالية: **فيما تتمثل الجرائم الإلكترونية التي تستهدف شركات المساهمة؟**

وعلى ضوء هذه الإشكالية تتفرع العديد من التساؤلات:

– ما مفهوم الجريمة الإلكترونية وما المحل الذي تنصب عليه في إطار شركات المساهمة؟

– ما هي الأساليب التي يلجأ الجناة إلى إستخدامها من أجل إختراق شركات المساهمة؟

---

[1] الدراسة عبارة عن أطروحة دكتوراه بجامعة الجزائر 1 للسنة الجامعية 2020–2021 ، تطرق الباحث من خلالها إلى كل من القواعد الموضوعية والإجرائية للجريمة الإلكترونية.

[2] الدراسة عبارة عن أطروحة دكتوراه بجامعة بجامعة أبي بكر بلقايد تلمسان للسنة الجامعية 2013–2014، حيث تناولت فيها الباحثة جرائم الأنترنت ضمن بابين جرائم الإعتداء على الأشخاص وجرائم الإعتداء على الأموال.

[3] والدراسة عبارة عن أطروحة دكتوراه بجامعة الجزائر 1 للسنة الجامعية 2010–2011، حيث عرض فيها الباحث أهم الجرائم المعلوماتية في القانون الجزائري واليمني وكذا قواعدها الإجرائية.

[4] الدراسة عبارة عن أطروحة دكتوراه بجامعة العربي التبسي تبسة للسنة الجامعية 2017–2018 وقد تطرقت الباحثة في هذه الدراسة إلى الجرائم الواقعة على المعطيات الرقمية والأحكام الإجرائية الخاصة بحمايتها.

– كيف تتم الإجراءات الخاصة بالتحري والتحقيق ضمن هذه الجرائم في إطار شركات المساهمة؟

– ما هو الدليل المناسب لإثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة وما الجهة القضائية المختصة بنظرها؟

– فيما تتمثل الآليات التي ينبغي على شركات المساهمة إتخاذها حتى تحقق أمنها المعلوماتي وتحمي نفسها من خطر الجرائم الإلكترونية؟

وحتى نتمكن من إنجاز هذه الدراسة بالشرح والتحليل فإن الأمر يتطلب منّا الإستعانة بالمنهج الوصفي والتحليلي، وذلك كونهما الأنسب لوصف الجرائم الإلكترونية والتعمق في تحليل كيفية إرتكابها على شركات المساهمة، دون أن نغفل عن الإستعانة في بعض الحالات بالمنهج المقارن حينما يستلزم منا الأمر المقارنة في بعض الجرائم الإلكترونية بينها وبين صورتها التقليدية أو المقارنة بين بعض هذه الجرائم في القانون الوطني وبعض القوانين الأخرى.

وحتى تتم الإجابة على الإشكالية المطروحة ومختلف التساؤلات المتفرعة عنها إرتأينا تقسيم هذه الدراسة إلى بابين:

الباب الأول تحت عنوان "**تكنولوجيا المعلومات والجرائم الإلكترونية** " بحيث نتعرض في الفصل الأول منه إلى تحديد الإطار المفاهيمي لتكنولوجيا المعلومات وذلك بتحديد مفهومها ومكوناتها والأحكام الخاصة بشركات المساهمة وانعكاس هذه التكنولوجيا عليها من خلال توجهها نحو الأعمال والتجارة الإلكترونية وانتقالها من الإدارة التقليدية إلى الإدارة الإلكترونية، أما الفصل الثاني فنتعرض فيه إلى ماهية الجرائم الإلكترونية في إطار شركات المساهمة والأحكام الخاصة بمحلها وأساليب إرتكابها وكذا الأركان التي تقوم عليها.

أما الباب الثاني تحت عنوان "**الجرائم الإلكترونية الواقعة على شركات المساهمة وقواعدها الإجرائية والأمنية**" حيث نتطرق في الفصل الأول منه إلى الصور المختلفة للجرائم الإلكترونية التي تتعرض لها شركات المساهمة، في حين نتطرق في الفصل الثاني منه

إلى القواعد الإجرائية والأمنية الخاصة بها سواء ما تعلق بإجراء التحري والتحقيق والمحاكمة وكذا عملية إثباتها وإجراءات الوقاية منها

لنختتم في الأخير هذه الدراسة بجملة النتائج المتوصل إليها وكذا جملة التوصيات المقدمة.

الباب الأول:

تكنولوجيا المعلومات والجرائم الإلكترونية

الباب الأول:

تكنولوجيا المعلومات والجرائم الإلكترونية.

دخل العالم في الفترة الأخيرة مرحلة جديدة تولدت عن جملة التطورات التكنولوجية التي شهدها والتي إنعكست على كافة مناحي الحياة ومجالاتها المختلفة، إذ أصبحت تلك التطورات عنوانا أساسيا في العصر الحالي الذي أصبح لا يعتد فيه بالحدود الزمانية والمكانية.

ومن دون أدنى شك بأن المجال التجاري يعد أول المجالات تأثرا بالتطورات التكنولوجية التي تشهد إنتشارا وعمقا متزايدا، وبطبيعة الحال نجد بأن شركات المساهمة باعتبارها من أهم ركائز المجال التجاري لم تبق بمنأى عن هذه التطورات، وإنما شهدت هي الأخرى عدة تغييرات نتيجة لذلك، إذ عرفت تحولات جذرية في طرق أدائها لأنشطتها وأعمالها التجارية وبالتأكيد هذا التحول كانت له نتائج إيجابية تجلت في نماذج أعمالها الجديدة كتوجهها نحو الأعمال والتجارة الإلكترونية وكذا إنتقالها من نمط الإدارة التقليدية إلى الإدارة الإلكترونية ، التي حققت لها نموا وتطورا سريعا ومكانة في ساحة الأسواق التجارية، المحلية وكذا الدولية.

لكن من جهة أخرى فإن جملة التطورات التكنولوجية التي إعتمدتها شركات المساهمة لم يكن لها الأثر الإيجابي والجانب المشرق فقط، وإنما كان لها في مقابل ذلك أثر سلبي يمثل الجانب المظلم لها والذي يتمثل في ميلاد نوع جديد من الجرائم لم تكن تعرفها هذه الشركات في ظل بيئة أعمالها التقليدية تسمى بالجرائم الإلكترونية والتي أضحت خطرا حقيقيا يهدد مكانتها، وذلك كونها جرائم ذات طبيعة منفردة تختلف عن نظيرتها التقليدية حيث تنفذ بوسائل تقنية جد دقيقة ذات تطور سريع مما يجعلها تتسم بالخفاء وصعبة الإثبات، كما تكمن خطورتها في المحل الذي تنصب عليه والمتمثل في النظام المعلوماتي الذي يعد مركز تخزين أسرارها التجارية إذ تتجاوز قيمته بالتأكيد قيمة أموالها المادية في ظل الجرائم التقليدية، ولتوضيح ذلك سنقوم بتقسيم هذا الباب إلى فصلين:

الفصل الأول: تكنولوجيا المعلومات وانعكاسها على شركات المساهمة.

الفصل الثاني: الإطار المفاهيمي للجرائم الإلكترونية في إطار شركات المساهمة.

الفصل الأول:

تكنولوجيا المعلومات وانعكاسها على شركات المساهمة

الفصل الأول:

تكنولوجيا المعلومات وانعكاسها على شركات المساهمة.

ترتكز المرحلة الجديدة التي دخل إليها العالم نتيجة التطورات التكنولوجية على المعلومات التي باتت تمثل المادة الأساسية لشركات المساهمة من أجل القيام بأعمالها وأداء وظائفها، إذ أصبحت تتسارع فيما بينها إلى الإعتماد على ما أسفرت عليه تلك التطورات، قصد التحكم في إدارة ذلك الكم الهائل من معلوماتها وبياناتها وتخزينها وتداولها بشكل دقيق ومنظم حتى تحافظ على وجودها وتضمن قدرتها على البقاء في مجال المنافسة أمام غيرها من الشركات.

ويعد هذا السبب وراء إعتماد شركات المساهمة على تكنولوجيا المعلومات والتي أضحت عاملا مهما لا يمكن الإستغناء عليه حتى تتمكن من تحقيق أهدافها التجارية، فهي تشتمل على مختلف التقنيات التي تمكنها من معالجة ذلك الكم الضخم من بياناتها والإحتفاظ بها واسترجاعها في أقل وقت ممكن عند الحاجة إليها، مما يضفي تحسينات جذرية عليها وبالتالي يسهل عليها عملية إتخاذ القرار، بالإضافة إلى تدعيم علاقاتها بعملائها.

لذلك فإن تكنولوجيا المعلومات لها إنعكاسات جد إيجابية على شركات المساهمة ولمعرفة الدور الذي تلعبه بالنسبة لها سنقوم بتقسيم هذا الفصل إلى مبحثين:

المبحث الأول:الإطار المفاهيمي لتكنولوجيا المعلومات.

المبحث الثاني: الأحكام الخاصة بشركات المساهمة وانعكاس تكنولوجيا المعلومات عليها.

المبحث الأول:

الإطار المفاهيمي لتكنولوجيا المعلومات.

أصبحت تكنولوجيا المعلومات وسيلة لا غنى عنها بالنسبة لشركات المساهمة من أجل أداء أعمالها التجارية في أسرع وقت ممكن وبأقل جهد وبصورة متقنة، فالعديد من الشركات تمكنت من فرض نفسها واحتلال الأسواق في فترة وجيزة بفضل إعتمادها لهذه التكنولوجيا التي رغم حداثتها إلا أنها تمكنت من إحداث قفزة في حياة تلك الشركات، لذا كانت محط إهتمام الباحثين والمختصين على إختلاف منطلاقاتهم الفكرية ومرجعياتهم العلمية ومن خلال هذا المبحث سنقوم بتوضيح الإطار المفاهيمي لتكنولوجيا المعلومات وذلك بتقسيمه إلى مطلبين:

المطلب الأول: مفهوم تكنولوجيا المعلومات.

المطلب الثاني: مكونات تكنولوجيا المعلومات.

المطلب الأول:

مفهوم تكنولوجيا المعلومات.

إذا كان مفهوم تكنولوجيا المعلومات يوحي بشكل عام إلى تلك البيانات والمعلومات التي يتم معالجتها وتخزينها بطريقة تكنولوجية أي الإنتقال من العمل اليدوي إلى العمل الإلكتروني، إلا أن مفهوم هذه التكنولوجيا كان محل إختلاف ويعود السبب في ذلك إلى حداثتها وتطورها الدائم، وللوقوف على ذلك سنقوم من خلال هذا المطلب بالتطرق إلى تعريف تكنولوجيا المعلومات وأهميتها **(فرع أول)** ثم خصائص تكنولوجيا المعلومات ومراحلها **(فرع ثاني)**.

الفرع الأول:

تعريف تكنولوجيا المعلومات وأهميتها.

لم تحض تكنولوجيا المعلومات بتعريف موحد وشامل فهناك العديد من التعريفات التي قيلت بشأنها وكل تعريف كان حسب وجهة نظر صاحبه لهذه التكنولوجيا، كما لها أهمية بالغة بالنسبة لشركات المساهمة.

أولا: تعريف تكنولوجيا المعلومات.

بالنسبة لمصطلح تكنولوجيا هو مصطلح يوناني الأصل [1] يتكون من مقطعين "TECHNO" ومعناه التطبيق،[2] (LOGHY) ومعناه العلم[3] وعند تركيب المصطلحين مع بعض يصبح مصطلح تكنولوجيا يعني ذلك العلم التطبيقي أو الطريقة ذات الطبيعة التقنية التي تستخدم بقصد تحقيق عمل.[4]

عرفها الأستاذ قاسم جميل بأنها كافة نماذج المعرفة وكذا المهارات الفنية اللازمة من أجل تطوير الآلات وكذا الطرق التي يتم بواسطتها الإنتاج والتصميم وذلك طبقا للقواعد الاقتصادية،[5] وهي أيضا كل ما يستند على أجهزة الحواسيب ومختلف الوسائل المتطورة من أجل معالجة البيانات المتحصل عليها بطريقة سريعة.[6]

كما تعرف على أنها تلك الوسائل التي يتم إستعمالها من أجل القيام بعمليات معالجة وتخزين وكذا إسترجاع البيانات والمعلومات، بغض النظر عن الشكل الذي تتخذه سواء كانت صوتا أو كتابة أو صورة.[7]

في حين عرفها "LUCAS" بأنها جميع أنواع التكنولوجيا التي يتم تطبيقها بهدف القيام بعملية المعالجة، التخزين وكذا التوزيع وذلك في شكل إلكتروني كما أنها تشمل إلى جانب ذلك الأجهزة

---

[1] عبد الإله النوايسة ، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، الأردن، دار وائل للنشر والتوزيع، 2017، ص 31.

[2] خلود عاصم ، (دور تكنولوجيا المعلومات والإتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية)، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية، الصادر في 2013، ص 232.

[3] عبد الإله النوايسة، مرجع سابق، ص 31.

[4] خلود عاصم، مرجع سابق، ص 232.

[5] مشري محمد الناصر، "سبل تفعيل دور تكنولوجيا المعلومات والإتصال في دعم التنمية المستدامة في المؤسسات الصناعية الجزائرية –دراسة عدد من المؤسسات في الشرق الجزائري–" (أطروحة دكتوراه، كلية كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة فرحات عباس سطيف 1، 2016–2017)، ص ص 19، 20.

[6] سراج طلعت عبد النبي الوحيدي، "أثر إستخدام تكنولوجيا المعلومات على كفاءة أساليب المحاسبة الإدارية الحديثة في الشركات الصناعية في قطاع غزة" (رسالة ماجستير، كلية التجارة، الجامعة الإسلامية غزة، 2017)، ص 47.

[7] أمال سلطان، صليحة عشبي، (تكنولوجيا المعلومات والإتصال وأثرها على كفاءة أداء المؤسسة، دراسة حالة مؤسسة نقاوس للمصبرات باتنة)، المجلة الجزائرية للأمن الإنساني، ع 1، مج 6، الصادر في جانفي 2021، ص 1365.

المعتمدة لهذا الغرض والتي تتمثل في الحواسيب والشبكات،[1] كما نجد بأن منظمة "اليونسكو" قد تطرقت إلى تعريفها بأنها، مصطلح يتم إستخدامه قصد وصف الوسائل والطرق المستعملة في عمليات المعالجة، التخزين، التنظيم وكذا تبادل المعلومات وذلك بطريقة إلكترونية من خلال إستخدام الأدوات الصلبة والمرنة والمعدنية والإتصالات في شكل حواسيب شخصية وماسحات ضوئية.[2]

وهناك من ينظر إليها على أنها تتمثل في أجهزة الحواسيب التي يتم الإعتماد عليها من قبل الأشخاص حتى يتمكنوا من التعامل مع كم المعلومات وتدعيمها قصد تفعيل تلك المعلومات وتسخيرها لتحقيق أهداف منظمة ما.[3]

وعلى ضوء ما تم ذكره، يمكننا أن نعرف تكنولوجيا المعلومات بأنها مختلف التقنيات والأجهزة التي توصل إليها التطور التكنولوجي والتي يتم الإعتماد عليها في معالجة ذلك الكم الضخم من البيانات وذلك في مختلف المراحل، إنطلاقا من إدخالها إلى تخزينها وتنظيمها واسترجاعها عند الحاجة إليها وذلك بطريقة آلية ودقيقة وسريعة.

ثانيا: أهمية تكنولوجيا المعلومات لشركات المساهمة.

نظرا للمستوى التكنولوجي الذي وصل إليه العالم فلا مجال للشك أبدا في أن إستخدام شركات المساهمة لهذه التكنولوجيا يمثل قيمة حقيقية لا غنى عنها، حيث تتجلى أهميتها في النقاط التالية:

1-تساهم في تطوير أعمال شركات المساهمة وإضفاء تحسينات جذرية عليها مما ينمي لديها الكفاءة التسويقية والإنتاجية وكذا الإدارية، وبالتالي إدارة مواردها بشكل متطور ومبتكر كما تمكنها من التعامل الإلكتروني.[4]

---

[1]وسيلة هني، "أثر إستخدام تكنولوجيا المعلومات على أداء المؤسسة الاقتصادية –دراسة نماذج بعض البلدان العربية–" (أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجيلالي اليابس سيدي بلعباس، 2017-2018)، ص 34.

[2]عبد الإله النوايسة ، مرجع سابق، ص 32.

[3]أديب محمد حسن هزايمه، "أثر تطبيق تكنولوجيا المعلومات على تحسين الميزة التنافسية في شركات المساهمة العامة" (أطروحة دكتوراه، كلية الأعمال، جامعة عمان العربية، 2011)، ص 24.

[4]المرجع نفسه، ص ص 26، 27.

2-تساعد على عمليات إتخاذ القرار بالنسبة لهذه الشركات وذلك من خلال قاعدة المعلومات الدقيقة التي توفرها عند الحاجة إليها وفي الوقت المناسب، بالإضافة إلى زيادة قنوات الإتصال والتي تسمح بتدفق المعلومات وتبادلها بشكل مضاعف وفي ظرف وجيز زيادة على عملية التنسيق بين فروع هذه الشركات بشكل أسرع وذلك عن طريق شبكات الإتصال التي تربط الحواسيب مع بعضها البعض.[1]

3-مكنت تكنولوجيا المعلومات هذه الشركات من تبادل المعلومات إلكترونيا مع غيرها من الشركات الأخرى وعقد الصفقات بطريقة إلكترونية وهذا ما يساهم في تحسين الجودة من خلال تقليل الأحطاء.

4-مساعدتها على تحسين وضعها ضمن البيئة التنافسية وذلك بواسطة البرامج والتطبيقات المبتكرة في هذا الإطار والتي تساعد على المنافسة بطريقة أكثر فعالية.[2]

5-تعمل تكنولوجيا المعلومات على تحسين المعلومات المحاسبية الخاصة بشركات المساهمة ويتحقق ذلك عن طريق إعتمادها لحزم برمجية محاسبية وكذا البرامج الخاصة بصياغة النماذج المالية، الأمر الذي يساعد محاسبيها الماليين على تجميع معلوماتها المالية وتحليلها بأسرع وقت وبأقل جهد مع ضمان أهداف المحاسبة وبجودة عالية ودقيقة، وبالتالي تكون ذات مصداقية وخالية من التحريف والتضليل وهذا ما ينعكس بالإيجاب على هذه الشركات في حسم قراراتها التجارية.[3]

6-تمكن تكنولوجيا المعلومات شركات المساهمة من تدعيم وتفعيل إدارة علاقاتها بعملائها وبالتالي ضمان إستمراريتهم معها، كما تسمح لها أيضا بتحويل عملائها الجدد إلى عملاء دائمين واستقطاب المزيد من الزبائن وبذلك تحافظ على مكانتها واستمراريتها في الأسواق التجارية.[4]

وما ينبغي أن نشير إليه هو أن توطيد العلاقة مع العميل ركيزة أساسية بالنسبة لهذه الشركات، حيث أن عميل واحد قد يوفر أموالا كبيرة وفي مقابل ذلك فإن فقدان عميل يعني ضياع صفقة الأمر

---

[1] ليلى هيكل، "أثر إستخدام تكنولوجيا المعلومات في أداء المنظمات –دراسة تطبيقية على شركة الأمل لصناعة الأدوية– " (رسالة ماجستير، الجامعة الإفتراضية السورية، 2015)، ص 18.

[2] علي جقريب، "أثر إستخدام تكنولوجيا المعلومات على أداء بورصة عمان للأوراق المالية " (رسالة ماجستير، كلية إدارة المال والأعمال، جامعة آل بيت، 2010)، ص 43.

[3] خلود عاصم ، مرجع سابق، ص ص 236، 237.

[4] عبد الله غالم، محمد قريشي، (دور تكنولوجيا المعلومات في تدعيم وتفعيل علاقات الزبائن)، مجلة أبحاث إقتصادية وإدارية، ع 10، الصادر في 2011، ص ص 146، 154.

الذي قد يؤدي بالشركة إلى الهاوية، خاصة في ظل المنافسة الشديدة بين الشركات والتي تسعى كل منها إلى إستقطاب أكبر عدد ممكن من العملاء لذلك سارعت إلى تبني تكنولوجيا المعلومات ضمن أعمالها التجارية باعتبارها الوسيلة التي تحقق لها ذلك.

الفرع الثاني:

خصائص تكنولوجيا المعلومات ومراحلها .

تتميز تكنولوديا المعلومات بالعديد من الخصائص الأمر الذي جعل منها ذات أهمية بالغة، كما أن هذه التكنولوجيا قطعت جملة من المراحل خلال عملية ظهورها، ومن خلال هذه الفرع نتطرق إلى ما تنفرد به هذه التكنولوجيا من خصائص ثم نتعرف على مراحلها.

أولا: خصائص تكنولوجيا المعلومات.

1-المرونة: وتعني هذه الخاصية بأن تكنولوجيا المعلومات تتعدد إستعمالاتها وذلك وفقا لمستخدميها فمثلا أجهزة الحواسيب قد يستخدمه شخص ما من أجل كتابة نصوص معينة،[1] وفي مقابل ذلك نجد بأن نفس الجهاز تستخدمه شركة المساهمة ولكن بهدف إستعمال برنامج معين يتعلق بعملياتها المالية مثلا، في حين قد تستخدمه شركة أخرى لأجل إبرام صفقاتها التجارية فالملاحظ هو أنه ذات الجهاز يتم إستخدامه في عدة أغراض مختلفة وهذا ما يعطيها خاصية المرونة.

2-تقليص الزمان والمكان: جعلت تكنولوجيا المعلومات كل الأماكن متجاورة إلكترونيا،[2] بالإضافة إلى أنه بفضل وسائل التخزين التي وفرتها جعلت إمكانية الإحتفاظ وتخزين ذلك الكم الضخم والهائل من المعلومات أمرا ممكنا وبسيطا، مع الوصول إليها بكل سهولة وكأن هذه الأجهزة تقاسمت المهام الفكرية مع القائمين عليها.[3]

---

[1] عبد الله غالم ، محمد قريشي، مرجع سابق، ص 138.

[2] الميلود سحانين ، "مساهمة تكنولوجيا المعلومات والإتصال في تحقيق أبعاد التنمية المستدامة -دراسة حالة الجزائر- " (أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجيلالي اليابس سيدي بلعباس، 2016-2017)، ص 35.

[3] أمال سلطان ، عشبي صليحة، مرجع سابق، ص 1366.

3-العالمية: وتعني أن البيئة الأساسية لتكنولوجيا المعلومات تتسم بالكونية وذلك راجع إلى طابعها الدولي، فنجد بأن المعلومات ضمن هذه التكنولوجيا تتجه في مسارات مختلفة ذات تعقيدات لتنتشر في مختلف المناطق من العالم، حيث أنها تمكن رأسمال من التدفق بطريقة إلكترونية متخطية بذلك عوائق المكان وتجاوز الحدود الدولية ويتضح هذا جليا من خلال سهولة المعاملات التجارية التي يعمل على تحريكها رأسمال المعلوماتي،[1] وكل هذا يتم في أجزاء من الثانية فقط.

4-اللاتزامنية: وتعني أنه بفضل تكنولوجيا المعلومات أصبح من الممكن جدا إرسال المعلومات عبر مختلف وسائلها ليستقبلها الطرف الآخر في الوقت الذي يناسبه دون أن تكون هناك حاجة لإستخدام الجهاز أو النظام في الوقت ذاته،[2] وتلجأ شركات المساهمة إلى إستخدام ذلك في التعامل مع عملائها.

فنجد شركة "DELL" وهي أكبر شركة رائدة في الولايات المتحدة الأمريكية متخصصة في أجهزة الحواسيب والتكنولوجيا حيث قامت بتأسيس قاعدة بيانات ومحطات تشغيل خصيصا لعملائها وفقا للتطبيقات التي يستعملونها، ليقوموا من خلالها بتحديد مواصفات الأجهزة التي يرغبون في إقتنائها وتوجيه الطلب المتضمن معلومات تلك المواصفات التي قاموا بتحديدها إلى الشركة في الوقت الذي يناسبه، كما أنه حتى في حالة ما إذا صادف العملاء مشكلات في هذه الأجهزة يتم توجيه رسائل إلى الشركة لتقوم هي بتوجيهها إلى مهندسي التصميم للتحري عنها واكتشاف المشكلة ومن ثم إصلاحها،[3] وكل هذا يتم من خلال عملية تبادل المعلومات بين الشركة وعملائها دون أن تكون هناك حاجة لإستعمال النظام في نفس الوقت.

---

[1] علي جقريب ، مرجع سابق، ص 32.

[2] حورية بولعويدات ، "إستخدام تكنولوجيا الإتصال الحديثة في المؤسسة الاقتصادية الجزائرية-دراسة ميدانية بمؤسسة سونلغاز فرع تسيير شبكة نقل الغاز بالشرق GRTG قسنطينة- " (رسالة ماجستير، كلية العلوم الإنسانية والعلوم الإجتماعية، جامعة منتوري قسنطينة، 2007-2008)، ص 83.

[3] إبراهيم لجلط، (دور قاعدة بيانات الزبائن في تحليل الحصة السوقية -دراسة حالة شركة دال DELL)، مجلة إقتصاديات شمال إفريقيا، ع 11، الصادر في 2013، ص 124.

5-النمنمة: حيث يشير هذا المصطلح إلى ثلاث خاصيات هي أسرع، أصغر وأقل تكلفة، وهذا أهم ما يميز تكنولوجيا المعلومات كونها تشهد تطورا دائما من حيث سرعتها وكذا ذاكرتها بالإضافة إلى قلة تكاليفها لذلك هي محل طلب مستمر ودائم ضمن مجالي التسيير والإقتصاد.[1]

6-التفاعلية: وتعني هذه الخاصية بأن المستعمل لتكنولوجيا المعلومات قد يكون مرسلا للبيانات كما قد يكون مستقبلا لها في نفس الوقت وهذا ما يؤدي إلى خلق نوع من التفاعل،[2] سواء بالنسبة للشركات فيما بينها أو فيما بينها وبين عملائها باعتبار أن شركات المساهمة قد تكون هي المرسلة للمعلومات إلى شركات أخرى أو عملاء ويمكن أن تكون أيضا مستقبلة لها.

إضافة إلى هذه الخصائص تتميز تكنولوجيا المعلومات كذلك بإمكانية تحويل المعلومات من وسيط إلى آخر كأن يتم تحويل المعلومات المسموعة إلى معلومات مطبوعة ويمكن قراءتها،[3] كما تتميز بالذكاء الإصطناعي وذلك من خلال تنمية المعارف وتدعيم الفرص من أجل تكوين المستخدمين بهدف الشمولية والتحكم في العمليات.[4]

ثانيا: مراحل تكنولوجيا المعلومات.

نجد بأن تكنولوجيا المعلومات قد قطعت عدة مراحل، ففي البداية شهدت ميلاد الجيل الأول من الحواسيب الآلية غير أنها لم تكن ضمن أعمال المؤسسات والسبب في ذلك هو ارتفاع تكاليفها بالإضافة إلى قلة العامل البشري المتخصص فيها، ليظهر بعد ذلك نوع آخر من الحواسيب والذي كان أسرع مقارنة بالنوع الأول حيث كانت تلك الحواسيب ذات حجم أقل وتم عن طريقها إستخدام الأقراص الصلبة، الأشرطة الممغنطة وهذا ما ساهم في رفع مستوى أدائها.[5]

وفي مرحلة ثالثة أطلق عليها مرحلة الجيل الثالث حيث تطورت خلالها تكنولوجيا المعلومات بطريقة جد سريعة فأجهزة الحواسيب خلال هذه المرحلة تميزت بحجم أصغر بكثير وذات قدرة أكبر

---

[1] عبد الله غالم، محمد قريشي، مرجع سابق، ص 138.

[2] مريم زلماط ، "دور تكنولوجيا الإعلام والإتصال في إدارة المعرفة داخل المؤسسة الجزائرية دراسة حال بسوناطراك فرع STH " (رسالة ماجستير، كلية العلوم الاقتصادية والتسيير، جامعة أبو بكر بلقايد تلمسان، 2009-2010)، ص 29.

[3] أمال سلطان ، عشبي صليحة، مرجع سابق، ص 1367.

[4] علي جقريب ، مرجع سابق، ص 32.

[5] مشري محمد الناصر، مرجع سابق، ص ص 23، 24.

في عملية التخزين، لتليها بعد ذلك مرحلة رابعة تم فيها إستخدام الدوائر المتكاملة الكبيرة كما شهدت تغيير في الهيكل التصميمي لأجهزة الحواسيب والتي تعرف حاليا بالحواسيب الشخصية إلى جانب ذلك ظهر ما يعرف بالذاكرة العشوائية وكذا ذاكرة القراءة.[1]

أما المرحلة الخامسة فيحدد المختصين إنطلاقاتها من سنة 1995 إلى غاية يومنا هذا حيث شهدت تكنولوجيا المعلومات ذروة التقدم والتطور فقد عرفت الشبكات تطورا مذهلا مكن من إنتقال المعلومات عبر النطاق العالمي كما ظهر الذكاء الإصطناعي.[2]

المطلب الثاني:

مكونات تكنولوجيا المعلومات.

الحديث عن إعتماد شركات المساهمة لتكنولوجيا المعلومات يقودنا إلى الحديث عن مكوناتها التي تعد مظهرا من مظاهرها، فحتى تقوم شركات المساهمة بأعمالها في ظل هذه التكنولوجيا هناك مجموعة من الأدوات تستخدمها حيث أنها تمثل عصب التكنولوجيا وبنيتها التحتية، هذا ما نتعرف عليه من خلال هذا المطلب وذلك بالتطرق إلى أجهزة الحاسوب **(فرع أول)** ثم الشبكات **(فرع ثاني)**.

الفرع الأول:

أجهزة الحاسوب.

وتعد من أهم ما تقوم عليه تكنولوجيا المعلومات إذ ينبغي على شركات المساهمة تدعيم هياكلها بهذه الأجهزة حتى تتمكن من أداء أعمالها، ومن خلال هذا الفرع نتطرق إلى تعريف أجهزة الحاسوب وأنواعها ثم مكوناتها.

أولا: تعريف أجهزة الحاسوب وأنواعها:

1-تعريف أجهزة الحاسوب: مصطلح حاسوب في اللغة مشتق من الفعل حسب، حيث أن علم الحاسب يعني علم الأعداد وهو ترجمة للمصطلح الإنجليزي "COMPUTER" والتي أطلق عليها

[1] مشري محمد الناصر، مرجع سابق ، ص 24.

[2] المرجع نفسه، ص 24.

بداية العقل الإلكتروني ثم الحاسب الآلي، غير أن المنظمة العربية للمواصفات والمقاييس تبنت مصطلح حاسوب فقط دون إضافة أي لفظ آخر[1].

وهناك عدة تعريفات تعرضت لجهاز الحاسوب من الناحية الإصطلاحية والتي نورد بعضا منها فيما يلي:

يعرف على أنه ذلك الجهاز الإلكتروني ذو القدرة على إستقبال المعطيات التي يريد صاحبها إدخالها ومعالجتها وتخزينها بداخله، وكذا قدرته على حفظ التعليمات التي تتعلق بالبرامج التطبيقية قصد معالجة المعطيات وإيجاد الحل وإخراجه بسرعة فائقة يمكن تقديرها بملايين العمليات في الثانية الواحدة.[2]

وهو أيضا عبارة عن تلك الآلة الإلكترونية المستخدمة وفقا لنظام ما، وذلك من أجل إدارة ومعالجة البيانات الإلكترونية التي يتم إدراجها فيه بناء على الأوامر والتعليمات المختارة من قبل مستعمله،[3] وهو الجهاز الذي يتشكل من مكونات تكون موصولة وموجهة عن طريق أوامر مخصصة لمعالجة البيانات بطريقة معينة، ليقوم بتنفيذ عملية ثلاثية تشمل إستقبال البيانات المدرجة من أجل التوصل إلى حقائق مجردة، معالجة البيانات إلى معلومات من خلال القيام بحسابات ومقارانات ثم إظهار المعلومات المخرجة والتوصل إلى النتائج.[4]

ويعرف بأنه الجهاز الذي يتشكل من جزئين، جزء مادي يتمثل في المكونات المادية وجزء آخر يتمثل في البرامج ليتم تشغيل هذا الجهاز عن طريق برنامج يحمل ويخزن في ذاكرته، حتى تتم عملية

---

[1] هبة علي زين عيدروس ، سرقة برامج الحاسب في القانون المقارن، ط1، د.ب.ن، دار علام للإصدارات القانونية، 2022، ص 14.

[2] محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د.ط ، الإسكندرية، دار الجامعة الجديدة للنشر، 2007، ص 17.

[3] أسامة أحمد المناعسة، جلال محمد الزعبي ، جرائم تقنية المعلومات الإلكترونية دراسة مقارنة وفقا لقانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2012، ط 2 ، عمان الأردن، دار الثقافة للنشر والتوزيع، ، 2014، ص 27.

[4] نهلا عبد القادر المومني ، الجرائم المعلوماتية، ط 2 ، عمان، دار الثقافة للنشر والتوزيع، 2010، ص 20.

إستقبال البيانات قصد معالجتها من خلال القيام بإجراء عدة عمليات وفقا لما هو مراد تحقيقه والتحصل على النتائج المحددة.[1]

كما نجد العديد من التشريعات التي تطرقت إلى تعريف هذا الجهاز ضمن نصوصها القانونية على غرار المشرع المصري الذي عرفه ضمن المادة الأولى فقرة 16 من القرار رقم 109 لسنة 2005 [2] بأنه ذلك الجهاز الإلكتروني الذي تكون له قدرة على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة إلكترونية.

كما عرفه المشرع الإماراتي في المادة الثانية من القانون رقم 2 لسنة 2002،[3] بأنه الجهاز الإلكتروني الذي يتعامل مع المعلومات والبيانات بتحليلها وبرمجتها وإظهارها وحفظها وإرسالها واستلامها، بواسطة برامج وأنظمة معلومات إلكترونية ويمكن أن يعمل بشكل مستقل أو بالإتصال مع أجهزة أو أنظمة إلكترونية أخرى.

إستناد إلى جملة هذه التعريفات المقدمة نخلص إلى القول بأن جهاز الحاسوب يمثل فعلا العصب الأساسي لتكنولوجيا المعلومات، فهو جهاز ذو تركيبة إلكترونية تعمل أجزاؤه بطريقة متكاملة فيما بينها ليتحصل مستعمله على النتائج التي يود الوصول إليها ويحقق غايته في الإحتفاظ بمعلوماته، كما أن النتائج التي يخرجها هذا الجهاز تكون في غاية الدقة، فهو الآلة التي تتربع على عرش إختراعات العقل البشري بالنظر إلى العمليات الدقيقة والمعقدة التي يقوم بها إضافة إلى سعته في الإحتفاظ وقدرته على التحليل والإسترجاع.

2-أنواع أجهزة الحاسوب: هناك عدة أنواع لهذه الأجهزة توردها فيما يلي.

---

[1] نسرين محسن نعمة الحسيني، محمد حسن مرعي ، الجرائم الإلكترونية الواقعة على الأموال، د.ط ، الإسكندرية، دار المكتب الجامعي الحديث، 2020، ص 45.

[2] قرار رقم 109 لسنة 2005 مؤرخ في 2005/05/15 يتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[3] القانون رقم 2 لسنة 2002 يتعلق بالمعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة.

أ-أجهزة الحاسوب بالنظر إلى وظيفتها وتركيبتها:

-جهاز الحاسوب الرقمي: حيث يعتمد هذا النوع على الأرقام خلال القيام بعملية الإدخال، المعالجة والإخراج وذلك من خلال قيامه باستقبال المعلومات في شكل رقمي وعند عملية إسترجاعها فإنها تكون في صورة معلومات يمكن قراءتها وليس في صورة أرقام مثلما كانت مخزنة في ذاكرته.[1]

-جهاز الحاسوب القياسي: أكثر ما يتم إستخدام هذا النوع من الحواسيب في القياسات الكمية والتي يكون من غير الممكن التعبير عنها عن طريق الأعداد مباشرة،[2] ولا يمكن إستخدامه من أجل عملية تخزين المعلومات في ذاكرته.[3]

-جهاز الحاسوب المختلط: ويتميز بأنه يجمع بين خصائص النوعين السابقين، ويتم ذلك من خلال التوصيل بين جهازي الحاسوب الرقمي والقياسي ليتم تنقل المعلومات بينهما بواسطة محولات معينة من الحاسوب القياسي إلى الحاسوب الرقمي والعكس كذلك[4].

ب-أجهزة الحاسوب بالنظر إلى حجمها:

-أجهزة الحاسوب ذات الحجم الكبير: من أهم ما يميز هذا النوع هو سعة وقدرة ذاكرته على معالجة البيانات بسرعة فائقة وفي أقل وقت ممكن، فقد يبلغ عدد التعليمات التي تنفذها الملايين وذلك في وقت وجيز جدا.[5]

-أجهزة الحاسوب ذات الحجم المتوسط: وهي أصغر حجما مقارنة بالنوع الأول، يستعمل هذا النوع بشكل أوسع في الأعمال التجارية التي تكون على مستوى من التعقيد.[6]

---

[1] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 54.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 21.

[3] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 53.

[4] محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقها، ط 1 ، القاهرة، دار الشروق، 1989، ص 68.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 22.

[6] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 52.

-أجهزة الحاسوب ذات الحجم الصغير: ويعد هذا النوع أكثر إنتشارا ويستعمل بشكل واسع من قبل الأشخاص ويرجع السبب في ذلك إلى صغر حجمها وقلة تكلفتها.[1]

ثانيا: مكونات أجهزة الحاسوب:

تحتوي أجهزة الحاسوب على جزئين، جزء محسوس يتمثل في الأجهزة والمعدات وآخر يتمثل في البرمجيات.

1-الأجهزة والمعدات: وتتمثل في مختلف الأجزاء ذات الطبيعة المادية .

أ-وحدات الإدخال: وهي تلك الأجزاء التي تكون مهمتها توصيل المعلومات للجهاز،[2] حتى يتم تنفيذ العمليات الأخرى عليها لاحقا ومن تلك الأجزاء نجد مثلا لوحة المفاتيح والتي من خلالها يتم كتابة البيانات المراد إدخالها،[3] كذلك الفأرة وهي الجزء الذي بواسطته يتم التأشير على شاشة جهاز الحاسوب حتى يتم تنفيذ الأوامر،[4] بالإضافة إلى الماسح الضوئي الذي يستعمل بقصد إدخال الوثائق المكتوبة والصور من أجل قراءتها، كما أن هناك أجزاء أخرى أكثر تطورا بإمكانها التعرف على مطبوعات الحبر المغناطيسي وتستعمل بشكل كبير في البنوك حتى يتم التعرف على الحروف التي تكون مدونة بحبر يتكون من مادة مغناطسية، إلى جانب ذلك هناك أجزاء تستخدم للتعرف على الحروف والعلامات ضوئيا ويتم إستخدامها من قبل شركات الطيران وكذا الشركات التجارية حتي يتم وضع الأسعار وكذا البيانات المتعلقة بالتخزين على البضائع.[5]

ب-وحدات الإخراج: وتتمثل في تلك الأجزاء التي تسمح باستقبال نتائج معالجة جهاز الحاسوب للبيانات ليتم عرضها في شكل واضح يفهمه الشخص المستخدم له،[6] ومن تلك الأجزاء مثلا الطابعة

---

[1] نهلا عبد القادر المومني، مرجع سابق، ص 22.

[2] علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، د، ط، عمان، دار اليازوردي العلمية، 2008، ص 13.

[3] محمد خليفة، مرجع سابق، ص 18.

[4] هاني شحادة الخوري، تكنولوجيا المعلومات على أعتاب القرن الحادي والعشرين، ج الأول مدخل تعريفي لتكنولوجيا المعلومات، ط 1، دمشق، مركز الرضا للكومبيوتر، 1998، ص 76.

[5] محمد خليفة، مرجع سابق، ص 19.

[6] عبد الله غالم، محمد قريشي، مرجع سابق، ص 140.

وهي التي تقوم باستخراج البيانات والنتائج المخزنة في الحاسوب في نسخ من المطبوعات، وأيضا شاشة العرض التي تعرض عبرها البيانات والمعلومات.[1]

ت–وحدة المعالجة المركزية: "CPU" حيث تعتبر وكأنها العقل الذي يدير ويسيطر ويتحكم في باقي الأجزاء التي يتكون منها جهاز الحاسوب،[2] ويندرج تحت هذه الوحدات وحدات أخرى مساعدة وتتمثل في:

•وحدة التحكم: وتقوم بمهمة تنظيم العلاقة بين وحدة المعالجة المركزية وباقي الوحدات الأخرى حتى يتم إستلام البيانات ثم إرسال النتائج، فهي تتحكم في عمل وحدات الجهاز وتضم هذه الوحدة جملة من المسجلات، العدادات وكذا دوائر فك الرموز وتحليلها.[3]

•وحدة الحساب والمنطق: تكون هذه الوحدة مسئولة عن جميع العمليات التي تتعلق بالحساب وكذا العمليات المتعلقة بالمقارنة المنطقية.[4]

•وحدة الذاكرة: وهي الجزء الذي يتم فيه تخزين المعلومات التي ترد إلى جهاز الحاسوب وكذا نتائج وحدة المعالجة المركزية،[5] وتنقسم هذه الذاكرة إلى نوعين:

–الذاكرة الرئيسية: ووظيفتها تخزين مجمل البيانات المراد تنفيذها حيث أنها تختفي فور الإنتهاء من تنفيذ البرامج وهي ذات سرعة تختلف حسب كل جهاز.[6]

–الذاكرة المساعدة: وتعتبر كوحدة تخزين ثانوية مقارنة بالذاكرة الرئيسية لذلك تكون سعتها أقل غير أنها تستطيع الإحتفاظ بالمعلومات لمدة طويلة تصل إلى سنوات.[7]

2–البرمجيات: لا يكتمل أداء أجهزة الحاسوب لوحدها فقط وإنما يتطلب الأمر من أجل تشغيلها وتوجيهها توفير جزء آخر وهو البرمجيات.

---

[1] هبة علي زين عيدروس، مرجع سابق، ص 21.

[2] أسامة أحمد المناعسة، جلال محمد الزعبي، ص 29.

[3] علي جبار الحسيناوي، مرجع سابق، ص 14.

[4] مشري محمد الناصر، مرجع سابق، ص 27.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 26.

[6] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 58.

[7] نهلا عبد القادر المومني، مرجع سابق، ص ص 27، 28.

أ–تعرف البرمجيات: تم تعريفها من قبل "SZYMANSKI ETAL" على أنها تلك الإرشادات والتوجيهات التي تكون مدونة بلغة جهاز الحاسوب والتي من خلالها يتم توجيه عملياته وتجعل المكونات المادية للجهاز تقوم بأعمالها،[1] وهي أيضا تلك القواعد والأساليب التي تتعلق بتشغيل وحدة معالجة البيانات،[2] كما تم تعريفها من التشريع الأمريكي على أنها جملة الأوامر والتعليمات التي تكون موجهة قصد الإستخدام المباشر في الحاسوب قصد الوصول إلى نتائج محددة،[3] وبالتالي يمكن القول بأن البرمجيات هي جملة التعليمات اللازمة حتى تتمكن أجهزة الحاسوب من تأدية وظيفته، ومنه تحقيق النتائج المطلوبة والمحددة، وهذه البرامج لا يمكن الإستغناء عليها.

ب–أنواع البرمجيات: وتنقسم إلى نوعين، برمجيات النظام وبرمجيات التطبيقات.

•برمجيات النظام: وهي ذات أهمية ضرورية حتى يتم التمكن من تشغيل جهاز الحاسوب وبالتالي تنسيق العلاقة بين أجزائه مع بعضها البعض،[4] ونجد بأن بعض هذه البرامج يبنى بداخل أجهزة الحاسوب في حين البعض الآخر يتم تخزينه ضمن الأقراص الممغنطة ومنها نظم التشغيل وكذا لغات البرمجة.[5]

•برمجيات التطبيقات: هذه البرمجيات يتم إعدادها قصد تشغيل عمليات محددة حيث أنها تحتوي على مجمل التعليمات والتي تحدد بشكل متسلسل العمليات الواجبة لمعالجة البيانات وطريقة تنفيذها، وتعتبر ذات أهمية بالغة في أداء أعمال الشركات[6]، وتوجد هي الأخرى على نوعين:

يتمثل النوع الأول في برمجيات التطبيقات العامة وهي من أوائل الأنواع التي ظهرت وتستخدم بشكل واسع في مختلف الشركات مثل البرمجيات التي تتعلق بكتابة النصوص ومعالجتها وتخزينها،

---

[1] نادية لونيس، "الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic– " (أطروحة دكتوراه، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2017–2018)، ص 38.

[2] علي جبار الحسيناوي، مرجع سابق، ص 15.

[3] هبة علي زين عيدروس، مرجع سابق، ص 23.

[4] الميلود سحانين ، مرجع سابق، ص 34.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 30.

[6] الميلود سحانين ، مرجع سابق، ص 34.

أما النوع الثاني فيتمثل في برمجيات التطبيقات المتخصصة وهي التي تتعلق بأنشطة معينة مثل التسويق، المحاسبة، إدارة علاقة الشركة بعملائها الإنتاج.[1]

الفرع الثاني:

الشبكات.

إضافة إلى أجهزة الحاسوب نجد كذلك الشبكات التي تعد الأساس الثاني الذي تقوم عليه تكنولوجيا المعلومات، فحتى تتمكن شركات المساهمة من ربط حواسيبها مع مختلف الحواسيب الأخرى قصد تبادل المعلومات وإتمام صفقاتها وضمان التوزيع التجاري لمنتوجاتها بشكل أسرع يتطلب منها الأمر توفير هذه الشبكات والتي توجد على ثلاثة أنواع تتمثل في الأنترنت، الأنترانت والإكسترنت، وهذه الأنواع قد تتواجد جميعا في الشركة الواحدة أو قد يوجد بعضها وذلك حسب حاجة الشركة لكل نوع، وفي هذا الفرع نتعرف على كل نوع على حدة.

أولا: شبكة الأنترنت.

1-تعريف شبكة الأنترنت: الأنترنت مصطلح إنجليزي يتكون من مقطعين "INTER" وهو إختصار لمصطلح "INTERNATIONAL" ومعناه دولي أو عالمي، "NET" وهو إختصار لمصطلح "NETWORK" والذي يعني الشبكة، فالأنترنت إذن هي الشبكة الدولية أو العالمية للمعلومات.[2]

وقد تعددت التعريفات التي قيلت بشأنها، فتعرف بأنها عبارة عن كم هائل من الحواسيب والأجهزة الأخرى التي تكون موزعة عبر مختلف أرجاء العالم والتي تكون مرتبطة مع بعضها البعض سواء سلكيا أو لا سلكيا،[3] وبذلك تكون الأنترنت عبارة عن مجال معلوماتي تنتقل عبره المحطات الرقمية بين مختلف الحواسيب المرتبطة مع بعضها.[4]

---

[1] نادية لونيس، "أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات –دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية– " (رسالة ماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2010-2011)، ص ص 40، 41.

[2] حمدي القبيلات، قانون الإدارة العامة الإلكترونية، ط 1، الأردن، دار وائل للنشر والتوزيع، 2014، ص 17.

[3] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 64.

[4] حمدي القبيلات، مرجع سابق، ص 18.

كما تم تعريفها أيضا بأنها تلك الشبكة التي تسمح بانضمام شبكات معلوماتية ذات أنساق مختلفة في إطارها بفضل إستخدام البروتوكول الوحيد TCP. IP والبريد الإلكتروني وكذا الصفحات والمعلومات والأراء وكذلك بنوك المعلومات.[1]

وكانت إحدى المحاكم بشرق فرجينيا قد تعرضت كذلك إلى تعريف الأنترنت على أنها الطريق العالمي للمعلومات، وهي عبارة عن شبكة إتصالات شائكة تتصل بها شبكات حاسوب أخرى قد تكون عامة أو خاصة وهي تتشكل من حواسيب وقواعد بيانات مرتبطة عبر خطوط الهاتف.[2]

عرفتها أيضا محكمة جنوب "أهايو" خلال حكمها الصادر بشأن قضية "COMPUSERVE" وشركة "STANFORD" على أنها شبكة الشبكات،[3] واستنادا إلى هذه التعريفات نصل إلى القول بأن الأنترنت تعد أكبر الشبكات المعلوماتية في العالم، والتي تربط بين عدد ضخم من الحواسيب الموجودة في مناطق متفرقة ومختلفة عبر أرجاء العالم، ومن خلالها يتم تبادل مختلف المعلومات سواء كانت بين الأفراد أو المؤسسات والشركات.

2-تطور شبكة الأنترنت: تعود بداية الظهور التاريخي لشبكة الأنترنت إلى الستينيات وبالضبط سنة 1996،[4] ففي هذا التاريخ قامت الولايات المتحدة الأمريكية عن طريق وزارة دفاعها بإنشاء الوكالة المسماة بمشاريع الأبحاث المتقدمة ARPA، " ADVANCED RESEARCH PROJECTS ADMIN".[5]

حيث رأت وزارة الدفاع بأن الأمر يتطلب منها شبكة إتصالات تكون لها القدرة على الصمود خلال فترة الحرب وأنه في حالة تدمير جزء منها يبقى بإمكانها إرسال رسالة تحقق هدفها المطلوب، فظهرت بذلك ما يعرف بشبكة "ARPA NET" وبالتالي فظهور الأنترنت في البداية كان بدواعي عسكرية.

---

[1] ناصر حمودي، "الحماية الجنائية للتجارة الإلكترونية " (رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2015)، ص 16.

[2] فتيحة رصاع، "الحماية الجنائية للمعلومات على شبكة الأنترنت " (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2011-2012)، ص 11.

[3] المرجع نفسه، ص 11.

[4] حمدي القبيلات، مرجع سابق، ص 18.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 37.

فشبكة "ARPA NET" كانت لها القدرة على الربط بين جهازين من الحاسوب تفصل بينهما مئات الكيلومترات وحينها تم الربط بين حاسوب بجامعة "لوس أنجلس" و4 مراكز بحث أخرى بتلك الشبكة، وبحلول سنة 1971 وصل عدد مراكز البحث المرتبطة بها 23 مركزا.[1]

غير أنه في سنة 1983 تم إستخدام شبكة "ARPA NET" بشكل واسع من طرف الجامعات الأمر الذي تولد عنه ضغط يفوق قدرتها مما إستدعى إستحداث شبكة جديدة تعرف باسم " MIL NET" حيث تستخدم في الأغراض العسكرية فقط بينما "ARPA NET " تستخدم في الأغراض غير العسكرية،[2] لتصبح فيما بعد متاحة لكافة أنواع البحث العلمي ويرجع ذلك إلى نقل تشغيلها من وزارة الدفاع إلى شبكة مؤسسة العلوم الوطنية " NSFNET"[3].

وبحلول عام 1992 تم إنشاء ما يسمى بالشبكة العنكبوتية العالمية "WWW" أي "WORLD WID WEB" وفي سنة 1995 شهدت "NSFNET " تطورا هائلا مما مهمد لظهور أضخم شبكة قادرة على الربط بين الملايين من أجهزة الحاسوب في مختلف أنحاء العالم وهي ما يعرف بشبكة الأنترنت.[4]

وبعد موجة التطور التي عرفتها شبكة الأنترنت فإن إستخدامها لم يعد مقتصرا على مجالات البحث العلمي فقط وإنما إمتد ليشمل إلى جانب ذلك الأفراد والشركات في الأغراض التجارية، فقد نجحت الشركات في تأدية أعمالها التجارية من خلال إجراء معاملاتها عن طريق هذه الشبكة لتحقق بذلك مكانة لها في الأسواق سواء على المستوى المحلي أو الدولي، حيث سارع العديد من رجال الأعمال وأصحاب أكبر الشركات إلى التفاعل مع هذه الشبكة وذلك من خلال إبرام العديد من

---

[1] نادية لونيس، أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات، دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، مرجع سابق، ص 54.

[2] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 67.

[3] فتيحة رصاع، مرجع سابق، ص 15.

[4] نادية لونيس، أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات، دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، مرجع سابق، ص 55.

الصفقات التجارية عن طريق شبكة الأنترنت، بعد عرضها على الشبكة وتلقي الردود الخاصة بها بذات الطريقة.

3-خدمات شبكة الأنترنت: ساعدت شبكة الأنترنت على فتح أبواب واسعة النطاق في جميع المجالات بما فيها المجال التجاري، حيث إستفادت شركات المساهمة بشكل كبير من هذه الشبكة وذلك من خلال جملة الخدمات المتنوعة التي تقدمها، وفي هذه النقطة نستعرض ونوضح تلك الخدمات التي إستفادت منها شركات المساهمة والتي تتمثل في:

أ-خدمة البريد الإلكتروني (E. MAIL): يعرف البريد الإلكتروني بأنه عبارة عن أداة من أجل تبادل المعلومات من خلال شبكة الأنترنت، ومن أجل خدمة البريد الإلكتروني يفترض أن يكون للمشترك عنوان إلكتروني حتى يتمكن من إرسال واستقبال المعلومات التي يرغب فيها،[1] كما يعرف على أنه ذلك الصندوق الشخصي الذي يتطلب العمل به توفر شبكة الأنترنت وكذا إسم مستخدم مع كلمة المرور حتى يتمكن المشترك من الإستفادة منه.[2]

وعرفه المشرع الفرنسي في قانون الثقة في الاقتصاد الرقمي،[3] وذلك في مادته الأولى بأنه عبارة عن أية وسيلة بغض النظر عن شكلها إن كانت نصية أو صوتية أو مرفقة بأصوات أو صور يتم تحويلها من خلال شبكة إتصالات، حيث يكون تخزينها عند أحد خوادم الشبكة أو في المعدات الطرفية للمرسل إليه حتى يكون بإمكانه إسترجاعها، فالبريد الإلكتروني يحتوي على ميزة السرية والأمان باعتباره يتم الولوج إليه عبر كلمة سرية محفوظة لدى صاحبه فقط لذلك يكون من الصعب إختراقه دون تلك الكلمة السرية.

وبالتأكيد البريد الإلكتروني يلعب دورا في غاية الأهمية بالنسبة لشركات المساهمة حيث يمثل لها أداة إتصال يسهل عليها عملية الإتصال بشركائها وعملاءها من خلال إعلامهم بمنتجاتها المختلفة وعروضها، فما يكون من العميل سوى إرسال رسالة إلى البريد الإلكتروني الخاص بالشركة لترد عليه

---

[1] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 70.

[2] مصطفى هنشور وسيمة، "النظام القانوني للتجارة الإلكترونية في التشريع الجزائري والمقارن " (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2016-2017)، ص 27.

[3] Loi N^0 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J,O,R,F du 22 juin 2004.

بملخص عن كل ما يتعلق بالمعلومات التي يرغب في الحصول عليها،[1] ليحل بذلك البريد الإلكتروني محل أدوات الإتصال التقليدية التي كانت تعتمد عليها الشركة كالهاتف والبريد التقليدي والفاكس.[2]

ب–خدمة الشبكة العنكبوتية العالمية (the world wid web- www): ويمكن إعتبار هذه الخدمة من أهم الخدمات التي يمكن لشبكة الأنترنت أن تقدمها حيث يطلق عليها ب "WEB" و الكثير يخلط بينها وبين شبكة الأنترنت ولا يفرق بينهما،[3] والحقيقة أن خدمة الويب هي جزء من شبكة الأنترنت وتسمح خدمة هذه الشبكة العنكبوتية العالمية بتصفح آلاف المواقع التي تضم معلومات في شتى الميادين ،[4] تكون مدعمة بمختلف الألوان والصور الأمر الذي يجعلها تتميز بشعبية أكبر، كما أنها تساعد على ربط العديد من المؤسسات ذات الطابع العلمي والصناعي والحكومي وخاصة التجاري،[5] لتكون بذلك خدمة الشبكة العنكبوتية العالمية من بين أهم وسائل الترويج والدعاية وكذا الإعلان التي يمكن الإعتماد عليها سواء كان ذلك على المستوى الإقليمي المحلي وكذا العالمي.[6]

فمن خلال هذه الخدمة نجد بأن شركات المساهمة تلجأ إلى الإستعانة بمواقع الأنترنت من أجل القيام تقديم عروضها ومنتجاتها المختلفة وكذا خداماتها ، ويمكن تشبيه المواقع التي تعتمدها هذه الشركات وكأنها عبارة عن المحلات التجارية المعتادة في الواقع بالنظر إلى واجهاتها الإلكترونية التي تتميز بها، وبذلك يمكن للعملاء تصفح مواقعها والإطلاع على ما تحتويه من عروض.

ت–خدمة التلنت (TELNET): أو ما يعرف بخدمة ربط عن بعد، حيث أن هذه الخدمة تسمح للمستخدم وتمكنه من ربط حاسوبه على حاسوب آخر مضيف ليصبح بذلك جهاز المستخدم وكأنه

---

[1] وسيلة هني، مرجع سابق، ص 51.

[2] مصطفى هنشور وسيمة، مرجع سابق، ص 28.

[3] مشري محمد الناصر، مرجع سابق، ص 59.

[4] نهلا عبد القادر المومني، مرجع سابق، ص 40.

[5] مصطفى هنشور وسيمة، مرجع سابق، ص 29.

[6] مشري محمد الناصر، مرجع سابق، ص 59.

جزء من الجهاز الثاني الذي يبعد عنه، بهذا يتم النفاذ إلى المعلومات التي تكون مخزنة فيه عن طريق الولوج الفعلي لجهاز الحاسوب واستخدامه بشكل عادي[1]، وكأنه موجود بذات المكان الذي يوجد فيه الحاسوب، غير أن ذلك يتطلب معرفة نظام التشغيل الخاص بالجهاز الذي يكون متصلا به وكذا الحصول على ترخيص باعتبار أن ذلك ينتج عنه الوصول إلى قواعد البيانات والتعامل معها.[2]

وعليه فخدمة التلنت تعرض حاسوب الطرف الثاني لأوامر المستخدم الذي يعد الطرف الأول مثل تمكينه من طباعة مستندات أو إضافة معلومات، وفي هذا الصدد هناك العديد من الشركات التي تلجأ إلى إتاحة حواسيبها الخاصة للعملاء والموردين الذين تتعامل معهم حتى تمكنهم من تخزين الأوامر المتعلقة بالشراء مثلا وتأكيد الطلبات.[3]

ث-خدمة نقل الملفات: وتنفذ هذه الخدمة عن طريق ما يسمى ببروتوكول نقل الملفات (FTP) "TRANSFER FILE PROTOCOL " ومن خلالها يتم إستخدام جهازين من الحاسوب وكذا برامج معينة حتى يتم نقل الملفات من أحد الجهازين اللذان يكونان موصولين بالشبكة إلى الجهاز الآخر،[4] وتلك الملفات قد تضم نصوصا أو صورا أو فيديو وحتى يتم تنفيذ هذه العملية فإن الأمر يستلزم الحصول على عنوان الحاسوب الذي يضم تلك الملفات وكذا تحديد المسار إلى الملف ذاته[5].

حيث أن بدخول الطرف العميل إلى حاسوب الشركة يتمكن من إفراغ المعلومات وكذا الملفات من حاسوبها إلى حاسوبه الخاص وبطبيعة الحال فإن ذلك يتم بعد معرفة كلمة المرور وإسم

---

[1] نجلاء محمد جابر، دراسة تحليلية في الإعلام الجماهيري، د، ط، د، ب، ن، دار المعتز للنشر والتوزيع، 2015، ص 364.

[2] الميلود سحانين ، مرجع سابق، ص 26.

[3] مصطفى هنشور وسيمة، مرجع سابق، ص 30.

[4] حشمت توفيق عزيز عياد، الإعلام وقضايا التنمية، د، ط، عمان الأردن، دار غيداء للنشر والتوزيع، 2016، ص 90.

[5] الميلود سحانين ، مرجع سابق، ص 26.

المستخدم،[1] فنجد بأنه من خلال خدمة نقل الملفات يمكن للشركة الإتصال بعملائها وذلك من خلال توزيع جملة من المعلومات التي تتعلق بقوائم المنتجات الخاصة بها وكذا قوائم أسعارها (الكتالوجات) ليقوم بعد ذلك هؤلاء بتحميلها وفقا لحاجتهم إليها.[2]

ج-خدمة المجموعات الإخبارية: هذه الخدمة عبارة عن مواقع إفتراضية بغية اللقاء والتحدث بين مستخدمين شبكة الأنترنت ولديهم إهتمامات مشتركة في مختلف المجالات والميادين، حيث يتبادلون الأراء والمعلومات المتعلقة بموضوع ما مثلا،[3] ومن خلال هذه الخدمة يمكن طرح مجموعة من الأسئلة من طرف أشخاص بحاجة إلى معرفة بعض المعلومات تخص قضية معينة ليقوم أطراف آخرون بالإجابة عن تلك الأسئلة وتقديم معلومات وتوضيحات،[4] من جهة أخرى فإنه يتم الإحتفاظ بتلك الأسئلة والردود عليها وتخزينها في الخادم، مما يسمح لمن يحوز بريد إلكتروني الإتصال بذلك الخادم وإرسال جملة الأسئلة والردود إلى المجموعات الإخبارية.[5]

أما عن الكيفية التي تستفيد بها شركات المساهمة من خلال هذه الخدمة فيكون عن طريق تصنيع منتج ويتم تداول الأسئلة حوله، وبواسطة المجموعات الإخبارية يمكن للشركة الحصول على التعليقات التي تتعلق به ولا يهم في ذلك إن كانت إيجابية أو سلبية طالما أن تلك الملاحظات ستستفيد منها الشركة حتما، إذ يمكن من خلال معرفة تلك التعليقات تغيير الخطة التسويقية مثلا والتفكير في كيفية طرحه في الأسواق[6].

كما يمكن لشركات المساهمة الإستفادة من الخدامات التي تقدمها شبكة الأنترنت من خلال المحادثة وكذا المشاهدة عبر هذه الشبكة والتي تكون فورية ومباشرة، بمعنى أن الطرف الثاني يرد عليها مباشرة في نفس اللحظة، ونجد بأن هذا يحدث عندما تلجأ هذه الشركات إلى إبرام الصفقات

---

[1] مصطفى هنشور وسيمة، مرجع سابق، ص 31.

[2] وسيلة هني، مرجع سابق، ص 53.

[3] نهلا عبد القادر المومني، مرجع سابق، ص 41.

[4] وسيلة هني، مرجع سابق، ص 52.

[5] مشري محمد الناصر، مرجع سابق، ص 59.

[6] وسيلة هني، مرجع سابق، ص 53.

والتعاقد مع أطراف أخرى فتكون تلك المحادثات والمشاهدة بمثابة مجلس تعاقد إفتراضي يتم فيه تبادل الإيجاب والقبول.[1]

ثانيا: شبكة الأنترانت:

يتجلى الفرق بين هذه الشبكة وشبكة الأنترنت التي أشرنا إليها سابقا، في أن هذه الشبكة هي عبارة عن شبكة أنترنت مصغرة داخل الشركة تسمح لها بتوفير المعلومات وإتحاتها لموظفيها قصد تسهيل عملية البحث عن المعلومات والمستندات الخاصة بها واسترجاعها، إذ من الممكن توصيلها بقاعدة البيانات الخاصة بالشركة وبالتالي تحقيق عملية الإتصال الجماعي بين الموظفين.[2]

وبالتالي فإن شبكة الأنترانت تعرف بالشبكة الداخلية وتكون خاصة بالشركة حيث أن معلوماتها تكون سرية وتقتصر بشكل حصري على موظفي الشركة فقط، فهي عبارة عن تطبيق التقنيات والأعراف الخاصة بالأنترنت على نطاق ضيق يشمل الشبكة الخاصة بالشركة فحسب،[3] ورغم إتصال هذه الشبكة بالأنترنت غير أن نسبة تأثرها بالمشاكل التي تكون بفعل المستخدمين من الخارج تكون ضئيلة.

لذلك هناك العديد من الشركات قد إبتعدت عن إستعمال شبكة الأنترنت ذات الطابع العالمي ولجأت إلى إنشاء شبكة أنترانت خاصة بها، فإذا كان إتصال الأنترانت بالأنترنت ممكنا فإن العكس غير ممكن، وهذه هي ميزة هذه الشبكة لا تتصل بالعالم الخارجي سوى في نطاق محدود[4].

ويوجد نوعين من شبكة الأنترانت، يتمثل النوع الأول في الشبكة المحلية وهي تلك التي يمكن من خلالها إتصال مجموعة من الحواسيب تكون متصلة فيما بينها عن طريق كوابل ومزودة ببرامج محددة وذلك ضمن إطار جغرافي ضيق لا يتجاوز 10 كلم، أما النوع الثاني فيتمثل في الشبكة

---

[1] آمال حابت، "التجارة الإلكترونية في الجزائر " (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2015)، ص 39.

[2] مشري محمد الناصر، مرجع سابق، ص 64.

[3] حورية بولعويدات، مرجع سابق، ص 98.

[4] مصطفى هنشور وسيمة، مرجع سابق، ص ص 23، 24.

الواسعة وأهم ما يميزها هو أن المسافة فيها تكون أكبر، بالإضافة إلى كونها تحتوي على أجهزة خاصة من أجل تنظيم عملية الإتصال لتكون بمثابة النقاط المركزية فيها.[1]

ثالثا: شبكة الإكسترنت (EXTRANET).

1-تعريف شبكة الإكسترنت: وتعرف على أنها تلك الشبكة التي تكون خاصة بالشركة والتي تصمم خصيصا بغية تلبية حاجيات الأفراد المتعلقة بالمعلومات ومتطلبات المنظمات الأخرى المتواجدة في بيئة الأعمال،[2] وهذه الشبكة يتم إستخدامها حينما يكون للشركة فروع متعددة متواجدة في عدة أماكن متفرقة حيث أنه يحتوي كل فرع من فروعها على شبكة أنترنت، وبالتالي عند القيام بعملية الربط بين تلك الشبكات نكون أمام ما يسمى بشبكة الإكسترنت[3]، فهي تستخدم بغرض ربط فروع الشركة مع بعضها البعض.

كما أن شبكة الإكسترنت تساهم في الربط بين شركاء العمل وجهات أخرى وذلك بطريقة تكون في غاية السرعة والفعالية، غير أن ما تجب الإشارة إليه هو أنه عند إستخدام هذه الشبكة ينبغي على كافة الأطراف إستعمال ذات برنامج التطبيق عند عملية الإتصال.[4]

لذلك يمكن إعتبارها على أنها برنامج تعاون بين الشركة والأطراف التي لها مصلحة كونها تتضمن العلاقة الدائمة المتواصلة فيما بينهم، إضافة إلى ذلك فإنها تسهل على الشركات حتى في عملية الحصول على اليد العاملة المؤهلة وذات الخبرة وذلك لإرتباطها في عدة أحيان بالجامعات ومراكز التكوين،[5] ومن الأمثلة على ذلك شبكات البنوك والمعاملات المصرفية وكذلك شبكات الطيران.[6]

---

[1] مصطفى هنشور وسيمة، مرجع سابق، ص ص 98، 100.

[2] سعد غالب ياسين، بشير عباس العلاق، التجارة الإلكترونية، د، ط، عمان الأردن، دار المناهج للنشر والتوزيع، 2015، ص 57.

[3] خضر مصباح إسماعيل طيطي، إدارة المعرفة، التحديات والتقنيات والحلول، ط 1، عمان ، دار االحامد للنشر والتوزيع، 2009، ص 168.

[4] المرجع نفسه، ص 168.

[5] مشري محمد الناصر، مرجع سابق، ص 65.

[6] مصطفى هنشور وسيمة، مرجع سابق، ص 24.

ومن بين الأمثلة التي يمكن إعطاؤها عن إستعمال شبكة الإكسترنت نجد شبكة سنغافورة للتجارة والتي تقوم بإدارة أنشطة الأعمال ضمن أكبر موانئ العالم، وذلك عن طريق ربط شركات الشحن مع المصارف وكذا المستفدين بالإضافة إلى الأجهزة الحكومية مثل الجمارك، حيث أن تلك الشبكة وصلت كلفتها إلى ما يزيد عن 50 مليون دولار غير أنها ساعدت على إنهاء عمليات الشحن الخاصة بأي مستفيد خلال وقت لا يتجاوز 10 دقائق بعد أن كان يتم في أيام نظرا للإجراءات المتعلقة بعملية الشحن.[1]

وبالتالي فإن شبكة الإكسترنت إذا ما تم إستخدامها بطريقة جيدة وفعالة فإنها تمكن شركات المساهمة من تحقيق الميزة التنافسية، إذ تساعد على الزيادة في فاعلية الأعمال من خلال تحقيق الجودة في الأنشطة وكذا التلقائية والمرونة في الإتصال المباشر والفوري مع باقي الأطراف، فشركة بحجم شركة "جنرال موتورز" تقوم بتقديم خداماتها الإلكترونية إلى 12 وحدة أعمال إستراتجية وكذا 40 000 شريك تجاري، حيث أن الشبكة الجديدة ستعمل على تحقيق حوالي 500 إلى 750 مليون دولار لهذه الشركة عن طريق عملية تقليص الأخطاء وكذا تعزيز وتدعيم الفعالية التشغيلية لوحداتها المختلفة.[2]

فأغلب شركات أصبحت تلجأ إلى إستخدام شبكة الإكسترنت حتى تتمكن من إدارة أعمالها على أتم وجه مثل إدارة أعمال التوريد، العلاقات مع العملاء والعمليات المتعلقة بالتسويق والتصنيع والتصميم.[3]

2-أنواع شبكة الإكسترنت: وجدت شبكة الإكسترنت بغية الإستجابة لمتطلبات قطاع الأعمال الذي هو بحاجة إلى تحالفات وشراكات، وكذا تأمين المعلومات التي يتم تبادلها عبر الشبكات في إطار تعامل الشركات مع بعضها البعض، لذلك فإن تقسيم هذه الشبكة يخضع لما يتطلبه قطاع الأعمال، حيث يتم تقسيمها وفقا لذلك إلى ثلاثة أنواع نوردها فيما يلي:

---

[1] سعد غالب ياسين، بشير عباس العلاق، مرجع سابق، ص 58.

[2] المرجع نفسه، ص 59.

[3] آمال حفناوي، الخامسة سايحي، التسويق الإلكتروني للخدمات، د، ط، الأردن ، دار اليازوردي العلمية للنشر والتوزيع، 2022، ص 71.

أ-شبكة إكسترنت التوريد: تتجلى مهمة هذا النوع من الشبكة في الربط بين الشبكات الخاصة بالمستودعات الرئيسية للبضائع مع المستدوعات الثانوية من أجل التمكن من إدارة العمل بطريقة آنية وتلقائية، وكذلك من أجل المحافظة على كميات ثابتة من البضائع داخل المستودعات مما يترتب على ذلك تجنب إحتمال رفض الطلبيات نتيجة العجز في تلك المستودعات، هذا إضافة إلى تحقيق عملية الرقابة الجيدة للمخزون وتسهيل إدارته.[1]

ب-شبكة إكسترنت التوزيع: تقوم هذه الشبكة بتقديم خدمات الطلب الإلكتروني للعملاء، وبالتالي تمكينهم من تسوية حساباتهم بطريقة إلكترونية وكذلك تقديم الحجوزات والإشتراكات،[2] إضافة إلى تزويدهم الدائم بحصيلة المنتجات الجديدة وكذا مواصفاتها التقنية،[3] إلى غير ذلك من الخدمات المتعددة حيث أن هذا النوع يعتبر أكثر إنتشارا واعتمادا من قبل الشركات.

ت-شبكة الإكسترنت التنافسية: تعمل هذه الشبكة على تعزيز عملية التنافس بين الشركات، وذلك من خلال عملية منح الشركات سواء الكبيرة والصغيرة فرصا تكون متكافئة فيما يتعلق بعمليات البيع والشراء، وذلك بواسطة الربط بين هذه الشركات حتى يتم تسهيل نقل الأسعار وكذا المواصفات التقنية فيما بينها، وبالتالي الرفع من مستوى الخدمات وجودة المنتجات ومن ثم القضاء على الإحتكار.[4]

ومن خلال عرض جملة هذه الشبكات يمكننا القول بأنها قد خلقت فرصا للشركات كونها مكنتها من تجسيد عملية التعاضد الداخلي الذي حققته لها شبكة الأنترانت والتعاضد الخارجي بفضل شبكتي الأنترنت والإكسترنت، وبالتالي هذا ما عاد عليها بالإيجاب حيث أصبحت تتعامل بطريقة آنية وفورية مع المعلومات المتعلقة بعملية المنافسة في الأسواق ومن ثمة تطبيق أساليب تقنية متقدمة في أعمالها وإدارتها.

---

[1] حورية بولعويدات ، مرجع سابق، ص 108.

[2] وسيلة هني، مرجع سابق، ص 55.

[3] سعد غالب ياسين، بشير عباس العلاق، مرجع سابق، ص 62.

[4] مصطفى هنشور وسيمة، مرجع سابق، ص 55.

المبحث الثاني:

الأحكام الخاصة بشركات المساهمة وانعكاس تكنولوجيا المعلومات عليها.

إكتساح تكنولوجيا المعلومات للمجال التجاري ألزم الشركات التجارية على التوجه نحو هذه التكنولوجيا وفي مقدمتها شركات المساهمة، حيث كانت دافعا قويا لها مكنها من إحداث تغيرات في طريقة أدائها لأعمالها فتمكنت بفضلها من الإستمرار في الأسواق والصمود في دائرة المنافسة أمام غيرها من الشركات، وفي هذا المبحث سنوضح الكيفية التي إنعكست بها تكنولوجيا المعلومات على شركات المساهمة، ولكن قبل ذلك نتطرق إلى الأحكام الخاصة بهذه الشركات باعتبارها محور الدراسة وذلك كن خلال تقسيمه إلى مطلبين:

المطلب الأول: الأحكام الخاصة بشركات المساهمة.

المطلب الثاني: إنعكاس تكنولوجيا المعلومات على شركات المساهمة.

المطلب الأول:

الأحكام الخاصة بشركات المساهمة.

تعتبر شركات المساهمة كوسيلة قانونية واقتصادية مؤشرا في غاية الأهمية على مدى تطور الحياة الاقتصادية بصفة عامة والنشاط التجاري بصفة خاصة، فهذه الشركات تعد من أهم الدعائم التي تستند عليها البيئة الاقتصادية في أية دولة كونها النموذج الأمثل لشركات الأموال، حيث وجدت من أجل إنجاز المشاريع الضخمة وتحقيق الأهداف التي عجزت عن تحقيقها الشركات الصغيرة وقد أولت التشريعات وعلى رأسها المشرع الجزائري إهتماما بالغا بها، هذا ما نوضحه من خلال هذا المطلب وذلك بالتطرق إلى الأحكام الخاصة بشركات المساهمة وفقا لأحكام القانون التجاري **(فرع أول)** والأحكام الخاصة بشركات المساهمة وفقا للقانون رقم 22-09 **(الفرع الثاني)**.

الفرع الأول:

الأحكام الخاصة بشركات المساهمة وفقا لأحكام القانون التجاري.

نظم المشرع الجزائري الأحكام الخاصة بشركات المساهمة في الفصل الثالث من الكتاب الخامس تحت عنوان "في الشركات التجارية" وذلك من المادة 592 إلى المادة 715 مكرر 132، ومن خلال هذا الفرع نتطرق إلى تعريف، وتأسيس شركات المساهمة أولا ثم إدارتها ثانيا.

أولا: تعريف شركة المساهمة وتأسيسها:

1-تعريف شركة المساهمة: تعرف على أنها تلك الشركة التي ينقسم رأسمالها إلى حصص وتتكون من شركاء لا يتحملون الخسائر إلا بقدر حصتهم، ولا يمكن أن يقل عدد شركائها عن سبعة[1].

ومن خلال هذه المادة يتبين بأن شركة المساهمة تتميز بمجموعة من الخصائص نوردها فيما يلي:

أ-رأسمال الشركة: حدد المشرع رأسمال شركة المساهمة من خلال المادة 594 من المرسوم التشريعي 93-08، فيجب ألا يقل عن 5 ملاين دينار جزائري في حالة لجوء الشركة في تأسيسها إلى علنية الإدخار أي الإكتتاب العام، أما في حالة إعتمادها على رأسمال المؤسسين لها فقط فيجب ألا يقل عن مليون دينار جزائري.

ب-عدد شركاء الشركة: تم تحديد الحد الأدنى للشركاء المساهمين في الفقرة الثانية من المادة 592 من المرسوم التشريعي 93-08 إذ يجب ألا يقل عن 7 شركاء، وللإشارة فإن هذا العدد غير مطلوب حينما يتعلق بالشركات التي تتخذ شكل شركات مساهمة وتكون ذات رؤوس أموال عمومية، باعتبار أن الشريك الوحيد فيها هي الدولة كالبنوك مثلا أو المؤسسات العمومية الاقتصادية، كما أن المشرع لم يحدد حد أقصى للشركاء فبإمكانها أن تستقطب ما تشاء من الشركاء المساهمين ويمكن لهؤلاء الشركاء أن يكونوا أشخاص طبيعين أو معنويين.

ت-إسم الشركة: يجب أن يكون لهذه الشركة إسم تنفرد به عن غيرها من الشركات، ويكون إسمها مستمد من الغرض الذي تأسست من أجله مع إلزامية أن يكون مسبوقا أو متبوعا بشكل الشركة ومبلغ رأسمالها، كما يمكن أن يدرج إسم شريك واحد أو أكثر.[2]

ث-حصة الشريك: من أهم ما تتميز به شركة المساهمة هو قابلية حصة الشريك فيها لعملية التداول،[3] بمعنى أن يجوز لكل شريك مساهم فيها أن ينقل ملكية أسهمه سواء بصفة كلية أو جزئية

---

[1] المادة 592 من المرسوم التشريعي رقم 93-08 مؤرخ في 25 أفريل 1993، يعدل ويتمم الأمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري، ج،ر، ع 27، الصادر في 25 أفريل 1993.

[2] المادة 593 من من نفس المرسوم.

[3] المادة 715 مكرر 40 من نفس المرسوم.

لغيره في أي وقت شاء ذلك، دون أن تكون هناك ضرورة لموافقة باقي المساهمين حيث يعد التداول معيار لعملية التفرقة بين شركات الأشخاص وشركات الأموال،[1] وخاصية التداول تشجع الجمهور على المساهمة من أجل الإدخار في هذه الشركة وتحقيق أرباح أكبر وهذا ما يترتب عليه إتساع المشاريع الكبرى وازدهار شركات المساهمة ورواجها.[2]

ج–مسؤولية الشريك: ما يميز مسؤولية الشريك فيها هو أنه لا يتحمل الخسائر ولا يسأل عن ديون الشركة إلا بقدر ما إكتتب فيها من أسهم أي في حدود حصته المقدمة،[3] وبالتالي فإن الشريك لا يكتسب فيها صفة التاجر ولا يلتزم بإلتزامه كما أن إفلاس الشركة لا يترتب عليه إفلاسه.

2– تأسيس شركة المساهمة: المقصود بتأسيس شركة المساهمة هو جملة الأعمال القانونية والمادية التي يتم القيام بها من قبل الشركاء المساهمين بغية إنشائها،[4] حيث أن تأسيس هذه الشركة يستدعي العديد من الإجراءات التي تتسم بطابعها المعقد الطويل كونها تختلف تماما عن غيرها من الشركات التي يتم تأسيسها بمجرد الإنتهاء من عملية إنشاء العقد، ويرجع السبب في ذلك إلى ضخامة المشاريع التي تقوم بها والتي تستلزم تجميع أموال ضخمة حتى يتم تحقيق تلك المشاريع وتجسيدها،[5] وبالرجوع إلى أحكام القانون التجاري نجد بأن المشرع الجزائري قد نص على طريقتين من أجل تأسيس شركة المساهمة وتتمثل هاتين الطريقتين في:

---

[1] عبد الباقي خلفاوي، (حرية تداول الأسهم في شركات المساهمة في التشريع الجزائري)، مجلة العلوم الإنسانية ، ع 2، مج 31، الصادر في جوان 2020 ، ص ص 127، 128.

[2] زهية عزيزي، (تداول الأسهم وعلاقته بالإعتبارين المالي والشخصي في شركة المساهمة)، مجلة الدراسات الحقوقية ، ع 2، مج 09، الصادر في ديسمبر 2022 ، ص 607.

[3] المادة 592 من المرسوم التشريعي رقم 93–08، مرجع سابق.

[4] حسام الدين خلفي، أحكام المسؤولية الجزائية لشركات المساهمة ، ط 1، جمهورية مصر العربية ، مركز الدراسات العربية للنشر والتوزيع، 2020، ص 33.

[5] نادية فضيل، شركات الأموال في القانون الجزائري ، ط 3، بن عكون، الجزائر ، ديوان المطبوعات الجامعية، 2008، ص 151.

أ-تأسيس شركة المساهمة عن طريق اللجوء إلى الإدخار العلني: ويسمى أيضا بالتأسيس المتتابع،[1] ويتم ذلك من خلال طرح أسهم الشركة للإكتتاب العام بغية شراءها من قبل الجمهور، حيث تتميز الإجراءات في هذا النوع من التأسيس بالصرامة وذلك من أجل المحافظة على أموال المكتتبين وحمايتها.

ففي البداية ينبغي على المؤسسين،[2] إعداد عقد إبتدائي يكون عبارة عن مشروع قانون أساسي للشركة حيث يعتبر وكأنه دستور تسير عليه، ويتم تحريره من قبل موثق وذلك بناء على طلب أحد المؤسسين أو أكثر ليتم بعدها إيداع نسخة منه بالمركز الوطني للسجل التجاري،[3] وينبغي أن يشتمل على البيانات التالية:

بيان تسمية الشركة، الغرض الذي أنشأت من أجله، مدة بقاءها، مقدار رأسمالها، كيفية إدارتها ورقابتها، سلطة المديرين وعدد الأسهم التي يحوز عليها عضو الإدارة وصلاحيته، القواعد المتعلقة بالجمعية العامة وأيضا حقوق المساهمين في عملية التصويت وطريقة المداولة، جرد أموال الشركة، كيفية توزيع الأرباح والخسائر والقواعد التي تحكم انقضائها وتصفيتها واقتسام أموالها.[4]

بعدها تأتي عملية الإكتتاب والذي يعرف على أنه ذلك العقد الذي يلتزم فيه شخص ما بالإنضمام إلى الشركة عن طريق تقديمه مال نقدي أو عيني يكون مساويا للقيمة الإسمية للأسهم،[5] ورغم أن المشرع الجزائري لم يتطرق إلى تعريفه غير أنه خصه بأحكام ضمن القانون التجاري وذلك

---

[1] حسام الدين خلفي، مرجع سابق، ص 34.

[2] يعرف المؤسس بأنه الشخص الذي يقوم بالإشتراك الفعلي في تأسيس الشركة مع نيته في تحمل المسؤولية المترتبة عن إجراء التأسيس وهو أيضا من يقوم بالتوقيع على العقد الإبتدائي أو يقدم حصة عينية أو يطلب ترخيص تأسيسها، كما يعرف أيضا على أنه من يقوم بالإشراف على إجراءات التأسيس مثل إجراءات التوثيق، القيد، الإيداع وكذا النشر، وللإشارة فإن المشرع الجزائري لم يعرف المؤسس، (عبد القادر حمر العين، (المركز القانوني للشريك المؤسس في شركة المساهمة قيد التأسيس)، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة الجزائر ، ع 3، مج 34، الصادر في 2020 ، ص 1230.

[3] المادة 592 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[4] نادية فضيل، مرجع سابق، ص ص 165، 166.

[5] عبد السلام زعرور، (الإكتتاب في رأسمال شركة المساهمة بين العقد والإرادة المنفردة)، مجلة الحقوق والعلوم السياسية ، ع 8، مج 02، الصادر في جوان 2017 ، ص 894.

من المادة 595 إلى المادة 599 بمناسبة تأسيس شركة المساهمة ومن المادة 702 إلى المادة 706 في حالة اللجوء إلى زيادة رأسمال الشركة.

وحين يتم الإنتهاء من عملية الإكتتاب في أسهم الشركة نجد بأن المشرع قد ألزم المؤسسين باستدعاء جميع المكتتبين لعقد جمعية عامة تأسيسية يثبت فيها أن رأسمال المكتتب به تماما وأن مبلغ الأسهم مستحق الدفع، كما تبدي رأيها في المصادقة على القانون الأساسي للشركة وتعيين القائمين بالإدارة الأوليين أو أعضاء مجلس المراقبة وتعيين واحد أو أكثر من مندوبي الحسابات[1]، وحتى يكتمل تأسيسها وتكتسب الشخصية المعنوية لا بد من قيدها في السجل التجاري[2]،

ب-تأسيس شركة المساهمة دون اللجوء إلى الإدخار العلني: ويعرف بالتأسيس الفوري وفي هذا النوع من التأسيس يكون الإكتتاب في رأسمال الشركة مقتصرا على المؤسسين فقط دون الإستعانة بالمدخرين الصغار وبالتالي لا يكون هناك أي خطر عليهم،[3] ومثلما سبقت الإشارة فإن الحد الأدنى في الرأسمال المطلوب في هذه الحالة يجب ألا يقل عن مليون دينار جزائري، ويخضع هذا التأسيس لإجراءات بسيطة مقارنة مع النوع الأول وقد تم تنظيم الأحكام الخاصة به من المادة 605 إلى المادة 609.

وبالنسبة لعملية الإكتتاب في رأسمال الشركة فإنه يجب على أحد المساهمين أو أكثر تحرير عقد لدى الموثق حتى يثبت فيه هذا الأخير المبالغ التي تم دفعها من طرف كل مؤسس أي أن المبالغ المصرح بها تتطابق مع المبالغ المدفوعة،[4] وباعتبار أن رأسمال قد يتكون من حصص عينية فإنه يجب أن يتضمن القانون الأساسي تقدير هذه الحصص العينية وذلك بموجب تقرير ملحق بالقانون الأساسي، حيث يتم إعداد هذا التقرير من قبل مندوب الحصص وتحت مسؤوليته.[5]

---

[1] المادة 600 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[2] المادة 549 من الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري،ج، ر، ع 101، الصادر في 19 ديسمبر 1975، المعدل والمتمم.

[3] نادية فضيل، مرجع سابق، ص 152.

[4] المادة 600 من الأمر رقم 75-59، مرجع سابق.

[5] المادة 607 من المرسوم التشريعي رقم 93-08، مرجع سابق.

وفيما يتعلق بالقانون الأساسي فإنه يجب أن يتم التوقيع عليه إما من قبل المساهمين أنفسهم أو عن طريق وكيل يكون مزود بتفويض خاص، وذلك بعد أن يتم تصريح الموثق بالدفعات وبعد وضع التقرير الخاص بالحصص العينية تحت تصرف المساهمين وفقا للشروط والآجال المحددة عن طريق التنظيم.[1]

ثانيا: إدارة شركة المساهمة:

بالإطلاع على أحكام القانون التجاري يتضح بأن إدارة شركة المساهمة يتم وفق نمطين، نمط تقليدي يقوم على مجلس الإدارة ونمط حديث يقوم على مجلس المديرين ومجلس المراقبة، وعلى شركة المساهمة أن تختار النظام الذي تسير عليه ويتم تحديد ذلك في قانونها الأساسي دون الجمع بين النظامين.

1-نمط التسيير التقليدي: وتتمثل أجهزة هذا النظام في مجلس الإدارة ورئيسه، حيث يعتبر مجلس الإدارة هو الهيئة الأساسية التي توكل لها مهمة تسيير وإدارة الشركة وتنفيذ القرارات التي تصدرها جمعية المساهمين وذلك من أجل تحقيق أهداف الشركة.[2]

يتشكل مجلس الإدارة من 3 أعضاء على الأقل و 12 عضوا على الأكثر، غير أنه في حالة الدمج يجوز رفع العدد للقائمين بالإدارة الممارسين منذ أكثر من 6 أشهر ولكن دون تجاوز 24 عضوا، وماعدا حالات الدمج الجديد فمن غير الممكن إستخلاف المنصب الشاغر بسبب الوفاة أو الإستقالة أو العزل إذا لم يخفض العدد إلى 12 عضوا.[3]

يتم تعيين أعضاء مجلس الإدارة عن طريق الإنتخاب من طرف الجمعية العامة التأسيسية أو الجمعية العامة العادية ويتم تحديد مدة عضويتهم ضمن القانون الأساسي للشركة دون أن يتجاوز 6 سنوات،[4] وتجدر الإشارة إلى أن عضو مجلس الإدارة إذا كان شخصا طبيعيا فإنه لا يجوز له الإنتماء

---

[1] المادة 608 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[2] سهام دربال، "شركة المساهمة ومبادئ الحوكمة الرشيدة " (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2018-2019)، ص 233.

[3] المادة 610 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[4] المادة 611 من نفس المرسوم.

إلى أكثر من 5 مجالس إدارة شركات مساهمة يكون مقرها موجود بالجزائر، وفي مقابل ذلك فإنه من الممكن أن يكون عضو مجلس الإدارة شخصا إعتباريا وفي هذه الحالة يجب عليه تعيين ممثل دائم له يخضع لذات الشروط والواجبات التي يخضع لها بقية أعضاء مجلس الإدارة، إذ يتحمل نفس المسؤوليات المدنية والجزائية وكأنه قائما بالإدارة باسمه الخاص ولكن دون أن يمس ذلك بالمسؤولية التضامنية للشخص الإعتباري الذي يمثله.[1]

وحتى يقوم مجلس الإدارة بأعماله على أحسن وجه فإن الأمر يتطلب أن يكون هناك شخص يترأس هذا المجلس ويمثل الشركة في علاقاتها مع الغير، حيث يتم تعيينه عن طريق إنتخابه من بين أعضاء المجلس ويشترط أن يكون شخصا طبيعيا ويتم تحديد أجره من قبل المجلس،[2] ويجب ألا تتجاوز مدة تعيينه مدة نيابته كقائم بالإدارة مع إمكانية إعادة إنتخابه ولمجلس الإدارة الحق في عزله في أي وقت.[3]

وفي حالة ما إذا كان هناك مانع مؤقت للرئيس أو تعرض لوفاة أو إستقالة أو عزل فإنه يجب على المجلس أن ينتدب قائما بالإدارة حتى يؤدي الوظائف المنوطة به، غير أنه في حالة ما إذا كان المانع مؤقتا ففي هذه الحالة فإن الإنتداب يتم منحه لمدة محددة فقط تكون قابلة للتجديد وذلك على خلاف الوفاة أو الإستقالة أو العزل فهنا تستمر مدة الإنتداب إلى حين إنتخاب رئيس جديد.[4]

وقد منح المشرع إمكانية تعيين شخصين طبيعيين أو شخصا واحدا كمدرين عامين من أجل مساعدة الرئيس،[5] ويتمتع رئيس مجلس الإدارة بالسلطات الواسعة التي تخوله التصرف باسم الشركة في كافة الظروف، وتكون الشركة ملزمة بأعمال الرئيس في علاقاتها مع الغير وذلك حتى في حالة

---

[1] المادة 611 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[2] المادة 635 من الأمر رقم 75-59، مرجع سابق.

[3] المادة 636 من نفس الأمر.

[4] المادة 637 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[5] المادة 639 من نفس المرسوم.

خروج الرئيس عن مجالات إختصاصه ما لم يثبت بأن الغير كان على علم بأن ذلك العمل يتجاوز إختصاصات الرئيس أو لا يمكن تجاهله نظرا للظروف.[1]

2-نمط التسيير الحديث: أول ما ظهر هذا النوع من التسيير كان في ألمانيا لينتقل بعدها إلى فرنسا حيث يقوم على الفصل بين الإدارة التي تعتمد على مجلس المديرين والمراقبة التي تعتمد على مجلس المراقبة،[2] ويجوز لأية شركة مساهمة أن تنص ضمن قانونها الأساسي على إعتماد هذا النظام، كما أنه بإمكان الجمعية العامة غير العادية أثناء وجود الشركة أن تدرج هذا الشرط في القانون الأساسي أو إلغاءه[3].

وهذا النمط يساعد الشركة على تجنب سلبيات النظام القديم، فالعديد من الشركات الفرنسية إعتمدته، الأمر الذي جعلها تحتل مقدمة الشركات الكبرى ذات الأهمية في المجال الاقتصادي[4].

بالنسبة لمجلس المديرين فإنه يتشكل من 3 إلى 5 أعضاء ويمارس وظائفه تحت رقابة مجلس المراقبة[5]، حيث يتولى هذا الأخير تعيين أعضاء مجلس الإدارة وتسند الرئاسة إلى أحدهم ويشترط أن يكونوا أشخاصا طبيعين[6].

ويجب أن يتضمن القانون الأساسي للشركة بصفة صريحة مدة عضوية مجلس المديرين بين سنتين إلى 6 سنوات، غير أنه في حالة عدم تضمن القانون الأساسي لهذه المدة فإنها تحدد بأربعة (4) سنوات ، وفي حالة شغور المجلس لأي سبب كالوفاة، الإستقالة فإنه يجوز تعيين عضو آخر حتى يتم تجديد المجلس،[7] ويكون لهذا المجلس سلطات واسعة للتصرف باسم الشركة.

إضافة إلى هذا المجلس فإن الشركة تكون ملزمة بتعيين مجلس آخر ليتولى مهمة الرقابة على أعمال مجلس الإدارة وهو ما يسمى بمجلس المراقبة.

---

[1] المادة 638 من الأمر رقم 75-59، مرجع سابق.

[2] حسام الدين خلفي، مرجع سابق، ص 41.

[3] المادة 642 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[4] نادية فضيل، مرجع سابق، ص 258.

[5] المادة 643 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[6] المادة 644 من نفس المرسوم.

[7] المادة 646 من نفس المرسوم.

حيث يتكون هذا المجلس من 7 أعضاء كحد أدنى و 12 عضو كحد أقصى،[1] وستثناء من الممكن تجاوز هذا العدد في حالة الشركات المدمجة ولكن بشرط ألا يتجاوز ذلك 24 عضوا، كما يشترط أن يكونوا قد أدوا مهام المراقبة أكثر من 6 أشهر،[2] ويتم إنتخاب أعضاء مجلس المراقبة من طرف الجمعية العامة التأسيسية أو الجمعية العامة العادية مع إمكانية إعادة إنتخابهم مرة أخرى في حالة عدم نص القانون الأساسي على ما يخالف ذلك، أما بالنسبة لمدة عضوية أعضائه فيتم تحديدها ضمن القانون الأساسي للشركة حيث تحدد ب ستة (6) سنوات في حالة ما إذا كان التعيين من قبل الجمعية العامة وثلاثة (3) سنوات في حالة التعيين بموجب القانون الأساسي، كما أنه من الممكن أن يتم التعيين من طرف الجمعية العامة غير العادية ويكون ذلك في حالة الدمج أو الإنفصال.[3]

وللإشارة فإن أعضاء مجلس المراقبة يمكن أن يكونوا أشخاصا طبيعين كما يمكن أن يكونوا أشخاصا معنويين، وفي هذه الحالة على الشخص المعنوي عند تعيينه أن يقوم بتعيين ممثل عنه،[4] ويجب على مجلس المراقبة أن يعين على مستواه رئيسا حتى يتولى مهمة إستدعاء المجلس وإدارة المناقشات وتكون مدة مهمته معادلة لمدة مهمة المجلس.[5]والمشرع لم يوضح الأحكام الخاصة بتعيين الرئيس واختصاصاته.

وبالنسبة للإختصاصات الرقابية الموكلة لمجلس المراقبة فهي تشبه إختصاصات مجلس الإدارة باعتبار أن كل منهما مخول بعملية الرقابة على جهاز آخر ضمن الشركة، غير أن الفقه الفرنسي رغم هذا التشابه يذهب إلى القول بأن المهمام الممنوحة لمجلس المراقبة تعتبر أقل من المهام الممنوحة لمجلس الإدارة.[6]

---

[1] المادة 657 من المرسوم التشريعي رقم 93-08، مرجع سابق.

[2] المادة 658 من نفس المرسوم.

[3] المادة 662 من نفس المرسوم.

[4] المادة 663 من نفس المرسوم.

[5] المادة 666 من نفس المرسوم.

[6] سهام دربال، مرجع سابق، ص 268.

الفرع الثاني:

الأحكام الخاصة بشركات المساهمة وفقا للقانون رقم 22-09

إضافة إلى شركة المساهمة الكلاسيكية التي سبق الإشارة إليها، نجد بأن المشرع الجزائري وبهدف تشجيع الإستثمار وتجسيد التنويع الاقتصادي قد إستحدث شكلا آخر من شركات المساهمة أطلق عليه إسم شركات المساهمة البسيطة "SOCETE PAR ACTIONS SIMPLIFIEE" وكان ذلك بموجب القانون رقم 22-09،[1] ليتمم بذلك الفصل الثالث من الباب الأول من الكتاب الخامس من الأمر رقم 75-59 بقسم ثاني عشر خصصه لهذه الشركة المستحدثة وذلك من المادة 715 مكرر 133 إلى المادة 715 مكرر 143، وبما أن هذه الشركة تعد من شركات المساهمة فيمكن أن تكون هي الأخرى عرضة للجرائم الإلكترونية، ومن خلال هذا الفرع نتعرف على الأحكام الخاصة بها وذلك بالتطرق إلى تعريفها وتأسيسها أولا ثم إدارتها.

أولا: تعريف شركة المساهمة البسيطة وتأسيسها:

1-تعريف شركة المساهمة البسيطة: نجد بأن أول من إستحدث شركة المساهمة البسيطة هو التشريع الفرنسي، حيث أطلق عليها تسمية "شركة الأسهم المبسطة" وكان ذلك بموجب القانون رقم 1-94 المؤرخ في 3 جانفي 1994 حيث عرف فيما بعد عدة تعديلات،[2] أما بالنسبة للمشرع الجزائري فقد عرفها من خلال المادة 715 مكرر 133 فقرة 1 على أنها تلك الشركة التي يتكون رأسمالها من أسهم كما أنها تتكون من شركاء لا يتحملون الخسائر إلا في حدود الحصص التي قدموها.

ويمكن أن يتم تأسيس شركة المساهمة البسيطة من طرف شخص واحد أو عدة أشخاص طبيعيين و/ أو معنويين، وفي حالة ما إذا كانت تضم شخصا واحدا فقط فتسمى حينها بشركة

---

[1] القانون رقم 22-09 مؤرخ في 5 ماي 2022، يعدل ويتمم الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري، ج،ر، ع 32، الصادر في 14 ماي 2022.

[2] نادية بوخرص، (الأحكام القانونية الخاصة الناظمة لشركة المساهمة البسيطة وفق للقانون رقم 22-09)، مجلة الدراسات القانونية، ع 1، مج 9، الصادر في جانفي 2023 ، ص 136.

المساهمة البسيطة ذات الشخص الوحيد، وتنشأ هذه الشركة حصريا من طرف الشركات الحاصلة على علامة "مؤسسة ناشئة"[1].

2-تأسيس شركة المساهمة البسيطة: بداية ينبغي أن نشير إلى أن شركة المساهمة البسيطة لم تحظ سوى بأحد عشر مادة فقط في التشريع الجزائري، وذلك كون أن المشرع قد أحال من خلال نص المادة 715 مكرر 35 من القانون 22-09 إلى تطبيق الأحكام الخاصة بشركة المساهمة على هذه الشركة شريطة ألا يتعارض ذلك مع أحكامها الخاصة وكذا ما تم إستثناؤه بموجب نص هذه المادة، وسنوضح الأحكام الخاصة بتأسيس شركة المساهمة البسيطة من خلال النقاط التالية:

أ-عدم إشتراط حد أدنى لعدد الشركاء: إذا كان المشرع مثلما رأينا قد إشترط حد أدنى لعدد الشركاء في شركة المساهمة، فإن الأمر يختلف بالنسبة لهذه الشركة فمن الممكن أن تؤسس من طرف شخص واحد أو عدة طبيعيين أو معنويين كما أجاز إمكانية تأسيسها حتى من طرف شخص واحد فقط سواء كان طبيعيا أو معنويا وسماها في هذه الحالة بشركة المساهمة ذات الشخص الوحيد[2].

ب-المسؤولية المحدودة للمساهمين فيها: الشركاء في هذه الشركة لا يتحملون الخسائر إلا في حدود ما قدموه من حصص،[3] وهو ما يتوافق مع الشركاء في شركة المساهمة حيث أن الشريك فيها لا يسأل عن ديون الشركة إلا في حدود الحصص التي قدمها، فلا يجوز مطالبته بأكثر من ذلك مهما بلغت ديونها.

وبما أن خاصية المسؤولية المحدودة بقدر الحصص المقدمة تعد من أبرز خصائص شركات الأموال فهذا ما يثبت الطابع المالي لهذه الشركة واعتبارها من شركات الأموال،[4] وبالتالي فعدم إشتراط حد أدنى للشركاء ومسؤوليتهم المحدودة تعد من أهم الأحكام التي تخص المساهمين بهذه الشركة.

---

[1] تعرف المؤسسة الناشئة بأنها كيان تم تصميمه بغرض خلق منتوجات أو خدمات جديدة وتكون هذه الكيانات على درجة من المخاطر بسبب ظروف عدم التأكد والمراحل الصعبة التي تمر بها في البداية. أنظر: آمنة مخانشة، (المؤسسات الناشئة في الجزائر الإطار المفاهيمي والقانوني)، مجلة صوت القانون، ع 1، مج 8، الصادر في 2021 ، ص 771.

[2] المادة 715 مكرر 133 فقرة 2، 3 من القانون رقم 22-09، مرجع سابق.

[3] المادة 715 مكرر 133 فقرة 1 من نفس القانون.

[4] صبرينة بوعمار، حمزة بوخروبة، (الطبيعة القانونية لشركة المساهمة البسيطة ، شركة المؤسسات الناشئة)، مجلة الدراسات والبحوث القانونية، ع 2، مج 8، الصادر في 2023 ، ص 244.

ت–رأسمال الشركة: يمكن إعتبار رأسمال الشركة بأنه جوهرها فهو مصدر لسلطتها ووسيلة من أجل تمويل نشاطها، فهو ذو قيمة بالغة سواء عند تأسيس الشركة أو خلال حياتها، كما أن أهميته تتجلى سواء بالنسبة للمساهمين فيها أو المتعاملين معها،[1] والمشرع الجزائري لم يشترط حد أدنى لرأسمال شركة المساهمة البسيطة وذلك حين إستثنى تطبيق أحكام المادة 594 فقرة 1 والتي تنص على تحديد الحد الأدنى لرأسمال شركة المساهمة .

وبهذا يكون المشرع الجزائري قد ترك الحرية للشركاء في تقدير رأسمالها وتحديده ضمن قانونها الأساسي،[2] وعلى العموم فإن رأسمالها يتكون من الحصص المقدمة من طرف الشركاء وقد تكون تلك الحصص إما نقدية أو عينية كما قد تكون عبارة عن حصص من عمل.[3]

وينبغي الإشارة إلى أنه في حالة الحصص العينية وباعتبار أنها لا تمنح أسهما لأصحابها إلا بعد أن يتم تقييمها حيث توكل هذه المهمة إلى مندوب الحصص الذي يعين من طرف الشركاء غير أنه يمكنهم الاتفاق على عدم اللجوء إلى هذا الأخير ولكن ذلك شريطة ألا يتجاوز قيمة الحصص العينية نصف رأسمال الشركة.[4]

وفي الحالة التي لا يتم فيها تعيين مندوب الحصص أو كان هناك إختلاف حول القيمة المحددة للحصص العينية عن تلك المقدمة من طرف مندوب الحصص فإن الشركاء تكون مسؤوليتهم تضامنية أمام الغير لمدة 5 سنوات عن القيمة الممنوحة للحصص العينية في القانون الأساسي للشركة.[5]ويمكن تقديم حصة من عمل في هذه الشركة ويعد هذا خروجا عن القاعدة التي تقضي بعدم

---

[1] ليلى بن عودة، (خصائص شركة المساهمة البسيطة الأكثر ملاءمة للمؤسسات الناشئة)، مجلة الدراسات القانونية المقارنة، ع 1، مج 9، الصادر في 2023 ، ص 169.

[2] المادة 715 مكرر 134 ، والمادة 715 مكرر 138 من القانون رقم 22–09، مرجع سابق.

[3] نادية بوخرص، مرجع سابق، ص 145.

[4] المادة 715 مكرر 141 ، من القانون رقم 22–09، مرجع سابق.

[5] المادة 715 مكرر 142 ، من نفس القانون .

جواز تقديم حصة العمل في شركات الأموال، ولعل سبب إجازة هذا النوع من الحصص هو أن المعلومات والأفكار أصبحت مصدرا خلاقا للثروة قد يتجاوز المصادر التقليدية المعروفة.[1]

غير أن هذه الحصص لا تدخل ضمن تأسيس رأسمال الشركة وإنما تدخل فقط في تقاسم أرباحها وصافي الأصول والخسائر ويتم تقدير قيمتها وما تخوله من أرباح ضمن قانونها الأساسي فالأسهم الناتجة عن تقديم حصص العمل تكون غير قابلة للتصرف فيها ،[2] وذلك على خلاف باقي الأسهم التي تكون قابلة للتداول والتصرف فيها من قبل أصحابها.

وقد منع المشرع على هذه الشركة اللجوء إلى الإدخار العلني من أجل طرح أسهمها للإكتتاب العام كما يحظر عليها طرح أسهمها في البورصة،[3] لذلك توصف بأنها شركة مغلقة.[4]

ثانيا: إدارة شركة المساهمة البسيطة:

حتى تتمكن هذه الشركة من أداء أعمالها فلا بد أن تكون هناك إدارة حتى يتم تسيير شؤونها، وبالتمعن في نصوص القانون رقم 22-09 نلاحظ بأن المشرع قد بسط من إجراءات إدارتها، حيث منح للمساهمين فيها الحرية الواسعة في كيفية تنظيمها وإدارتها وتحديد ذلك ضمن القانون الأساسي الخاص بها، [5] لذلك فيمكن القول بأن قانونها الأساسي يتسم بنوع من المرونة فالطرق التي يتم بها إدارة هذه الشركة قد يختلف من شركة إلى أخرى، ومن خلال هذه النقطة سنتطرق إلى رئيس هذه الشركة ثم الجمعية العامة للمساهمين فيها.

1-رئيس شركة المساهمة البسيطة: يتم تعيين رئيس الشركة باعتباره مديرا عاما أو مديرا مفوضا من قبل الشركاء ضمن قانونها الأساسي،[6] إذ يتعين عليهم أن يحددوا الشروط الواجبة لتعينه كالخبرة والكفاءة مثلا كذلك طريقة التعيين، العزل، المدة، الأجر الذي يتقضاه حيث يتولى ممارسة صلاحيات

---

[1] ثامر خالدي، (شركة المساهمة البسيطة في ظل القانون التجاري رقم 22-09)، المجلة الجزائرية للعلوم القانونية والسياسية، ع 3، مج 60، الصادر في 2023 ، ص 459.

[2] المادة 715 مكرر 140 فقرة 2، من القانون رقم 22-09، مرجع سابق.

[3] المادة 715 مكرر 139 من نفس القانون.

[4] ثامر خالدي، مرجع سابق، ص 459.

[5] المادة 715 مكرر 134 ، من القانون رقم 22-09، مرجع سابق.

[6] المادة 715 مكرر 136 فقرة 1 ، من نفس القانون.

مجلس الإدارة ورئيس مجلس الإدارة في شركة المساهمة العادية،[1] غير أنه في الحالة التي تتكون فيها هذه الشركة من شخص واحد أي شركة مساهمة بسيطة ذات الشخص الوحيد فإن ذلك الشخص الوحيد هو الذي يتولى ممارسة مهام الرئيس كما أنه يتخذ القرارات الممنوحة لجمعية الشركاء.[2]

كما تطبق على الرئيس أو المدير العام أو المدير العام المفوض لهذه الشركة ذات قواعد المسؤولية التي يتم تطبيقها على رئيس شركة المساهمة أو القائمين بإدارتها.[3]

2-الجمعية العامة للمساهمين: تعتبر الجمعية العامة للمساهمين الهيئة التي تختص بالفصل في كل ما يتعلق بتسيير وتقرير مصير الشركة،[4] وبالرجوع إلى المادة 715 مكرر 137 من القانون رقم 22-09 نجد بأن المشرع قد أعطى صلاحيات واسعة للمساهمين من أجل تحديد القرارات التي تخضع عملية إتخاذها للجمعية العامة للمساهمين ضمن القانون الأساسي للشركة.

لكن بالرجوع إلى الفقرة الثانية من ذات المادة نجد بأنه قد قيد هذه الصلاحيات حينما نص على أن قرارات الجمعية العامة العادية وغير العادية التي تتعلق بمسألة زيادة وتخفيض واستهلاك رأسمال والإدماج والإنفصال وحل الشركة وتغييرها إلى شكل آخر وتعيين محافظي الحسابات والحسابات السنوية وكذا الأرباح يجب إتخاذها جماعيا من قبل المساهمين ووفقا للكيفيات التي تم تحديدها ضمن القانون الأساسي للشركة.

وبالتالي ما يتضح من خلال هذه الفقرة هو أن المشرع لم بفصل بين تلك القرارات التي تعتبر من ضمن صلاحيات الجمعية العامة العادية والقرارات التي تندرج ضمن صلاحيات الجمعية العامة غير العادية، وذلك على خلاف شركة المساهمة العادية حيت تم تحديد الصلاحيات الخاصة بكل منهما، أما فيما يتعلق بمحافظوا الحسابات في هذه الشركة فإن تعيينهم يكون من طرف الجمعية العامة للمساهمين.

---

[1] أحمد لمين مناجلي، (النظام القانوني لشركة المساهمة البسيطة وملاءمته للمؤسسات الناشئة)، مجلة العلوم القانونية والإجتماعية ع 3، مجئءئ 8، الصادر في سبتمبر 2023 ، ص 602.

[2] المادة 715 مكرر 136 فقرة 2 ، من القانون رقم 22-09، مرجع سابق.

[3] المادة 715 مكرر 143 ، من نفس القانون.

[4] صبرينة بوعمار، مرجع سابق، ص 250.

وفي حالة ما إذا كانت الشركة البسيطة تتكون من شريك واحد فقط فيعين من طرف هذا الأخير، ويعد تعيينه إختياري إذا لم يتجاوز قيمة الحصص العينية مصف رأسمال الشركة،[1] رغم أن تعيينه إلزامي في شركة المساهمة العادية.

وما يمكن قوله عن شركة المساهمة البسيطة أنها تعتبر كنوع من شركات المساهمة وليس كشكل جديد من شركات الأموال، وذلك باعتبار أن المشرع قام بإدراجها ضمن الفصل الثالث حيث تممه بقسم ثاني عشر مخصص لهذه الشركة دون أن يخصها بفصل مستقل لوحدها.

المطلب الثاني:

إنعكاس تكنولوجيا المعلومات على شركات المساهمة.

توجه شركات المساهمة نحو تكنولوجيا المعلومات مواكبة للتطورات التقنية الحاصلة كان له عدة إنعكاسات على هذه الشركات، حيث أنها غيرت من النمط التقليدي الذي كانت تتبعه إلى نمط ذو طبيعة تقنية، هذا ما نوضحه من خلال هذا المطلب وذلك بالتطرق إلى توجه شركات المساهمة نحو الأعمال والتجارة الإلكترونية **(فرع أول)** ثم إنتقالها من الإدارة التقليدية إلى الإدارة الإلكترونية **(فرع ثاني)**.

الفرع الأول:

توجه شركات المساهمة نحو الأعمال والتجارة الإلكترونية.

نتيجة للبيئة الإلكترونية التي وجدت شركات المساهمة نفسها فيها كان لزاما عليها التغيير من طبيعة أعمالها لذلك إتجهت نحو الأعمال والتجارة الإلكترونية والتي أصبحت من المسائل التي حظيت باهتمام هذه الشركات نظرا لأهميتها، هذا ما نوضحه من خلال هذا الفرع.

أولا: توجه شركات المساهمة نحو الأعمال الإلكترونية:

1-تعريف الأعمال الإلكترونية: بداية نشير إلى أن مصطلح الأعمال الإلكترونية أول ما تم إستعماله كان من طرف شركة "IBM" وكان ذلك خلال سنة 1997 حينما قامت بإطلاق حملتها تحت

[1] المادة 715 مكرر 141 ، من القانون رقم 22-09، مرجع سابق.

مصطلح "الأعمال الإلكترونية" من أجل تمييز الأعمال ذات الطابع الإلكتروني عن الأنشطة التي تتعلق بالتجارة الإلكترونية،[1] وهناك عدة تعريفات تطرقت إلى موضوع الأعمال الإلكترونية نوردها فيما يلي:

عرف "P. KOTTLER" الأعمال الإلكترونية على أنها لجوء الشركة إلى إستخدام التكنولوجيا والبرمجيات وكذا مختلف الشبكات المتمثلة في الأنترنت، الأنترانت والإكسترنت من أجل تنظيم أعمالها وإدارتها.[2]

عرفها أيضا "CHAFFEY" على أنها كافة الوسائل التي تتعلق بتكنولوجيا المعلومات والتي يتم إستخدامها قصد التبادل بين الشركات فيما بينها، أو في علاقاتها مع المحيط الخارجي ومتغيراته المتختلفة،[3] أما "ROBBINS" فينظر إلى الأعمال الإلكترونية على أنه لا يمكن إعتبارها برمجيات وتقنيات فحسب قصد تسهيل أعمال الشركة، وإنما تتمثل في تلك الرؤية الإستراتجية التي تمكن الشركة من تحقيق أهدافها التي تصبو إليها، فهي عبارة عن الإطار الشامل الذي يمكن من خلاله وصف طرق أداء الأعمال عن طريق إستعمال التقنيات الإلكترونية التي تقوم على شبكة الأنترنت سواء كان ذلك مع موظفيها أو مديريها وعملاءها.[4]

في حين يرى محمد عبد العظيم أبو النجا الأعمال الإلكترونية بأنها، الأعمال التي تضم كافة الوسائل الإلكترونية التي تسمح بأداء أنشطة وأعمال الشركة داخلها أو بينها وبين غيرها من الشركات وكذا العملاء والموزعين والموردين الذين تتعامل معهم وذلك بطريقة أسرع وأدق مهما إختلف وتباعد

---

[1] رشيد فراح، كريمة فرحي، (متطلبات الأعمال الإلكترونية في العالم العربي بين الواقع وضرورة التحسين)، مجلة علوم الاقتصاد والتسيير والتجارة ع 32، الصادر في 2015 ، ص 151.

[2] غسان قاسم اللامي، تكنولوجيا المعلومات في منظمات الأعمال ، ط 1، الأردن ، دار الرواق للنشر والتوزيع، 2020، ص 130.

[3] صباح بلقيدوم، "أثر تكنولوجيا المعلومات والإتصالات الحديثة، NTIC، على التسيير الإستراتيجي للمؤسسات الإقتصادية " (أطروحة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة قسنطينة 2، 2012-2013)، ص 168.

[4] رشيد فراح، مرجع سابق، ص 151.

النطاق الزماني والمكاني،[1] وعرفتها شركة "IBM" بأنها تحويل نمط الأعمال واللجوء إلى إستخدام التقنيات التكنولوجية والأنترنت.[2]

وبعد عرض هذه التعريفات نصل إلى القول بأن الأعمال الإلكترونية تتمثل في كافة الأعمال والأنشطة الخاصة بالشركة والتي يتم تنفيذها إعتمادا على ما أوجدته تكنولوجيا المعلومات من تقنيات ووسائل، كما أن هذه الأعمال لا تشمل أنشطة الشركة ضمن محيطها الداخلي فقط وإنما تشمل إلى جانب ذلك جملة الأعمال التي تقوم بها في إطار علاقاتها مع الغير، شركاء عملاء وهذا ما يعطيها مفهوم أوسع وأشمل وبالتالي الخروج عن ذلك الإطار الضيق التي يحصرها فقط في الأعمال التي تتم على مستوى النطاق الداخلي للشركة.

2-مراحل الأعمال الإلكترونية: بما ان الأعمال الإلكترونية هي وليدة تكنولوجيا المعلومات فأكيد أن تطورها إرتبط بتطور هذه التكنولوجيا، وشركات المساهمة لم تلجأ إلى إعتماد هذه الأعمال دفعة واحدة وإنما كان ذلك عبر مراحل عدة وهي:

أ-المرحلة الأولى: تبدأ ببداية ظهور شبكة الأنترنت إلى الوجود إلى غاية 1994، حيث أنه خلال هذه الفترة أصبحت الشركات تلجأ إلى عرض أعمالها عبر شبكة الأنترنت وهذا العرض يمكن تشبيهه بالعروض التقليدية للإشهار.[3]

ب-المرحلة الثانية: والي يتم تحديدها إنطلاقا من سنة 1995 إلى غاية 1997 حيث أن الشركات خلال هذه المرحلة شرعت في تقديم خدمات جديدة لمتكن موجودة من قبل، الأمر الذي ترتب عنه نجاح هذه الأعمال الإلكترونية بشكل أوسع مما كانت عليه في البداية،[4]

---

[1] رشيد فراح، مرجع سابق ، ص 151.

[2] مزهر شعبان العاني، الأعمال الإلكترونية منظور إداري تكنولوجي ، ط 1، عمان ، دار الإعصار العلمي للنشر والتوزيع، 2015، ص 31.

[3] العياشي زرزار، كريمة غياد، إستخدامات تكنولوجيا المعلومات والإتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية ، ط 1، عمان ، دار صفاء للنشر والتوزيع، 2016، ص 112.

[4] رشيد فراح، مرجع سابق، ص 153.

كما أن خلال هذه الفترة ظهرت بعض محركات البحث والتي سمحت للعملاء من الوصول إلى المعلومات المطلوبة التي تتعلق بالسلع والخدمات التي يرغبون فيها، لكن ما يميز هذه المرحلة هو أنه لم يتم التأكد من مدى نجاح هذه الأعمال الإلكترونية المقدمة.[1]

ت–المرحلة الثالثة: والتي تحدد فترتها من سنة 1997 إلى غاية 1998 وتم خلالها إنشاء مختلف الشبكات (الأنترنت والأنترانت) على مستوى الشركات،[2] وبالتالي فإن نشوء هذه الشبكات ساعد على تعزيز وتدعيم مختلف الأعمال الإلكترونية كما أن أعمال الشركة أصبحت تنفذ بشكل منسق وإلكتروني.

ث–المرحلة الرابعة: والتي تبدأ من سنة 1998 إلى غاية 2001 وما ميز هذه المرحلة هو ظهور شبكة الإكسترنت، والتي بظهورها تدعمت الأعمال الإلكترونية للشركة والتي تقوم بها مع غيرها من الأطراف الخارجية كالموردين والمتعاملين الماليين.[3]

ج–المرحلة الخامسة: والتي تنطلق من سنة 2001 إلى غاية الفترة الراهنة والتي تم فيها فعلا ممارسة الأعمال الإلكترونية وتجسيدها بشكل أكثر دقة، ونتيجة لذلك إرتفعت عمليات التبادل التجاري الإلكتروني بين مختلف الشركات وكذلك بين الشركات وعملاءها، كما كان هناك إتجاه فعال يعمل على تعزيز الأعمال الإلكترونية بالإعتماد في ذلك على التكامل بين الشبكات الثلاثة.[4]

3–مزايا الأعمال الإلكترونية لشركات المساهمة: من دون شك أن توجه هذه الشركات نحو الأعمال الإلكترونية حقق لها العديد من الفوائد والمزايا والتي منها:

أ–تمكين شركات المساهمة من تحسين صورتها وتحسين ما تقدمه للعملاء كما سمح لها بالدخول في علاقات شراكة جديدة.[5]

---

[1] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic، مرجع سابق، ص 6.

[2] رشيد فراح، مرجع سابق، ص 153.

[3] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic، مرجع سابق، ص 6.

[4] العياشي زرزار، كريمة غياد، مرجع سابق، ص 112.

[5] مزهر شعبان العاني، مرجع سابق، ص 203.

ب-إتاحة فرصة ربط وإيصال النظم الداخلية للشركة وقواعد بياناتها ضمن نظام شبكي متكامل.

ت-مساعدة الشركة على تطوير العديد من الأعمال مما يقدم دعما للعملاء والمستفدين من أعمالها ومنتجاتها.

ث-تساعد على تأمين التطبيقات التفاعلية وهذا ما يساهم في تحسن عملية التدفقات النقدية وغير النقدية للشركة.[1]

ثانيا: توجه شركات المساهمة نحو التجارة الإلكترونية:

نوضح بداية العلاقة بين التجارة الإلكترونية والأعمال الإلكترونية، فهناك من يرى بأنهما على نفس الدرجة من التداخل وهناك من يرى بأنهما متساويان على النطاق الواسع، في حين هناك من يرى بأن التجارة الإلكترونية ما هي إلا فرع من الأعمال الإلكترونية ويعد هذا الرأي هو الأرجح كون أن التجارة الإلكترونية أضيق من الأعمال الإلكترونية[2].

1-تعريف التجارة الإلكترونية: هناك عدة تعريفات تطرقت إليها، فتعرف على أنها مختلف العمليات المتعلقة بالبيع والشراء سواء بين المستهلكين أو المنتجين أو فيما بين الشركات مع بعضها البعض وذلك من خلال إستخدام تكنولوجيا المعلوما ت[3]، وهي تلك المجموعة المتكاملة من العمليات الخاصة بعقد الصفقات وتأسيس الروابط التجارية وكذا عملية تسويق المنتجات من خلال الوسائط الإلكترونية،[4] كما تعرف على أنها الأنشطة التجارية المتعلقة بالبيع والشراء للخدمات والمنتجات من خلال إستخدام التقنيات التكنولوجية وشبكة الأنترنت ومختلف الشبكات العالمية.[5]

---

[1] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة -دراسة حالة مؤسسة Emploitic، مرجع سابق، ص ص 8، 9.

[2] صباح بلقيدوم، مرجع سابق، ص 170.

[3] أحمد سلام عبد العاطي، التجارة الإلكترونية ، ط 1، القاهرة مؤسسة طيبة للنشر والتوزيع، 2021، ص 35.

[4] محمود بوزيدين، سهام عباسي، (الأمن المعلوماتي في ظل قانون التجارة الإلكترونية في الجزائر)، مجلة البيبان للدراسات القانونية والسياسية ع 1، مج 3، الصادر في جوان 2018 ، ص 82.

[5] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة -دراسة حالة مؤسسة Emploitic، مرجع سابق، ص 52.

وكان توجيه البرلمان والمجلس الأوربي رقم 2000-31 الصادر بتاريخ 8 جويلية 2000 بخصوص الجوانب القانونية لخدمات شركة المعلومات، قد عرفها من خلال المادة 2 منه على أنها أي نمط من أنماط الإتصال يكون هدفه عملية تسويق بطريقة مباشرة أو غير مباشرة لبضائع أو خدمات[1]، وعرفتها منظمة التعاون الاقتصادي والتنمية على أنها جملة الصفقات التجارية التي يتم تنفيذها عبر الشبكات العالمية المفتوحة للإتصال،[2] أما الوثائق الحكومية الأمريكية فترى بأنها الإستخدام الأمثل لكافة أنماط تكنولوجيا الاتصالات المتوفرة بهدف تطوير النشاط التجاري للمشروعات وتنميته،[3] وفي فرنسا كانت مجموعة العمل المتكونة برئاسة وزير الاقتصاد في 1998 قد عرفتها بأنها كافة المعاملات الرقمية التي تكون مرتبطة بأعمال تجارية، إما بين المشروعات فيما بينها أو بين المشروعات والأفراد أو بين المشروعات والإدارة.[4]

وبعد عرض هذه التعريفات يمكننا القول بأن التجارة الإلكترونية هي تلك العملية التي تتضمن كافة الأنشطة والمعاملات التجارية المتنوعة والتي تنفذ من خلال التقنيات التي أتاحتها تكنولوجيا المعلومات عن طريق تبادل المعطيات إلكترونيا، أو هي إنتقال التجارة من النمط التقليدي إلى النمط الإلكتروني.

2-أهمية التجارة الإلكترونية لشركات المساهمة:

أ-تؤدي التجارة الإلكترونية إلى تخفيض التكاليف وهذا ما يسمح لهذه الشركات بزيادة حجم أرباحها نتيجة عرض منتجاتها وخدماتها عبر العالم دون أي إنقطاع في ذلك وبالتالي الوصول إلى أكبر عدد ممكن من الزبائن.

---

[1] محمد بودالي، "الحماية الجزائية للتجارة الإلكترونية " (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، 2015-2016)، ص 18.

[2] سميرة حمادوش، "دور تكنولوجيا المعلومات والإتصالات في تعزيز الميزة التنافسية لشركات التأمين في الجزائر " (أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة حسيبة بن بوعلي الشلف، 2019-2020)، ص 30.

[3] ماء العينين سعداني، (حماية التجارة الإلكترونية في ضوء المستجدات التشريعية)، المجلة الإلكترونية للأبحاث القانونية ع 5، الصادر في 2020 ، ص 34.

[4] محمد بودالي، مرجع سابق، ص 19.

ب–تفادي الأعباء الإدارية والمالية الناتجة عن عمليات الإعلان، معلومات التصنبع والتصميم وكذا الشحن ليتم بذلك إنخفاض مصاريفها.

ت–يكون لها القدرة على إنشاء شركات عالمية التخصص.[1]

ث–تلبي إحتياجات عملاءها بشكل يسير وسهل حيث أن التجارة الإلكترونية تسمح لهذه الشركات من معرفة إحتياجات العملاء فتعمل على إتاحة خيارات التسويق أمامهم على أوسع نطاق وهذا ما يحقق نسبة عالية من الرضى لديهم لا تحققه التجارة التقليدية، ومن خلال هذه التجارة يكون أمام العميل فرصة التعريف على أصناف المنتجات ومميزاتها وكذا أسعارها.[2]

ج–بفضل التجارة الإلكترونية لم يعد تعامل هذه الشركات مقتصرا على العملاء المحليين فقط كما كان عليه الأمر في السابق، حيث كان وصولها إلى عملاء دوليين يكلفها أعباء مالية كبيرة دون أن يكون هناك ضمان لعائداتها، على خلاف ما هو عليه الأمر حاليا فبإمكان أي عميل الإطلاع على منتجاتها خاصة بعدما غزت شبكات الأنترنت كل دول العالم.[3]

3–أقسام التجارة الإلكترونية: من خلال تعريفات التجارة الإلكترونية التي سبقت الإشارة إليها يتضح بأن لهذه التجارة عدة أقسام، لذلك سنوضح الأقسام التي تكون فيها شركات المساهمة طرفا فيها:

أ–التجارة الإلكترونية بين الشركات والزبائن: هذا النوع من التجارة الإلكترونية يتضمن تلك النشاطات التجارية الإلكترونية التي تتم بين الشركة والزبون وذلك من خلال قيام الشركة بتسويق منتجاتها وعرض خدماتها لزبائنها وبيعها لهم والإجابة عن أي إستفسار مقدم من طرفهم إلكترونيا،[4] أي أن هذا النوع تتم عملية التجارة مباشرة بين الشركة والزبون.

---

[1] وسيلة هني، مرجع سابق، ص 69.

[2] مريم مالكي، (أهمية التجارة الإلكترونية في تحسين مستويات التنمية المستدامة في الدول العربية)، مجلة الناقد للدراسات السياسية ، ع 1، مج 7 ، الصادر في 2023 ، ص 204.

[3] رمزي محمود، النقود والبنوك والتجارة الإلكترونية ثورة نقدية تقرع أبواب القرن الحادي والعشرين وإعادة صياغة مستقبل الشعوب ، د، ط، الإسكندرية ، دار التعليم الجامعي، 2022، ص 205.

[4] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic، مرجع سابق، ص ص 53.

ب–التجارة الإلكترونية بين الشركة والشركة: حيث أن التجارة الإلكترونية في هذا النوع تتم بين الشركات مع بعضها البعض، وينبغي أن نشير إلى أن أساليب التعامل في هذا النوع تختلف عن تلك التي تكون بين الشركة والزبون فالمعاملات التجارية بين الشركات تتخطى بالتأكيد عمليات البيع والشراء المباشر ويتم تنفيذ تلك المعاملات عن طريق الإتصال بالشركة وبطبيعة الحال بعد أخذ إحتياطات الأمان مثل كلمات المرور، عناوين إلكترونية خاصة، وهذا النوع من التجارة مشهود له بالنجاح خاصة في الفترة الأخيرة فقد إكتسح ساحة التجارة الإلكترونية، ووفقا للدراسات فإن التجارة الإلكترونية بين الشركات تتجاوز بعشرة أضعاف على الأقل تلك التي تكون موجهة مباشرة نحو الزبائن،[1] فهي تستحوذ على ما نسبته 80% من الحجم الإجمالي للتجارة الإلكترونية.[2] والسبب في ذلك يعود إلى أن هذا النوع لا تكون فيه نفس نسبة المجازفة التي تتعرض لها الشركة مع الأفراد.

ت–التجارة الإلكترونية بين الشركات والحكومة: وتتمثل في تلك التعاملات التي تتم ما بين الشركات والحكومة والتي تندرج ضمن الحيز التجاري من ذلك مثلا عمليات الشراء التي تقوم بها الحكومة من هذه الشركات.[3]

وللإشارة فإن حجم التجارة الإلكترونية في تطور متزايد خاصة بالنسبة للنوع الأول والثاني، ففي مؤتمر الأمم المتحدة المنعقد في أفريل من سنة 2018 حيث أكد الخبراء أن نسبة المبيعات من هذه التجارة بلغ معدلها السنوي 25،3 تريليون دولار وأن ما نسبته 22،4 هي تلك التي تتم بين الشركات فيما بينها، أما تلك التي تكون بين الشركات والأفراد فقد بلغت حوالي 2،9 تريليون دولار سنويا.[4]

---

[1] أحمد سلام عبد العاطي، مرجع سابق ، ص 36.

[2] نعيمة يحياوي، مريم يوسف، (التجارة الإلكترونية وآثارها على إقتصاديات الأعمال العربية)، المجلة الجزائرية للتنمية الإقتصادية ، ع 6، الصادر في جوان 2017 ، ص 184.

[3] محمد بودالي، مرجع سابق، ص 25.

[4] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic، مرجع سابق، ص ص 57.

الفرع الثاني:

إنتقال شركات المساهمة من الإدارة التقليدية إلى الإدارة الإلكترونية.

يجب أن نشير إلى مصطلح الإدارة لا يقتصر فقط على الإدارات والمؤسسات العمومية وإنما يعد عاملا مهما حتى في بيئة الأعمال التجارية، إذ لا يمكن تصور شركات بحجم شركات المساهمة تقوم بتأدية أعمالها دون الإعتماد على إدارة تعمل على تسيير شؤونها وإدارة علاقاتها التجارية، واتجاه هذه الشركات نحو تكنولوجيا المعلومات ترتب عنه إنتقالها من الإدارة التقليدية إلى الإدارة الإلكترونية هذا ما نوضحه من خلال هذا الفرع.

أولا: تعريف الإدارة الإلكترونية وأهميتها.

1-تعريف الإدارة الإلكترونية: هناك من يطرح مصطلح الإدارة الإلكترونية بشكل مترادف مع مصطلح الأعمال الإلكترونية، غير أنه ينبغي أن نشير إلى أن مصطلح الإدارة الإلكترونية ظهر بعد جملة التطورات التي شهدتها الأعمال الإلكترونية حيث كانت هذه الأخيرة بحاجة إلى إدارة حديثة تتناسب مع طبيعة هذه الأعمال وكل ما يرتبط بها من تقنيات تكنولوجية.[1]

والإدارة كمصطلح عام يعرفها "FAYOL HENRY" بأن تحقيقها يستلزم التنبؤ، التخطيط، التنظيم، القيادة، التنسيق والرقابة،[2] وهناك العديد من التعريفات التي تناولت الإدارة الإلكترونية.

فتعرف على أنها تلك العملية التي يكون قوامها التقنيات المتميزة للأنترنت وكذا شبكات الأعمال في التخطيط، التوجيه وكذا الرقابة على قدرات وموارد الشركة بدون حدود وذلك من أجل تحقيق أهدافها،[3] وهي أيضا إستبدال المعاملات الورقية ليحل محلها المكتب الإلكتروني وذلك من خلال إستخدام تكنولوجيا المعلومات، وبذلك يتم تحويل الخدمات العامة إلى إجراءات مكتبية لتتم عملية

---

[1] نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة –دراسة حالة مؤسسة Emploitic، مرجع سابق ، ص 45.

[2] فطيمة الزهرة المفيدة ، نجاح عصام بن أوجيت ، (إستراتجيات التحول من الإدارة التقليدية إلى الإدارة الإلكترونية في ظل الأزمات، أزمة كورونا COVID 19)، مجلة التنمية البشرية والتعليم للأبحاث التخصصية ، ع 3، مج 7 ، الصادر في 2021 ، ص 551.

[3] نجم عبود نجم، الإدارة الإلكترونية الإستراتجية والوظائف والمشكلات ، د، ط، الرياض ، دار المريخ للنشر، 2004، ص 127.

معالجتها وفقا لخطوات متسلسلة منفذة مسبقا،[1] وهي كذلك تنفيذ جملة المعاملات والأعمال بواسطة إستخدام شبكات الإتصال سواء كانت تلك المعاملات تتم بين الأشخاص أو الشركات.[2]

ومن خلال ما تم عرضه من تعريفات نصل إلى القول بأن الإدارة الإلكترونية هي نمط إداري حديث يقوم في الأساس على التقنيات التكنولوجية، وأهم ما يميزها هو إختفاء التعاملات الورقية التقليدية ليحل محلها تطبيقات معلوماتية، ومن خلال تطبيق هذا النمط الإداري الحديث في شركات المساهمة يصبح بإمكانها إدارة كافة شؤونها لتصبح أكثر تنسيقا وجودة وفعالية.

2-أهمية الإدارة الإلكترونية لشركات المساهمة: بالتأكيد أن هذه الإدارة لها أهمية بالغة بالنسبة لهذه الشركات من خلال المزايا التي تحققها لها، حيث تمكنها من تجاوز العوائق التي تحد من إتخاذ القرار وذلك من خلال توفير مختلف البيانات المطلوبة وربطها مع بعضها البعض، إذ أصبح توفير البيانات يتم بشكل فوري وآني إلى جانب تحقيق الترابط القوي بين مختلف فروعها وإدارة كافة موارد الشركة ومتابعتها بشكل جيد[3].

كما أن الإدارة الإلكترونية تشكل حافزا لموظفي هذه الشركات وذلك من خلال السماح للموظف بالولوج إلى شبكاتها الداخلية بغض النظر عن الزمان والمكان الذي يكون موجود فيه للقيام بأي عمل يطلب منه القيام به، فالمكاتب الإلكترونية للشركات ليست لها أية حدود فضلا على أن تخزين البيانات والمعلومات يتم بطريقة إلكترونية وبذلك يجنبها تلفها نتيجة مختلف الحوادث[4].

ونتيجة لهذه الأهمية هناك العديد من الشركات في الجزائر إتجهت إلى نمط الإدارة الإلكترونية كبديل للإدارة التقليدية، فمثلا شركة إتصالات الجزائر وهي الشركة الرائجة في الخدمات المتعلقة بالهاتف الثابت والأنترنت قد خففت بشكل ملحوظ من معاناة زبائنها وتمكينهم من تعبئة الأنترنت ودفع

---

[1] أحمد فتحي الحيت، محمد مفضي الكساسبة، (تأثير وظائف الإدارة الإلكترونية في فاعلية وكفاءة البنوك في الأردن)، المجلة العربية الدولية للمعلوماتية ، ع 4، مج 2 ، الصادر في يناير 2013 ، ص 2.

[2] محمد هشام فريجة، (ضرورة التعامل بأسلوب الإدارة بالأهداف كأداة للإدارة الإلكترونية)، مجلة الاقتصاد الخليجي ، ع 28، الصادر في حزيران 2016 ، ص 83.

[3] أحمد مسعود أسامة، (فعالية الإدارة الإلكترونية في تطوير منظمات الأعمال دراسة ميدانية على بعض الشركات الخاصة بولاية البليدة)، مجلة التنمية وإدارة الموارد البشرية بحوث ودراسات ، ع 1، مج 10، الصادر في 2023 ، ص 491.

[4] صباح بلقيدوم، مرجع سابق، ص ص 181، 182.

الفواتير بطريقة إلكترونية من خلال البطاقة الذهبية وذلك بدلا من تنقليهم إلى مراكزها، كذلك شركة توزيع الكهرباء والغاز أتاحت لزبائنها إمكانية دفع الفواتير عن طريق الأنترنت وذلك من خلال أربعة مواقع إلكترونية خاصة بها.[1]

أيضا شركة مصير الحياة المختصة في عملية التأمين عن الحياة، الصحة وكذا السفر مكنت عملاءها من الإشتراك في خدمات التأمين لديها دون أن يكلفهم ذلك عناء التنقل إليها، وإنما يتم ذلك فقط عبر الرابط الذي خصصته لهذا الشأن والدفع عن طريق البطاقة الذهبية.[2]

وبهذا تكون الإدارة الإلكترونية قد مكنت الشركات من القيام بأعمالها في أسرع وقت ممكن وبذلك حققت الإرتقاء بخدماتها إتجاه عملاءها وهذا ما يعزز مكانتها في الأسواق.

ثانيا: متطلبات الإدارة الإلكترونية في شركات المساهمة.

حتى يتم تجسيد الإدارة الإلكترونية في هذه الشركات بصورة فعالة فإن الأمر يتطلب منها توفير عدة عوامل منها:

1-متطلبات تقنية: حيث تعد تقنيات تكنولوجيا المعلومات الركيزة الأساسية للإدارة الإلكترونية لذلك بتوجب على شركات المساهمة توفير هذه التقنيات من أجهزة ومعدات وبرامج ومختلف الشبكات وإتاحتها للإستخدام حتى يتم بذلك ضمان عملية التواصل وانتقال المعلومات بين مختلف فروعها من جهة وكذا بينها وبين موظفيها وعملاءها من جهة أخرى،[3] وهذا ما يسمى بالبنية التحتية التي تحتوي شبكة حديثة للإتصالات والمعلومات.[4]

---

[1] جميلة سلايمي، يوسف بوشي، (التحول الرقمي بين الضرورة والمخاطر)، مجلة العلوم القانونية والسياسية ، ع 2، مج 10، الصادر في سبتمبر 2019 ، ص 959.

[2] المرجع نفسه، ص 961.

[3] وهيبة بوعنينيبة، زهرة سعد قرمش، وفاء سلامة، (متطلبات التحول من الإدارة التقليدية إلى الإدارة الإلكترونية ومعوقاتها)، مجلة الحدث للدراسات المالية والإقتصادية ، ع 7، الصادر في ديسمبر 2021 ، ص 114.

[4] أفنان عبد علي الأسدي، (الإدارة الإلكترونية بين النظرية ومتطلبات التطبيق في بيئة منظمات الأعمال العراقية)، مجلة دراسات الكوفة ، ع 15، الصادر في 2009 ، ص 15.

2- متطلبات بشرية: بطبيعة الحال فحتى يتم إستخدام التقنيات التكنولوجية التي سبق الإشارة إليها من طرف شركات المساهمة إستخداما جيدا ودقيقا، فإن ذلك لن يتحقق إلا من خلال العنصر البشري المؤهل.

لذلك وجب على هذه الشركات إعداد الكوادر المتخصصة في مجال تكنولوجيا المعلومات كأن تستقطب مثلا أفضل الكوادر وتعمل على تطويريهم وتحفيزهم والمحافظة عليهم،[1] وفي هذا نجد العديد من مسيري الشركات الكبرى وفروع الشركات الأجنبية العاملة بالجزائر يبحثون عن المحترفين في مجال تكنولوجيا المعلومات تكون مهمتهم الإشراف على الرقمنة في شركاتهم ومن ذلك شركة كوندور وسيفيتال.[2]

3- متطلبات مالية: وتتمثل في الموارد المالية والسيولة النقدية التي تعمل الشركة على توفيرها من أجل تطبيق الإدارة الإلكترونية بشكل سهل وناجح حيث أن تجسيدها بحاجة إلى تكاليف كتلك المتعلقة بشراء الأجهزة والمعدات وكذا تكاليف تدريب موظفيها في مجال الحواسيب الصيانات الدورية وكذا مختلف الشبكات.[3]

4-متطلبات أمنية: وفي إعتقادنا بأن هذا العنصر يعد أهم المتطلبات التي يجب على شركات المساهمة توفيرها قبل رقمنة إدارتها، إذ بدون توفير الجانب الأمني يعتبر إقبالها وتوجهها نحو الإدارة الإلكترونية خطرا عليها ويعود عليها بالسلب أكثر من الإيجاب، حيث أن ذلك الخطر يتمثل في تعرضها إلى مختلف الجرائم الإلكترونية والتي هي موضوع هذه الرسالة.

لذلك فإن الأمر يتطلب منها البحث عن الأساليب والإجراءات الأمنية الكفيلة بتوفير الحماية لبياناتها ومعلوماتها من مختلف الجرائم والتي سنتطرق إليها في الباب الثاني من هذه الدراسة، ونشير إلى أن توفير هذه المتطلبات التي تم عرضها أمر لازم مع ضرورة تحقيق التكامل فيما بينها حتى تتمكن هذه الشركات من تجسيد الإدارة الإلكترونية بها.

---

[1] محمد هشام فريجة، مرجع سابق، ص 89.

[2] جميلة سلايمي، يوسف بوشي، مرجع سابق، ص 962.

[3] فطيمة الزهرة المفيدة بن أوجيت، نجاح عصام، مرجع سابق، ص 565.

وللإشارة فإن إنتقال شركات المساهمة إلى هذا النوع من الإدارة كان وراءه عدة أسباب، والتي منه الرقابة الإلكترونية، فمن خلال الإدارة الإلكترونية يمكن لهذه الشركات تقوية نظام رقابتها على كامل أقسامها وبشكل مباشر، وبالتالي تفادي جملة الإنحرافات التي قد تتعرض لها خاصة من قبل العاملين بها.[1]

[1] غسان كوريل إبراهيم، آراس قادر خوشناو (دور إستخدام الأعمال الإلكترونية في إعداد الميزانية العمومية للشركات للحد من التهرب الضريبي)، مجلة يوليتكنيك للعلوم الإنسانية والإجتماعية ، ع 2، مج 4، الصادر في 2023 ، ص 608.

الفصل الثاني:
الإطار المفاهيمي للجرائم الإلكترونية في إطار شركات المساهمة

الفصل الثاني:

الإطار المفاهيمي للجرائم الإلكترونية في إطار شركات المساهمة

إتجاه شركات المساهمة نحو تكنولوجيا المعلومات بسبب التطورات الحاصلة في هذا المجال خاصة فيما يتعلق بالإستخدام المطرد لأجهزة الحاسب الآلي ومختلف الشبكات، وإن كان له العديد من المزايا التي تتعلق بتيسير أعمالها التجارية واختزال المسافات ورفع العراقيل والصعوبات التي تعترضها في ذلك، غير أن هذه التطورات كان لها جانب مظلم والذي يتمثل في تعرضها للجرائم الإلكترونية.

حيث كانت هذه الجرائم الظاهرة التي تجسد من خلالها الإنحراف عن الأغراض المتوخاة من التكنولوجيا وسوء تسخير مزاياها، من طرف جناة لم يعد يستهويهم المسرح التقليدي من أجل إرتكاب جرائمهم على هذه الشركات ، فجعلوا من الفضاء الرقمي ساحة للصراع الإلكتروني ضدها، فكانت بذلك ذات طبيعة خاصة تختلف تماما عن نظيرتها التقليدية، وحتى نتمكن من ضبطها والوقوف على جوانبها، يتوجب علينا الأمر شرح الإطار المفاهيمي للجرائم الإلكترونية وذلك بتقسيم هذا الفصل إلى مبحثين:

المبحث الأول: ماهية الجرائم الإلكترونية في إطار شركات المساهمة.

المبحث الثاني:الأحكام الخاصة بالجرائم الإلكترونية في إطار شركات المساهمة.

المبحث الأول:

ماهية الجرائم الإلكترونية في إطار شركات المساهمة

باعتبار أن الجرائم الإلكترونية هي وليدة التطورات التكنولوجية المتسارعة الأمر الذي نتج عنه صعوبة في فهم هذه الجرائم نتيجة للطابع التقني الذي تتميز وغموض أساليب إرتكابها وتطورها الدائم، وهذا ما أدى إلى غياب الاتفاق على تحديد معنى لهذه الجرائم، ومن أجل الإلمام بها والوقوف على مختلف جوانبها خاصة حينما يتم إرتكابها في إطار شركات المساهمة، يتطلب منا الأمر تحديد ماهيتها وحتى نتمكن من ذلك سنقوم بتقسم هذا المبحث إلى مطلبين:

المطلب الأول: مفهوم الجرائم الإلكترونية.

المطلب الثاني: دوافع إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة وأطرافها.

المطلب الأول:

مفهوم الجرائم الإلكترونية.

يُعد تحديد مفهوم الجرائم الإلكترونية أهم خطوة من أجل التعرف عليها، ونظرا لحداثتها وطابعها المميز مقارنة بالجرائم التقليدية فقد شغلت إهتمام الفقهاء ورجال القانون، ومن أجل ضبط مفهوم هذه الجرائم نتطرق من خلال هذا المطلب إلى تعريفها **(فرع أول)** ثم تحديد خصائصها **(فرع ثاني)**.

الفرع الأول:

تعريف الجرائم الإلكترونية.

تعد مسألة تعريف الجرائم الإلكترونية من المسائل الشائكة حيث يبدو بأن الاتفاق على ضبط تعريف موحد ودقيق قد يبدو أمرا مستحيلا وذلك نتيجة إختلاف وجهات النظر إليها وكذا الغموض الذي يكتنفها، حيث وصفت بتسميات عديدة ومختلفة وإن كانت تهدف إلى ذات المعنى وهو الجرائم الإلكترونية، ومن أجل التفصيل أكثر في هذه المسألة نتناول في النقطة الأولى أزمة المصطلح الذي تعاني منه الجرائم الإلكترونية، ثم التعريف الإصطلاحي، التشريعي وكذا الفقهي في النقطة الثانية.

أولا: الجرائم الإلكترونية وإشكالية المصطلح.

خلال عملية البحث في مسألة تعريف الجرائم الإلكترونية واجهتنا العديد من المصطلحات التي أستخدمت لدلالة عليها، حيث بدت في البداية وكأنها تدل على جرائم متعددة لذلك كان لا بد علينا من الإشارة إلى هذه المصطلحات والتي نرى في تعددها دلالة على إختلاف وجهات نظر الفقهاء والباحثين في المجال القانوني لموضوع الجرائم الإلكترونية، هذا من جهة ومن جهة أخرى فإن الإختلاف مرتبط بمسيرة تطور تلك الجرائم الناشئة في البيئة الإلكترونية والتي تعد ذات بعدين قانوني وتقني في ذات الوقت.

ففي البداية أولى التسميات التي أطلقت عليها كانت إحتيال الحاسوب،[1] " FRAUDE INFORMATIQUE" ويرجع سبب هذه التسمية إلى فعل الإحتيال الذي كان يعتبر من أكثر الأفعال شيوعا أنذاك والذي إقترن بشكل وطيد بجهاز الحاسوب، لكن ما يلاحظ على هذه التسمية هو أن فعل الإحتيال يدل على نوع واحد من الجرائم ولا يشمل الأنواع الأخرى التي تنطوي تحت مظلة الجرائم الإلكترونية، وبالتالي فإن هذه التسمية ضيقة ولا تستوعب غيرها من الجرائم.

ليطلق عليها فيما بعد إساءة إستخدام الحاسوب[2] حيث أنه وبعد الإنتشار الواسع للحواسيب وتزايد إستعمالها صاحبتها بعض الأفعال كجرائم العبث أو التخريب الموجه إلى الحاسوب، سرقة المعلومات أو الممتلكات والإستخدام غير المصرح به لخدمات الحاسوب،[3] فكان هناك خلاف حول طبيعة هذه الأفعال إن كانت تعتبر مجرد سلوكيات غير أخلاقية أم أنها سلوكات غير قانونية، ونظرا لتفاقم تلك الأفعال كانت هناك ضرورة لتجريمها واعتبارها جرائم مستحدثة تستدعي توقيع الجزاء على فاعلها، وذلك تطبيقا لقاعدة "لاجريمة ولا عقوبة إلا بنص قانوني" وهكذا أصبحت أفعال إجرامية وفقا للمعنى القانوني.

---

[1] أيمن عبد الله فكري ، الجرائم المعلوماتية –دراسة مقارنة في التشريعات العربية والأجنبية– ط 1، الرياض، مكتبة القانون والإقتصاد، ، 2014 ، ص 86.

[2] ياسمينة بونعارة ، (الجريمة الإلكترونية)، مجلة المعيار، ع 39، مج 20، الصادر في 2015/06/19، ص 276.

[3] علي جبار الحسيناوي ، جرائم الحاسوب والأنترنت، د،ط، عمان، دار اليازوردي العلمية، 2009، ص 8.

وما ينبغي أن نشير إليه فيما يخص هذه التسمية هي أنها حصرت إرتكاب الجرائم الإلكترونية في فعل الإساءة وهذا غير صحيح، إذ هناك العديد من الأفعال التي يتم القيام بها بواسطة الحاسوب ولكن بطريقة مشروعة، حيث تصحبها في نفس الوقت إرتكاب أفعال إجرامية كالموظف بإحدى شركات المساهمة الذي يُخول له إدراج بعض المعلومات التي تكون من إختصاصه فيستغل ذلك ويقوم بتغيير البعض منها.

ومن بين الدول التي إعتمدت هذه التسمية نجد إنجلترا حيث إستعمل المشرع مصطلح "قانون إساءة إستخدام الحاسوب" لسنة 1991، كما صدر في سنغافورة قانون سمي بقانون إساءة إستخدام الحاسوب[1].

كما سميت كذلك بمصطلح الجرائم المعلوماتية[2]، ويعود الفضل في إقتراح هذا المصطلح إلى الأستاذ الفرنسي "DREFNS" الذي إستخدمه سنة 1962 من أجل التعبير عن المعالجة الآلية للبيانات والمعلومات، تبنته بعد ذلك الأكاديمية الفرنسية في أفريل 1966، وعرفته بأنه علم المعالجة المنطقية للمعلومات التي تعد بمثابة دعامة للمعارف الإنسانية والإتصالات في المجالات الفنية والإقتصادية والإجتماعية من خلال إستخدام المعدات الآلية،[3] فهو مصطلح يشمل جميع الجرائم ذات الصلة بالمعلوماتية وبالتالي فإن الفكرة الجوهرية التي تقوم وتبنى عليها الجريمة وفقا لهذا المصطلح هو المعلومات.

ومن بين التشريعات التي ربطت التسمية بمصطلح المعلومات أو المعلوماتية نجد قانون دولة الإمارات العربية المتحدة تحت إسم " قانون مكافحة جرائم تقنية المعلومات"[4] كما درج البعض على تسميتها بمصطلح جرائم الكمبيوتر أو الجرائم المرتبطة بالكمبيوتر،[5] وفي هذا المصطلح دلالة على أن هذه الجريمة تشمل جميع الجرائم التي يكون للكمبيوتر دور فيها، سواء كان هدفا لها أو أداة لتنفيذها

---

[1] عبد الإله النوايسة ، مرجع سابق، ص 35.

2 المرجع نفسه، ص 40.

[3] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 19.

4 مرسوم بقانون إتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

[5] أسامة أحمد المناعسة ، جلال محمد الزعبي ، مرجع سابق، ص 67.

وقد شاع إستخدام هذين المصطلحين لدى العديد من الباحثين والفقهاء على غرار الأستاذ "PARKER" والفقيه الألماني "ULRICH SEIHER" كما أستعمل في الدليل الخاص بمنع ومكافحة الجرائم المتصلة بالحاسوب الذي أصدرته هيئة الأمم المتحدة سنة 1994،[1] لكن و في إعتقادنا بأن هذه التسمية غير دقيقة كون أنها ركزت على أداة رئيسية واحدة في إرتكابها والمتمثلة في جهاز الكمبيوتر، مهملة بذلك عدة جوانب ذات الدور المهم في إرتكاب هذه الجريمة.

أيضا شاعت تسميتها بمصطلح جرائم التقنية العالية،[2] والواقع أن هذا المصطلح يتجاوز تكنولوجيا المعلومات ليشمل التطورات التكنولوجية الأخرى مثل التكنولوجيا النووية والهندسة الحيوية.[3] وبالتالي يمكننا القول بأنه مصطلح فضفاض مطلق يتعارض مع الجريمة التي نحن بصدد دراستها، حيث هناك جرائم يمكن إرتكابها بأجهزة تقنية ذات مستوى عالي من التطور ولكن لا تصنف ضمن طائفة الجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة، كتلك المرتكبة في المجال الطبي مثلا.

من المصطلحات التي أطلقت عليها كذلك نجد مصطلح السيبر كرايم[4] "CRIME CYBER" أو الجريمة السيبرانية،[5] وقد أستخدم هذا المصطلح في النطاق الأوربي وخارجه إذ يعد شاملا لجرائم

---

[1] عبد القادر عميمر ، "آليات إثبات الجريمة المعلوماتية في التشريع الجزائري –دراسة مقارنة–" (أطروحة دكتوراه، كلية الحقوق ، جامعة الجزائر1، 2019–2020)، ص 11.

[2] محمد مكاوي محمد، دينا عبد الله صالح ، (الجرائم ذات التقنية العالية والحماية من الهجمات الإلكترونية في النظام السعودي)، مجلة الإجتهاد القضائي ع 1،، مج 13، الصادر في مارس 2021، ص 42.

[3] مشتاق طالب وهيب، (مفهوم الجريمة المعلوماتية ودور الحاسوب في ارتكابها)، مجلة العلوم القانونية والسياسية، ع 1، مج 3، الصادر في 2014، ص 336.

[4] خالد ممدوح إبراهيم ، الجرائم المعلوماتية، مقال منشور بتاريخ 26 نوفمبر 2008، تاريخ الدخول: 2022/08/13، متاح على الرابط: https://kenanaonline.com

[5] مصطلح إنجلزي مشتق من "Cyber" ويعني متصل بالحاسوب أوشبكاته كما يعني فضاء الأنترنت، ويقال أيضا أنها مصطلح يوناني مشتق من "KYBERNETES" ومعناه الشخص الذي يدير دفة السفينة مجازا للمتحكم، أنظر: داود عبد العزيز بن فهد بن محمد بن داود، (الجرائم السيبرانية –دراسة تأصيلية مقارنة–)، مجلة الإجتهاد للدراسات القانونية والإقتصادية، ع 3، مج 9، الصادر في 2020، ص 148.

المعلوماتية وجرائم الشبكات، فكلمة "CYBER" يستخدمها الكثير بمعنى الأنترنت ذاتها أو العالم الإفتراضي[1]، أطلق عليها كذلك جرائم الهاكرز،[2] لكن ما لاحظناه من خلال البحث في هذه الجرائم هو أن العديد من شركات المساهمة تعرضت لهذه الجرائم ولكن من طرف أشخاص عاديين لا يتمتعون بمستوى عالي من المهارة في مجال البرمجة والحواسيب.

كما نجد أيضا من بين المصطلحات التي أطلقت عليها جرائم الأنترنت،[3] حيث تم إطلاق هذا المصطلح في مؤتمر جرائم الأنترنت المنعقد في أستراليا عام 1988[4].

إضافة إلى هذه المصطلحات سميت بمصطلح الجرائم الإلكترونية[5] وهو المصطلح الذي إرتأينا إعتماده كعنوان لهذه الدراسة باعتباره المصطلح الأكثر شيوعا واستعمالا في الدراسات الحديثة، كما أنه مصطلح واسع يشمل جميع الجرائم التي ترتكب عبر التجهيزات والتقنيات الإلكترونية بما فيها الحاسوب ،الأنترنت وكذا ما سيسفر عليه التقدم العلمي من أجهزة إلكترونية مستقبلا، وبالتالي فهذا المصطلح له قدرة على إستيعاب جميع الإنشطة الإجرامية الإلكترونية التي يمكن أن تتعرض لها شركات المساهمة والتي يتعذر حصرها وتحديدها وذلك نظرا للتطور التقني السريع.

ومصطلح "Cyber" لايوجد مصطلح يقابله في اللغة العربية لذلك فإن أغلب الترجمات العربية له كانت غير صائبة، هذا ما حدث في ترجمة عنوان إتفاقية أوربا المتعلقة بالجريمة السيبرانية حيث ترجمت إلى اللغة العربية، بالإتفاقية المتعلقة بالجريمة الإلكترونية (أنظر: العيسى طلال ياسين، عناب محمد عدي ، (المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر) ، مجلة الزرقاء للبحوث والدراسات الإنسانية، ع 1، مج 19، الصادر في 2019، ص 83.

[1] فارس محمد العمارات ، إبراهيم الحمامصة ، الأمن السيبراني المفهوم وتحديات العصر، ط 1، عمان، دار الخليج للنشر والتوزيع، 2022، ص 91.

[2] SEFFARI ASMA, (information security and the need to move towards the application of standard specification in Algerian institutions), **J. H. S**, VOL 9, N^{O} 2, JUIN 2022, P 23.

[3] شيرين دبابنة ، جرائم الأنترنت في المجتمع من منظور إجتماعي، د،ط، الأردن، دار الحامد للنشر والتوزيع، 2018، ص 49.

[4] علي جبار الحسيناوي، مرجع سابق، ص 34.

[5] علي عدنان الفيل ، الإجرام الإلكتروني، ط 1، بيروت، منشورات زين الحقوقية، 2011، ص 9.
والإلكترونية نسبة إلى الإلكترون، وله عدة تعريفات منها دقيقة ذات شحنة كهربائية سالبة تشكل جزءا من الذرة، (أنظر: أحمد علي محمود إبراهيم، (الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية –دراسة فقهية مقارنة–)، مجلة كلية الشريعة والقانون، ع 32، الصادر في يونيو 2020، ص 1111.

وترى الدكتورة "غنية باطلي" في هذا الشأن أن إستعمال مصطلح الجرائم الإلكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية، الغش المعلوماتي، جرائم الأنترنت...إلخ، وبالتالي تنطوي تحت جوانبه العديد من السلوكات الضارة وهذا ما يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق إستغلال التقدم العلمي وما يجلبه من إمكانيات لم تكن موجودة من قبل، فالجريمة الإلكترونية محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر أو أية وسيلة إلكترونية أخرى[1].

ورغم تعدد التسميات والمصطلحات فهي في النهاية تصب في معنى واحد وهو الجرائم التي ترتكب في بيئة إفتراضية تختلف عن البيئة المادية الملموسة للجريمة التقليدية، وهو الأمر الذي نتج عنه تعرض شركات المساهمة لهذه الجرائم كونها غيرت من نمط أعمالها التي كانت تتم بطريقة تقليدية واتجهت إلى الإعتماد في ذلك على الوسائل التقنية التي جعلت من أعمالها ذات طبيعة إلكترونية.

ويجب علينا أن نشير في هذه النقطة إلى موقف المشرع الجزائري بخصوص تسيمة هذه الجرائم، فنجد بأن المصطلح الذي إعتمد عليه من أجل الدلالة على هذه الجريمة هو: "المساس بأنظمة المعالجة الآلية للمعطيات" وذلك من خلال إدخال تعديلات على قانون العقوبات بموجب القانون رقم 04-15،[2]حيث أصدر بعض العقوبات التي تجرم المساس بذلك النظام، ليضيف بعدها مصطلح آخر وهو: "الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" وذلك بموجب القانون رقم 09-04[3].

واستعمال مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال يتوافق مع مصطلح الجريمة الإلكترونية بالمفهوم الواسع وذلك بسبب:

---

[1] رحيمة نمدلي ، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، مداخلة مقدمة إلى المؤتمر الدولي الرابع عشر –الجرائم الإلكترونية، المنعقد في 24 و 25 مارس 2017، بطرابلس، ص 4.

[2] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، ج،ر، ع 71، الصادر في 10 نوفمبر 2004.

[3] القانون رقم 09-04، المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج،ر، ع 47، الصادر في 16 غشت 2009.

-أنه مصطلح ذو مفهوم واسع يحتوي جميع الإعتداءات التي ترتكب في البيئة الإفتراضية، بما فيها الجرائم المرتكبة ضد نظم المعالجة الآلية للمعطيات وتكون وسيلة لإرتكابها؛

-أنه مصطلح يعبر عن الطابع التقني والمميز للجرائم الإلكترونية.[1]

ثانيا: التعريف الإصطلاحي، التشريعي والفقهي للجرائم الإلكترونية.

حتى نتمكن من ضبط مدلول هذه الجريمة وجب علينا الأمر التطرق إلى تعريفها من جميع الجوانب، الإصطلاحي، التشريعي حتى نوضح موقف مختلف الدول في معالجتها وكذا الجانب الفقهي من خلال إبراز نظرة الفقهاء وعرض التعريفات التي قدموها لهذه الجرائم وذلك في النقاط التالية:

1-التعريف الإصطلاحي: مصطلح الجريمة في اللغة هو "الجرم" بمعنى الذنب،[2] وجمع المصطلح "إجرام" و "جروم" وهو الجريمة،[3] فيقال جرّم يُجرم جرمًا، وأُجرم واجتُرم فهو مجرم، وتَجرّم علي فلان بمعنى إدعّى علي ذنبا لم أفعله وجَرّم عليهم جريمة أي يجني عليهم جناية، فالجارم، الجاني والمجرم المذنب[4]، والجريمة هي فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا إحترازيا،[5] وهي أيضا فعل أو إمتناع عن فعل مسند إلى صاحبه ينص عليه القانون ويعاقب من أجله بعقوبة جزائية.[6]

---

[1] مونة مقلاتي ، راضية مشري ، (الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية)، مجلة أبحاث قانونية وسياسية، ع 1، مج 6، الصادر في جوان 2021، ص 496.

[2] حمدي محمد أحمد الجداوي ، غسل الأموال عبر الأنترنت دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، ط1، جمهورية مصر العربية، مركز الدراسات العربية للنشر والتوزيع، 2022، ص 27.

[3] عمر طه خليل ، عفاف بديع جميل ، (التكييف الفقهي والقانوني لجرائم الأنترنت)، مجلة كلية التراث الجامعة ،ع 17، الصادر في 2015 ، ص 165.

[4] آمنة زعيطي ، (مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري -دراسة مقارنة-)، مجلة حقوق الإنسان والحريات العامة، العدد 7، مج 4، الصادر في جوان 2019، ص222.

[5] محمد محسن حسينات ، (جرائم الحاسوب والأنترنت)، مجلة جامعة فلسطين للأبحاث والدراسات، ع 2، الصادر في يناير 2012، ص 351.

[6] حفصي عباس، "جرائم التزوير الإلكترونية"، (أطروحة دكتوراه، كلية العلوم الإنسانية والعلوم الإسلامية جامعة وهران 1، 2014-2015)، ص 2.

وهناك من عرفها بأنها، الإعتداء على مصلحة محمية ويتم النص عليها بموجب القانون الجنائي الذي يبين أركانها والعقوبات المقررة لمرتكبها،[1] ومصطلح الإلكترونية حتى يتم وصف فكرة جزء من الحاسوب أو عصر المعلومات.[2]

2-التعريف التشريعي للجرائم الإلكترونية:

من خلال البحث في هذه النقطة لاحظنا بأن أغلب التشريعات لم تتعرض إلى تعريف الجرائم الإلكترونية، في حين هناك بعض الدول تعرضت إلى تعريفها ضمن منظومتها القانونية لذلك سنقوم بالتطرق إلى تعريف المشرع الجزائري للجريمة الإلكترونية كنقطة أولى ثم تعريفها في التشريعات المقارنة.

أ-تعريف المشرع الجزائري للجرائم الإلكترونية: نجد بأن المشرع الجزائري قد أغفل إلى وقت قريب عن تنظيم مجال الجرائم الإلكترونية لكن سرعان ما تدارك ذلك الفراغ القانوني الموجود وبادر إلى سن قوانين وإصدار تشريعات لمجابهتها، خاصة حينما اتسع نطاقها ليشمل أهم دعائم الاقتصاد الوطني -شركات المساهمة- فكانت البداية بإصداره للقانون 04-15، والذي خصص فيه القسم السابع مكرر من الباب الأول مكرر لهذه الجريمة تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات وذلك من المادة 394 مكرر إلى المادة 394 مكرر7، فمن خلال هذا القانون نجد بأن المشرع تبنى الجرائم الإلكترونية دون أن يتطرق إلى تعريفها، حيث نص على تجريم الأفعال التي فيها مساس بأنظمة المعالجة الآلية للمعطيات ، وسنتطرق إلى هذه الأفعال التي قد تتعرض لها شركات المساهمة والتي يشكل إرتكابها جرائم إلكترونية في الفصل الأول من الباب الثاني من هذه الدراسة.

ونظرا للتقدم المتواصل الذي شهدته وسائل الإعلام والإتصال الحديثة والتي ساعدت على بروز أشكال جديدة من هذه الجرائم، سارع المشرع الجزائري مرة أخرى إلى مواكبة هذه التطورات من أجل مواجهة الجرائم الإلكترونية المتولدة عنها وذلك بإصداره لقانون ثاني، وهو القانون رقم

---

[1] مريم أحمد مسعود ، "آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 09-04"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح، 2012-2013)، ص 8.

[2] إسراء جبريل رشاد مرعي ، (الجرائم الإلكترونية، الأهداف، الأسباب، طرق الجريمة ومعالجتها)، مجلة الدراسات الإعلامية، ع 1، الصادر في يناير 2018، ص 424.

09-04 والذي عرف من خلاله هذه الجرائم وذلك بموجب المادة 2 فقرة أ والتي جاء فيها " الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية".

وبالتالي فإن المشرع قد إعتمد على معيارين من أجل تعريف الجرائم الإلكترونية وهما، معيار المحل والذي بموجبه يكون موضوع الجريمة هو المساس بأنظمة المعالجة الآلية للمعطيات، وكذا معيار الوسيلة والذي يعني بأن يتم إرتكابها إما بواسطة منظومة معلوماتية، أو نظام للإتصالات الإلكترونية، واستعمال المشرع لعبارة "و أي جريمة أخرى" توحي في مضمونها أنه قد إعتمد على تعريف موسع للجريمة الإلكترونية، متبنيا بذلك مبدأ المرونة كونه لم يقم بحصر الأفعال التي تعتبر ضمن هذه الجريمة كما فعل في القانون السابق، وبالتالي ما يمكننا قوله هو انه حسنا ما فعله المشرع باعتماده لهذا التعريف الذي يمكنه إستيعاب جميع الأفعال التي يصعب ضبطها وحصرها، نتيجة التطور السريع الذي تشهده وسائل إرتكاب الجرائم الإلكترونية إذ بموجبه تندرج ضمن دائرة هذه الجريمة ما سيسفر عنه المستقبل من أنواع أخرى.

ب-تعريف الجرائم الإلكترونية في بعض التشريعات: والبداية بالتشريعات العربية والتي نجد منها من تطرق إلى تعريف الجريمة الإلكترونية ضمن منظومتها القانونية مثلما فعل المشرع السعودي " أي فعل يرتكب متضمنا إستخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[1] أيضا المشرع السوري الذي عرفها بأنها " جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة"[2]، في حين عرفها المشرع الكويتي بأنها " كل فعل يرتكب من خلال إستخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات

[1] المادة 1 فقرة 8 من نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم 17 في بتاريخ 2007/03/26.

[2] المادة 1 فقرة 14 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، الصادر بموجب المرسوم التشريعي رقم 17 لسنة 2012.

بالمخالفة لأحكام هذا القانون"،[1] أما المشرع القطري فقد نص على أن الجريمة الإلكترونية هي أي فعل ينطوي على إستخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف أحكام القانون.[2]

وعلى خلاف ذلك نجد بعض القوانين الأخرى التي لم تتطرق إلى تعريف الجرائم الإلكترونية ضمن منظومتها القانونية مثل المشرع المصري الذي قام بإصدار القانون رقم 175 لسنة 2018[3] والذي إكتفى فيه بتحديد الأفعال التي يعتبر إرتكابها جرائم إلكترونية يعاقب عليها وقد تم تحديد العقوبة الخاصة بكل فعل، كما نجد المشرع الإماراتي قد إنتهج نفس النهج بإصداره للقانون 34 لسنة 2021،[4] حيث قام بتعريف تقنية المعلومات ثم عدد أشكال الجرائم الواقعة عليها وتحديد العقوبات المقررة لها.

الشيئ الذي لاحظناه في هذه النقطة هو أن التشريعات التي تعرضت إلى تعريف الجرائم الإلكترونية لم تقم بحصرها في أفعال محددة وإنما وسعت من دائرتها، لتشمل بذلك كل الأفعال التي يتم تنفيذها باستخدام وسائل تقنية أو شبكة معلوماتية وتكون مخالفة لأحكام القانون، وفي إعتقادنا حسنا ما فعلته هذه التشريعات باعتبار أن هذه الجرائم تأبى أن تكون معرفة أو أن تكون مقيدة ومحصورة في أفعال محددة .

أما بالنسبة للتشريع الفرنسي فإن أولى محاولاته من أجل وضع قانون يتعلق بالجريمة الإلكترونية تعود إلى سنة 1985، حيث قام وزير العدل بتقديم مشروع قانون من أجل تعديل قانون العقوبات وأدرج فيه بابا رابعا للكتاب الثالث منه تحت عنوان " الجرائم في المادة المعلوماتية" يضم

---

[1] المادة 1 من القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

[2] المادة 1 من القانون رقم 14 الصادر بتاريخ 2014/09/15، يتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، ج،ر، لدولة قطر، ع 15 الصادر في 2014/10/02.

[3] القانون رقم 175 لسنة 2018، يتعلق بمكافحة جرائم تقنية المعلومات، ج،ر لجمهورية مصر العربية، رقم 32 مكرر (ج)، الصادر في أغسطس 2018.

[4] القانون رقم 34 لسنة 2021، يتعلق بمكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة.

ثمانية (8) مواد من المادة 307 فقرة1 إلى المادة 307 فقرة 8،[1] غير أن هذا المشروع لم يعرف طريقا للتطبيق لتتوالى بعدها المحاولات وهذه المرة من طرف النائب العام "GODFRAIN" الذي قدم مشروع قانون هو الآخر ليتم بعدها إصدار القانون رقم 88-19[2] حيث حمل إسم النائب الفرنسي" LOI GODFRAIN" يتعلق بالغش المعلوماتي "LA FRAUDE INFORMATIQUE".

تلاه بعد ذلك إصدار القانون 92-683[3] يتضمن تعديل قانون العقوبات والذي لم يعرف تطبيقا إلا في مارس 1994، وبموجبه تم إضافة فصل ثالث للباب الثاني من القسم الثالث في قانون العقوبات وذلك من المادة 1/323 إلى غاية المادة 7/323 تحت عنوان "الإعتداءات على نظام المعالجة الآلية للمعطيات"، ثم القانون 2004-575 [4]يتعلق بالثقة في الاقتصاد الرقمي، ثم توالت بعد ذلك إصدار مجموعة من القوانين على غرار القانون رقم 2009-1311[5]، القانون رقم 2012-287،[6] القانون رقم 2013-1168،[7] وكذا القانون رقم 2014-1353[8]، والملاحظ في هذه القوانين هو أن المشرع الفرنسي لم يعط تعريفا للجريمة الإلكترونية وإنما حدد صورها فقط.

أما بالنسبة للولايات المتحدة الأمريكية فنجد بأنها قد شهدت إصدار العديد من القوانين المتعلقة بالجريمة الإلكترونية وذلك بحسب ولاياتها وحكوماتها الفيدرالية،[9] ويعد قانون فلوريدا لجرائم الحاسوب

---

[1] عبد القادر عميمر ، التحديات القانونية لإثبات الجريمة المعلوماتية، د،ط، الجزائر، النشر الجامعي الجديد، 2021، ص 20.

[2] Loi N°88-19 du 5 janvier 1988, relative à la Froude informatique, J,O,R,F, du 6 janvier 1988.

[3] Loi N° 92-683 du 22 juillet 1992 portant reforme du code pénale, J,O,R,F, du 23 juillet 1992.

[4] Loi N°2004-575 op, cit.

[5] Loi N° 2009-1311 du 28 octobre 2009, relative à la protection pénale de la propriété littéraire et artistique sur internet, J,O,R,F, du 29octobre 2009.

[6] Loi N°2012-287 du 1er mars 2012, relative à l'exploitation numérique des livres indisponible du xxe siécle, J,O,R,F, du 2 mars 2012.

[7] Loi N° 2013-1168 du 18 décembre 2013, relative à la programmation militaire pour les années 2014 à 2019 et portant diverses disposition concernant la défense et la sécurité nationale, J,O,R,F, du 19 décembre 2013.

[8] Loi N° 2014-1353 du 13 novembre 2014, renforçant les dispositions relative à la lutte contre le terrorisme, J,O,R,F, du 14 novembre 2014.

[9] مراد يرمش ، "خصوصية الجريمة الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق جامعة الجزائر 1، 2020-2021)، ص 31.

الصادر سنة 1978 أول قانون بها يتعلق بالإحتيال والتطفل على الحاسوب،[1] وقد أعتبر هذا القانون أن كل دخول غير مشروع يعد جريمة حتى وإن لم تصاحبه نية سيئة.[2]

أما على الصعيد الفيديرالي قامت لجنة الكونجرس الخاصة بحماية إستخدام الحاسوب بتقديم مشروع قانون يتعلق بحماية الحاسوب سنة 1984، إلا أنه خلال عرضه ومناقشته من طرف الكونجرس وكذا لجانه المختصة أُجري عليه تعديلات جوهرية، ليصدر في العاشر من شهر أكتوبر من سنة 1984 ولكن هذه المرة باسم مغاير وهو " قانون الإحتيال وإساءة إستخدام الحاسوب"، وقد تم النص فيه على تجريم مجرد الإتصال دون تصريح بنظام حاسوب وعلى الإتصال المصرح به الذي يقوم فيه الفاعل باستخدام الحاسوب لأغراض غير مصرح بها مثل تعديل أو إتلاف أو تدمير أو إفشاء المعلومات المخزنة في الحاسوب، كما نص أيضا على عقاب من يرتكب فعلا يحول دون الإستخدام المصرح به للحاسوب،[3] وقد شهد هذا القانون تعديلات واكبت التطورات التقنية وكذا قانون أمن الحاسوب سنة 1987 الذي منح الوكالات الفيديرالية صلاحية إتخاذ خطوات مناسبة لتأمين وحماية أنظمة حواسيبها.[4]

كما تم إصدار القانون رقم 77" بتاريخ 2010/06/08 والذي بموجبه تم منح الرئيس الأمريكي صلاحية فرض سيطرته على شبكة الأنترنت في حالة الطوارئ حيث يعرف هذا القانون باسم حماية الفضاء الإلكتروني كثروة وطنية.[5]

كما نجد المشرع البريطاني الذي قام بإصدار قانون إساءة إستخدام الكمبيوتر "COMPUTER A BUSE ACT" لعام 1990، حيث نص في القسم الأول منه على تجريم الدخول غير المشروع للنظام المعلوماتي، وفي القسم الثاني تم تجريم الدخول غير المشروع مع إضافة النية لإرتكاب أو

---

[1] أبقال عبد المنعم، الإطار القانوني لمكافحة الجريمة الإلكترونية –دراسة مقارنة–، مقال منشور بتاريخ،01 نوفمبر 2020، تاريخ الدخول: 2022/08/25، متاح على الرابط: https://revuealmanara.com

[2] طارق الخن، جرائم المعلوماتية، د،ط، الجمهورية العربية السورية، الجامعة الإفتراضية السورية، 2018، ص 14.

[3] مراد يرمش ، مرجع سابق، ص 32.

[4] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 23.

[5] عبد القادر عميمر ، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري –دراسة مقارنة، مرجع سابق، ص 25.

تسهيل إرتكاب جرائم، في حين تضمن القسم الثالث تجريم أي تعديل لمحتوى الحاسوب كما تم إصدار قانون الإحتيال لسنة 2006.[1]

أما بالنسبة لتعريف الجرائم الإلكترونية في المعاهدات فنجد إتفاقية بودابست ،[2] والتي قامت بتصنيف هذه الجرائم ضمن أربعة مجموعات، أيضا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،[3] حيث نصت في الفصل الثاني منها على تجريم مجموعة من الأفعال التي يعتبر إرتكابها جرائم تقنية فهي بذلك لم تورد تعريفا للجرائم الإلكترونية.

3-التعريف الفقهي للجرائم الإلكترونية: تعددت أراء الفقهاء واختلفت إتجهاتهم حول تعريف الجرائم الإلكترونية وذلك بتعدد الزاويا التي ينظر إليها كل إتجاه، فهناك من عرفها إستنادا إلى وسيلة إرتكابها في حين عرفها البعض بالنظر إلى الإلمام بالمعرفة التقنية، والبعض الآخر إعتمد في تعريفه على موضوع هذه الجريمة، إضافة إلى كل هذا هناك تعريفات إعتمدت على معايير متعددة وسنقوم بتوضيح كل هذه الإتجاهات في النقاط التالية:

---

[1] طارق الخن ، مرجع سابق، ص ص 14،15.

[2] إتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001، الموقعة في 23 نوفمبر 2001 بالعاصمة المجرية بودابست. في فبراير 2001 طالب وزراء العدل ووزراء الداخلية للدول الثماني الكبار من الخبراء في الاجتماع الذي عقد في ميلانو بإيطاليا، وضع توصيات عن إقتفاء أثر المجرمين على شبكات المعلومات مع الأخذ باحترام الحقوق الأساسية، مثل حماية= خصوصية الأفراد والحريات الأساسية، وفي موسكو طلب الوزراء مرة أخرى من الخبراء أن يستشيروا ممثلي الصناعات المتطورة في المجالات التقنية حول الملاحقة وحول بعض المسائل الأخرى المتصلة بالجريمة ذات التقنية العالية، ثم توالت المؤتمرات وورش العمل في باريس وبرلين وطوكيو، وهي التي شارك فيها أكثر من مائة ممثل عن شركات التقنية العالية في العالم أجمع، وقد تنامت الجهود الدولية بشكل مطرد، حيث وقعت ثلاثون دولة في بودابست في 23 نوفمبر 2001 الإتفاقية الأوربية لمكافحة جرائم الأنترنت، وكان من بين الموقعين 26 دولة من مجلس أوربا إضافة إلى الولايات المتحدة الأمريكية، كندا، اليابان وجنوب إفريقيا، بينما إمتنعت 17 دولة أوربية عن التوقيع من بينها إيرلندا والدانمارك ودخلت حيز التنفيذ في يوليو من عام 2004. (أنظر: سليمان قطاف ، عبد الحليم بوقرين ، (الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري)، المجلة الأكاديمية للبحوث القانونية والسياسية، (مج 6، ع 2، الصادر في 2022)، ص 338.

[3] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الأمانة العامة لجامعة الدول العربية، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014، ج،ر، ع 57، الصادر في 28 سبتمبر 2014.

أ-تعريف الجرائم الإلكترونية إستنادا إلى وسيلة إرتكابها: إعتمد أصحاب هذا الإتجاه في تعريفهم لها إلى الأداة الي يتم بواسطتها إرتكابها، ومن هذه التعريفات نجد تعريف الفقيه الألماني "TIEDEMAN" بأنها كافة أنماط السلوك غير القانوني الذي يتم إرتكابه باستخدام الكمبيوتر،[1] أيضا الفقيه "MERWE" الذي يعرفها بأنها الأفعال غير القانونية الذي يتورط في إرتكابها جهاز الحاسوب أو الأفعال الإجرامية التي يستخدم فيها البرامج المعلوماتية كأداة رئيسية،[2] كما يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا في إرتكابها[3].

ومن بين الإنتقادات التي تم توجهيها إلى هذا التعريف هي أن الوسيلة لا تعتبر محل إعتبار عند التجريم كون أغلب الوسائل متساوية، والتكوين القانوني للجريمة يكون بقيام أركانها هو محل الإعتبار عند تطبيق نصوص التجريم فضلا على انه تعريف يوسع من نطاق الجريمة الإلكترونية.[4]

ب-تعريف الجريمة الإلكترونية إستنادا إلى الإلمام بالمعرفة التقنية: على عكس الإتجاه الأول نجد أنصار هذا التعريف قد إشترطوا توفر درجة كبيرة من المعرفة بتقنية المعلومات لدى مرتكب الجريمة الإلكترونية، وتفوقه في مجال إستخدام جهاز الحاسوب.

ومن بين هذه التعريفات نجد تعريف وزارة العدل الأمريكية التي تعرف الجريمة الإلكترونية بأنها إنتهاك للقانون الجنائي يتطلب المعرفة بتكنولوجيا المعلومات من أجل إرتكابها أو التحقيق فيها أو إجراءاتها الإدارية،[5] كما عرفها الفقيه "STEINSCKJOBERG" بأنها أي فعل غير مشروع تكون

---

[1] REZKI KETTAF, (Cyberspace and cyber crime-towards modeling behavior and controlling action-) J H S, (N°2, VOL 09, JUIN, 2022, P 604.

[2] NASSIMA AZIZI , IBTISSEM KHEDRI, (Cybercriminalité un fléau planétaire) ,R D E J, (N° 1, VOL 1, 2020, P 3.

[3] يعيش تمام شوقي، الجريمة المعلوماتية دراسة تأصيلية مقارنة، ط 1، الجزائر، مطبعة الرمال، 2019، ص 19.

[4] خليل يوسف جندي ، (المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني -دراسة مقارنة-)، مجلة كلية القانون للعلوم القانونية والسياسية، ع 36، مج 7، الصادر في 2018، ص 86.

[5] MOHAMED CHAWKI, Essai sur la notion de cybercriminalité, juillet 2006, consulté le 01/09/2022, sur le site: http://www.iehei.org .

المعرفة بتقنية المعلومات أساسية لمرتكبه،[1] فهي الجريمة التي يكون العلم بتكنولوجيا الحاسوب لازما لإرتكابها.[2]

فهذا التعريف ربط الجرائم الإلكترونية بالسمات الخاصة لمرتكبها وهذا ما يجعله تعريف قاصر حيث ضيق من مفهومها وحصرها في فئات محددة وهذا غير صحيح، فالواقع أثبت أن هناك العديد من الجرائم الإلكترونية تم إرتكابها من طرف أشخاص عاديين ليس لهم مستوى عالي من المهارة في مجال تكنولوجيا المعلومات إضافة إلى هذا هناك جرائم يبقى مرتكبوها مجهولين دون التحقق من مستواهم في مجال تقنية المعلومات، هذا ما حصل في الجرائم المرتكبة في إطار شركات المساهمة والتي تم إكتشافها عن طريق الصدفة دون الوصول إلى مرتكبيها ومعرفة ما إذا كانوا فعلا على درجة كبيرة بتقنيات المعلومات أم لا.

ت–تعريف الجرائم الإلكترونية إستنادا إلى موضوعها: يعتمد هذا الإتجاه في تعريفه للجرائم الإلكترونية على محلها الذي يتمثل في المصالح المحمية والتي تتعرض للإعتداء من خلالها، ومن هذه التعريفات نجد الفقيه "ROS BELAT" الذي يرى بأنها، أي نشاط غير مشروع موجه لنسخ أو تعديل أو حذف أو التوصل إلى المعلومات المحفوظة بجهاز الحاسوب والتي تُحول عن طريقه،[3] وعرفت أيضا بأنها، الولوج غير المشروع إلى الشبكات الخاصة والعبث ببيناتها الرقمية التي تحتويها أو إتلافها أو محوها مما يسبب إضرار بتلك البيانات والمعلومات ذاتها وكذا البرامج والأجهزة التي تحتويها،[4] وهي سلوك غير مشروع معاقب عليه قانونا يصدر عن إرادة جرمية محله معطيات الحاسوب.[5]

---

[1] سميرة معاشي ، (الجريمة المعلوماتية –دراسة تحليلية لمفهوم الجريمة المعلوماتية–)، مجلة المفكر، ع 7، الصادر في جوان 2018، ص 402.

[2] عبد الوهاب جعيجع ، الأمن المعلوماتي وإدارة العلاقات الدولية، د،ط، الجزائر، منشورات دار الخلدونية، 2017، ص 87.

[3] NASSIMA AZIZI , IBTISSEM KHEDRI, op, cit, P 3.

[4] نسيمة جدي ، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، (رسالة ماجستير، كلية الحقوق جامعة وهران، 2013–2014)،ص 8.

[5] ثنيان ناصر آل ثنيان، "إثبات الجريمة الإلكترونية –دراسة تأصيلية تطبيقية"، (رسالة ماجستير، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، 2012)،ص 19.

وعرفت بانها غش معلوماتي ينصرف إلى سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها،[1] وفي نفس السياق يرى الفقيهين "MICHEL ET CREDO" بأن الجرائم الإلكترونية هي الولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به،[2] وعرفتها الدكتورة "هدى قشقوش" بأنها جرائم الإعتداء على الأموال المعلوماتية والتي تتمثل في الأدوات المكونة للحاسب وبرامجه ومعداته،[3] فهذه التعريفات جعلت الجرائم الإلكترونية مقتصرة فقط على المصالح المحمية وهي جهاز الحاسوب وكذا البرامج والبيانات التي يحتويها نظامه.

ث-تعريف الجرائم الإلكترونية إستنادا إلى الجمع بين أساليب إرتكابها وموضوعها: وهو تعريف ذو طابع مزدوج يجمع في تعريفه لها بين الأساليب والموضوع، حيث ظهر نتيجة للإنتقادات التي وجهت إلى التعريفات السابقة، فالجرائم الإلكترونية وفقا لهذا التعريف هي "كل سلوك تكون فيه الأنظمة والشبكات المعلوماتية وسيلة أو هدفا أو محلا لإرتكاب أفعالا إجرامية،[4] وعرفها خبراء متخصصون من بلجيكا في معرض ردهم على إستبيان منظمة التعاون الاقتصادي والتنمية (OCDE) حول الغش المعلوماتي سنة 1982 بأنها كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية،[5] وهي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية تنشأ عنه خسارة تلحق

---

[1] رمزي حوحو ، منيرة بلورغي ، (مواجهة الجريمة المعلوماتية في الجزائر)، مجلة الحقوق والحريات، ع 2، الصادر في 2014، ص 41.

[2] نعيم سعيداني ، "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر، 2012-2013)، ص 29.

[3] سميرة معاشي ، مرجع سابق، ص 29.

[4] هبة نبيلة هروال ، "جرائم الأنترنت -دراسة مقارنة-"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2013-2014)، ص 21.

[5] عبد العزيز بوذراع ، "خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، (رسالة ماجستير، كلية الحقوق جامعة الجزائر 1، 2011-2012)، ص 16.

بالمجني عليه أو كسب يحققه الفاعل ،[1] ويعرفها "BOLOGNA" كذلك بأنها الجرائم التي يستخدم فيها الحاسوب كوسيلة لإرتكابها أو يمثل إغراء بذلك أو جريمة يكون الحاسوب نفسه ضحية لها.[2]

رغم أن هذا التعريف حاول الإلمام بجوانب الجرائم الإلكترونية من أجل تعريفها وإن كان يبدو أكثر شمولا من التعريفات السابقة إلا أنه لم يسلم هو الآخر من الإنتقاد، وهذا شيئ طبيعي بالتأكيد كونها جرائم مستحدثة ذات طبيعة خاصة سواء من حيث أساليب إرتكابها أو موضوعها ، غير أنه يبقى التعريف الأقرب والأنسب كونه لم يركز على جانب واحد فقط من جوانبها مثلما ذهبت إليه الإتجاهات السابقة.

ومن خلال ما تم طرحه فيمكننا أن نعرف الجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة بأنها كافة الأنشطة الإجرامية سواء كانت إيجابية أو سلبية، والتي يتم إرتكابها بمختلف الأساليب التقنية مما يشكل إعتداء على نظامها المعلوماتي وما يحويه من معلومات وأسرار تجارية تتعلق بأعمالها بغض النظر عن غاية مرتكبيها، فهي جرائم تستهدف هذه الشركات ضمن البيئة الإفتراضية.

الفرع الثاني:

خصائص الجرائم الإلكترونية.

بما أن الجرائم الإلكترونية أوجدها التطور التكنولوجي ويتم إرتكابها في بيئة إفتراضية حيث إرتبطت بها إرتباطا وثيقا الشيئ الذي أضفى عليها ميزة منفردة عن نظيرتها التقليدية، لذلك من خلال هذا الفرع نتعرف على الخصائص التي تتميز بها والتي يمكن إدراجها في النقاط التالية:

---

[1] أحمد برادي ، (آليات مكافحة الجريمة الإلكترونية في ضوء قانون العقوبات الجزائري)، مجلة وميض الفكر للبحوث، ع 7، الصادر في أيلول 2020، ص 450.

[2] محمد رحموني ، (خصائص الجريمة الإلكترونية ومجالات إستخدامها)، مجلة الحقيقة، ع 41، د،ت،ص، ص 437.

أولا: ذات طبيعة دولية وتتسم بالهدوء والخفاء.

1-أنها جرائم ذات طبيعة دولية[1]: ويعود ذلك إلى الطبيعة الخاصة التي تفرضها شبكات الأنترنت،[2] والتي بفضلها أصبحت معظم دول العالم في حالة إتصال دائم على الخط مما يسهل إرتكاب هذه الجرائم من دولة إلى أخرى،[3] فلم تعد هناك حدود مرئية أو ملموسة تقف حاجزا أمام نقل المعلومات فقدرة الحاسبات الآلية على تبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال[4] قد أدت إلى نتيجة تتمثل في إختراق الجرائم الإلكترونية لأي شخص سواء طبيعي أو معنوي في أي مكان من العالم، وبالتأكيد طبيعة الدولية التي تتسم بها هذه الجرائم جعلت من شركات المساهمة أحد أهدافها نتيجة إعتمادها على أجهزة الحواسيب ومختلف الشبكات في القيام بأعمالها، فمعظم معلومات أصبح يتم تبادلها بطريقة إلكترونية مع غيرها من الشركات أو حتى مع العملاء، كما أنه بسبب هذه الخاصية أصبحت هذه الشركات معرضة للإعتداء جناة الفضاء الإفتراضي دون أن تقف الحدود الجغرافية حاجزا أمامهم مثلما هو الحال في الجرائم التقليدية.

2-أنها جرائم تتسم بالهدوء والخفاء: فتنفيذها قد لا يتجاوز مجرد لمسة بسيطة لمفاتيح التشغيل الخاصة بجهاز الحاسوب أو أحد ملحقاته،[5] فهي عكس الإجرام التقليدي تماما لا تحدث ضجيجا أو

---

[1] من أهم القضايا التي أكدت هذه الخاصية قضية عرفت بمرض نقص المناعة المكتسبة، حيث أنه في سنة 1989 قام شخص يسمى " جوزيف بيب" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض "الإيدز" لكن في الواقع يحتوي ذلك البرنامج على فيروس يتسبب في تعطيل جهاز الحاسوب، فيقوم بعدها الفاعل بطلب مبلغ مالي للحصول على عنوان إلكتروني مضاد للفيروس، في الثالث من فبراير تم إلقاء القبض على الجاني في " أوهايو" بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرسال البرنامج على أراضيها وبالفعل تمت محاكمته أمام القضاء الإنجلزي. (أنظر: مروة أبو العلا ، خصوصية الجرائم الإلكترونية في التشريع الجزائري والتشريعات المقارنة، مقال منشور بتاريخ 20 أفريل 2018، تاريخ الدخول: 2022/09/02، متاح على الرابط: https://www.mohamah.net

[2] فاديا سليمان، (الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية)، مجلة الدراسات المالية والمصرفية، ع 1 ، الصادر في 2015، ص 7.

[3] بشير عادل حامد، الإثبات الجنائي للجريمة الإلكترونية، ط 1، القاهرة، دار النهضة العربية، 2021، ص 13.

[4] شول بن شهرة، مراد مشوش، (السمات الخاصة للجريمة المعلوماتية)، مجلة المستقبل للدراسات القانونية والسياسية، ، ع 1، مج 4، الصادر في جوان 2020، ص 8.

[5] خضرة شنتير،" الآليات القانونية لمكافحة الجريمة الإلكترونية –دراسة مقارنة–" (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أحمد دراية، 2020-2021)، ص 15.

ضوضاء كجريمة القتل أو السرقة مثلا، بل أن فاعلها ينفذها في صمت وسكون تامين كما أنها لا تحتاج منه أن يبذل مجهودا عضليا كالكسر، حيث توصف بالجرائم الناعمة كونها تعتمد على المجهود الذهني المحكم والتفكير العلمي المدروس والتعامل الدقيق مع الشبكات.[1]

وخاصية الهدوء التي تتميز بها تلازمها خاصية أخرى تتمثل في الخفاء[2] لأنه يصعب ملاحظتها فهي مستترة ومن الصعب جدا الإنتباه لها واكتشافها، ونتيجة لذلك العديد من الجرائم الإلكترونية التي تعرضت لها شركات المساهمة لم يتم إكتشافها سوى صدفة والبعض الآخر لم تكتشف.

ثانيا: صعبة الإثبات و سريعة التطور من حيث أساليب إرتكابها.

1-أنها جرائم صعبة الإثبات: وهذه الخاصة تعد من أهم خصائصها خاصة في إطار شركات المساهمة، ويرجع السبب في ذلك إلى طبيعة الأساليب التي تنفذ بها والتي تتسم بالطابع التقني[3] الذي لا يترك خلفه أي دليل مادي ملموس، إذ يتم نقل المعلومات إلكترونيا فضلا على إمكانية تدمير المعلومات التي يمكن إستخدامها كدليل في الإثبات في مدة قد لا تتجاوز الثانية الواحدة.[4] وتعتمد على الخداع في إرتكابها وعلى التضليل في التعرف على مرتكبها نظرا لعدم دخوله إلى الشبكة بهويته الحقيقية وإنما تحت إسم مستعار.[5]

ويترتب على هذه الخاصية صعوبة التحقيق فيها إذ تتطلب مهارات وكفاءات وخبرة قد لا تتوفر لدى المحقق العادي، لذلك يستلزم الأمر الإستعانة بفريق متكون من كوادر على مستوى من الخبرة

---

[1] لامية طالة ، كهينة سلام ، (الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الإحتماعي)، مجلة الرواق للدراسات الاجتماعية والإنسانية، ع 2، مج 6، الصادر في ديسمبر 2020، ص 75.

[2] يوسف صغير ، "الجريمة المرتكبة عبر الأنترنت"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة مولود معمري، 2013)، ص 14.

[3] سفيان سوير ، "جرائم المعلوماتية"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة أو بكر بلقايد، 2010-2011)، ص 19.

[4] حمزة خضري ، حمزة عشاش ، (خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري)، مجلة الدراسات القانونية والسياسية، ع 2، مج 6، الصادر في جوان 2020، ص 171.

[5] ضرغام جابر عطوش آل مواش ، جريمة التجسس المعلوماتي -دراسة مقارنة- ط 1، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2017، ص 31.

والتأهيل في مجال التقنية المعلوماتية من أجل القدرة على إستخلاص الدليل المناسب والذي يكون ذو طبيعة تقنية مثلها حتى يتم إثباتها، وسنتطرق إلى الإجراءات الخاصة بالتحري والتحقيق من أجل إستخلاص الأدلة الخاصة بها في الفصل الثاني من الباب الثاني من هذه الدراسة.

2-أنها جرائم سريعة التطور من حيث أساليب إرتكابها: وذلك نتيجة للتطور السريع الذي تعرفه التكنولوجيا بحيث كان إنعكاسه واضحا عليها خاصة فيما يتعلق بأساليب إرتكابها والتي هي في تطور دائم،[1] إذ يستغل الجناة ذلك ويعملوا على تطوير خبراتهم الإجرامية،[2] من خلال تبادل الأفكار والخبرات الهدامة مع العديد من المجرمين حول العالم عبر الشبكات الإلكترونية وتطور التقنيات المستخدمة،[3] ويتجلى ذلك بصورة واضحة في مختلف المواقع الإلكترونية ومنتديات القراصنة التي تضمن لهم الإتصال فيما بينهم لتبادل المعارف والتقنيات الإجرامية ، فضلا عن مختلف المؤتمرات التي يعقدها القراصنة والتي تسمح لهم بابتكار وسائل وطرق في غاية التعقيد لم تعرفها التشريعات من قبل من أجل تنفيذ جرائمهم،[4] هذا ما يجعل الجرائم الإلكترونية تتسم بالتعقيد من الصعب فك شفراتها والتعرف على تقنيات إرتكابها فهي جريمة مستعصية.

ثالثا: ذات أضرار بالغة الخطورة ومستحدثة.

1-أنها جرائم ذات أضرار بالغة الخطورة: الجرائم الإلكترونية ذات أبعاد خطيرة وغير مسبوقة على حجم الأضرار والخسائر التي تنجم عن إرتكابها،[5] إذ تكبدت العديد من الدول كما هائلا من الخسائر المادية والمعنوية وكان على رأس القطاعات، قطاع التجارة، والمؤسسات المالية الأكثر عرضة

---

[1] صفيان بخدة ، ناصر وقاص ، (الطبيعة القانونية للجرائم المستحثة ووسائل إرتكابها –جريمة الأنترنت كنموذج–)، مجلة البحوث القانونية والسياسية، ع 16، مج 3، الصادر في 2021، ص 124.

[2] نسيمة جدي ، مرجع سابق، ص 27.

[3] عزيزة رابحي ، "الأسرار المعلوماتية وحمايتها الجزائية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد، 2017-2018)، ص ص 97،98.

[4] عيسى سليم داود الزيدي ، جرائم القرصنة الإلكترونية –دراسة مقارنة– د، ط، مصر، دار الكتب القانونية، 2020، ص 29.

[5] حنان مسكين ، (واقع مكافحة الجرائم المعلوماتية وإتجاهاتها التشريعية في الجزائر)، المجلة الأكاديمية للبحوث القانونية والسياسية، ع 1، مج 4، الصادر في 2020، ص 614.

للخسائر الناجمة عنها ،[1] ويكمن السبب في ذلك بوقوع هذه الجرائم في إطار تقنيات ذات مستوى عالي من التقدم يزداد الإعتماد عليها يوما بعد يوم في إدارة المعاملات التجارية والمالية، سواء الوطنية وحتى الدولية ،[2] حيث نجد في التقرير الذي أعدته "RSA" العالمية لأمن المعلومات للربع الأول والثاني من سنة 2018، أن الدول الأكثر إستهدافا لهجمات صيد المعلومات هي الولايات المتحدة الأمريكية، كندا وخلال مسح أجري سنة 2017 مس حوالي 254 شركة عالمية تبين أن 98 % منها تعرضت لهجمات ضارة، 69% تعرضت للإحتيال عن طريق الصيد باستخدام الهندسة الاجتماعية التي تعتمد على التحايل على العقول للإفصاح عن معلومات سرية، 67% تعرضت للصيد عن طريق الأنترنت.[3]

وفي مقال ورد في جريدة "LES ECHOS" الفرنسية المختصة في أخبار الاقتصاد والمالية للصحفية "LEILA MARCHAND" بأن حجم أضرار الجرائم الإلكترونية يصل إلى 600 مليار دولار سنويا هذا ما يعادل 0.8% من الناتج الخام المحلي العالمي وبحسب تقرير مركز الدراسات الإستراتجية والدولية "CSIS" وكذا الشركة المختصة في الحماية من هجمات الكمبيوتر "MCAFEE" فإن هناك زيادة كبيرة في حجم أضرار هذه الجرائم بعد أن كانت سنة 2014 تقدر ب 445 مليار دولار،[4] وهذا إن دل على شيئ فإنما يدل على خطورتها على إقتصاد الدول سيّما بعد إستهدافها لأهم شركاتها.

2-أنها جرائم مستحدثة: تستمد حداثتها من حداثة المحل الذي ترد عليه والمتمثل في المعلومات المالية المخزنة في النظام المعلوماتي، كما تستمد حداثتها من وسائل إرتكابها والتي تتمثل في مختلف أجهزة الحاسوب والشبكات والتي عمدت الشركات إلى إستعمالها بشكل مطرد فاستغل جناة الفضاء

---

[1] مشتاق طالب وهيب، مرجع سابق، ص 348.

[2] صابرين يوسف عبد الله الحياني، "جرائم الأموال الناجمة عن إستعمال الحاسوب –دراسة مقارنة–"، (رسالة ماجستير، كلية الحقوق جامعة النهرين، 2014)، ص 13.

[3] وهيبة عبد الرحيم ، أمين بن سعيد ، نادية عبد الرحيم ،(الجريمة الإلكترونية من خلال مؤشرات عالمية وآثارها على المؤسسات)، مجلة دراسات، ع 1، مج 16، الصادر في جانفي 2019، ص ص 38،40.

[4] LEILA MARCHAND, La cybercriminalité coute 600 milliard de dollars par an, publie le 21/02/2018, consulté le 08/09/2022, sur le site: https://lesechos.fr

الإلكتروني هذه التقنيات الحديثة في تنفيذ إعتداءاتهم الإجرامية، وذلك باعتبار أن الحاسوب والشبكات يمثلان، الطريق الأسرع للوصول إلى المعلومات المالية والأسرار التجارية المخزنة في حواسيب هذه الشركات.[1]

المطلب الثاني:

دوافع إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة وأطرافها.

خلف كل جريمة دافع وراء إرتكابها، باعتبار أن الدافع هو العامل المحرك الأساسي للإرادة إذ يعمل على توجيه السلوك الإجرامي وإذا كانت الجرائم التقليدية ترتكب في أغلب الأحيان بدافع الربح أو الكسب المادي فإن الأمر يختلف بالنسبة للجرائم الإلكترونية في إطار شركات المساهمة إضافة إلى دافع الربح هناك جملة من الدوافع الأخرى التي تكون وراء إرتكابها هذا من جهة، ومن جهة أخرى فإن قيام هذه الجرائم يتطلب وجود طرف جاني يسمى بالمجرم الإلكتروني والذي يختلف تماما عن المجرم التقليدي، ينفذ إعتداءه على هذه الشركات التي تكون ضحية لها، هذا ما نتعرف عليه من خلال هذا المطلب وذلك بالتطرق إلى دوافع إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة **(فرع أول)** ثم أطراف الجرائم الإلكترونية في إطار شركات المساهمة **(فرع ثاني)**.

الفرع الأول:

دوافع إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة.

تتعدد الدوافع التي تؤثر على نفسية مرتكبي الجرائم الإلكترونية في إطار شركات المساهمة وتدفعهم إلى تنفيذ تجسيد أفعالهم الإجرامية عليها، ويمكن إجمال هذه الدوافع في النقاط التالية:

أولا: دافع التعلم، التفوق وإثبات الذات.

1-دافع التعلم: العديد من الجناة يرتكبون الجرائم الإلكترونية بهدف الحصول على الجديد من المعلومات،[2] من أجل الإستيلاء عليها والتصرف فيها، حيث يشير الأستاذ " ليفي" مؤلف كتاب "قراصنة الأنظمة" "HACHERS" أن أخلقيات هؤلاء الجناة تستند إلى مبدأين أساسين هما:

---

[1] صابرين يوسف عبد الله الحياني، مرجع سابق، ص 10.

[2] عيسى سليم داود الزيدي ، مرجع سابق، ص 41.

أ-أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم؛

ب-أن جمع المعلومات يجب أن تكون غير خاضعة للقيود.[1]

فمن وجهة نظرهم فإنه يجب عدم إخضاع المعلومات بوجه عام لأية قيود مهما كانت، إذ يكرسون جهدهم ووقتهم لتعلم كيفية إختراق المواقع المحمية ،[2] ويعملون في مجموعات من أجل التعاون فيما بينهم وتبادل المعلومات والمعارف، كما أنهم يفضلون البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الإستمرار في التواجد داخل المنظمة،[3] وقد كتب أحد قراصنة الأنظمة يقول: نكتشف نقطة ضعف أمنية فنحاول إستغلالها كونها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن ما نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والإنهماك،[4] فشغف التعلم وولع جمع المعلومات يجعل هؤلاء الجناة يرتكبون أفعال غير قانونية تصنف ضمن الجرائم الإلكترونية حتى وإن كانت نيتهم حب التعلم فقط دون نية الإضرار بهذه الشركات.

2-دافع التفوق وإثبات الذات: إذ أن التفوق على النظام المعلوماتي لهذه الشركات وقهر أساليب الحماية الخاصة بها متعة تجعل الجناة يتباهون بإنجازاتهم ويثبتون بذلك تفوقهم العلمي،[5] فدافع الرغبة في قهر النظام أقوى من لذة الحصول على الربح، رغم أن دافع السعي إلى تحقيق الربح يظهر أكثر تحريكا لمجرمي الكمبيوتر، غير أن دافع الرغبة في قهر النظام تجسد في العديد من الجرائم

---

[1] رمزي حوحو ، منيرة بلورغي ، مرجع سابق، ص 50.

[2] نبيل دريس ، (الجريمة السيبرانية بين المفاهيم والنصوص التشريعية -الجزائر نموذجا-)، مجلة القانون والمجتمع، ع 2، مج 5، الصادر في 2017/12/01، ص 31.

[3] عيسى سليم داود الزيدي ، مرجع سابق، ص 41.

[4] مركز هردو لدعم التعبير الرقمي، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مصر، منشورات مركز هردو، ، 2014، ص 11.

[5] إسماعيل بن يحي ، "التحقيق الجنائي في الجرائم الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2020-2021)، ص 33.

الإلكترونية خاصة ما يعرف بأنشطة المتطفلين وهؤلاء ليسوا على مستوى كبير من الخطورة الإجرامية وإنما يفضلون تحقيق إنتصارات تقنية دون أن يكون لديهم أية نوايا سيئة.[1]

فمرتكبوا الجرائم الإلكترونية يتملكهم شعور بالبحث عن القوة ويؤدي إرتكابهم لها بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، فأحيانا وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لإرتكاب فعل الإحتيال الإلكتروني، فقد ينتاب المحلل أو المبرمج الذي يعتبر مفتاح كل نظام إحساس بالإهمال أو النقص داخل الشركة التي يزاول بها عمله فيندفع تحت تأثير رغبة قوية من أجل إثبات قدراته التقنية لإدارة هذه الشركة إلى إرتكاب جرائم الإلكترونية،[2] ويعتبر هذا الدافع من أكثر الدوافع التي يتم إستغلالها من قبل المنظمات الإجرامية حتى يتم إستدارج محترفي الإختراق إلى قبول المشاركة في أشطة إعتداء معقدة أو إستئجارهم للقيام بالجريمة[3].

ثانيا: دافع الإنتقام.

يعد هذا الدافع من أخطر الدوافع التي تكون وراء إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة حيث تكمن خطورته في أن الجاني يكون من داخلها، ، كأن يكون أحد موظفيها الذي يحوز على الكثير من المعلومات والبيانات السرية التي لا تتوفر لدى غيره من المجرمين، فقد يكون الفصل من الوظيفة أو حرمانه من بعض الحقوق دافعا يزرع داخله حقدا ويولد لديه رغبة جامحة في الإنتقام من مديريه.

كما تكمن خطورة هذا الدافع أيضا في أن هذا الشخص يقوم بالإستعداد مسبقا لمثل هذا الموقف، كأن يقوم بزرع فيروسات أو برنامج يحمل تعليمات بمسح كافة البيانات في حالة عدم وجود إسمه في كشف الموظفين بالشركة ويقوم عند فصله منها بالإنتقام عن طريق تشغيل هذا البرنامج، أو

[1] رابحي عزيزة، مرجع سابق، ص 101.

[2] نهلا عبد القادر المومني ، مرجع سابق، ص 92.

[3] سوير سفيان، مرجع سابق، ص 28.

أنه يقوم بتسليم كلمة السر الخاصة بالدخول إلى نظام الحاسب الآلي الخاص بالشركة إلى شركة أخرى منافسة حتى تتمكن من الدخول إلى أنظمة تلك الشركة والتجسس على البيانات الخاصة بها.[1]

ومن أبرز الجرائم التي أرتكبت بدافع الإنتقام حادثة شركة "OMEGA" التي تعود وقائعها في أن مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لهذه الشركة من مدينة "DELAWARE" ويدعى "TIMOTHY ALLEN LIOYD" تم إعتقاله في 17 فيفري 1998 بسبب إقدامه على إطلاق قنبلة إلكترونية بعد عزله من منصب عمله، حيث إستطاعت تلك القنبلة إلغاء كافة التصاميم وبرامج الإنتاج لإحدى كبرى مصانع التقنية العالمية في "نيوجرسي" والتي تؤثر على نظم تحكم مستخدمة في "NASA" والبحرية الأمريكية، ملحقا خسائر بلغت قيمتها 10 ملايين دولار حيث تعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الأنترنت.[2]

كذلك ما حدث في الولايات المتحدة الأمريكية إذ تم الحكم على أحد الموظفين الذي كان يعمل في إحدى شركات التأمين بالسجن مدة سبع سنوات وغرامة قدرها 150 ألف دولار، لأنه قام بزرع فيروس في أجهزة الشركة مما تسبب عن ضياع 160 سجلا من السجلات الخاصة بالعملاء وذلك إنتقاما من الشركة بعدما قامت بفصله من العمل،[3] فالضرر الذي تلحقه الشركة بالموظف تدفعه إلى إرتكاب جريمة تكبدها خسائر كبيرة تستلزم وقت طويل من أجل إصلاحها وجبرها، إذ يتسبب التعطيل الذي يصيب أجهزة الشركة في توقف نشاط عملها وهذا ما يفوت عليها الكثير من فرص الربح أمامها، ويتسبب أحيانا أخرى في فقدان عدد هائل من عملائها .

ثالثا: دافع الكسب المادي، الثقة والمنافسة.

1-دافع الكسب المادي: إذ يعتبر هذا الدافع ذو أثر بالغ في تحريك إرادة الجناة لإرتكاب الجرائم الإلكترونية فيتعمدون رغبة منهم في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للشركات، أو

---

[1] نصيرة بوحزمة ، "التحقيق الجنائي في الجرائم الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة الجيلالي اليابس، 2021-2022)، ص 84.

[2] بشرى غربي ، (خصوصية المجرم المعلوماتي ودوافعه)، مجلة نوميروس الأكاديمية، ع 2، مج 2، الصادر في 2021/06/01، ص 111.

[3] عيسى سليم داود الزيدي ، مرجع سابق، ص 45.

إختراق أنظمة المعالجة الآلية من خلال إكتشافهم لفجواتها الأمنية فيعملون على إستغلالها وبرمجتها لتحويل مبالغ مالية لحسابهم أو لحساب شركائهم أو لحساب من يعملون لحسابهم إن كانوا من خارج الشركة، كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج والمعلومات المتحصل عليها بطريق الإختلاس من الحاسوب.[1]

كما يتعزز تحقيق هذا الدافع من خلال غش الحاسوب أو الإحتيال المرتبط بالحاسوب، ففي دراسة قام بها الفقيه " BARKER" يظهر أن 43% من حالات الغش المعلن عنها قد تمت من أجل إختلاس الأموال، 23% من أجل سرقة معلومات، 19% أفعال إتلاف ،[2] أما في الجزائر فإن الدوافع المادية للجريمة الإلكترونية تمثل ما نسبته 65% أمام باقي الدوافع الأخرى.[3]

وقد يتحقق الربح المادي عن طريق التهديد والإبتزاز، فحسب تقرير "MIKKO HYPOMEN" مدير مركز البحوث لدى شركة "F.SECURE" فإن بعض الجناة يعمدون إلى إرسال رسائل إلكترونية لضحاياهم مسبقا يخبرونهم فيها بأمر إكتشاف ثغرات أمنية على أنظمتهم المعلوماتية وبأنهم سيقومون بمحو بياناتهم وتدميرها كليا في حال عدم تحويل أموال إلى حساباتهم وهو ما حدث مع شركة "GOOGLE" في ماي 2004 أين قام "MICHEL BRADLY" بإرسال تهديدات لهذه الشركة بضرورة دفعها مبلغ قدره 100.000 دولار وإلا فإنه سيقوم بنشر فيروس وبرنامج غامض من شأنه أن يحدث عطل بالنظام المعلوماتي الخاص بتحصيل عائدات الإشهار من

---

[1] إيمان بومدين ، حنان مزيان ، الجريمة الإلكترونية بين دوافع إرتكابها وآليات مواجهتها –الإستراتجية الأمنية للدولة الجزائرية في مكافحة الجرائم الإلكترونية نموذجا– مداخلة مقدمة إلى: المؤتمر الدولي الإفتراضي المنعقد في14 و 15 ماي 2022، بألمانيا ص 92.

[2] حمزة بن عقون "السلوك الإجرامي للمجرم المعلوماتي، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011–2012)، ص 47.

[3] عائشة بوخبزة ، "الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري"، (رسالة ماجستير، جامعة وهران، 2012–2013)، ص ص 29،30.

الصفحات المدعمة من قبلها، وقد ألقي عليه القبض في ولاية كاليفورنيا الأمريكية بتاريخ 17 ماي 2004.[1]

يروي أحد المجرمين المحترفين في سجن كاليفورنيا بقوله "لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في أي وقت، لقد كان شيئا سهلا فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني"[2] وبالتالي فالربح المادي وإن كان يبدو دافعا للجرائم التقليدية إلا أنه يعتبر دافعا أكثر لإرتكاب الجرائم الإلكترونية ذلك أنه يمكن من كسب مبالغ طائلة في ظرف وجيز ودون عناء أو جهد من الجاني.

2-دوافع تتعلق بالثقة والمنافسة: حيث أن هناك شركات تضع ثقة عمياء في موظفيها ويمارسون مهامهم دون الخضوع لأية رقابة نتيجة لتلك الثقة مما يخولهم إستعمال نظامها المعلوماتي دون قيود وبحرية مطلقة، وبالتالي فإن الشركة تساعدهم على إرتكاب الجرائم الإلكترونية ضدها من خلال إتاحة وسيلة إرتكابها التي يقوم هؤلاء الموظفين باستغلالها لتحقيق غاياتهم غير المشروعة.

فإناطة كل المسؤوليات المتعلقة بمركز المعالجة إلى المحلل أو المبرمج يكون أفضل سلاح يمكنه من إرتكاب الجريمة الإلكترونية، كما أن التساهل والتسامح في تطبيق إجراءات المراقبة وممارسة التفتيش من العوامل الرئيسية التي ساعدت على تضخيم الإعتداءات المالية، فالعديد من الشركات أغنتها الثقة العمياء التي وضعتها في المسؤولين العاملين لديها عن مراقبتهم، الأمر الذي جعلها فريسة سهلة لكثير من ضعاف النفوس الذين إستغلوا تلك الثقة التي وضعت فيهم لزيادة أعمالهم الإجرامية.[3]

---

[1] حسين ربيعي ، (المجرم المعلوماتي، شخصيته وأصنافه)، مجلة العلوم الإنسانية، ع 40، الصادر في جوان 2015، ص ص 292، 293.

[2] أسماء فيلالي ، "مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة"، (أطروحة دكتوراه، كلية العلوم الإقتصادية والعلوم التجارية جامعة أب بكر بلقايد، 2018-2019)، ص 86.

[3] صابرين يوسف عبد الله الحياني ، مرجع سابق، ص 18.

ومن الأمثلة عن ذلك قيام مستشار لدى أحد البنك الكبرى يسمى "STANLEN RIFKIN" حيث كان يتمتع بثقة كبيرة من طرف هذا البنك حيث سمح له إختصاصه بالولوج والتحكم في مفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الإلكترونية للنقود من بنك إلى آخر وقد تمكن من الوصول إلى المفتاح الثالث واستطاع أن ينقل 100 مليون دولار إلى حساب بنكي فتح بإسمه في سويسرا،[1]وبالتالي فعدم ممارسة رقابة الشركة على أداء عمل موظفيها مهما كانت أهمية المركز الذي يشتغلون فيه بها قد يجعلها ضحية لهذه الجرائم وتكون هي سببها الرئيسي.

أما بالنسبة لدافع المنافسة، فيكون ذلك بين شركات المساهمة نظرا للحرب التنافسية فيما بينها الشيئ الذي يجعلها عرضة للجرائم الإلكترونية في أية لحظة من أجل إختراقها والإعتداء على أسرارها التجارية وسرقة خططها المستقبلية.

فالمنافسة التجارية غير الشريفة تدفع ببعض الشركات إلى شن هجمات إلكترونية للإضرار بمصالح شركات أخرى، أو من أجل تشويه سمعتها لدى زبائنها حتى يصرفوا نظرهم عن منتجاتها وكثيرا ما يتم هذا الفعل بعيدا عن محيط الشركة المهاجمة، وذلك عن طريق الإستعانة بمحترفين يقومون نيابة عنها بمهاجمة أنظمة المعلومات واختراق أو تعطيل الموقع الإلكتروني للشركات المنافسة، وذلك حتى تكون الشركة المهاجمة بعيدة عن الشبهات وتنجو من الملاحقة القضائية،[2] فالجرائم الإلكترونية أقحمت هذه الشركات في حرب إلكترونية، فكل شركة معرضة للإختراق في أية لحظة من أجل إضعاف قدرتها التنافسية وإزاحتها عن الساحة التجارية وفسح المجال لغيرها من الشركات المهاجمة.

الفرع الثاني:

أطراف الجرائم الإلكترونية في إطار شركات المساهمة

لقيام جريمة ما يتطلب الأمر وجود طرف جاني يقوم بتنفيذ السلوك الإجرامي الذي يستهدف من وراءه الإعتداء على طرف آخر وهو المجني عليه أو الضحية، هذا بالنسبة للإجرام التقليدي ونفس

[1] نصيرة بوحزمة ، "مرجع سابق، ص 85.

[2] عبد القادر بن عبد الله الفنتوخ ، الجريمة في الأنترنت وطرق الحماية منها، ط 1، الرياض، مكتبة العبيكان، 2012، ص 79.

الشيئ بالنسبة للجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة ، حيث أن الطرف الجاني يتمثل في المجرم الإلكتروني الذي يعتدي على هذه الشركات لتكون بذلك الطرف المجني عليه أو الضحية هذا ما نتعرف عليه من خلال هذا الفرع.

أولا: الجاني في الجرائم الإلكترونية في إطار شركات المساهمة.

بما أن الجرائم الإلكترونية أصبحت تستهدف شركات المساهمة نتيجة القفزة التي شهدها في مجال تكنولوجيا المعلومات، فقد ظهر مع هذه الجرائم مجرم أو جاني جديد ذو شخصية مغايرة تماما للمجرم المعتاد الذي كان يعتدي عليها في ظل الجرائم التقليدية، حيث يعرف بالمجرم الإلكتروني نسبة إلى هذه الجرائم التي يرتكبها، وهو شخص منفرد سواء من حيث السمات التي يتصف بها وكذا الأنماط المختلفة له.

1- تعريف المجرم الإلكتروني: بداية يجب أن نشير إلى أن المجرم الإلكتروني هو شخص طبيعي،[1] أحيانا يقدم على تنفيذ الجرائم الإلكترونية لحسابه الخاص وذلك بغية تحقيق أهداف معينة تخدم مصلحته كتحقيق مكاسب مالية، وفي بعض الأحيان يرتكب جريمته ولكن لحساب طرف آخر قد تكون شركة أخرى كأن يكون المجرم الإلكتروني أحد موظفيها أو لا تربطه بها أية علاقة، فقد أثبت الواقع أنه كثيرا ما تتعرض شركات المساهمة إلى جرائم إلكترونية ترتكب ضدها من طرف شركات أخرى مستعينة في ذلك بشخص ينفذها لصالحها مقابل مبالغ معينة، خاصة عندما يتعلق الأمر بسرقة الأسرار التجارية وخطط العمل المستقبلية وكذا الحصول على قائمة العملاء والزبائن، فالمجرم الإلكتروني مثله مثل المجرم التقليدي من حيث كونه شخص طبيعي إلا أنه وردت تعريفات خاصة بشأنها.

---

[1] الشخص الطبيعي هو الإنسان العادي الذي يقر له القانون بالشخصة القانونية ، والتي تعني قدرة الشخص على إكتساب الحقوق على إختلاف أنواعها وتحمل الإلتزامات التي يفرضها عليه القانون، أنظر: مها دحام ، تعريف الشخصية القانونية، مقال منشور في 8 أغسطس 2022، تاريخ الدخول: 2022/09/30، متاح على الرابط: https://mawdoo3.com
,وتبدأ الشخصية القانونية للإنسان بتمام ولادته حيا وتنتهي بموته، (المادة 25 من القانون رقم 05-10 المؤرخ في 20 يونيو 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني المعدل والمتمم، ج،ر، ع 44 الصادر في 26 يونيو 2005.

يعتبر المجرم الإلكتروني ظاهرة جديدة وبالتالي فهو فكرة جديدة في الفقه الجنائي وعلم الإجرام وحتى علم النفس الجنائي،[1] وقد أطلق عليه هذا المصطلح من طرف فقهاء القانون الجنائي وهو الشخص الذي يكون لديه مهارات تقنية والدراية بالتكتيك المستخدم في نظام الحاسب الآلي، حيث يعمل على إستخدام ذلك التكتيك من أجل إختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق إستخدام الحاسوب نفسه،[2] في حين أطلق عليه خبراء أمن المعلومات الإلكترونية مصطلح "HACKERS" وهي جمع لكلمة هاكر،[3] وهو الإنسان الذي يقوم بعمليات الإختراق والتخريب عبر شبكة الأنترنت،[4] ويعود الفضل في وصف المجرم الإلكتروني واستخدام مصطلح الهاكر إلى كاتب الخيال العلمي الكندي الأمريكي "وليم جيبسون".[5]

وهناك من يطلق عليه المجرم الإلكتروني الرقمي حيث يقصد بمصطلح الرقمي "DIGTAL" تخزين البيانات في ذاكرة الحاسب الآلي الرقمي في شكل أرقام وإذا طُلبت تخرج على شاشة الحاسوب أو الطابعة في الشكل المقروء حسب اللغة التي خزنت بها وليس كما هي مسجلة في ذاكرته،[6] وبالتالي فهو الذي يملك القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني في ملحقاته ووسائل الإتصال الرقمية،.[7]

---

[1] دلال مولاي ملياني ، "إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2017-2018،) ص 42.

[2] نصيرة بوحزمة ، مرجع سابق، ص 38.

[3] HACKERS وتعني القرصان أو المخترق حيث تم إطلاق هذا المصطلح على الشخص الذي يحوز على مهارات في مجال الحاسوب وأمن المعلوماتية، وأطلقت كلمة هاكر على مجموعة المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة محاولين إقتحامها دون أن تكون في نيتهم إرتكاب جريمة، فالهاكر لا يعني بالضرورة أنه شخص سيئ فهناك هاكر يستخدم مهارته في الخير وهناك من يستخدمها في إلحاق الضرر بالغير. أنظر: عبد القادر عميمر ، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 45.

[4] سهام خليلي ، (خصوصية المجرم الإلكتروني)، مجلة المفكر، ع 15، الصادر في جوان 2017، ص 405.

[5] عبد القادر غالب ، المجرم الإلكتروني، مقال منشور بتاريخ 2021/12/16، تاريخ الدخول: 2022/09/16، متاح على الرابط" https://www.africanewsanalysis.com

[6] سهام خليلي ، مرجع سابق، ص 405.

[7] محمد أمين بكوش ، هبة نبيلة هروال ، (خصوصية المجرم الإلكتروني –مجرم الأنترنت نموذجا-)، مجلة البحوث في الحقوق والعلوم السياسية، ع 1، مج 7، الصادر في جوان 2021، ص 76.

وهناك من عرفه بأنه عندما لا نكون أمام مجرم عادي بل أمام مجرم ذو مهارات تقنية وذو علم بالتكنيك المستخدم في نظام الحاسبات الآلية، وشخصيته وآلية إرتكابه للجريمة تجعله يتسم بصفات تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي،[1] كما عرفته جامعة "ميري لاند" بأنه الشخص الذي يكون قد تلقى تأهيل أكاديمي في علم الحاسوب ويقوم بالبحث عن المعطيات بشكل عشوائي حتى تظهر أي معلومة يمكن أن يبني عليها ويستفيد منها،[2] وهناك من يذهب إلى تشبيهه بالمجرمين ذوي اللياقات البيضاء،[3] كما عرفه مكتب "QUEBECOIS" للغة الفرنسية (OLF) بأن المجرم الإلكتروني هو الذي يستغل الثغرات الموجودة في إجراء الوصول لكسر نظام الكمبيوتر، وانتهاك سلامة هذا النظام وذلك بسرقة معلوماته أو تغييرها أو إتلافها أو نسخ البرامج عن طريق الإحتيال.[4]

بعد عرض هذه التعريفات للمجرم الإلكتروني يتضح لنا بأنه ظهر بظهور الجرائم الإلكترونية، فكلاهما يعتبر نتيجة للتطور التكنولوجي –وجهان لعملة واحدة– حيث يستمد تميزه وانفراده منها، فهو شخص مولع بالفضاء الرقمي، شغوف بمعرفة كل جديد في عالم الحواسيب وتكنولوجيا المعلومات، ونتيجة لذلك الشغف يدمن إستعمال الوسائل التكنولوجية .

2– السمات الخاصة لمرتكب الجرائم الإلكترونية في إطار شركات المساهمة: بالنظر إلى مرتكب الجرائم الإلكترونية في إطار شركات المساهمة نجد بأنه يتسم بمجموعة من الخصائص والسمات التي

---

[1] عفاف خذيري ، "الحماية الجنائية للمعطيات الرقمية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، 2017–2018) ، ص 24.

[2] هبة نبيلة هروال ، مرجع سابق، ص 46.

[3] أطلق مصطلح جرائم اللياقات البيضاء لأول مرة سنة 1993، إذ يتعامل مجرمين هذه الجرائم مع الوقائع بذكائهم يتقلدون مناصب مهمة والكثير منهم أثرياء هدفهم جمع المال من أجل زيادة ثروتهم، ويستغلون الجاه والإسم العائلي والمركز الاجتماعي للوصول إلى أهداف غير مشروعة، وتهدف جرائم الياقات البيضاء إلى الكسب المادي السريع الضخم وغير المشروع دون أي مظاهر للعنف وتعد جرائم غسيل الأموال من أبرز الجرائم التي يرتكبها أصحاب اللياقات البضاء. أنظر: إبراهيم علوني ، جرائم اللياقات البيضاء، مقال منشور بتاريخ 24 يوليو 2020، تاريخ الدخول: 2022/09/16، متاح على الرابط: https://www.okaz.com.sa

[4] MOHAMED CHAWKI, op, cit, P 33.

تجعله منفردا ومتميزا عن نظيره التقليدي، وهذا نتيجة لتميز هذه الجرائم وفي هذه النقطة نوضح أهم هذه والتي تتمثل في :

أ-الذكاء: المعروف أن الجرائم الإلكترونية هي جرائم الأذكياء وذلك نظرا للوسيلة التي ترتكب بها والتي تكون على مستوى من التعقيد، وبالتالي فالذكاء الذي يتسم به مُرتكبها يُعد المفتاح أو ورقة العبور إلى تمكنه من فهم تعقيداتها وفك ألغازها التي قد يعجز أمامها العديد من الأشخاص الذين يكون ذكاؤهم محدود.

فالجرائم الإلكترونية التي تتعرض لها شركات المساهمة تنتمي إلى ما يمكن أن يطلق عليه تقنيات التدمير الناعمة، إذ تتطلب الكثير من الدقة والتخصص من أجل التغلب على العقبات التي أوجدها المتخصصون قصد حماية أنظمتها المعلوماتية لذلك فمرتكبها تكون له قدرة فائقة ومهارة تقنية عالية تمكنه من إختراق الشبكات والتجول في عالمها ليحصل على كل غال وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسيب،[1] فحتى تقوم يكفي أن يعبث ببيانات وبرامج الحاسوب إما بتغييرها أو إتلافها وأكيد أن من يقوم بهذه الأفعال لا يمكن أبدا أن ينتمي إلى خانة الأغبياء، بل أنه ذو ذهن متقد نشيط يمكنه من التغلب على الوسائل التكنولوجية ولا تعجزه شفاراتها.

ب-الخبرة والمهارة: فمستوى الخبرة والمهارة الي يكون عليها مرتكب هذه الجرائم هي التي تحدد الأسلوب الذي ترتكب به ، والمقصود بالمهارة هي أن يكون له مستوى من العلم والدراية في التعامل في مجال المعالجة الآلية للمعلومات، وكذا الإلمام بالمهارات والمعارف التقنية التي يجب توفرها حتى يتم تنفيذ العمل الإجرامي والتي قد يكتسبها عن طريق الدراسة المتخصصة أو بواسطة الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو حتى عن طريق التفاعل الاجتماعي مع الآخرين،[2] فكلما كانت مهارته محدودة كانت جرائمه تتسم بالبساطة كجريمة الإتلاف مثلا أو النسخ.

كما تساعده المهارة التي يتميز بها على تكوين صورة عن جرائمه، إذ يكون بإمكانه أن يطبقها على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذها حتى لا يتفاجأ بأمور غير متوقعة من شأنها

[1] بشرى غربي ، مرجع سابق، ص 104.

[2] نصيرة بوحزمة ، مرجع سابق، ص ص 40، 41.

إفشال مخططاته أو الكشف عنها، فعادة ما يلجأ إلى التمهيد لإرتكاب جرائمه بالتعرف على المحيط الذي تدور فيه وكذا الظروف التي تكون محيطة بها وإمكانيات نجاحها واحتمالات فشلها ويساعده في ذلك درجة المهارة التي يتمتع بها،[1] وكأنه بذلك يقوم بدراسة نظرية تشمل تقدير نسبة النجاح وكذا العوامل التي تعيق تنفيذ هذه الجرائم والتي تحول دون تحقق ما يصبو إليه، ويعتبر المجرمين الموظفين في هذه الشركات أكثر مهارة من غيرهم باعتبار أن لديهم نظرة مسبقة عن المحيط الذي يريدون تنفيذها فيه.

ت–يخشى كشف جرائمه: المعروف عن مرتكب الجرائم الإلكترونية في إطار شركات المساهمة هو أنه يعتريه خوف دائم خشية إنكشافها ، وبالتالي يفضح أمره، مما قد يتسبب في فقدان وظيفته ومركزه،[2] و الشيئ الذي قد يعرضه إلى إكتشاف جرائمه هو جملة العوامل التي قد تفاجئه أثناء تنفيذها والتي لم تكن في الحسبان، أما عن أهم الأسباب التي تساعده على نجاحها هي طريقة عمل الحواسيب بحيث تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها،[3] ما ينبغي أن نشير إليه هو أنه حتى في حالة إكتشافها تكون هناك صعوبة في الوصول إلى مرتكبها، فالشخصية المستعارة تظلل جهات التحقيق وتصعب عليهم مهمة الوصول إلى الفاعل الحقيقي.

ث– السلطة على النظام المعلوماتي: بحيث يقصد بهذه السلطة الحقوق والمزايا التي يتمتع بها مرتكب الجرائم الإلكترونية في هذه الشركات والتي تمكنه من إرتكابها ،[4] فأغلبية مرتكبيها تكون لهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة،[5] كسلطتهم مثلا في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي لعهم إمكانية فتح الملفات وقراءتها وكتابتها وكذا محو المعلومات،[6] الشيئ الذي يدفعهم إلى إستغلال هذه السلطة فيقومون بتدوين بيانات

---

[1] نعيم سعيداني ، مرجع سابق، ص 52.

[2] نهلا عبد القادر المومني ، مرجع سابق، ص 79.

[3] حمزة بن عقون ، مرجع سابق، ص 31.

[4] عائشة بوخبزة ، مرجع سابق، ص 26.

[5] فتيحة رصاع ، مرجع سابق، ص 55.

[6] عبد السلام محمد المايل ، عادل محمد الشريجي ، (الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم الأسباب سبل المكافحة مع التعرض لحالة ليبيا)، مجلة أفاق للبحوث والدراسات، ع 4، الصادر في جوان 2019، ص 247.

وهمية لا أساس لها من الصحة، والمثال الذي يمكن تقديمه هو مثل المسؤول المشرف على الموظفين في مصالح المحاسبة وصرف الأجور فيقوم بإدراج أسماء موظفين وهميين ضمن قائمة الموظفين ثم يمرر عملية صرف الراوتب ويتولى إيداع رواتب الموظفين الوهميين في حسابه الخاص،[1] نتيجة لذلك ينبغي على شركات المساهمة أن لا تمنح لموظفيها سلطة مطلقة على نظامها المعلوماتي لأن تلك السلطة تستخدم ضدها لاحقا وتكلفها الكثير.

ج-عدم الشعور بالذنب وتبرير الجريمة: أهم ما يميز مرتكب هذه الجرائم هو أنه لا يعتريه أي إحساس أو شعور بأنه مذنب، فهو يبرر جريمته خاصة تلك التي تتعلق بالدخول غير المصرح به طالما أنه لم يترتب عنها الحرمان المطلق من الملكية،[2] فارتكاب الجرائم عن بعد دون أن تكون هناك إراقة دماء تبعث داخله إحساس بمشروعية أفعاله، نجد هذا خاصة عند تلك الطائفة من المجرمين الذين يكون لديهم ولع بقهر التقنية المعلوماتية لأن هدفهم يكون مركز على التفوق على النظام المعلوماتي وليس إلحاق الضرر بهذه الشركات.

وفي هذا الصدد يقول الأستاذ "باركر" وهو أحد أهم الباحثين الذين عنوا بالجرائم الإلكترونية بشكل عام وبمرتكبيها بصفة خاصة، أن الفاعل في هذه الجرائم لا يتصور أن سلوكه يمكن أن يتصف بالإجرامي وأن يستتبع ذلك توقيع العقاب عليه، فمن خلال لقائه بإثنين من المحكوم عليهم بسبب إستعمال الحواسيب الخاصة برؤسائهم لأغراض شخصية وهو ما يندرج تحت جريمة الإستعمال غير المصرح به للنظام المعلوماتي، ذكر المتهمان أن ما فعلاه هو سلوك شائع ومقبول في المؤسسة التي يعملان بها وأن العاملين في المؤسسة يقومون باستخدام النظام لأغراض شخصية بعضها لتحقيق ربح مادي.[3]

3- أنماط مرتكبوا الجرائم الإلكترونية في إطار شركات المساهمة: بعد أن قمنا بتوضيح السمات التي يتميز بها مرتكبوا الجرائم الإلكترونية في إطار شركات المساهمة نقوم الآن بعرض الأنماط المختلفة

---

[1] حسين ربيعي ، "آليات البحث والتحقيق في الجرائم المعلوماتية"،(أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016)، ص 37.

[2] عبد الإله النوايسة ، مرجع سابق، ص 86.

[3] فتيحة رصاع ، مرجع سابق.

لهم، ولكن ما تجب الإشارة إليه هو أنه ليس بالضرورة كل جاني يندرج ضمن فئة معينة وإنما يمكن للجاني الواحد أن يكون عبارة عن مزيج من عدة فئات.

أ-فئة صغار مجرمي المعلوماتية: هناك من يطلق عليهم صغار نوابغ المعلوماتية "PRANKSTERS"[1] وهم شباب لديهم ولع بالمعلوماتية والحاسبات الآلية يقومون بانتهاك ذاكرة الحواسيب للقيام بأعمال غير قانونية، حيث أنهم لا يقدرون مطلقا النتائج المحتملة لأعمالهم الإجرامية،[2] وغالبا ما تكون هذه الفئة في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أن لديهم قدرة على إقتحام كافة أنواع الأنظمة المعلوماتية ويعتقدون أن ما يقومون به لا يعد جريمة، فهم يرون بأن النظام غير قادر على حماية نفسه ليس من الخطأ إقتحامه، لذلك يعتبرون أنفسهم أبطالا يقدمون المساعدة من أجل تحديد نقاط الضعف الخاصة بالبرنامج الذي تم إقتحامه،[3] ومن بين الأمثلة عن بعض الجرائم الإلكترونية التي قامت بها هذه الفئة ما قام به شاب في ألمانيا يبلغ من العمر 19 سنة، من نسخ وإفشاء البيانات الخاصة بحاسوب إحدى الشركات مما كلفها خسارة قدرت بثلاثة وعشرون ألف مارك ألماني،[4] كذلك قضية تلاميذ المدرسة الثانوية في ولاية "مانهاتن" حيث إستخدموا طرفيات غرف الدرس للدخول إلى شبكة إتصالات ودمروا ملفات زبائن الشركة،[5] فهذه الفئة تقدم على إرتكاب الجريمة الإلكترونية بدافع التسلية دون أن تكون لديهم نية إجرامية مسبقة لذلك قد لا تبدو هذه الفئة خطيرة، لكن ما يجب الإشارة إليه هو أن خطورتها تكمن في إستغلالها من قبل جماعات إجرامية سواء باستئجارهم لتنفيذ مخططاتها الإجرامية، أو باستدراجهم للإنخراط معها وتحويلهم إلى قراصنة خطرين.

ب-فئة القراصنة: حيث أن هذه الفئة تكون على درجة عالية من الذكاء ويسمون كذلك بالمخترقين نظرا لقدرتهم على إختراق الأنظمة المعلوماتية وتنقسم هذه الفئة بدورها إلى فئتين:

---

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت د، ط ، الإسكندرية، دار الفكر الجامعي، 2007، ص 51.

[2] ضرغام جابر عطوش آل مواش، مرجع سابق، ص 39.

[3] نصيرة بوحزمة ، مرجع سابق، ص ص 46،47.

[4] نسرين محسن نعمة الحسيني ، محمد حسن مرعي ، مرجع سابق، ص 87.

[5] نعيم سعيداني ، مرجع سابق، ص 54.

-القراصنة الهواة "HACKERS": وهم المتطفلون،[1] الذين يتحدون إجراءات أمن نظم الشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وذلك بكسر الحواجز الأمنية الموضوعة لهذا الغرض،[2] ليس لديهم دوافع تخريبية وهم عادة أشخاص عاديون يشتغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الإلكترونية،[3] حيث يرون أن إختراق الأنظمة المعلوماتية تمثل تحديا لقدراتهم الذاتية، فيقومون بأعمالهم فقط من أجل إبراز مقدرتهم على إختراق المواقع الأمنية أحيانا أو لترك بصماتهم كدليل على وصولهم لتلك المواقع أحيانا أخرى،[4]

لكن ما يجب أن لا نغفله في هذه النقطة هو أن الهاكرز كان له الفضل في إكتشاف العديد من الفجوات الأمنية في الأنظمة المعلوماتية الخاصة بالشركات الأمر الذي جعلها تعمل على تطوير نظام الحماية من الإختراقات وبالتالي تجنب الوقوع في خسائر فادحة.

-القراصنة المحترفينCRACKERS:[5] تتراوح أعمار هذه الفئة ما بين 25 إلى 45 سنة وهم ممن لديهم درجات جامعية عليا في تخصصات الحاسوب والمعلوماتية، حيث يعملون كمحللي نظم ومبرمجين ولديهم دراية عالية ببرامج التشغيل ومعرفة عميقة بالخبايا والثغرات الموجود بها، تعرف هذه الفئة إنتشارا واسعا في كل من أمريكا وأوربا كما عرفت إنتشارا كذلك في المنطقة العربية،[6] فهذه الفئة لا تسعى إلى إثبات قدراتها ومهاراتها التقنية، وإنما تقوم بتنفيذ عملها بنية إلحاق أضرار بالغير وتكبيده خسائر، فعملها تسبقه نوايا إجرامية خبيثة.

---

[1] نعيم سعيداني، مرجع سابق، ص 54.

[2] نصيرة بوحزمة ، مرجع سابق، ص48.

[3] حمزة بن عقون ، مرجع سابق، ص 39.

[4] مراد يرمش ، مرجع سابق، ص 53.

[5] CRACKER مأخوذة من الفعل CRACK بالإنجليزية وتعني الكسر أو التحطيم، وهي الصفة التي يتميز بها كل شخص يمتلك قدرات متقدمة في مجال المعلومات وأنظمة التشغيل والحماية عامة وفي مجال البرمجة بشكل محدد. أنظر: عبد الغفور الوازني ، تصنيفات المجرم المعلوماتي بين تباين الدوافع واختلاف الأهداف، مقال منشور بتاريخ 2020/04/17، تاريخ الدخول: 2022/09/26متاح على الرابط: https://revuealmanara.com

[6] عفاف خذيري ، مرجع سابق، ص 25.

فالكراكر يقومون بأعمال تخريبية وغير مشروعة،[1] حيث تعتريهم رغبة في إنشاء أدوات برمجية تسمح لهم بالهجوم على أنظمة معلوماتية وإحداث تخريب وتجاوز أو تحطيم أنظمة حماية برمجية حاسوب أو شبكة معلوماتية،[2] كما أنه هاكر ولكنه خبيث كونه أكثر خطورة منه وتكمن خطورته في إقباله على إرتكاب أفعال فقط بنية إلحاق الضرر بالمجني عليه ، فالكراكر هو أكبر تهديد للنظام المعلوماتي كونه مُدمر ومخرب لا مكتشف.

ت–فئة الحاقدون: أهم ما يميز هذه الفئة أن الدافع المحرك لجرائمهم هو الرغبة في الإنتقام والثأر كأثر لتصرف هذه الشركات معهم، لذلك فإما أن يكونوا مستخدمين للنظام بصفتهم موظفين بها أي على علاقة بالنظام محل الإعتداء، أو غرباء عنه تتوفر لديهم أسباب الإنتقام من الشركات المستهدفة في نشاطهم،[3] فهذه الفئة لا يهمها مطلقا إثبات مهارتها واحترافيتها في النظام المعلوماتي ولا حتى الكسب المادي فهي تعبر عن غضبها واستيائها من الجهة المستهدفة عن طريق الإنتقام منها.

وغالبا ما تلجأ هذه الفئة إلى إستخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطياته أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدف مما يتسبب في أضرار بالغة وخسائر فادحة للشركات،[4] وتبقى هذه الفئة حريصة على إخفاء نشاطها وعدم المجاهرة بها من أجل عدم إكتشافها والتوصل إليها، كما أن المنتمين إلى هذه الفئة ليس لديهم إلمام واسع بالمجال المعلوماتي وإنما يشقون ويبذلون كل ما في وسعهم من أجل الوصول إلى نشاطهم وتحقيق الإنتقام.

ث–فئة الجواسيس: يعرف الجاسوس بأنه الشخص الذي يعمل في خفية أو تحت ستار مظهر كاذب في جمع أو محاولة جمع معلومات عن منظمة الأعمال الحربية لإحدى الدول التجارية بقصد إيصال

---

[1] بشرى حسين الحمداني ، القرصنة الإلكترونية –أسلحة الحرب الحديثة– ط 1، الأردن، دار أسامة للنشر والتوزيع، 2014، ص 20.

[2] عائشة بوخبزة ، مرجع سابق، ص 31.

[3] عبد السلام محمد المايل ، عادل محمد الشريجي ، مرجع سابق، ص 248.

[4] هبة نبيلة هروال ، مرجع سابق، ص 54.

هذه المعلومات لدولة العدو،[1] هذا بالنسبة للتعريف العام للجاسوس حيث كان يقتصر دوره على جمع الأسرار الحربية فقط، لكن نتيجة للتطور التكنولوجي لم يعد مقتصرا على ذلك فقط وإنما تطور ليصبح يشمل أيضا المجال التجاري خاصة فيما يتعلق بالأسرار التجارية لأكبر الشركات.

فالمهمة الأساسية لهذه الفئة تكون إستخبارية بحث تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها، سواء كانوا يعملون لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها،[2] ونجد بأن من يقوم بمهمة التجسس في الغالب تربطه علاقة بالجهة المستهدفة كأن يكون أحد موظفي الشركة باعتباره على دراية تامة بالأسرار الخاصة بأعمالها فيقوم بنسخها وإرسالها إلى الشركة المنافسة لها، كما أن أهم ما يميز هذه الفئة هي إحترافيتها في التعامل مع جهاز الحاسوب وكذا قدرتها على طمس معالم جريمتها لذلك لا يتم إختيار أيا كان للقيام بمهمة التجسس.

5-**فئة المخادعون:** إذ يتمتع هؤلاء بقدرات فنية عالية باعتبارهم من المختصين في المعلوماتية ومن أصحاب الكفاءات، حيث تقع معظم جرائمهم على شبكات تحويل الأموال كما يمكنهم التلاعب بحسابات المصارف أو فواتر الكهرباء والهاتف وكذا تزوير بطاقات الإعتماد أو شابه ذلك.[3]

ثانيا: شركات المساهمة كضحية للجرائم الإلكترونية:

الضحية وفقا للمعنى العام كل شخص سواء كان طبيعيا أو معنويا تعرض لضرر ما أو خسارة وذلك إما عن طريق إرتكاب فعل أو الإمتناع عنه، أما بالنسبة للضحية في الجرائم الإلكترونية فهو كل شخص أصابه ضرر مادي أو معنوي نتيجة الإستخدام غير المشروع لتقنية المعلومات،[4] حيث أن الإستعمال الواسع لجهاز الحاسوب وشبكات الأنترنت ساهم في توسيع فئات ضحايا الجرائم الإلكترونية، لتمتد إلى شركات المساهمة فلم تعد بمنأى عنها بل أصبحت مستهدفة بشكل واسع، فمرتكبوا الجرائم الإلكترونية أصبحوا ينجذبون نحوها أكثر كونها تمثل قطاع المال والأعمال.

---

[1] عزيزة رابحي ، مرجع سابق، ص 108.

[2] محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها –دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني– د ط، مصر، دار الكتب القانونية، 2014، ص 82.

[3] نسرين محسن نعمة الحسيني ، مرجع سابق، ص 91.

[4] رمزي حوحو ، منيرة بلورغي ، مرجع سابق، ص 49.

وبعد أن كان الإعتداء عليها في ظل الإجرام التقليدي صعب جدا خاصة ما يتعلق بسرقة المعلومات والأسرار التجارية، أصبح ذلك ممكنا بل ومتيسرا جدا في ظل العالم الرقمي الذي أصبح في ظله كل المعلومات تخزن إلكترونيا وهذا ما سهل عملية الوصول إليها والإعتداء عليها.

وعلى سبيل المثال فقد تكبدت البنوك الأمريكية خسائر قدرت ب 90 مليون دولار في ظل السرقة التقليدية، بينما بلغت خسائرها 12 مليار دولار في ظل الجريمة الإلكترونية،[1] وفي الجزائر فقد قدمت غرفة التحقيق بمحكمة سيدي أمحمد أنه خلال سنة 2012 تم تسجيل 07 إعتداءات على على شركات خاصة، أي ما نسبته 20% من هذه الجرائم كما تم تسجيل 04 إعتداءات ضد شركات أجنبية بالجزائر أي بنسبة 6%،[2] وهذا إن دل على شيئ فإنما يدل على تنامي الجرائم الإلكترونية بشكل ملفت للنظر في ظل هذه الشركات، وسنفصل في كيفية تعرض شركات المساهمة للجرائم الإلكترونية في الفصل الأول من الباب الثاني من هذه الدراسة ونبين أنواع هذه الجرائم التي تتعرض لها.

[1] حسين ربيعي آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 44.

[2] المرجع نفسه، ص 45.

المبحث الثاني:

الأحكام الخاصة بالجرائم الإلكترونية في إطار شركات المساهمة.

كما أشرنا في المبحث الأول فإن الجرائم الإلكترونية هي ثمرة التطور التكنولوجي ووليدته فكانت بذلك الجانب السلبي له، وبما أنها ظاهرة إجرامية ترتبط بالمجال الإلكتروني الأمر الذي أدى إلى إنفرادها وتميزها خاصة عندما تتعلق هذه الجريمة بكبرى الشركات كشركة المساهمة.

ومن خلال عملية البحث في هذه الجريمة إتضح لنا بأن الموضوع الذي تنصب عليه ذو طابع معنوي يختلف عن موضوع الجريمة التقليدية التي ترتبط بالجانب المادي الملموس، لذلك فأساليب إرتكابها مختلفة تتناسب وطبيعة موضوعها وباعتبار أن الجريمة الإلكترونية هي جريمة قائمة بذاتها مجرمة في أغلب تشريعات الدول، فإن قيامها يتطلب توفر أركان مثلها مثل أية جريمة أخرى.

وحتى نتمكن من توضيح الأحكام التي تنفرد بها الجريمة الإلكترونية في إطار شركة المساهمة سنقوم بالبحث عن محل وأساليب إرتكابها وكذا الأركان التي تتحقق بوقوعها، وذلك بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: الأحكام الخاصة بمحل الجرائم الإلكترونية والأساليب المستخدمة في إرتكابها.

المطلب الثاني: الأحكام الخاصة بأركان الجرائم الإلكترونية.

المطلب الأول:

الأحكام الخاصة بمحل الجرائم الإلكترونية والأساليب المستخدمة في إرتكابها.

إذا كان محل الإعتداء على شركات المساهمة في ظل الجرائم التقليدية ينصب على الأموال المادية بالوسائل التقليدية المعروفة، فإن الأمر تغير في ظل الجرائم الإلكترونية التي أصبحت تستهدف النظام المعلوماتي لهذه الشركات، كونه مستودعا لمعلوماتها وأسرارها التجارية والتي تفوق قيمتها قيمة الأموال المادية، كما أن الأساليب المستخدمة من أجل تنفيذ هذه الجرائم تتسم بالطابع التقني حتى تتوافق والبيئة الإفتراضية، هذا ما نوضحه من خلال هذا المطلب وذلك بالتطرق إلى محل الجريمة الإلكترونية في إطار شركات المساهمة **(فرع أول)** ثم الأساليب المستخدمة في إرتكاب الجرائم الإلكترونية في إطار شركات المساهمة **(فرع ثاني)**.

الفرع الأول:

محل الجرائم الإلكترونية في إطار شركات المساهمة.

بما أن الجرائم الإلكترونية تستهدف النظام المعلوماتي لشركات المساهمة، بمعنى هذا النظام يكون موضوعا لها وهو المعيار الذي إعتمده المشرع الجزائري –معيار المحل– من أجل تعريف الجريمة الإلكترونية كما سبقت الإشارة إلى ذلك في المبحث الأول.

ويعرف النظام المعلوماتي وفقا لإتفاقية بودابست المتعلقة بالجريمة الإلكترونية في مادتها الأولى بأنه، "أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة والتي يقوم واحد منها أو أكثر وفقا لبرنامج بالمعالجة الآلية للبيانات".

أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد عرفته في المادة الثانية فقرة 5 منها بأنه " مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

في حين عرفه المشرع الجزائري في المادة الثانية فقرة ب من القانون 09-04 بأنه" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" فنلاحظ بأن المشرع الجزائري قد أخذ بذات التعريف الذي إعتمدته إتفاقية بودابست، فقط ما تجب الإشارة إليه هو أن المشرع الجزائري إعتمد مصطلح نظام في حين إتفاقية بودابست إعتمدت مصطلح جهاز.

فكلا هاذين المصطلحين يشملان في طياتهما كافة الأجهزة الجديدة كالحواسيب المحمولة والهواتف الذكية، فلا يجب أن يفهم أن عبارة النظام المعلوماتي تقتصر على الحاسب الآلي فقط.[1]

ويعرفه السيناتور الفرنسي "THYRAUD" بأنه كل وحدة أو مجموعة من الوحدات لها القدرة على معالجة أو تخزين البرامج والمعلومات أو أجزاء الدخول والخروج أو الإرتباط، والتي تهدف إلى نتيجة محددة في هذه المجموعة وتكون موضوعا للحماية بنظام الأمن،[2] كما عرفه الفقيه خالد ممدوح

---

[1]نسمة بطيحي، "الإعتداءات ذات الصلة بالنظام المعلوماتي"، (أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر 1، 2019-2020)، ص 18.

[2]الطيبي البركة، "الحماية الجنائية لنظام المعالجة الآلية للمعطيات –دراسة مقارنة–" (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020-2021)، ص 24.

إبراهيم بأنه مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها البعض والتي تعمل على جمع البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات، والتنسيق وتأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة.[1]

في حين تم تعريفه ضمن قانون منع ومكافحة جرائم الأنترنت الروماني رقم 161-2003 في المادة 35 فقرة 1 بأنه النظام الذي يتضمن أي جهاز أو مجموعة من الأجهزة مترابطة أو ذات الصلة، واحدة أو أكثر منها، وفقا لبرنامج ينفذ المعالجة التلقائية للبيانات.[2]

وبعد عرض هذه التعريفات يمكن القول بأن النظام المعلوماتي وظيفته الأساسية هي معالجة البيانات والإحتفاظ بها من خلال تخزينها على جهاز الحاسوب بطريقة آمنة، بحيث يمكن إرسال تلك البيانات إلى أجهزة أخرى تكون ذات صلة فيما بينها أو إسترجاعها وتتم هذه العملية من خلال برنامج معد لهذا الغرض.

لذلك نجد بأن شركات المساهمة في ظل التطور التكنولوجي الذي غزى جميع الميادين أصبحت تعتمد في ممارسة نشاطاتها وإدارة أعمالها على النظام المعلوماتي، من أجل جمع ومعالجة بياناتها وتبادلها مع جهات أخرى سواء كانت شركات مثلها أو حتى عملائها من الأفراد مثل عمليات التسويق، من أجل تزويدهم بالمعلومات الخاصة بها كعلاماتها التجارية وكذا المنتجات والخدمات التي تقوم بها، أو تزويدهم كذلك بالمعلومات المتعلقة بعملية الدفع، وهذا كله بعيدا عن إستخدام أية وثائق ورقية الشيئ الذي يمكنها من ممارسة أعمالها بطريقة سهلة وتقديم خداماتها في أية نقطة من العالم، فالنظام المعلوماتي بالنسبة لشركة المساهمة أصبح العصب الأساسي لها من أجل القيام بأعمالها، لذلك قد يتعرض نظامها المعلوماتي إلى الإعتداء فتكون بذلك ضحية للجريمة الإلكترونية.

أما بالنسبة للعناصر التي يتكون منها النظام المعلوماتي، فنجد بأن المشرع الجزائري لم يتطرق إليها مقتديا في ذلك باتفاقية بودابست، غير أن التقرير التوضيحي لهذه الإتفاقية أشار إلى أن النظام

---

[1] نسيمة جدي، مرجع سابق. ص ص 16، 17.

[2] محمد بن فردية، "الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية"، (أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2015)، ص 29.

المعلوماتي يتكون من مكونات مادية وأخرى معنوية تهدف إلى المعالجة الآلية للمعطيات المعلوماتية.[1]

وبالتالي فإن النظام المعلوماتي يتكون من جزئين كيان منطقي وكيان مادي وكلاهما معرض لأن يكون محلا للإعتداء الإلكتروني.

ففي حالة ما إذا كان المحل هو الكيان المادي، والذي يتكون أساسا من جهاز الحاسوب وما يشمله من ملحقات ووسائط توصل به والتي من خلالها يتم تلقي المعطيات والمعلومات وكذا إخراج النتائج بعد المعالجة،[2] ففي هذه الحالة نكون بصدد جريمة تقليدية ولا تثار أية مشكلة باعتبار أن هذه المكونات المادية مشمولة بالحماية الجنائية ضمن نصوص قانون العقوبات على أساس أنها معرضة للسرقة أو الإتلاف العمدي كالتكسير مثلا.

لذلك فهي تعتبر من قبيل الأموال المنقولة التي تخضع في سرقتها وإتلافها للنصوص التقليدية وليس هناك إشكال فيما يخص تطبيق هذه النصوص على هذه الأموال،[3] والحديث عن الإعتداءات التي يتعرض لها الكيان المادي في نطاق ظاهرة الجريمة الإلكترونية يتعلق فقط بقيمتها الإستراتجية باعتبارها مخزن للمعلومات وأدوات لمعالجتها وتبادلها، الأمر الذي يستدعي تطوير آليات حمايتها ويكون ذلك في نطاق النصوص التقليدية لا في نطاق ظاهرة الجريمة الإلكترونية.[4]

لكن الإشكال الذي يثور في مسألة محل الجريمة الإلكترونية هو عندما يتعرض الكيان المنطقي أو المعنوي لهذه الجريمة فيكون محلا لها، وهذا هو الشيئ المستجد في هذه الجريمة فلو لا ذلك لما كنا أمام جريمة مستجدة، كونها تستهدف المعلومات بمعزل عن وعائها المادي المخزنة فيه وذلك بغية إستهداف الكيان المنطقي الذي يعتبر بمثابة روح للنظام المعلوماتي والسيطرة عليه دون إذن صاحبه، حيث أن ذلك الكيان المنطقي هو مال معلوماتي.

---

[1] نسمة بطيحي ، مرجع سابق، ص 21.

[2] نبيل دريس، مرجع سابق، ص 25.

[3] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، ط1، الإسكندرية، دار الفكر الجامعي، 2019، ص 30.

[4] يونس عرب، جرائم الكمبيوتر والأنترنت، مداخلة مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، المنعقد في 2002/12/10، أبو ظبي.

وإذا كان الكيان المادي الذي يمثل المال الطبيعي مشمولا بالحماية الجنائية في أغلب تشريعات الدول كما سبق الإشارة إلى ذلك، فإن الحاجة أصبحت ملحة وضرورية من أجل توسيع هذه الحماية لتشمل كذلك المال المعلوماتي، واعتباره من القيم المالية التي تستوجب الحماية خاصة عندما يتعلق الأمر بالمال المعلوماتي للشركات الكبرى وعلى رأسها شركة المساهمة، فالقيمة الاقتصادية لهذا المال في إطار هذه الشركات تفوق بكثير قيمة المال المادي، نظرا للقوة التي يشكلها لشركات المساهمة الأمر الذي جعلها تتهافت وتتسارع فيما بينها على هذه الأموال المعلوماتية، وباعتباره يشكل لها قوة يجعلها تتبوأ الريادة في مجال الاقتصاد والمال كان محل إعتداء حتى من طرف الأفراد.

حيث أن إستهداف شركات المساهمة في مالها المعلوماتي يشكل أكبر خطر يقع عليها فالخسائر التي تتكبدها وتنجر عنه تتجاوز الخسائر التي تصيبها جراء الإعتداء التقليدي عليها، ونجد بأن المادة الخام لهذا المال هي المعلومات بكل أنواعها من بيانات ومعطيات وكذا البرامج، وما تجب الإشارة إليه هو أن هذا الكيان المنطقي أثار مشكلات قانونية وعلى رأسها تأخر بعض الأنظمة القانونية بالإعتراف بالمعلومات كقيم مالية، ولمعرفة أحكام هذا المحل نتطرق إلى تعريف المعلومات ثم تحديد طبيعتها القانونية.

أولا: تعريف المعلومات.

نجد بأن المعلومات في المدلول اللغوي مشتقة من لفظ "علم" والتي تعني العلم، الإحاطة ببواطن الأمور والوعي، الإدراك واليقين، الإرشاد، الإعلام، الشهرة، المعرفة، الدراية...إلخ من المعاني، "INFORMATION" هي المقابل الإنجليزي لكلمة معلومات وهذه الكلمة الإنجليزية مشتقة من اللاتينية "INFORMATION" التي تعني في الأصل عملية الإتصال أو ما يتم إيصاله أو تلقيه[1].

كما أن هناك معنى آخر للمعلومات مشتق من التصور "INFORMATUM" والذي يعني الرسم أو التخطيط، إلا أن هاذين المصطلحين وجهان لحقيقة واحدة الأول يوضح الجانب الحركي للمعلومة في حين الثاني يوضح الجانب الوصفي لها.[2]

[1] عفاف خذيري، مرجع سابق، ص 16.

[2] فتيحة رصاع، مرجع سابق، ص 26.

تعرف أيضا بأنها مجموعة الرموز أو المفاهيم والتعليمات التي تصلح لأن تكون محلا للتبادل والإتصال أو التفسير والتأويل أو المعالجة، سواء بواسطة الأفراد أو الأنشطة الإلكترونية وتمتاز بالمرونة بحيث يمكن تغييرها أو تجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة[1].

كما تعرف أيضا بأنها كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو إستقراء دلالاتها أو إستنتاج ما يمكن إسنتاجه منها وحدها أو متداخلة مع غيرها، أو تفسيرها على نحو يثري متخذي القرار ومساعدتهم على الحكم السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية،[2] وهي أيضا تعبير يستهدف جعل رسالة معينة صادرة من شخص معين قابلة للتوصيل إلى شخص آخر، وذلك بفضل علاقة أو إشارة من شأنها أن توصل المعلومة للغير،[3] فالمعلومات عبارة عن رسالة لها معنى وقيمة مالية بحيث تكون هذه المعلومات قابلة للنقل والإسترجاع أو التداول بمختلف الوسائل.[4]

بعد عرض هذه التعريفات يمكن لنا أن نقدم تعريف للمعلومات بأنها كل ما يمكن أن يكون محلا للتبادل بحيث يمكن تخزينه أو إرساله من خلال النظام المعلوماتي، وذلك مهما كان الشكل الذي تتخذه سواء كان رموزا أو صورا ويكون ذا قيمة.

أما فيما يخص تعريف التشريعات للمعلومات فنجد المشرع الفرنسي قد عرفها لأول مرة من خلال القانون الصادر في 29 يوليو 1982 بشأن الاتصالات السمعية والبصرية بأنها، رنين صور الوثائق والبيانات أو رسائل من أي نوع فهي تعني رمزا أو مجموعة رموز تخطو على إمكانية الإفضاء إلى المعنى.[5]

---

[1] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، ص 120.

[2] حمزة بن عقون، مرجع سابق، ص ص 131،132.

[3] سمير بردال، (خصوصية الجرائم المرتبطة بنظام الحاسب الآلي ومظاهر تمييزها عن الجرائم التقليدية)، مجلة البحوث في الحقوق والعلوم السياسية، ، ع 4، مج 2، الصادر في أكتوبر 2016)، ص 88.

[4] صورية بوربابة، "قواعد الأمن المعلوماتي –دراسة مقارنة–" (أطروحة مقدة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، 2015–2016) ص 14.

[5] نصيرة، بوحزمة مرجع سابق، ص 57.

كما عرفها المشرع الأمريكي في قانون المعاملات التجارية الإلكترونية لسنة 1999 بأنها، تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.[1]

أما بالنسبة للمشرع الجزائري فنجد بأنه قد إعتمد على مصطلح معطيات بدلا من مصطلح معلومات وذلك تأثرا بنظيره الفرنسي الذي درج على إعتماد مصطلح معطيات "DONNEE" بدلا من مصطلح "INFORMATION" منذ إصداره لقانون الغش المعلوماتي سنة 1988،[2] وقد ورد تعريف المعطيات في القانون 09-04 وذلك من خلال نص المادة الثانية فقرة ج التي عرفتها بأنها "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" ونجد بأن هذا التعريف هو ذاته الذي ورد في المادة الأولى فقرة ب من إتفاقية بودابست المتعلقة بمكافحة الجريمة الإلكترونية، فالشيء الملاحظ على التعريف الذي جاء به المشرع الجزائري هو تعريف يتسم بالعمومية يفتقد إلى الدقة التي تتسم بها المعلومة.

فإذا كانت المعلومات عبارة عن مادة معنوية فإن المعطيات تكون هي القالب المادي الذي تتجسد فيه المعلومات، بمعنى أن المعطيات هي عرض للمعلومات بطريقة آلية، فالعلاقة بين المصطلحين تتمثل في أن المعطيات هي عبارة عن معلومات، إلا أن المعلومات لا تمثل بالضرورة معطيات معلوماتية فيمكن للمعلومة أن تتجسد في شكل آلي يمكنها أيضا أن تتجسد في شكل آخر،[3] فمن خلال التعريف السابق للمشرع الجزائري نجد بأنه قد أقر هذا التمييز وذلك حينما عرف المعطيات بأنها عبارة عن عملية عرض للمعلومات، وبالتالي فالنتيجة المترتبة على ذلك هي أن المعطيات تمثل القالب بالنسبة للمعلومات.

كذلك ينبغي علينا أن نشير إلى أن المعلومات تختلف عن البيانات والتي هي عبارة عن مجموعة من الحقائق، أو القياسات أو المعطيات التي تتخذ صورة أرقام أو حروف أو رموز أو أشكال

---

[1] فتيحة رصاع ، مرجع سابق، ص 27.

[2] نسمة بطيحي ، مرجع سابق، ص 24.

[3] المرجع نفسه ، ص 25.

خاصة وتعبر عن فكرة أو موضوعا أو حديثا أو هدفا معينا، فهي المادة الخام التي يتم تحويلها عن طريق الحاسوب بغرض إستخراج معلومات معينة،[1] حيث تسمى العلاقة بين المعلومات والبيانات بالدورة الإسترجاعية، وذلك من خلال عملية تجميع وتشغيل البيانات للحصول على المعلومات ثم تستخدم في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات والقيام بتجميعها ومعالجتها مرة أخرى يؤدي إلى الحصول على معلومات إضافية يستند عليها في إصدار قرارات جديدة.[2]

كما تعرف البيانات بأنها حقائق تعبر عن مواقف وأفعال معينة وذلك إما عن طريق كلمات أو رموز، والبيانات على هذه الصورة لا تفيد في شيئ وإنما وجب الأمر تحليلها وإجراء العملية الحسابية والمنطقية عليها، بمعنى معالجة البيانات للإستدلال منها على مجموعة من المعلومات وبذلك تتحول تلك البيانات إلى معلومات، فهي تعتبر النتيجة النهائية التي تترتب على تشغيل البيانات وتحليلها أو إستقراء دلالتها واستنتاج ما يمكن إستنتاجه منها، فالبيانات هي مدخلات الحاسب الآلي التي تمثل الخادمات التي يتم تشغيلها والمعلومات هي المخرجات بعد عملية المعالجة،[3] وبذلك تكون المعلومات هي المعنى المستخلص من البيانات، وبعبارة أخرى المعلومات عبارة عن بيانات تمت معالجتها وأصبحت لها دلالة.

أما بالنسبة للبرامج فنجد بأن شركات المساهمة لا تقتصر في إهتمامها على إختيار الأجهزة المادية للحاسوب، وإنما تركز إهتمامها كذلك على حسن إختيار البرامج والتي تكون بطبيعة الحال مناسبة لتشغيل جهاز الحاسوب، كون تلك البرامج هي التي توجه جهاز الحاسوب إلى أن يعمل وفق طريقة معينة وذلك بهدف الحصول على نتائج معينة ومحددة،[4] فنجد بأن جهاز الحاسوب لا يقوم بعمله إلا من خلال تضمنه مجموعة من البرامج تمكنه من القيام بعمليات مختلفة عند إعطائها أوامر بذلك.[5]

---

[1] خضرة شنتير ، مرجع سابق، ص 19.

[2] حمزة بن عقون ، مرجع سابق، ص 132.

[3] نصيرة بوحزمة ، مرجع سابق، ص ص 57،58.

[4] نسمة بطيحي ، مرجع سابق ، ص 26.

[5] نصيرة بوحزمة ، مرجع سابق، ص 59.

حيث تقوم البرامج بإرسال الأوامر إلى جهاز الحاسوب فيقوم بتنفيذها وذلك بناءا على توجيهات المستخدم،[1] وقد تطرقت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى تعريف البرنامج المعلوماتي، وذلك من خلال مادتها الثانية فقرة 5 بأنه عبارة عن مجموعة من التعليمات والأوامر قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما، كما ورد تعريفه في التقرير التوضيحي لإتفاقية بودابست، بأنه عبارة عن مجموعة من التعليمات تنفذ من خلال جهاز الحاسوب وذلك بغية تحقيق الغاية المرجوة، أما بالنسبة للمشرع الجزائري فنجد بأنه لم ينص صراحة على تعريف البرنامج المعلوماتي غير أنه أشار إليه بطريقة ضمنية وذلك عندما تطرق إلى تعريف المنظومة المعلوماتية من خلال إدراجه لعبارة "تنفيذا لبرنامج معين" وبطبيعة الحال فإن في هذا تنويه إلى أن المعلومات تتم معالجتها بواسطة البرنامج المعلوماتي، فالبرامج تعد بمثابة العقل المدبر للحاسوب.

أما بالنسبة لإستخدام هذه البرامج في شركات المساهمة فهي تعتمدها بشكل واسع من أجل تسهيل إنتقال المعلومات بين مختلف الأقسام والفروع التابعة لها، فمثلا يمكنها إعتماد برنامج يكتفي بكتابة حروف مختصرة من أسماء زبائنها الأمر الذي يجعلها تحافظ على قائمة عملائها فتصعب مهمة الوصول إليهم، كما أن إستخدام البرامج يساعدها على إسترجاع المعلومات المتعلقة بقائمة وحجم مبيعاتها وذلك بعد أن كانت في السابق تعتمد في الحصول على تلك المعلومات بطريقة يدوية، الأمر الذي يتطلب منها جهدا مضنيا ووقتا طويلا بالإضافة إلى إمكانية تعرض تلك المعلومات إلى الإتلاف وبطريقة سهلة إذ لا حاجة لها في إعتماد أجهزة حواسيب دون برامج معلوماتية، والتي تمكن شركة المساهمة من ترتيب معلوماتها وإظهارها وقت الحاجة إليها بطريقة تخدم أهدافها الرئيسية.

وتعطي "أليسون وتباي" خبيرة في أنظمة المعلومات الذكية مثالا يتعلق بتثبيت أوامر الشراء، كان هناك موظف في الشركة يتلقى أمرا بالشراء ولكن بيانات النظام تشير إلى أن هذا الزبون لم يقم بتسديد فاتورته الأخيرة، فهنا وبدلا من إيقاف أمر الشراء فإنه ومن خلال البرنامج المعلوماتي يحدد ما إذا كان ذلك الزبون يعد من كبار المشترين فعلا أو أنه من الممكن أن يتسبب في إحداث مشاكل وأضرار للشركة، فالمعلومات المتوفرة في البرنامج تسهل على الموظف عملية الحصول على

[1] نسيمة جدي ، مرجع سابق. ص 20.

معلومات أكثر حول ذلك الزبون، وبالتالي يمكن للموظف إتخاذ قرار مستنير حول ما إذا كان عليه تلبية أمر الشراء أم لا.[1]

وبعد التطرق إلى شرح هذه المصطلحات ومن خلال الإطلاع على بعض المراجع التي تناولتهم، تبين لنا بأن هناك ترابط فيما بينهم باعتبارهم المادة المكونة للنظام المعلوماتي خاصة في ظل التطورات التي تشهدها تكنولوجيا المعلومات.

لذلك فالنقطة التي تثير الاهتمام هنا هو حماية هذا المال المعلوماتي خاصة وأن الجريمة الإلكترونية تستهدف شركة المساهمة في معلوماتها، كون أن هذه الأخيرة تشكل ثروة مالية وذات قيمة إقتصادية عالية باعتبارها تضم أسرار أعمالها وتعاملاتها، لذلك وحتى تكون هذه المعلومات محلا للجريمة الإلكترونية لا بد أن تتوفر على شروط فطبيعة الحال ليس كل المعلومات قابلة لأن تكون محل إعتداء إلكتروني.

1-التجديد والإبتكار: بالنسبة للتجديد الشيئ البديهي والمتعارف عليه هو أنه حتى يكون هناك إعتداء لا بد أن يقع على شيئ محدد بذاته، بمعنى أن تكون هناك إمكانية لحصر ذلك الشيئ ضمن نطاق معين وإلا فلا حديث عن وقوع إعتداء وكذلك الأمر بالنسبة لمعلومات شركة المساهمة، فلكي تكون ذات معنى حقيقي ومحلا للجريمة الإلكترونية لا بد أن تكون محددة "PRECISE" فعدم التحديد معناه عدم وجود المعلومة أساسا وانعدام يؤدي إلى إنعدام المحل، الذي يترتب عليه إنتفاء وقوع الجريمة الإلكترونية.

وهذا الصدد نجد الأستاذ "CATALA" يذهب إلى القول بأن المعلومة وقبل كل شيئ تعبير وصياغة مخصصة من أجل تبليغ رسالة أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل رسالة إلى الغيير[2] ، أما أن تكون المعلومة مبتكرة " L'INFORMATION ORIGINALE" فالمقصود بالإبتكار الإنتاج الذهني الذي يتميز بالجدة والأصالة والذي تبرز من

---

[1] كيف تحقق الشركات الإستراتجية المعلوماتية من أنظمة البرمجيات الذكية، جريدة العرب الاقتصادية الدولية، مقال منشور بتاريخ 1 ماي 2009، تاريخ الدخول 2022/12/04، متاح على الرابط: https://www.aleqt.com

[2] سمير بردال ، مرجع سابق، ص 89.

خلال شخصية صاحبه،[1] حيث تتميز عن باقي المعلومات المتاحة باعتبارها نتاج فكري خاص،[2] فكون المعلومة مبتكرة معناه أنها غير موجودة في السابق، أما أن تكون شائعة بين الناس ومتداولة فيما بينهم بحيث يمكن لأي شخص أن يصل إليها ففي هذه الحالة لا تعتبر معلومة حقيقية تحظى بالحماية وتكون محلا للإعتداء، وفيما يتعلق بشركة المساهمة فهي تحوز على العديد من المعلومات المبتكرة خاصة عندما يتعلق بطريقة تصنيع منتوج معين مثلا.

2-السرية والإستئثار: بالنسبة لصفة السرية يجب أن تكون ملازمة للمعلومة حتى تكون محل إعتداء للجريمة الإلكترونية، لذلك فصفة السرية تقتضي ضرورة الإحتفاظ بالمعلومة والحرص على عدم إشاعتها فتصبح بذلك معلومة مباحة يحوزها الجميع، وسرية المعلومة في إطار شركة المساهمة معناه عدم إفشاء أسرارها التجارية إلى منافسيها من الشركات الأخرى.

فنجد مثلا شركة كوكاكولا للمشروبات الغازية قد نجحت في الإحتفاظ بسرية الوصفة التي تتضمن تركيبة المواد التي تستعمل في صناعة مشروبها وذلك لفترة تزيد عن القرن، حيث أن تلك الوصفة مودعة لدى بنك معلومات في ولاية أطلنطا بالولايات المتحدة الأمريكية ويمنع على الغير الإطلاع عليها إلا بقرار من مجلس إدارة الشركة، وهي معروفة فقط لدى عدد محدد من كبار العاملين في الشركة، ومن أجل الحفاظ على سرية الوصفة قامت بسحب إستثمارها من الهند بدلا من كشف سر وصفتها وذلك عندما طلب منها أن تتخلى عن الإدارة للجانب الهندي ونقل التكنولوجيا لهم.[3]

وسرية المعلومة لا يعني عدم العلم المطلق وإنما يمكن لبعض الأشخاص الإطلاع عليها وذلك نتيجة العمل الذي يقومون به داخل الشركة، كالشركاء شرط أن يلتزموا هم أيضا بالمحافظة على سريتها فالسرية المقصودة هي سرية النسبية،[4] وتتجلى أهمية سرية معلومات شركة المساهمة في أنها

---

[1] إسماعيل بن يحي ، مرجع سابق، ص 42.

[2] دلال مولاي ملياني ، مرجع سابق، ص 19.

[3] شهرزاد لكحل ، ميلود سلامي ، (الأسرار التجارية وأثرها على نقل التكنولوجيا) مجلة الإجتهاد القضائي، ع 28، مج 13، الصادر في نوفمبر 2021، ص ص 535،536.

[4] عبد العزيز زردازي ، (الأسرار التجارية في التشريع الجزائري)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 2، مج 6، الصادر في ديسمبر 2021، ص ص 765،766.

تكسبها قدرة تنافسية كبيرة في مواجهة غيرها من الشركات، فكلما كانت المعلومات سرية أكثر كلما زادت قيمتها الاقتصادية مما يجعل الغير يتهافت على الحصول عليها بأية طريقة.

أما بالنسبة لخاصية الإستئثار في المعلومات فهي ضرورية كون الفاعل يقوم بالإعتداء على حق مملوك للغير وذلك على سبيل الإستئثار،[1] ومعناه أن تكون المعلومة خاصة بأحد الأشخاص وله سلطة التصرف في تلك المعلومة التي تخصه، ففي حالة الإعتداء عليها نجد بأن الفاعل يستأثر بسلطة تخص الغير بصفة مطلقة،[2] لذلك حينما يتم الإعتداء الإلكتروني على المعلومات التجارية لشركة المساهمة والتي تكون هي صاحبة السلطة في التصرف في تلك المعلومات فإن الجاني باعتدائه يكون قد إستأثر بسلطة تخص هذه الشركة، فخاصية الإستئثار لا غنى عليها حتى تستكمل المعلومات التجارية الخاصة بشركة المساهمة عناصرها القانونية.

ثانيا: الطبيعة القانونية للمعلومات.

ثار خلاف حول تحديد الطبيعة القانونية للمعلومات وذلك على أساس إعتبارها محلا يقع عليه الإعتداء وهي ذات طبيعة غير مادية مستقلة تماما عن الوسائط المادية التي تفرغ فيها، مما أدى إلى تباين المواقف حول ما إذا كان يمكن إدراجها ضمن القيم المالية التي تكون محلا قابلا للإعتداء وهناك موقفين:

1-الموقف الأول: ويمثله الفقه التقليدي إذ يرى بأن المعلومات ذات طبيعة من نوع خاص وذلك على أساس أن وصف القيمة ينطبق فقط على الأشياء المادية،[3] والتي تكون وحدها قابلة للتملك والإستئثار،[4]معنى ذلك أن الأشياء القابلة للإستئثار تدرج ضمن القيم المالية، وبالنظر إلى المعلومات نجد بأنها ذات طبيعة معنوية الشيئ الذي يترتب عليه عدم إمكانية الإستئثار بها، وبالتالي إخراجها من دائرة القيم المالية التي تحظى بالحماية القانونية.

---

[1] سمير بردال ، مرجع سابق، ص 90.

[2] فتيحة رصاع ، مرجع سابق، ص 31.

[3] سمير بردال ، مرجع سابق، ص 90.

[4] صابرين يوسف عبد الله الحياني، مرجع سابق، ص 22.

فلا يمكن إعتبار المعلومات ذات قيمة مالية إلا ما تعلق بحقوق الملكية الأدبية أو الفنية أو الصناعية،[1] لكن ما تجب الإشارة إليه أن ذلك لا يعني إستبعاد باقي المعلومات وتركها دون حماية في حالة الاستيلاء عليها، وإنما المسؤولية التي تقوم حينها تكون وفقا لقواعد المسؤولية المدنية التي تستند إلى نص المادة 1382 من القانون الفرنسي،[2] فالفقه الفرنسي حاول إيجاد حماية قانونية للمعلومات ولك من الناحية المدنية.

2-الموقف الثاني: أدى التطور الحاصل في تكنولوجيا المعلومات بالفقه الحديث إلى تبني معيار آخر غير معيار مادية المال لذلك تم إعتماد معيار القيمة الاقتصادية للشيئ،[3] ووفقا لهذا الإتجاه فإنه يمكن إعتبار المعلومات أموالا منقولة وبالتالي يمكن تقويمها بالمال وذلك إنطلاقا من القيمة الاقتصادية لها،[4] بل نجد أحيانا أن القيمة الاقتصادية للمعلومات تفوق وتتجاوز بشكل كبير قيمة المال المادي، الشيئ الذي جعلها مستهدفة بشكل أكبر منه من أجل الإعتداء عليها لذلك وجب إخضاعها للحماية القانونية.

من أنصار هذا الإتجاه الأستاذ " CATALA" الذي يرى بأن المعلومة شبيهة بالسلعة باعتبارها من إنتاج الفكر البشري وهي تنتمي في الأساس إلى من يحوز على المكونات الأساسية لها وذلك بطريقة مشروعة ويجب وضعها في شكل يسهل إمكانية الإطلاع عليها وتبليغها بشكل مفهوم[5].

ومن أجل إضفاء القيمة المالية على المعلومة فقد إعتمد الأستاذ "CATALA" على حجة القيمة الاقتصادية للمعلومة والتي من الممكن أن تقوم بسعر السوق، وأيضا حجة التبعية وهي العلاقة التي تربط بين المعلومة ومؤلفها، أي العلاقة بين المالك والشيئ المملوك وبالتالي يكون لصاحبها الحق في سرية المعلومة والتعريض في حالة أي عمل غير مشروع يمسها[6].

---

[1]عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة، 2011-2012) ، ص 20.

[2]صورية بوربابة ، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 27.

[3]حمزة بن عقون ، مرجع سابق، ص 135.

[4]نعيم سعيداني ، مرجع سابق، ص 39.

[5]عبد اللطيف معتوق ، مرجع سابق، ص 20.

[6]فتيحة رصاع ، مرجع سابق، ص 34.

أما في الفقه العربي فنجد الأستاذ " محمد سامي الشوا" والذي أكد على أن المعلومة وإن كانت مستقلة عن كيانها المادي إلا أنها تعد ذات قيمة رغم طابعها المعنوي وأنه يمكن إدراجها ضمن القيم المالية التي تكون لها قابلية الحيازة غير المشروعة كونها ذات قيمة إقتصادية تتطلب حماية قانونية من الإعتداءات وأهمها الإعتداء على الأموال،[1] ومن بين القضايا التي أكدت صلاحية المعلومات لأن تكون محلا للإعتداء الإلكتروني وبالتالي إعتبارها قيمًا مالية ذات قيمة إقتصادية مهمة، قضية "ANTONIOLLI" والتي من خلالها كانت محكمة النقض الفرنسية قد أبدت حكما قضت فيه بإدانة محاسب شركة وذلك بسبب قيامه بإطلاع شركة أخرى منافسة على معلومات تتضمن جداول وخطوط بيانية. حيث تم إعتبار ذلك سرقة كون المعطيات المسلمة إلى الغير تشكل أموالا تعود ملكيتها إلى الشركة الأولى دون سواها.[2]

وأمام تضارب الأراء حول الطبيعة القانونية للمعلومات فإن موقفنا من هذه الفكرة يذهب إلى تأييد الإتجاه الثاني، حيث أن القيمة الاقتصادية للمعلومات تفرض إخضاعها للحماية القانونية خاصة في ظل التسارع التكنولوجي حيث أصبح التسابق نحو إكتساب المعلومة أكبر من التسابق نحو المال المادي، كما أن هذه المعلومات رغم طابعها المعنوي إلا أنه يمكن إفراغها في شكل مادي مثل المطبوعات والأقراص الليزرية، فالمعلومات هي إحدى القيم المستحدثة التي أفرزتها الثورة المعلوماتية، فلا قيمة للشكل الخارجي للمعلومات بمعزل عن قيمتها الاقتصادية التي تشكل جوهرها خاصة عندما يتعلق الأمر بالمعلومات الخاصة بشركات المساهمة، حيث أن هذه الشركات تكون ضحية الإعتداء على معلوماتها وذلك نظرا لقيمتها الاقتصادية الكبيرة، فالحصول على تلك المعلومات قد يؤدي إلى تدميرها والقضاء على تواجدها رغم أنها لم تستهدف في مالها المادي وهذا إن دل فإنما يدل على أن قيمة المعلومة تفوق قيمة المال المادي.

---

[1] سمير بردال، مرجع سابق، ص 92.

[2] حمزة بن عقون ، مرجع سابق، ص ص 135،136.

الفرع الثاني:

الأساليب المستخدمة في إرتكاب الجرائم الإلكترونية في إطار شركة المساهمة.

إذا كان الإعتداء على الكيان المادي للنظام المعلوماتي لشركات المساهمة يندرج ضمن نطاق الجرائم التقليدية حيث يتم الإعتداء عليه بوسائل تقليدية كتحطيمه أو سرقته أو حرقه، إلا أن هذه الأساليب تصبح غير مناسبة حينما يكون محل الإعتداء هو المعلومات المخزنة في النظام المعلوماتي، إذ أن التطورات التكنولوجية الحديثة في تقنية المعلومات مكنت المجرم الإلكتروني من إختراع أساليب وتقنيات جديدة تتناسب مع الكيان المنطقي الذي ينوي الإعتداء عليه، لكن ما ينبغي الإشارة إليه هو أن هذه الأساليب الفنية التي يستخدمها لتدمير الكيان المنطقي للنظام المعلوماتي كثيرة ومعقدة ومن الصعب حصر أنماطها عمليا وحتى لو أمكن ذلك في الوقت الحاضر إلا أنه من غير الممكن التنبؤ بالأساليب التي قد تسفر عنها التكنولوجيا في المستقبل وذلك نظرا لسرعة تطور هذا المجال.

لذلك من خلال هذا الفرع سنقوم بالتركيز على أهم الأساليب التي يتم بواسطتها إختراق النظام المعلوماتي لشركات المساهمة، والإعتداء عليه حيث تتمثل تلك الأساليب في مختلف البرامج الخبيثة وسنقوم فيما يلي بالتطرق إلى أهم هذه البرامج.

أولا: الفيروسات.

وتعد الفيروسات،[1] من أهم الأساليب التي يعتمد عليها الجناة بقصد الإعتداء على هذه الشركات حيث تعرف على أنها برامج خبيثة يتم صنعها عمدا وذلك بهدف تحريف خصائص الملفات عند

[1]كلمة فيروس ليست عربية وتعني في اللغة اللاتينية " السم" أما بالإنجلزية فهي تعني كائن صغير جدا لا يرى إلا عن طريق المجهر ينقل الأمراض بين الناس، وقد أصابت الفيروسات الحاسب الآلي قبل تسميتها بهذا الإسم وأول من أطلقه عليها هو "FIEDCOHEN" عام 1983 وأول من فكر في فيروس الحاسوب هو "جون فاينومان" عام 1949 عندما طرح الفكرة الأساسية في تصميم الفيروس الإلكتروني وذلك في مقاله المنشور تحت عنوان " نظرية التعقيد الأتوماتيكي" والذي جاء فيه أن جهاز الحاسوب يمكنه أن يدمر نفسه بنفسه ولم يلق حينها هذا المقال أهمية وذلك لقلة إنتشار الحواسيب: أنظر ميرفت محمد حبابية، كتاب مكافحة الجريمة الإلكترونية –دراسة مقارنة في التشريع الجزائري والفلسطيني– د، ط، الأردن، دار اليازوردي العلمية، 2022 ص 91.

إصابتها بهذه الفيروسات، لتقوم بتنفيذ بعض الأوامر وذلك إما بالإزالة أو التعديل أو الحذف أو التخريب.[1]

فالفيروسات برامج يتم إعدادها بطريقة معينة وذلك بغية إلحاق الضرر بحاسوب آخر أو السيطرة عليه ولها قدرة على التناسخ والإنتشار،[2] حيث تعتبر الفيروسات من أهم الأساليب التي يتم إستخدامها من أجل المساس بمعطيات النظام المعلوماتي فهي تتشابه إلى حد كبير بالفيروس العضوي الذي يصيب جسم الإنسان وذلك كونها تنتقل عن طريق العدوى من جهاز إلى آخر.[3]

تعرف كذلك بأنها برنامج خبيث يتشكل من أجزاء عدة تكون مكتوبة بإحدى لغات البرمجة وذلك بطريقة تسمح لها بالتحكم في برامج أخرى ويحتاج إلى برنامج وسيط –كعائل له– أو مساحة تنفيذية على الأسطوانة،[4] وتكمن خطورته في قدرته التدميرية للكيان المنطقي إضافة إلى قدرته على إخفاء نفسه حيث تظهر آثاره بصورة مفاجئة ودون سابق إنذار ويصعب التخلص منه، وذلك من خلال إفراغ الكيان المنطقي من جميع الملفات التي يحتويها خشية أن تكون قد أصيبت كلها أو إنتقلت إليها العدوى.[5]

بعد عرض جملة هذه التعريفات نصل إلى القول بأن الفيروس المعلوماتي هو برنامج ضار يحتوي على تعليمات مبرمجة من قبل أحد المبرمجين والتي تنتشر وتتكاثر بمجرد أن يصاب بها جهاز الحاسوب، مما يتسبب في تعطيله عن القيام بوظيفته الطبيعية، وذلك إما بشكل كلي أو جزئي وبالتالي تدمير ما يحويه من معلومات وبيانات محولا بذلك جهاز الحاسوب إلى مجرد آلة صماء دون فائدة، وهذا ما يلحق أضرار بشركة المساهمة ولا يشترط أن تكون تلك الأضرار مادية وإنما قد تمس

---

[1] إيهاب خليفة، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، ط 1، القاهرة، العربي للنشر والتوزيع، ، 2019 ، ص 116.

[2] أسامة سمير حسين، الإحتيال الإلكتروني –الأسباب والحلول– ط 1، الأردن، الجنادرية للنشر والتوزيع، ، 2011، ص 156.

[3] ميرفت محمد حبابية، مرجع سابق، ص ص 91،92.

[4] حسين خليل مطر، (التحقيق وجمع الأدلة في الجرائم الإلكترونية) مجلة الكوفة،ع 36، مج 1، الصادر في 2018، ص 398.

[5] محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها –دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، مرجع سابق، ص 473.

سمعتها كحالة تدمير ملفات عملائها، ورغم أن النتيجة المترتبة عن الفيروس المعلوماتي هي التدمير إلا أنه قد يستعمل لتحقيق غرضين:

1-الغرض الحمائي: وذلك بغية حماية النسخ الأصلية من بيانات وبرامج من خطر النسخ غير المشروع، ففي هذه الحالة يستعيد الفيروس نشاطه بمجرد النسخ ويقوم بتدمير نظام الحاسوب الذي يعمل عليه ويعتبر ذلك بمثابة عقوبة توقع على الناسخ،[1] وتلجأ شركة المساهمة إلى الإستعانة بالفيروسات من أجل تحقيق الغرض الحمائي والذي يعتبر كحيلة منها بهدف حماية برامجها وبياناتها من النسخ غير المرخص به خاصة عندما ما يتعلق بنسخ أسرارها التجارية وخططها التسويقية من طرف شركات منافسة.

2-الغرض التخريبي: وذلك مثلما رأينا في تعريف الفيروسات التي يعدها المبرمج وهدفه من وراء ذلك هو إما التدمير بحد ذاته كتدمير برامج شركة من أجل إزاحتها عن ساحة المنافسة وترك المجال لغيرها من الشركات المنافسة، وقد يكون التدمير بهدف الحصول على مكاسب شخصية من خلال إبتزاز الشركة الضحية بتقديم تلك المكاسب مقابل العدول عن فعل التدمير أو فعل التشهير بضعف نظامها الأمني، الشيئ الذي يلحق بها أضرارا تتجاوز الجانب المادي إلى المساس بسمعتها.

كما تنقسم الفيروسات المعلوماتية إلى أنواع متعددة والتي يستحيل بطبيعة الحال إحصاؤها على وجه التحديد، إلا أنه يمكن تقسيمها من حيث تكوينها وأهدافها إلى:

أ-فيروسات ذات عدوى عامة: حيث ينتقل هذا النوع من برنامج إلى ملف أو برنامج آخر؛

ب-فيروسات ذات عدوى محددة: وهي تقوم باستهداف نوع محدد فقط من النظم المعلوماتية لتهاجمه، وما يميز هذا النوع أنها بطيئة الإنتشار وصعبة الإثبات؛

ت-فيروسات ذات هدف عام: حيث أن الغالبية العظمى من الفيروسات تندرج تحت غطاء هذا النوع وذو مدى واسع من حيث التدمير؛

[1] ميرفت محمد حبابية، مرجع سابق، ص 101.

ث–فيروسات ذات هدف محدد: فهي لا تهدف إلى تعطيل عمل البرامج وإنما تعمل على تغيير الهدف من تلك البرامج، كأن يحدث تلاعبا ماليا وحتى يتم إعداد هذا النوع من الفيروسات بتطلب الأمر درجة عالية من المهارة والدراية التامة بالبرامج المستهدفة.[1]

وكمثال عن أنواع هذه الفيروسات ما جاء في مقال "شيماء عزت" على صفحة " FRANCE 24" حيث أنه في 12 ماي 2017 كانت هناك هجمات إلكترونية بواسطة فيروس يدعى "الفدية" حيث تمكن من إصابة 155 دولة على الأقل وأكثر من 200 ألف جهاز حاسوب لشركات تجارية كبرى، وبعد تشفير البيانات والمعلومات المتواجدة على أجهزة الحاسوب قام القراصنة بطلب فدية مقابل فك الشيفرة وإعادة تشغيل الأجهزة وإلا فسيتم تدميره، وقد بلغت قيمة تلك الفدية في البداية 300 دولار لتتضاعف بعدها إلى 600 دولار، حيث كلف هذا الهجوم الولايات المتحدة الأمريكية 120 مليون دولار بالإضافة إلى تكاليف عالمية تجاوزت 7 مليار دولار.[2]

كذلك ما تعرضت له الشركة الأمريكية "كولونيال بايبلاين" المسؤولة عن نقل قرابة 45% من البنزين والديزل ووقود الطائرات إلى الساحل الشرقي، حين تم مهاجمة شبكات الحاسوب الخاصة بخطوط الأنابيب بفيروس الفدية وقد أحتجز القراصنة البيانات حتى تدفع الشركة فدية قيمتها 4.4 مليون دولار وهذا ما تم بالفعل، بعدها أصدر الرئيس الأمريكي "جون بايدن" أمرا تنفيذيا لتعزيز الأمن السيبراني وحماية القطاع العام والخاص من الهجمات الإلكترونية المتطورة.[3]

---

[1] فاطمة مصفح، "حماية برامج الحاسوب في ظل التشريعات الوطنية والإتفاقيات الدولية"، (رسالة الدكتوراه، كلية الحقوق جامعة الجزائر 1، 2017–2018)، ص ص 189،190.

[2] شيماء عزت، كيف يمكنكم حماية حواسيبكم من فيروس الفدية الخطير، France 24، مقال منشور بتاريخ: 2017/05/15، تاريخ الدخول: 2022/12/31، متاح على الرابط: https://www.france24.com ›

[3] مي مجدي، أخطر هجمات سيبرانية تستهدف شركات الطاقة...إبتزاز أرامكو أشهرها،مقال منشور بتاريخ، 2022/03/06، تاريخ الدخول: 2022/12/31، متاح على الرابط: https://attaqa.net

ثانيا: الديدان الإلكترونية.

تعرف الديدان الإلكترونية،[1] على أنها برامج صغيرة قائمة بذاتها دون أن تعتمد على غيرها من البرامج،[2] فهي مستقلة دون الحاجة لتدخلات بشرية حيث أنها تستقر في ذاكرة أنظمة المعلومات بذات الكيفية التي تستقر بها الدودة البيولوجية داخل التفاحة[3]، وتنتشر هذه الديدان من خلال الخطوط التوصيلية الإلكترونية كما أنها تصيب جزءا محددا من النظام المعلوماتي والذي يتمثل في الجزء الخاص بنظام التشغيل[4]، كما تعمل هذه الديدان على شغل أكبر حيز من سعة الشبكة وبالتالي تقليل أو خفض كفاءتها،[5] إذ يقوم بوضع أصفار في الأماكن الموجودة داخل الذاكرة والتي تمر عليها أو تقوم بتحويل محتويات مكان في الذاكرة مع محتويات المكان المجاور له، مما يصعب من عملية إكتشافها وعندما يصاب الجهاز بهذه الديدان تستمر برامجه بالعمل ولكن بقيم مختلفة عن المعطيات التي تعمل عليها القيم الأصلية، وذلك نظرا لتحويل البعض منها إلى أصفار أو تحويل أماكن المعطيات مع بعضها البعض، ليتحصل مستعمل البرنامج على نتائج مزيفة ولكن دون أن يشعر وعلى أساس ذلك يقوم باتخاذ قرارات خاطئة،[6] وتكمن خطورة هذه الديدان في إستقلاليتها دون أن تكون بحاجة لبرامج أخرى، الشيئ الذي يمكنها من الإنتشار السريع وبحرية تامة، كما تكمن خطورتها في قدرتها على نسخ نفسها بطريقة أتوماتيكية إلى نسخ عديدة ومن الصعب جدا التخلص منها نظرا لقدرتها الفائقة على التناسخ والمراوغة.

---

[1]ظهرت لأول مرة على يد الطالب الأمريكي "ROPER TAPPAN MORRIS " وكان ذلك سنة 1988 لذلك عرفت حينها بدودة موريس، حيث تسببت في تدمير الآلاف من شبكات الحواسيب في الولايات المتحدة الأمريكية هذا بالإضافة إلى الخسائر المادية الكبيرة من أجل مواجهة هذه الدودة حيث أدين هذا الطالب بانتهاك قانون الإحتيال وإساءة إستخدام الكمبيوتر، حيث حكم عليه بثلاث سنوات حبس والعمل لمدة 400 ساعة في الخدمة الاجتماعية وغرامة مالية قدرت ب 10.500 دولار بالإضافة إلى تكاليف المراقبة: أنظر: صورية بورابة، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 46.

[2]ضرغام جابر عطوش آل مواش، مرجع سابق، ص 50.

[3]أسماء فيلالي ، عبد اللطيف شليل ، (تهديدات أمن المعلومات وسبل التصدي لها) مجلة البشائر، ع 3، مج 4، الصادر في 2019، ص 167.

[4]نسمة بطيحي ، مرجع سابق، ص 180.

[5]نهلا عبد القادر المومني، مرجع سابق، ص 131.

[6]نصيرة بوحزمة ، مرجع سابق، 77.

ومن أنواع الديدان الإلكترونية التخريبية نذكر دودة "ستاكسنت" التي عطلت مفاعل بوشهر النووي الإيراني، دودة "دوكو" التي برمجت بدقة عالية وخصيصا للمنشآت الصناعية ودودة "فلايم" التي إستهدفت بشكل أساسي المؤسسات المصرفية في الشرق الأوسط، وكذلك دودة "ريحين" التي إستهدفت شركات الاتصالات خاصة في روسيا والمملكة العربية السعودية.[1]

ثالثا: حصان طراودة.

سمي بهذا الإسم نسبة إلى الأسطورة اليونانية والتي تروي قصة ذلك الحصان الخشبي حيث تم تقديمه كهدية وعربون سلام إلا أنه كان يحمل بداخله غزاة دخلوا المدينة من أجل الإستلاء عليها، أما عن كونه برنامج خبيث فذلك لأنه يتضمن وظائف يعرفها الجاني فقط،[2] ويتميز بقدرته على الإختفاء في البرنامج الأصلي للمستخدم إلا أنه ينشط بمجرد تشغيل ذلك البرنامج،[3] وما يميز هذا البرنامج عن الفيروس هو أنه لا يتكاثر كما أنه لا يلتصق بالملفات، وإنما هو برنامج ذو إستقلالية يتضمن توقيت وأسلوب إستيقاضه،[4] فهو برنامج لا يشتغل أتوماتيكيا وإنما بصفة يدوية والشيئ الملاحظ على هذا البرنامج من خلال عملية البحث فيه، هو أنه يظهر بمظهر بريئ وغطاء مسالم إلا أنه يحمل في ثناياه أسلحة فتاكة وخطر تدميريا وهنا تكمن خطورته، كون مظهره السلمي يظلل مضادات الفيروسات ويجعلها لا تتمكن من إكتشافه لذلك فغرضه القضاء على هذا البرنامج الخبيث صعبة جدا إذ لمنقول أنها شبه مستحيلة.

يتم إستخدام هذا البرنامج في عمليات الإختراق مثال ذلك، إختراق البريد الإلكتروني للإستيلاء على الأرقام السرية وكذا عمليات التجسس على الحسابات المالية وبطاقات الإئتمان وذلك من خلال زرعه في حاسب الضحية،[5] ومن أمثلة هذه البرامج، البرنامج الذي وجد في الولايات المتحدة الأمريكية والذي يعرف باسم "ZOXOON" حيث يظهر في بدايته أنه عبارة عن ألعاب تسلية لكنه يقوم بمحو

---

[1] نايلة الصليبي، أسلوب تجسس واختراق يهدد ملايين شاشات الكمبيوتر، مقال منشور بتاريخ 2016/08/19، تاريخ الدخول: 2023/01/01، متاح على الرابط: https://www.mc-doualiya.com

[2] نسيمة جدي ، مرجع سابق، ص 35.

[3] ضرغام جابر عطوش آل مواش، مرجع سابق، ص 52.

[4] صورية بوربابة ، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 44.

[5] ضرغام جابر عطوش آل مواش، مرجع سابق، ص 53.

أقراص النظام، كذلك برنامج "FILER" فظاهريا يبدو أنه مناسب جدا لعملية تنظيم الملفات ولكنه في حقيقة الأمر يقوم بحذفها، كما أنه عادة ما توجد هذه البرامج في برنامج العمال كبرامج معالجة النصوص والجداول للتلاعب برواتبهم ومستحقاتهم فتعطي نتائج غير صحيحة تماما،[1] وكانت إحدى الصحف العربية قد نشرت قصة حول أجهزة إتصال في غاية التطور منحتها دول عظمى على سبيل الهدية لدولة عربية وبعدما تم فحصها إتضح أنها تتضمن برنامج حصان طراودة تم إعداده خصيصا بهدف جمع المعلومات عن إستخدام الجهاز وكذا التردد التي أستخدمت عليه.[2]

وفي إعتقادنا فإن هذا البرنامج من إخطر البرامج التي تشكل تهديدا حقيقيا صامتا خاصة عندما يتعلق الأمر بكبرى الشركات –شركة المساهمة– إذ من الممكن أن يتم إدخاله إلى نظامها المعلوماتي على أنه برنامج صحيح ومفيد ومناسب لتأدية أعمالها، ولا تكشف ذلك إلا في اللحظة التدميرية لهذا البرنامج بعد أن يكون قد أدى وظيفته التخريبية وألحق بها ما ألحق من أضرار.

رابعا: القنبلة المعلوماتية.

يطلق إصطلاح القنبلة المعلوماتية على نوع من البرامج الخبيثة صغيرة الحجم بحيث يتم إدخالها خفية مع برامج أخرى، فهي عبارة عن شفرة تنضم إلى مجموعة ملفات البرامج وذلك من خلال تقسيمها إلى عدة أجزاء مشتتة هنا وهناك، فهي تتجمع فيما بينها بحسب الأمر المعطى لها في زمن معين أو حدوث واقعة معينة،[3] والشيئ المميز لهذه القنبلة هو أنه بعد أن يتم إدخالها وتثبيتها لا تعمل إلا بعد مرور مدة من إستعمال النظام وذلك بغية تعطيليه أو تدميره أو إتلاف بياناته.

حيث تبرز في البرامج المؤقتة التي تشتمل عليها الحملات الإعلانية مثل المجلات التي يتم توزيع بعض الأسطوانات وذلك كهدية معها وهي تتضمن في الأصل بعض هذه البرامج، كما توجد كذلك على شبكة الأنترنت مواقع تشمل هذه البرامج والتي من الممكن أن تظهر في البرامج المدخرة التي لا يفقد عليها مالكها حقوق الملكية وإنما يقوم بتأجيرها لا أكثر، وفي حالة توقف المستأجر عن

---

[1] نسيمة جدي ، مرجع سابق، ص 35، 36.

[2] صورية بوربابة، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 45.

[3] المرجع نفسه، ص 46.

الوفاء بالقيمة الإيجارية التي تم الاتفاق عليها يقوم المالك بإرسال قنبلة بل أنها تكون موجودة أساسا في البرنامج المستأجر ويمتنع المالك عن إرسال ما يوقف تفجيرها،[1] ونجد بأنها تنقسم إلى قسمين:

1-القنبلة المنطقية: وهي برنامج يتم تنفيذه في لحظة محددة بحيث يوضع في شبكة للمعلومات مع تحديد هدفها في ظرف معين، وذلك بهدف تسهيل القيام بعمل غير مشروع،[2] من خلال قيامها بعملية مسح للنظام المعلوماتي وما يميز هذه القنبلة أنها تكون في بداية الأمر ساكنة دون أن تقوم بأي إعتداء على النظام المعلوماتي لذلك يكون من الصعب إكتشافها، وبعد أن يتم أحد الشروط المنطقية تنفعل فعملها التخريبي يشبه الإنفجار،[3] فالنشاط التخريبي للقنبلة المنطقية مرتبط بالمؤشر الموجود داخلها، حيث أن ذلك المؤشر قد يرتبط بالمدة الزمنية سواء كانت طويلة أو قصيرة كما يرتبط بتوفر شرط ما وبمجرد أن تحل تلك المدة أو يتحقق ذلك الشرط تباشر هذه القنبلة نشاطها العدواني بهدف التخريب.

ومن الأمثلة على ذلك القيام بزرع قنبلة منطقية لتؤدي وظيفتها عند إضافة سجل موظف، والنتيجة إنفجار سجلات الموظفين التي توجد داخل المنشأة،[4] كذلك ما حدث سنة 1985 في ولاية تكساس بالولايات المتحدة الأمريكية وذلك عند إقبال أحد المبرمجين بزرع قنبلة منطقية داخل حاسوب الشركة التي كان يعمل بها، وذلك إنتقاما عن فصله من وظيفته مما أدى إلى تدمير سجلات عمولة المبيعات مرة كل شهر.[5]

2-القنبلة الزمنية: هناك من يطلق عليها تسمية القنبلة الموقوتة كذلك، حيث تظهر من خلال تسميتها بأن نشاطها مرتبط بوقت محدد أي تكون محددة اليوم والساعة كذلك.

---

[1] صورية بوربابة، قواعد الأمن المعلوماتي -دراسة مقارنة، مرجع سابق ، 47.

[2] نسيمة جدي ، مرجع سابق، ص 33.

[3] عبد الله محمد الحضري، "جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري -دراسة تحليلية مقارنة-" (رسالة ماجستير، كلية الحقوق، جامعة قطر 2020)، ص 51.

[4] حمزة بن عقون ، مرجع سابق، ص 165.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 133.

وتعرف بأنها عبارة عن كود يتم زرعه في برنامج معين،[1] حيث يتم تنفيذه في جزء من ثانية أو بضع ثوان أو دقائق وذلك وفقا للوقت الذي يتم تحديده مسبقا كأن يتم ضبطه مثلا للإنفجار بعد عام،[2] أما عن الخطر الذي يمكن أن تشكله هو أن تأجيلها إلى وقت محدد يمكن أن يسمح لها بأن تشمل عمليتها التدميرية حتى النسخ الإحتياطية للبرامج التي تكون شركة المساهمة قد أعدتها لذلك تكون خسائرها التي تلحق بالحاسوب مضاعفة.

ومن الأمثلة عن ذلك ما حدث لشركة "أوميغا" حين أقدم أحد الموظفين بوضع برنامج لإتلاف بيانات الشركة وذلك بعد 6 أشهر من طرده من هذه الشركة.[3] وتعد هذه الأساليب من أهم الطرق التي يتم إستخدامها من أجل الإعتداء على شركة المساهمة، وهي في تطور مستمر تبعا للتطورات الحاصلة في عالم التكنولوجيا.

المطلب الثاني:

الأحكام الخاصة بأركان الجرائم الإلكترونية.

الركن في الإصطلاح يعني الداخل في حقيقة الشيئ المُحقق لماهيته وهو أيضا ما يتم به الشيئ وهو داخل فيه،[4] والأصل أن الركن جزء لا يتجزأ عن الطبيعة القانونية للجريمة، حتى تقوم الجريمة هناك أركان يجب توفرها حيث أن غياب أو تخلف أحد الأركان يلغي قيامها، وبالتالي يمنع تحققها والقاعدة المعمول بها قانونا هو أن الجريمة تقوم على أركان ثلاثة، ركن شرعي، ركن مادي وكذا ركن معنوي.

وفي الشريعة الإسلامية لكي تقوم الجريمة يجب أن يكون هناك نص يجرم الفعل ويعاقب على إتيانه، ولكن بشرط أن يكون ذلك النص نافذ المفعول وقت إرتكاب الفعل وأن يكون ساريا على المكان الذي أرتكب وعلى الشخص الذي إرتكبه، وهو ما يسمى بالركن الشرعي وأن يقع من المجرم الأمر

---

[1] ضرغام جابر عطوش آل مواش، مرجع سابق، ص 54.

[2] نصيرة بوحزمة ، مرجع سابق، ص 78.

[3] نسيمة جدي، مرجع سابق، ص 33.

[4] أيمن بن ناصر بن محمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي –دراسة مقارنة– ، ط 1، الرياض ، مكتبة القانون والإقتصاد، ، 2016، ص 76.

المادي المكون للجريمة سواء كان ذلك إيجابا أو سلبا، فعلا أصليا أو إشتراكيا، جريمة تامة أو شروعا ويسمى هذا بالركن المادي.[1]

أما الركن الثالث وهو الركن الأدبي والذي يكون الأصل فيه التكليف، والتكليف في الشريعة هو الخطاب بأمر أو النهي ومن شروطه أن يكون المكلف عاقلا يفهم الخطاب.

هذا بالنسبة للجريمة بصفة عامة أما بالنسبة للجريمة الإلكترونية التي نحن بصدد دراستها وإن كانت تتميز ببعض الخصوصيات التي تجعلها تنفرد عن نظيرتها التقليدية، إلا أنها هي الأخرى تقوم على الأركان التي سبقت الإشارة إليها، حيث تلعب دورا مهما بالنسبة لأعمال التحقيق إذ يتعين على المحقق إظهار هذه الأركان من أجل إثبات وقوع الجريمة فعلا، هذا ما نوضحه من خلال هذا المطلب وذلك بالتطرق إلى الركن الشرعي **(فرع أول)** ثم الركن المادي والمعنوي **(فرع ثاني)**.

الفرع الأول:

الركن الشرعي.

ويسمى كذلك بمبدأ الشرعية الجنائية إذ يعد أول وأهم ركن تقوم عليه الجريمة إذ لا يمكن تصور قيام جريمة ما دون أن يكون هناك نص، وهو مجسد حتى في الشريعة الإسلامية والتي من قواعدها "لا حكم لأفعال العقلاء قبل ورود النص[2].

أما تاريخ هذا المبدأ في القانون الوضعي فيعود إلى تاريخ الفصل بين السلطات، إذ كان قبل ذلك إنفراد الملك بسلطة تجريم الأفعال، بعدها في القرون الوسطى أصبح الأمر مخولا للقضاة وحدهم يملكون سلطة تجريم الأفعال وتوقيع العقاب عليها دون أي نص قانوني، ثم تم النص عليه بصدور ميثاق "هنري الأول" في إنجلترا ثم دستور " كلاريندون" وقد أكد عليه العهد الأعظم، ويرجع الفضل في ظهوره إلى النور إلى الفقيه الإيطالي "شيزاري دي بكاريا" صاحب الكتاب الشهير "الجرائم

[1] إبراهيم محمد بن حمود الزنداني، "الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني –دراسة مقارنة–" (رسالة ماجستير، قسم الدراسات الإسلامية، جامعة فطاني، 2018)، ص 29.

[2] بالضياف خزاني، "مبدأ الشرعية الجزائية وأثره على السلطة التقديرية للقاضي الجزائي"، (رسالة ماجستير، معهد العلوم القانونية والإدارية، المركز الجامعي العربي بن مهيدي بأم البواقي، 2007–2008)، ص 13.

والعقوبات" الذي تم إصداره سنه 1764 حيث جاء فيه "أن القوانين وحدها هي التي تحدد العقوبات التي تقابل الجرائم، ولا يستطيع القاضي أن يوقع سواها"[1].

كما تم التأكيد عليه كذلك من خلال المادة السابعة من إعلان حقوق الإنسان والمواطن الصادر سنة 1789،[2] والي جاء فيها بأنه لا يجوز إتهام أي شخص أو إعتقاله أو إحتجازه إلا وفق الحالات التي يحددها القانون، كذلك المادة 11 من الإعلان العالمي لحقوق الإنسان الصادر سنة 1948،[3] والتي جاء فيها بأنه لا يمكن إدانة أي شخص جراء أداة عمل أو الإمتناع عن أداة عمل إلا إذا كان ذلك يعتبر جرما وفقا للقانون الوطني أو الدولي وقت الإرتكاب، كذلك لا توقع عليه عقوبة أشد من تلك التي كان يجوز توقيعها وقت إرتكاب الجريمة.

ومبدأ الشرعية من أهم المبادئ التي تقوم عليها التشريعات العقابية ومن بينها التشريع الوطني الذي كفله بموجب دساتير الجمهورية المتعاقبة وآخرها التعديل الدستوري سنة 2020،[4] الذي نص في المادة 43 منه "لا إدانة لا بمقتضى قانون صادر قبل إرتكاب الفعل المجرم"، وكذلك قانون العقوبات الذي نص في مادته الأولى بأنه "لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون".

وقد قام مبدأ الشرعية الجنائية من أجل حماية مصالح الأفراد، حيث يقوم المشرع من خلاله بإعلامهم بجميع الأفعال التي تدخل في نطاق التجريم مسبقا، ثم يبين عقوبتها ويتم النص على ذلك في قوانين فيصبح الأفراد على دراية تامة بالأفعال المشروعة وكذا الأفعال التي تعتبر جرائم، فلا يوجد ما يمنع الأفراد من القيام بأي فعل لم يرد بشأنه نص قانوني يجرمه.[5]

---

[1] الشرعية الجنائية الجزء الثاني، مقال منشور بتاريخ، 2020/09/05،: تاريخ الدخول: 10/15/ 2020 متاح على الربط: https://www.academia.edu

[2] Art: 07 de la déclaration des droits de l'homme et du citoyen de 1789.
Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la loi.

[3] Art: 11 de la déclaration universelle des droits de l'homme de 1948.
Nul ne sera condamné pour des actions ou omissions qui, ou moment ou elles ont été commises, ne constituaient pas un acte délictueux d'après le droit national ou international, De même, il ne sera infligé aucune peine plus forte que celle qui était applicable au moment ou l'acte délictueux a été commis.

[4] دستور الجمهورية الجزائرية الديمقراطية الشعبية المعدل في 2020، الصادر بموجب المرسوم رقم 20-442 مؤرخ في 30 ديسمبر 2020، ج، ر، ع 82 الصادر بتاريخ 2020/12/30.

[5] عماد الدين رضا علي لدادوه، "مدى ملائمة نصوص قانون الجرائم الإلكترونية الأردني للأحكام العامة لقانون العقوبات"، (رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2021)، ص 44.

ويعرف مبدأ الشرعية على أنه حصر الجرائم والعقوبات في نصوص مكتوبة من خلال تحديد الأفعال التي تعد جرائم وبيان أركانها وكذا العقوبات المقررة لها ونوعها ومدتها،[1] وهي الصفة غير المشروعة التي تتكون نتيجة إنطباق نص التجريم المنصوص عليه في القانون على السلوك أو الفعل الذي إقترفه الفاعل، ويمكن لهذه الصفة أن تزول عن الفعل إذ توفر سبب من أسباب الإباحة الذي ينفي عنه هذه الصفة،[2] وهو مبدأ يمنع المساءلة الجنائية إذ لم يكن هناك نص قانوني، وبالتالي إنتفاء النص على تجريم الأفعال التي لا تطالها النصوص القائمة يؤدي إلى عدم قيام المسؤولية ويتحقق القصور في مكافحة الجرائم[3]، ويترتب على مبدأ الشرعية :

-حصر التجريم والعقاب بيد المشرع: وبالتالي تصبح السلطة التشريعية الجهة المخولة وذات الصلاحية بتحديد الأفعال التي تعتبر من قبيل الجرائم كما تحدد في نفس الوقت الجزاء الواجب التطبيق على تلك الأفعال.

إذ يصبح دور القاضي لا يتعدى تطبيق النصوص القانونية على الوقائع التي تفرض عليه،[4] وذلك ضمن الحدود التي رسمها الشرع فليس للقاضي في حالة عدم وجود نص يقضي بتجريم الفعل والعقاب عليه أن يحكم بالإدانة وإنما وجب عليه أن يحكم بالبراءة وإلا كان حكمه مشوبا بالخطأ.[5]

-الإلتزام بالتفسير الضيق للنص الجنائي: بمعنى الكشف عن حقيقة إرادة المشرع وتحديدها وذلك من خلال الألفاظ والعبارات التي وردت في القاعدة القانونية المراد تفسيرها،[6] لكن يحدث أحيانا أن يجد

---

[1] خالد ضو، (التأصيل لمبدأ الشرعية الجنائية في الفقه الإسلامي والتشريعات الوضعية)، مجلة الأبحاث القانونية والسياسية، ع 1، مج 3، الصادر في 2020)، ص 288.

[2] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 87.

[3] يوسف صغير ، مرجع سابق، ص 60.

[4] صليحة يحياوي ، "السلطة التقديرية للقاضي الجنائي"، (رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2015-2016)، ص 217.

[5] حفصي عباس ، مرجع سابق، ص 56.

[6] بالضياف خزاني، مرجع سابق، ص 29.

القاضي نفسه أمام نص غامض في هذه الحالة يلزم بتفسير النص وإزاحة الغموض عليه ولكن بشرط أن لا يؤدي ذلك إلى خلق جريمة أو عقوبة جديدة.

–حضر القياس: القياس هو إعطاء حالة غير منصوص عليها في القانون حكم حالة أخرى وذلك لإتفاقهما في العلة،[1] معنى ذلك أنه تعرض على القاضي مسألة لم ينظمها القانون ولكن في مقابل ذلك قد نظم مسألة أخرى مشابهة لها، فيحكم القاضي في المسألة الثانية قياسا على المسألة الأولى وبطبيعة الحال هذا غير ممكن فيما يتعلق بالنص الجنائي، إذ لا يجوز للقاضي أن يجرم فعلا قياسا على فعل آخر مشابه له ورد نص بتجريمه، ويرجع السبب في حضر القياس في النصوص الجنائية باعتبار أنه يؤدي إلى خلق جرائم وعقوبات جديدة وهذا مخالف لقاعدة "لاجريمة ولا عقوبة بغير نص".

لكن السؤال الذي يطرح نفسه ونحن نتكلم عن مبدأ الشرعية هو مدى إمكانية تطبيقه على الجرائم الإلكترونية؟ هذا التساؤل يقودنا للحديث عن نقطتين هما:

أولا: مدى كفاية النصوص التقليدية واتساعها للجريمة الإلكترونية وتحقيق مبدأ الشرعية؟

بالنسبة للجريمة الإلكترونية التي كانت رفيقة النهضة التقنية والتطور التكنولوجي الذي غزى جميع مناحي الحياة الإنسانية، أصبحت هناك ضرورة ملحة تستوجب توقيع العقاب على مرتكب هذه الجريمة، إذ هناك العديد من الدول وخاصة النامية منها وجدت نفسها مضطرة إلى العودة إلى النصوص التقليدية من أجل تكييف سلوك الجاني وفقا لمفهوم هذه الجرائم، لكن الشيئ الذي تم ملاحظته حينها هو إفلات العديد من الجناة من قبضة العقاب لماذا ذلك؟

يرجع ذلك إلى كون الجريمة الإلكترونية ظاهرة جديدة، فبطبيعة الحال أنها أسفرت عن أفعال جديدة ترتبط باستعمال الحاسوب حيث وقفت النصوص التقليدية عاجزة عن احتوائها، من ذلك مثلا الدخول في نظام الحاسب الآلي وتغيير البيانات التي يحتويها –تعد هذه الصورة من أكثر الجرائم التي تتعرض لها شركة المساهمة– فهذه الصورة لم يعرفها قانون العقوبات من قبل.

---

[1] فاضل عواد محمد الدليمي، نتائج مبدأ الشرعية الجنائية ودورها في تحديد ذاتية القواعد الجنائية الموضوعية، 2017/04/18، تاريخ الدخول: 2022/10/27، متاح على الرابط: https://almerja.com ›

فالإكتفاء بالنص التقليدي والذي بات تطبيقه على الجريمة الإلكترونية غير ملائم، بل أنه يضع القضاء أمام خيارين لا ثالث لهما وهما إما أن يتم تطبيقه على الجريمة الإلكترونية لإتحاد العلة وبالتالي الوقوع في القياس المحضور، وإما أن يقف القضاء مكتوف الأيدي أمام هذه الجريمة لعدم قدرته على خلق جرائم وعقوبات إعمالا لمبدأ الشرعية، فهناك العديد من المواقف القضائية من خلال أحكام أمريكية وفرنسية صدرت تقضي برفض فكرة تطبيق النص التقليدي مثل السرقة وخيانة الأمانة على الجريمة الإلكترونية.[1]

وبالتالي فالنتيجة المترتبة على تطبيق النصوص التقليدية على الجريمة الإلكترونية يؤدي إلى الإخلال بالبنيان القانوني للجريمة، كما أن تحقيق مبدأ الشرعية بتطبيق النصوص التقليدية يؤدي بالقاضي إلى الوقوع في التفاسير الموسعة الفضفاضة وفي هذا إخلال بمبدأ الشرعية كون أن السلطة القضائية ليس بإمكانها ملاحقة أفعال وتقرير عقوبات لها، في حين أن تلك الأفعال التي لم تجرم من قبل السلطة التشريعية، وهذا ما يوحي بقصور النصوص التقليدية وعدم كفايتها أمام الجريمة الإلكترونية مما يترتب عليه عجز السلطة القضائية عن ردع هذه الجريمة إحتراما لمبدأ الشرعية الجنائية.

ثانيا: إلزامية سن نصوص قانونية خاصة بالجريمة الإلكترونية.

نظرا للطبيعة الخاصة للجريمة الإلكترونية والتي ترتكز على تقنيات عالية المستوى وذات تطور مستمر كان لزاما إصدار تشريعات قادرة على مواجهة هذه الجريمة، خاصة بعد أن أصبح العالم الرقمي حقيقة واقعية حيث تكمن أهمية إصدار نصوص خاصة بها في التعقيدات التي تتسم بها والتي تتطلب إلماما دقيقا بالمصطلحات التقنية وحصر الأفعال التي تشكل جريمة إلكترونية بصورة دقيقة.

وفي هذا الصدد نجد المجلس الأوربي قد قام بإصدار توصية وكان ذلك في سنة 1989، والهدف منها هو تشجيع الدول الأعضاء على تبني نصوص عقابية خاصة بهذه الجريمة،[2] ونجد بأن العديد من الدول الغربية قد إستجابت للتطورات التي أنتجها الحاسب الآلي، وذلك بإدخال تعديلات

---

[1] أحمد أسامة حسنية، (الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية)، مجلة جامعة الأزهر، (ع خاص بمؤتمر كلية الحقوق الخامس المحكم، مج 19، الصادر في 2017، ص 19.

[2] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 88.

جوهرية على قوانينها الجزائية فلا أحد ينكر صعوبة تحديد البرامج التي يتم إستخدامها سواء من حيث أنواعها أو من حيث أعدادها،[1] أما على المستوى الدولي فهناك فجوة رقمية رهيبة خاصة بالنسبة للدول التي تعاني من التخلف في المجال المعلوماتي،[2] بحيث أن هذه الدول لا تزال تستند إلى النصوص التقليدية في مواجهة الجريمة الإلكترونية وذلك من خلال القيام بعملية التفسير الموسع بدلا من سن قوانين خاصة بها.

ويكون التفسير الموسع يمنح للسلطات القضائية حرية تفسير النصوص التقليدية بشكل مرن يسمح بوضع الجرائم الإلكترونية تحت طائلة التجريم والمتابعة وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي.[3]

فرغم أن هذه الجريمة أصبحت حقيقة واقعية والجميع معرض لأن يكون ضحية لها خاصة إذا كان هذا الضحية شركة مساهمة التي تعد النموذج الأمثل للشركات وعصب الاقتصاد، حيث يصبح خطرها هنا مرعب إلا أننا نجد بأن هناك من ينادي بفكرة الجريمة الإلكترونية هي جريمة عادية يتم إستعمال الحاسب الآلي فيها على إعتبار أنه مجرد وسيلة لتنفيذها، حيث تعتبر النصوص التقليدية كافية لمواجهتها، وفي اعتقادنا بأن ذلك يشكل اعتداءا صارخا على مبدأ الشرعية الجنائية، إذ يستحيل أن تتوافق وتنسجم الجريمة الإلكترونية مع نظيرتها التقليدية إلى درجة مواجهتها بنفس النصوص القانونية.

أما بالنسبة للمشرع الجزائري فبعد الفراغ التشريعي وتأخره في تنظيمه لهذه الجريمة إلا أنه سرعان ما تدارك ذلك وساير ولو نسبيا ركب التشريعات التي واجهت الجريمة الإلكترونية بموجب قوانين خاصة، كان ذلك بداية بالقانون 04-15 بعدها القانون 09-04 كما سبقت الإشارة إلى ذلك في المبحث الأول.

---

[1] حفصي عباس ، مرجع سابق، ص 56.

[2] يوسف صغير ، مرجع سابق، ص 63.

[3] عبد المومن بن صغير، (الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن)، مجلة الحقوق والحريات، ع 2، الصادر في 2014، ص ص 86،87.

هذا إضافة إلى قيامه بإصدار جملة من النصوص القانونية الأخرى مثل القانون 03-05[1] المتعلق بحقوق المؤلف والحقوق المجاورة، كذلك القانون 15-04[2] المتعلق بالتوقيع والتصديق الإلكترونيين، القانون 18-04[3] المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، وكذا القانون 18-07[4] المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي.

كل هذه النصوص القانونية التي جاء بها المشرع الجزائري كان رغبة منه في مكافحة الجريمة الإلكترونية بموجب قوانين خاصة، نتيجة لقصور النصوص التقليدية وعجزها عن مواجهتها وبذلك يكون قد تفادى التفسير الموسع لتلك النصوص والتي فيها مساس بمبدأ الشرعية الجنائية، إذ لا يمكن الحديث عن الشرعية الجنائية في الجريمة الإلكترونية دون أن تكون هناك قوانين خاصة بها.

الفرع الثاني:

الركن المادي والمعنوي.

إضافة إلى الركن الشرعي الذي يحدد الجريمة والعقوبة المقررة لها، وحتى تتحقق الجريمة يتطلب الأمر قيام ركنين آخرين، ركن مادي والذي يمثل الكيان المادي الملموس منها وكذا ركن معنوي وهو الذي يترجم إرادة المجرم الإلكتروني هذا ما نوضحه من خلال هذا الفرع وذلك بالتطرق إلى الركن المادي أولا ثم الركن المعنوي ثانيا.

---

[1] الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج، ر، ع 44، الصادر في 23 يوليو 2003.

[2] القانون رقم 15-04 مؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، ج، ر، ع 6 الصادر في 10 فبراير 2015.

[3] القانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، ج، ر، ع 27 الصادر في 13 ماي 2018.

[4] القانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، ج، ر ، ع 34، الصادر في 10 يونيو 2018.

أولا: الركن المادي.

المعروف أنه لا قيام لجريمة ما دون إستنادها إلى ركن مادي والذي يتمثل في ذلك السلوك الذي يأتي به الجاني بغية تحقيق غاية ما وفي مقابل ذلك يحدد له القانون العقوبة اللازمة.

ويعرف بأنه إرتكاب بالفعل أو القول بالأمر الذي ورد به النهي وقررت له عقوبة يطبقها القضاء، وقيل بأنه إرتكاب ما قرر الشارع له عقابا سواء كان بالفعل الإيجابي أو بالفعل السلبي المتمثل في الترك،[1] ويترجم إلى مظهر خارجي ملموس بحيث أنه يتباين ويختلف من جريمة إلى أخرى، ويقوم هذا الركن على علاقة ثلاثية تتمثل في السلوك الإجرامي والنتيجة المترتبة عن ذلك وكذا العلاقة السببية التي تربط بينهما.

وما تجب الإشارة إليه في هذه النقطة هو أنه لا يشترط توفر هذه العناصر الثلاثة في جميع الجرائم وإنما تختلف بحسب نوع الجريمة، فهناك جرائم تقوم على تحقق السلوك الإجرامي فقط وتسمى بالجرائم الشكلية والتي تنعدم فيها النتيجة الإجرامية تماما، في حين هناك نوع آخر من الجرائم يستلزم توفر العناصر الثلاثة السالفة الذكر حتى تتحقق وتسمى بالجرائم ذات النتيجة.

هذا فيما يتعلق بالركن المادي في الجرائم بصفة عامة لكن عندما يتعلق الأمر بالجريمة الإلكترونية فإن الأمر يختلف، فالمشكلة الأساسية التي تواجه هذه الجريمة هي طبيعة الركن المادي وذلك باعتبار أن التجريم يطال فيها وسط إلكتروني إما بإساءة إستخدامه وإما باقتحامه بطريقة غير قانونية.

1-السلوك الإجرامي: ويعد أهم العناصر المكونة للركن المادي باعتبار أن هناك جرائم تتحقق بتحققه فقط كما سبقت الإشارة إلى ذلك.

حيث يعرف بأنه ذلك السلوك المادي الذي يتعارض مع القانون ويصدر عن إرادة الجاني،[2] وبغير هذا السلوك لا يمكن معاقبة الشخص على أفكاره وهواجسه الداخلية وذلك مهما بلغت درجة

---

[1] أسامة سيد اللبان، (الركن المادي للجريمة عناصره ومظاهره في الفقه الإسلامي)، مجلة مصر المعاصرة، ع 543، الصادر في يوليو 2021، ص 182.

[2] إبراهيم محمد بن حمود الزنداني، "الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني –دراسة مقارنة–" (رسالة ماجستير، جامعة فطاني، 2018)، ص 30.

خطورتها، فالسلوك هو الذي يخرج النية والتفكير في الإجرام إلى حيز الوجود،[1] وبالتالي ترجمتها في شكل مادي ملموس يترتب عليه إحداث أثر في الواقع الخارجي ويتحقق السلوك الإجرامي وفق صورتين، تتمثل الصورة الأولى في السلوك الإيجابي بمعنى الفعل والصورة الثانية تتمثل في السلوك السلبي بمنعى الترك.

أ-السلوك الإيجابي: السلوك المادي في أغلب الجرائم هو عبارة عن نشاط إيجابي محضور قانونا[2] ويتحقق في صورة فعل، أو قول مجرم قانونا دون الاهتمام بالوسيلة المستعملة في ذلك طالما أنه يحقق نتيجة منعها القانون.[3] ومن الأمثلة عن السلوك الإيجابي بالنسبة للجريمة الإلكترونية في شركة المساهمة دخول الجاني إلى نظامها المعلوماتي وتدمير بياناته ففعل الدخول إلى هذا النظام مجرم قانونا ويترتب على إتيانه قيام جريمة إلكترونية في حق هذه الشركة.

ب- السلوك السلبي: ويتمثل في الترك أو الإمتناع حيث يفرض القانون على الشخص قاعدة ما يتوجب عليه القيام بها فيمتنع الشخص عن القيام بذلك، ففعل الإمتناع في هذه الحالة يشكل جريمة قائمة بذاتها.

ويعرف السلوك السلبي بأنه إحجام شخص عن إتيان فعل إيجابي معين كان الشارع ينتظره منه في ظروف معينة بشرط أن يوجد واجب قانوني يلزم بهذا الفعل وأن يكون في إستطاعة الممتنع وإرادته،[4] حيث جعل المشرع فعل الإمتناع مساويا للفعل الإيجابي من حيث كونهما يحققان السلوك الإجرامي وبالتالي تحقق الجريمة، وفي شركة المساهمة كأن توكل مهمة ملئ البيانات الخاصة بالزبائن إلى أحد موظفيها ضمن برنامج خاص فيمتنع عن إدراج بيانات محددة متعمدا في ذلك ففعل الإمتناع يعتبر جريمة في هذه الحالة.

---

[1] يوسف صغير ، مرجع سابق، ص 65.

[2] محمد ياسين بوزوينة ، "الآليات القانونية لمكافحة الجريمة الاقتصادية في القانون الجنائي الجزائري"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2018-2019)، ص 38.

[3] يوسف صغير ، مرجع سابق، ص 65.

[4] مسعود خثير ، (الإمتناع كعنصر لقيام الركن المادي في الجريمة السلبية)، مجلة القانون والمجتمع، ع 2، مج 1، الصادر في 2013/12/01، ص 1888

والملاحظ أن السلوك الإجرامي في الجريمة التقليدية يختلف تماما عن السلوك الإجرامي في الجريمة الإلكترونية، حيث أنه في الجريمة التقليدية يتم ملاحظة ذلك السلوك ورؤيته كونه يتجسد في فعل مادي ملموس كالقتل مثلا، أما بالنسبة للجريمة الإلكترونية فإن هذا السلوك لا يمكن ملاحظته باعتبار أنها ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي، ولا يمكن الإمساك بها ماديا فيمكن تشبيهها بالتيار الكهربائي الذي يسري في توصلة دون التمكن من رؤيته،[1]حيث يرتبط هذا السلوك دوما بالمعلومات التي يتم إدخالها إلى الحاسب الآلي وتخزينها فيه وبمجرد الضغط على زر فقط يتم تدمير ذلك النظام المعلوماتي أو حصول السرقة أو التسلل إلى نظام أرصدة العملاء في البنوك،[2] كما يتطلب هذا السلوك وجود بيئة رقمية وأن يكون هناك إتصال بالأنترنت وكذا معرفة بداية هذا النشاط والشروع فيه، ونتيجته كأن يقوم الجاني بتجهيز جهاز الحاسوب وتحميله ببرامج إختراق أو أن يقوم بإعداد هذه البرامج بنفسه.[3]

والحديث عن السلوك الإجرامي يقودنا إلى الحديث عن الأعمال التحضيرية التي تسبقه، فبطبيعة الحال أن هناك جرائم يسبقها تحضير يهدف الجاني من وراءه إلى خلق وسط ملائم من أجل تنفيذ جريمته والقاعدة أن هذه الأعمال التحضيرية غير معاقب عليها كونها لا تعتبر شروعا في الجريمة التي هي محل التحضير.

لكن ما يجب التأكيد عليه هو أنه حينما نكون بصدد جريمة إلكترونية فإن الأمر يختلف تماما، باعتبار أن في هذه الجريمة من الصعب جدا الفصل والتمييز بين الأعمال التحضيرية والبدء في عملية تنفيذ السلوك الإجرامي، لذلك فإن العمل التحضيري للجريمة الإلكترونية يعد جريمة في حد ذاتها كمن يقدم على شراء برنامج مخصص لإختراق جهاز حاسوب إحدى الشركات أو إختراق موقعها الإلكتروني، أو مثلا الحصول على معدات من أجل فك شفرات المرور.

---

[1] عبد الله دغش العجمي، "المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة"، (رسالة ماجستير، جامعة الشرق الأوسط، 2014)، ص 27.

[2] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص 46.

[3] يوسف صغير ، مرجع سابق، ص 67.

في هذا الصدد نجد المشرع قد نص في المادة 394 مكرر 5 من القانون 04-15 " كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها"

كما أن ما يميز السلوك الإجرامي في الجريمة الإلكترونية منه ما يكون مؤقت، بمعنى أنه يبدأ وينتهي بمجرد تمامه والمثال على هذه الحالة جريمة السرقة المعلوماتية وفي مقابل ذلك قد يكون السلوك مستمرا لفترة غير محددة.[1]

2-النتيجة الإجرامية: تعرف على أنها الآثار التي تترتب على السلوك الإجرامي سواء كان إيجابيا أو سلبيا فهي نتيجة الأعمال التي بدءها الجاني،[2] وللنتيجة الجرمية مدلولان، الأول مدلول مادي ويتعلق بالتغيير الذي يلحقه الجاني بالعالم الخارجي جراء السلوك الإجرامي الذي قام بارتكابه، والثاني مدلول قانوني يتمثل في الإعتداء على الحق الذي يحميه القانون،[3] والنتيجة الإجرامية قد لا تكون عنصرا في بعض الجرائم التي يكتمل وقوعها دون تحقق نتيجة،[4] كمن يقوم بإنشاء مواقع من أجل التشهير بإعلانات ضد إحدى الشركات مما ينجم عنه المساس بسمعتها، ولكن دون أن يطرح هذه المواقع على الشبكة ففي هذه الحالة النتيجة لم تتحقق فعلا ولكنها تعتبر جريمة قائمة بذاتها رغم أن تلك الشركة لم تتضرر من هذه المواقع التي لم تطرح.

وإذا جئنا إلى البحث عن طبيعة الجريمة الإلكترونية إن كانت تعتبر جريمة شكلية أم جريمة ذات نتيجة ، بقراءاتنا للنصوص القانونية التي نظم بها المشرع الجزائري هذه الجريمة نجد بأنه يعاقب على مجرد فعل الدخول أو البقاء بطريق الغش في كل أو جزء من منظومة معلوماتية، وتضاعف هذه العقوبة في حالة ما إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة المعلوماتية وذلك

---

[1] عبد اللطيف معتوق ، مرجع سابق، ص 24.

[2] أسامة سيد اللبان، مرجع سابق، ص 189.

[3] محمد ياسين بوزوينة ، مرجع سابق، ص 39.

[4] محمد بن أحمد ، "المسؤولية الجنائية للمجرم المعلوماتي -دراسة تأصيلية موضوعية في التشريع الجزائري والمقران-"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس مستغانم، 2021-2022)، ص 96.

حسب المادة 394 مكرر من القانون 04-15، فوفقا لنص هذه المادة لم يشترط تحقق نتيجة معينة على الجريمة الإلكترونية وإنما جعل النتيجة المترتبة عليها ظرف مشدد لمضاعفة العقوبة المقررة لها.

وحسن ما ذهب إليه المشرع فمن خلال عملية البحث في هذا الموضوع إتضح لنا بأن أي جريمة إلكترونية تحمل بين طياتها نتيجة إجرامية حتى وإن لم تكن بشكل ظاهر، فمجرد الدخول أو البقاء في معطيات المنظومة المعلوماتية لشركة المساهمة فيه نتيجة إجرامية خفية تتمثل في الإطلاع على أسرارها ومعلوماتها بغض النظر عما إذا كان هناك حذف أو تغيير والذي يعتبر بمثابة نتيجة ثانية تشدد العقوبة.

لذلك فإن الضرر في الجريمة الإلكترونية يختلف عن الضرر في الجريمة التقليدية باعتباره ذو طبيعة غير محددة وكونه متصل بتقنية المعلومات، وقد يكون ماديا أو معنويا ومن أكثر الأضرار المادية شيوعا في الوسط الإلكتروني تتمثل في تدمير البيانات المخزنة في الشبكة المعلوماتية مما يتسبب في خسائر فادحة للجهات المعنية بتلك البيانات، كتدمير بيانات الشركة أما الأضرار المعنوية فتكون مثل التجسس الإلكتروني أو إختراق الأجهزة والحصول على بيانات أو صور سرية خاصة.[1]

كما تثير النتيجة الإجرامية في الجريمة الإلكترونية العديد من الصعوبات كمسألة تحديد زمان ومكان تحقق تلك النتيجة إن كانت تتحقق في العالم الإفتراضي أم في العالم المادي، أم يتحقق أولها في العالم الإفتراضي ويكون هناك إمتداد في النتيجة من العالم الإفتراضي إلى العالم المادي،[2] وهل تقتصر النتيجة الإجرامية على مكان واحد أم أنها تمتد لتشمل عدة دول وأقاليم،[3] كأن يقوم أحد المجرمين في بلد ما باختراق جهاز خادم "SERVER" أحد البنوك في بلد آخر وهذا الخادم موجود في بلد ثالث، فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم؟ أم توقيت بلد البنك

[1] أحمد محمد براك بن حمد، (المواجهة التشريعية للجريمة المعلوماتية بين الواقع والمأمول) مجلة جامعة الأزهر، ع خاص بمؤتمر كلية الحقوق الخامس، مج 19، الصادر في 2017، ص 50.

[2] محمد بن أحمد ، مرجع سابق، ص 97.

[3] يوسف صغير ، مرجع سابق، ص 68.

المسروق؟ أم توقيت جهاز الخادم؟[1] وهذا ما يترتب عليه إشكالية القانون الواجب التطبيق كما أن الجريمة الإلكترونية التي تتحقق نتيجتها في العالم الإفتراضي تكون هناك صعوبة في إكتشافها وإثباتها وتعيق مسألة التحقيق فيها.

3-الرابطة السببية: حتى يكتمل البناء القانوني للجريمة من حيث الركن المادي يستلزم أن يكون هناك إرتباط بين السلوك، سواء كان فعلا أو إمتناعا وبين النتيجة التي ترتبت بفعل إرتباط السبب بالمسبب،[2] فهي الرباط الذي يصل بين الفعل الإجرامي والنتيجة الإجرامية وبها يتم إثبات أن هذا الفعل أدى إلى تلك النتيجة.

فلا يمكن مساءلة الجاني عن نتيجة فعله إلا إذا كانت هناك رابطة بين الفعل والنتيجة، فمتى توفرت هذه الرابطة كان الجاني مسؤولا عن نتيجة فعله أما إذا إنعدمت فإنه يسأل عن فعله ولا يسأل عن نتيجته،[3] فالرابطة السببية هي دستور الجانب المادي في نظرية الجريمة والمسؤولية الجنائية مثلما أن مبدأ الشرعية هو دستور التجريم والعقاب تماما.[4]

ويجب أن نشير في هذه النقطة إلى أن الرابطة السببية باعتبارها عنصرا في الركن المادي للجريمة فإنها تختلف عن فكرة النية الإجرامية باعتبارها عنصرا في الركن المعنوي، فهذه الرابطة هي ذات طبيعة موضوعية يمكن إستخلاصها من الخواص المادية للسلوك ذاته في إحداثه النتيجة المحظورة قانونا، في حين النية الإجرامية هي ذات طبيعة شخصية معنوية تستخلص من الموقف النفسي للجاني في مدى علمه بصلاحية ذلك السلوك لإحداث النتيجة وكذا مدى رغبته ونيته في تحقيق ذلك.[5]

---

[1] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص 48.

[2] محمد بن أحمد ، مرجع سابق، ص 98.

[3] [3] أسامة سيد اللبان، مرجع سابق، ص 19.

[4] جميلة مقدم ،" قيام الرابطة السببية في الجرائم الطبية –دراسة مقارنة–" (أطروحة دكتوراه، كلية الحقوق والعلوم الساسية جامعة الجيلالي اليابس سيدي بلعباس، 2018-2019)، ص 47.

[5] محمد بن أحمد ، مرجع سابق، ص 99.

لكن حينما يتعلق الأمر بالجريمة الإلكترونية ونحاول أن نربط السلوك الإجرامي بالنتيجة المترتبة عنه تثور عدة صعوبات وذلك بسبب الطبيعة المعقدة لهذه الجريمة، حيث هناك إمكانية حدوث عدة نتائج بسبب سلوك إجرامي واحد وذلك راجع لطبيعة النشاط التقني.

فمسألة تحديد الرابطة السببية في هذه الجريمة من المسائل الصعبة والمعقدة جدا وذلك نتيجة للتطور المتسارع في إمكانياتها وكذا تعدد وتنوع أساليب الإتصال بين الأجهزة الإلكترونية وتعدد المراحل التي تمر بها الأوامر المدخلة حتى تخرج وتنفذ النتيجة المراد الحصول عليها.[1]

ثانيا: الركن المعنوي.

قيام الركن المادي الذي سبق الحديث عنه لا يعد مبررا كافيا لمساءلة الجاني باعتباره إرتكب ماديات الجريمة، وإنما حتى يتحقق قيام الجريمة بشكل قانوني لا بد أن يتوفر لدى الجاني القصد الجنائي الذي يقوم عليه الركن المعنوي والذي يسمى كذلك بالركن الأدبي أو الشخصي، والذي يقوم عليه الركن المعنوي ويسمى كذلك بالركن الأدبي أو الشخصي، حيث يعنى بالجانب النفسي للمجرم أو حالته النفسية أثناء إرتكاب الجريمة فإذا كان الركن المادي يعتبر الوجه الخارجي والملموس لها فإن الركن المعنوي يعتبر وجهها الباطيني.

يعرف الركن المعنوي بأنه العلاقة أو الصلة التي تربط بين ماديات الجريمة وشخصية الجاني،[2] وهو إرادة إتجهت على نحو معين وسيطرت على ماديات الجريمة، وبالتالي فهو يعكس مدى خطورة المجرم ويعتبر نتيجة مؤكدة على الإدانة[3]، بمعنى أن المجرم يقدم على إرتكاب الفعل الذي تم تجريمه قانونا بعلمه وإرادته الفعلية طواعية ورغبة وعن إدراك للأهداف التخريبية،[4] فالركن المعنوي هو المسلك الذهني والنفسي للجاني باعتباره محور القانون الجنائي، ففي إطار هذا الركن

---

[1] يوسف صغير ، مرجع سابق، 68.

[2] عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية، ط 1، الرياض، مكتبة القانون والإقتصاد للنشر والتوزيع، ، 2012، ص ص 276، 277.

[3] لورنس سعيد الحوامدة، (الجرائم المعلوماتية أركانها وآلية مكافحتها –دراسة مقارنة–)، مجلة الميزان للدراسات الإسلامية والقانونية، د ع، الصادر في 2017، ص 24.

[4] محمد مكاوي محمد، دينا عبد الله صالح، مرجع سابق، ص 43.

تقوم كافة مقومات المسؤولية الجنائية من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات.[1]

يراد بالركن المعنوي كذلك الإرادة الإجرامية أو الإرادة الآثمة المقترنة بالفعل سواء إتخذت صورة القصد الجرمي وتسمى في هذه الحالة بالجريمة العمدية، أم إتخذت صورة الخطأ غير العمدي وتسمى حينها بالجريمة غير العمدية،[2] ويقوم القصد الجنائي على عنصرين هما:

1-العلم: وهو إدراك الفاعل للأمور،[3] بمعنى أن الجاني خلال إقدامه على إرتكاب جريمته يكون مدركا تماما بأن ما يقوم به مخالف للنصوص القانونية وأن ذلك يدخل في دائرة التجريم، ويترتب عليه عقاب فهو يحيط بكل الوقائع التي يتطلبها القانون لتحقق قيام الجريمة مستوفية لجميع أركانها، فمثلا الذي يقدم على السرقة يكون على علم بأن المال المسروق هو ملك للغير وأنه يتعدى على حق يحميه القانون، ونفس الشيئ الذي يقدم على إختراق النظام المعلوماتي لشركة المساهمة والإعتداء عليه حيث يكون لديه علم بأن هذا النظام يحتوي على معلومات وأسرار تخص هذه الشركة وأن الإعتداء عليه يشكل جريمة إلكترونية معاقب عليها بموجب النصوص القانونية، وانتفاء عنصر العلم يترتب عليه إنتفاء القصد الجنائي.

2-الإرادة: وهي إتجاه السلوك الإجرامي لتحقيق النتيجة،[4] وهي قوة نفسية أو نشاط نفسي توجه نحو تحقيق هدف معين غير مشروع،[5] حيث يسيطر هذا النشاط على الحركات العضوية ويدفعها إلى تحقيق الهدف، فالفعل الإرادي هو الذي يجمع بين الحركة العضوية والعوامل النفسية التي تكون المحرك والدافع للحركات، حيث يتصور الشخص الغرض الذي يسعى إلى بلوغه ثم يتصور الوسيلة التي تؤدي إلى بلوغ الهدف ويفرغ ذلك كله في النشاط المجرم تحقيقا للنتيجة الجرمية.[6] فإرادة

---

[1] عفاف خذيري، مرجع سابق، ص 45.

[2] شريهان ممدوح، (الجرائم المعلوماتية وسبل مواجهتها على المستووين الوطني والدولي)، المجلة الإلكترونية الشاملة، ع 21، الصادر في 2020، ص 14.

[3] لامية طالة، كهينة سلام، مرجع سابق، ص 69.

[4] لامية طالة، كهينة المرجع نفسه، ص 69.

[5] أحمد محمد براك بن حمد، مرجع سابق، ص 51.

[6] محمد ياسين بوزوينة ، مرجع سابق، ص 45.

الفعل لا تعد كافية لوحدها لقيام القصد الجنائي وإنما يستلزم الأمر توجيه تلك الإرادة من أجل تحقيق النتيجة المترتبة عن الفعل، ويجب أن تكون تلك الإرادة حرة لأنه في حالة ما إذا أقدم الجاني على إرتكاب جريمة تحت فعل التهديد أو الإكراه ففي هذه الحالة لا تعتبر الجريمة من إرادته البحتة وهذا ما ينفي عنه القصد الجنائي والذي له صورتين هما:

أ-القصد الجنائي العام: ويعني هذا القصد بأن تنصرف إرادة الجاني إلى تحقيق الفعل المجرم مع العلم بعناصر ذلك الفعل الممنوع قانونا[1]، ونجد بأن هذا القصد يتوفر في جميع الجرائم العمدية وينتفي في الجرائم غير العمدية التي تقوم بسبب الخطأ والإهمال.

ب-القصد الجنائي الخاص: ويتطلب توفره في بعض الجرائم دون الأخرى إلى جانب القصد الجنائي العام، إذ لا يكتفي الفاعل بارتكاب الجريمة وإنما يتأكد من تحقق النتيجة،[2] ففي جريمة القتل مثلا لا يكفي القصد العام فقط وهو إرادة إرتكاب السلوك مع العلم بعدم مشروعية ذلك، بل يجب أن تكون هناك نية إحداث النتيجة المتمثلة في الوفاة، ففرضا قام شخص ما بضرب شخص آخر ولكن دون أن يكون القصد هو القتل ولكن الضحية توفي بسبب ذلك الضرب، ففي هذه الحالة لا نكون بصدد جريمة قتل عمدي وإنما نكون أمام جريمة الضرب والجرح المفضي إلى الوفاة دون قصد وذلك لتخلف القصد الجنائي الخاص.[3]

أما بالنسبة للركن المعنوي في الجريمة الإلكترونية فتعد مسألة تحديده في هذه الجريمة في غاية الأهمية لأنه بناءا على هذا الركن يمكن تحديد طبيعة السلوك المرتكب من قبل الجاني وتكييفه لمعرفة ما إذا كان يستوجب المساءلة الجنائية أم لا؟ وذلك بتحديد القصد الجنائي لديه والذي تنتفي الجريمة الإلكترونية بانتفائه، ففي هذه الجريمة يقوم المجرم الإلكتروني بتوجيه إرادته نحو تحقيق نتيجة إجرامية وذلك بارتكاب أحد الجرائم المنصوص عليها في القوانين والتشريعات مع علمه بأركان تلك الجريمة.

---

[1] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 90.

[2] إسمهان بوضياف، (الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 11، الصادر في سبتمبر 2018، ص 354.

[3] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 91.

والحديث عن الركن المعنوي في الجريمة الإلكترونية يقودنا إلى التساؤل عن القصد الجنائي المطلوب توفره فيها إن كان قصدا عاما أو خاصا؟ حيث أنه يحدث في أحيانا كثيرة أن المجرم الإلكتروني يبرر تصرفه وينفي علمه وأن ما قام به لا يعد جريمة فهو قام بذلك بداعي الفضول فقط أو أن فعله كان من باب الصدفة دون أن تكون له نية الإجرام.

فالأصل أن الفاعل في الجريمة الإلكترونية يكون سلوكه إجرامي نحو إرتكاب فعل ممنوع قانونا مع علمه وقاصدا ذلك ومهما يكن لا يستطيع إثبات إنتفاء علمه كركن للقصد العام،[1] حيث أن هذه الجريمة ترتكب بشكل قصدي بسبب طبيعتها فالمجرم الإلكتروني له قدرة على إستخدام الحاسوب والبيئة الإلكترونية، فهو من الأشخاص الأذكياء الذين لديهم مهارات عالية في إستخدام الأنترنت وبالتالي يكون لديه العلم والإرادة الكاملة بتحقق النتيجة الإجرامية.[2]

فالجريمة الإلكترونية من الجرائم العمدية التي يكفي لقيامها توفر القصد الجنائي العام المتمثل في علم الجاني بعناصر الجريمة مع إتجاه إرادته إلى إلحاق الضرر[3]، كالإضرار بسمعة شركة المساهمة أو بياناتها المخزنة في النظام المعلوماتي.

فمثلا في جريمة الإعتداء على برامج الحاسب الآلي هي جريمة عمدية تقوم بتوفر القصد الجنائي العام لدى الجاني بعنصريه (العلم والإرادة) فالجاني يفترض أن يكون على علم بأن الفعل الذي قام به هو فعل غير مشروع ويشكل إعتداءا على برامج حاسوبية مملوكة للغير، ويجب أن يرافق ذلك العلم إتجاه الإرادة إلى مباشرة الفعل الإجرامي المتمثل في فعل التعدي بالمخالفة للقانون،[4] لكن إذا كان القصد الجنائي العام مطلوب توفره في جميع الجرائم الإلكترونية دون إستثناء كقاعدة عامة ففي مقابل ذلك هناك جرائم إلكترونية تتطلب توفر القصد الجنائي الخاص إلى جانب القصد الجنائي العام.

---

[1] عفاف خذيري، مرجع سابق، ص 46.

[2] مخلد إبراهيم الزعبي، (فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية –دراسة مقارنة–)، المجلة العربية للنشر والتوزيع، ع 37، الصادر في تشرين الثاني 2021، ص 283.

[3] عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، مرجع سابق، ص 91.

[4] لورنس سعيد الحوامدة، مرجع سابق، ص 25.

فمثلا جريمة نشر فيروسات تتطلب لقيامها قصد جنائي خاص فالمجرم يهدف إلى تعطيل عمل الشبكة ونفس الأمر بالنسبة لجريمة تشويه السمعة،[1] أيضا جريمة الدخول غير المشروع إلى مواقع التجارة الإلكترونية تتطلب قصد عام وهو ضرورة علم الجاني بأن فعله المتمثل في الدخول إلى مواقع غير مصرح له الدخول إليها مخالف للقانون وغير مشروع، وأن يتفق مع العلم إرادة الجاني التي تدفعه للقيام بفعل الدخول أما القصد الخاص في هذه الجريمة فيتلخص في نية الإضرار بالغير.[2]

ونجد بأن القضاء الفرنسي قد إستقر على فكرة "سوء النية" وإصباغها على كافة النصوص القانونية التي تطبق بشأن جرائم الحاسوب والأنترنت، حيث إشترط قانون العقوبات الفرنسي مبدأ "سوء النية" حين وجود عدوان حقيقي على النظام المعلوماتي وأن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوفر سوء النية في منطق القصد الخاص وإرادة الإضرار.[3]

أما بالنسبة للجريمة الإلكترونية في التشريع الجزائري فنجد بأنها جريمة عمدية تقوم على الإرادة ولا مجال للخطأ فيها وهذا ما يتجلى من خلال إستعمال المشرع لمصطلح " الغش و العمد" وذلك في المواد 394 مكرر، 394 مكرر1، 394 مكرر2 وبالتالي يعتبر فعل الغش شرطا ضروريا وأساسيا لقيام الجريمة الإلكترونية.

[1] عمر طه خليل، عفاف بديع جميل، مرجع سابق، ص 170.

[2] لورنس سعيد الحوامدة، مرجع سابق، ص 25.

[3] محمد بن أحمد ، مرجع سابق، ص 101.

خلاصة الباب الأول:

من خلال ما تم عرضه في هذا الباب نخلص إلى القول بأن إتجاه شركات المساهمة إلى إعتماد ما أسفرت عليه التطورات التكنولوجية من أجهزة حواسيب ومختلف الشبكات كان حتمية لا بد منها، نظرا لخداماتها الجليلة التي قدمتها لها والتي كانت لها إنعكاسات من خلال توجه هذه الشركات نحو الأعمال والتجارة الإلكترونية وكذا تغيير نمط إدارتها التقليدية بإدارة إلكترونية.

هذا الأمر عمل الجناة على إستغلاله من أجل الإعتداء على شركات المساهمة التي أصبحت بفعل هذه التطورات هدفا للجرائم الإلكترونية ذات الطبيعة المعقدة والغامضة والتي كانت لها أضرار في منتهى الخطورة باعتبارها تستهدف ما يحتويه نظامها المعلوماتي من معطيات وأسرار تخص أعمالها التجارية وذلك من خلال الإعتماد على الأساليب ذات طبيعة تقنية تتناسب والبيئة الإفتراضية لهذه الجرائم وبهذا كانت شركات المساهمة أما نوع جديد من الجرائم أقل ما يقال عنها أنها أخطر من الجرائم التقليدية.

الباب الثاني:
الجرائم الإلكترونية الواقعة على شركات المساهمة وقواعدها الإجرائية والأمنية.

الباب الثاني:
الجرائم الإلكترونية الواقعة على شركات المساهمة وقواعدها الإجرائية والأمنية.

مثلما سبقت الإشارة في الباب الأول فإن التطورات التكنولوجية التي لجأت شركات المساهمة إلى إعتمادها من أجل القيام بأعمالها كان لها الأثر السلبي، والذي لا يمكن في أي حال من الأحوال إخفاؤه كونها سهلت أمام الجناة تنفيذ أعمالهم الإجرامية على هذه الشركات بطريقة إلكترونية، لتتعدد بذلك الجرائم الإلكترونية التي ترتكب ضدها فهي لا تنحصر ضمن صورة واحدة فقط حيث أنه إضافة إلى النوع المستحدث من هذه الجرائم التي تستهدف النظام المعلوماتي لشركات المساهمة من خلال الولوج إليه والبقاء فيه، أو من خلال الإعتداء على معطياته ووظائفه شملت أيضا العديد من الجرائم التقليدية وارتكابها بطريقة إلكترونية.

ونظرا للطابع المعقد الذي تنفرد هذه الجرائم فإن الأمر يستلزم إتباع مجموعة من الإجراءات المحددة حتى يتم القيام بعملية التحري عنها والتحقيق فيها وإسنادها إلى الجهات القضائية المختصة التي تكون كفيلة بالفصل فيها، وحتى يتم ذلك لا بد من الحصول على دليل ذو طابع تقني يتناسب والطبيعة الخاصة لهذه الجرائم كونها لا تخلف وراءها دليل مادي ملموس مثلما هو عليه الحال في ظل الجرائم التقليدية ، وباعتبار أن الجرائم الإلكترونية تشهد إنتشارا رهيبا ضد هذه الشركات إذ أصبحت بالفعل خطرا حقيقيا يهددها، كان لزاما عليها البحث عن آليات تقنية تحقق من خلالها أمنها المعلوماتي، وحتى يتم التطرق إلى كل هذا قمنا بتقسيم هذا الباب إلى فصلين:

الفصل الأول: صور الجرائم الإلكترونية الواقعة على شركات المساهمة.

الفصل الثاني: القواعد الإجرائية والأمنية للجرائم الإلكترونية الواقعة على شركات المساهمة.

الفصل الأول:
صور الجرائم الإلكترونية الواقعة على شركات المساهمة.

الفصل الأول:

صور الجرائم الإلكترونية الواقعة على شركات المساهمة.

تتعدد وتتنوع الجرائم الإلكترونية التي باتت تعترض شركات المساهمة من قبل جناة الفضاء الرقمي على عكس ما كانت عليه في السابق في ظل البيئة التقليدية، حيث كانت الجرائم التي تتعرض لها معروفة ومألوفة تستهدف أموالها المادية.

فالجرائم التي تعترضها اليوم لا تقتصر على نوع واحد فقط، فإضافة إلى تلك الجرائم التقليدية التي كانت تتعرض لها وهي بطبيعة الحال مجرمة بموجب نصوص عقابية سابقة، أصبحت ترتكب ضدها بطريقة تقنية بالنظر إلى الوسيلة التي تنفذ بها، فهي جرائم تقليدية في صورة إلكترونية.

إلى جانب ذلك هناك مجموعة من الجرائم المستحدثة نتيجة التطورات التكنولوجية تستهلك سلامة نظامها المعلوماتي من خلال الدخول والبقاء فيه بطريق الغش أو من خلال الإعتداء على سلامة معطياته ووظائفه، هذا ما سنتطرق إليه بالمناقشة والتحليل ضمن هذا الفصل وذلك بتقسيمه إلى مبحثين:

المبحث الأول: جرائم تقليدية تستهدف شركات المساهمة بطريقة إلكترونية.

المبحث الثاني: جرائم إلكترونية مستحدثة تستهدف شركات المساهمة في نظامها المعلوماتي

.

المبحث الأول:

جرائم تقليدية تستهدف شركات المساهمة بطريقة إلكترونية.

الإعتداء على شركات المساهمة في ظل الجرائم الإلكترونية لم يتوقف عند تلك الجرائم المستحدثة التي إستهدفت شركات المساهمة في نظامها المعلوماتي، بل أن جناة العالم الرقمي عمدوا إلى تطوير أساليبهم الإجرامية أكثر والتي مكنتهم من إرتكاب حتى تلك الجرائم التقليدية بطريقة إلكترونية، لتتعرض بذلك هذه الشركات إلى طائفة أخرى من الجرائم والتي سنتطرق إليها من خلال هذا المبحث وذلك بتقسيمه إلى مطلبين:

المطلب الأول: جريمة التجسس، التزوير وخيانة الأمانة.

المطلب الثاني: جريمة السرقة، النصب وغسيل الأموال.

المطلب الأول:

جريمة التجسس، التزوير وخيانة الأمانة.

في هذا المطلب نتعرض إلى المجموعة الأولى من طائفة الجرائم التقليدية والتي أصبحت ترتكب بطريقة إلكترونية ضد شركات المساهمة والتي تتمثل في كل من جريمة التجسس الإلكتروني **(فرع أول)**، جريمة التزوير الإلكتروني وخيانة الأمانة **(فرع ثاني)**.

الفرع الأول:

جريمة التجسس الإلكتروني.

بعد أن كانت جريمة التجسس تعد من أهم وأخطر الجرائم التي تستهدف كيانات الدول بالدرجة الأولى باعتبارها ذات تأثير بالغ على الوجود السياسي لهذه الدول، حيث كان يمارس ضدها بطرق تقليدية غير أن التغيير الذي شهده العالم على إثر الثورة المعلوماتية التي تمخضت عنها تكنولوجيا رقمية ذات مستوى عال ودقيق من التطور، الشيئ الذي أثر على هذه الجريمة إذ بدأ المفهوم التقليدي لها يتلاشى، فالطرق التقليدية التي كان يعتمد عليها من أجل إرتكابها لم تعد تجدي نفعا في العالم الرقمي كما أن مفهوم هذه الجريمة أصبح أكثر إتساعا من ذي قبل، فلم تعد تقتصر على المجال السياسي والدبلوماسي والعسكري فحسب بل أصبح يشمل إلى جانب ذلك حتى المجال التجاري الذي

أصبح أكثر عرضة لها، وبذلك أصبحت الشركات التجارية وعلى رأسها شركات المساهمة هدفا للتجسس الإلكتروني.

ففي تقرير صادر عن عن وزارة التجارة والصناعة البريطانية حيث تمت الإشارة فيه إلى ارتفاع نسبة جريمة التجسس التي ترتكب ضد الشركات وذلك من 36% سنة 1994 إلى 45% سنة 1999، وحسب إستفتاء تم إجراؤه سنة 1996 لمسؤولي الأمن الصناعي بالشركات في الولايات المتحدة الأمريكية بأن هناك العديد من الدول قد تحصلت بطريقة غير مشروعة على معلومات سرية تخص الأنشطة التجارية والصناعية لتلك الشركات،[1] وهناك دراسات قد بينت التنافس الشديد الحاصل بين الشركات إذ تضاعف حجم نفقاتها على التجسس من أجل جمع معلومات عن الشركات المنافسة، ففي بعض الحالات بلغ حجم نفقة الشركة الواحدة فقط أكثر من مليار دولار سنويا على عمليات التجسس،[2] ومن أجل التفصيل أكثر نتطرق إلى تعريف جريمة التجسس الإلكتروني أولا ثم الأركان التي تقوم عليها.

أولا: تعريف التجسس الإلكتروني.

تم تعريفه على أنه الكشف والإطلاع على أسرار تخص الغير قد تم حفظها على أحد الأجهزة الإلكترونية ويمنع على غير المسموح لهم من الإطلاع عليها،[3] وهو أيضا عبارة عن إختراق للمواقع الإلكترونية قصد التوصل إلى معلومات تكون على درجة كبيرة من الأهمية بالنسبة للطرف المستهدف،[4] كما أنه ترصد ومراقبة من خلال عملية التسلل إلى الأجهزة الحاسوبية وذلك باعتراض

---

[1] عبد الصبور عبد القوي علي مصري، منال عبد اللاه عبد الرحمن،، المحكمة الرقمية والجريمة المعلوماتية، مرجع سابق، ص 159.

[2] رواء زكي يونس الطويل، (التجارة الإلكترونية والتجسس الاقتصادي)، مجلة آداب الرافدين، ع 51، الصادر في 2008، ص 9.

[3] عبد الحليم بن بادة، محمد سعد بوحادة، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة –دراسة سياسية قانونية– مداخلة مقدمة إلى" الملتقى الدولي الأول ، أمن المعلومات في الفضاء الإلكتروني الرهانات والتحديات في شمال إفريقيا" ،كلية الحقوق والعلوم السياسية، جامعة غرداية، المنعقد في 17 و 18 فيفري 2020، الجزائر، ص 5.

[4] حنان أوشن ، عماد الدين وادي ، (التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري)، "مجلة الحقوق والعلوم السياسية"، ع 2 الصادر في جويلية 2014، ص 132.

الإشارات والمعطيات التي يتم إرسالها عبر تلك الأجهزة، لذلك يمكن إعتبار أجهزة الحاسوب من أكثر وأهم الوسائل التي يتم الإستعانة بها من أجل القيام بعملية التجسس إذ تمكن المختصين من الحصول على المعلومات دون علم أصحابها بذلك،[1] وهو كذلك ولوج الجاني القائم بعملية التجسس إلى شبكة معلوماتية أو نظام معلوماتي أو مواقع إلكترونية بغية الحصول على محتوى لا يكون متاح لكافة الأشخاص، حيث أن الوصول إليه يترتب عليه المساس بأصحابها[2].

وبالتالي الشيئ الملاحظ على جملة التعريفات المقدمة هو أنها حتى وإن إختلفت في الألفاظ إلا أن المضمون واحد، حيث أن التجسس الإلكتروني يستهدف الحصول على معلومات سرية بوسائل تقنية، كما أن الشيئ المميز في هذا التجسس هو أن الوسيلة المستخدمة فيه قد ساعدت الجاني ويسرت الطريق أمامه في القيام بعملية التجسس وذلك بعيدا عن أعين المستهدفين.

أما عن أساس جريمة التجسس الإلكتروني ضمن المجال التشريعي فنجد بأنها قد سميت أحيانا بالإعتراض غير القانوني، هذا ما تم التص عليه في المادة الثالثة من إتفاقية بودابست والتي جاء فيها " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما أرتكب عمدا وبغير حق الإعتراض باستخدام وسائل فنية للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من داخل نظام كومبيوتر، بما في ذلك الإنبعاثات الكهرومغناطسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات، ويجوز للدولة الطرف أن تستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية بنية غير صادقة أو في إرتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر".

فالشيئ الملاحظ هو أن هذه المادة جاءت من أجل تكريس حماية البيانات والمعلومات والمراسلات التي يتم نقلها عبر الوسائل الفنية غير العلنية، حيث أن تدخل أطراف أخرى في ذلك يعد إنتهاكا مجرما، ونفس التسمية جاءت أيضا في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي نصت في مادتها السابقة على أن الإعتراض المتعمد الذي يتم دون وجه حق لخط سير البيانات بأي

---

[1] حنان أوشن ، عماد الدين وادي، مرجع سابق ، ص 132.

[2] إسراء يونس هادي، أسامة أحمد النعيمي، (جريمة التجسس الإلكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011)، مجلة كلية القانون للعلوم القانونية والسياسية ، ع 36، مج 10، الصادر في 2021، ص 37.

من الوسائل الفنية وقطع بث أو إستقبال بيانات تقنية المعلومات، فكلا المادتين لم تحدد نوع المعلومات التي يقع عليها فعل الإعتراض ولم تحصرها في مجال معين كالمجال العسكري مثلا، وإنما جاءت شاملة لجميع المعلومات والإتصالات التي تكون لها خصوصية وسرية بما ذلك المعلومات التجارية ومنها المعلومات الخاصة بشركات المساهمة.

ورغم أن تسمية الإعتراض قد تم إنتقادها على أساس أن الإعتراض غير القانوني للبيانات والمعلومات ما هو في الأصل إلا ركن مادي للجريمة الأساسية –جريمة التجسس الإلكتروني– وبما أن هذا الفعل يرتكب في بيئة رقمية يكون التجسس إلكترونيا لذلك كان من الأفضل والأصح إصطلاح تسمية التجسس الإلكتروني.[1]

أما بالنسة للمشرع الجزائري فقد نص على جريمة التجسس ضمن قانون العقوبات من المادة 61 إلى المادة 65، حيث نجد بأن المادة 63 قد نصت في فقرتها الثانية على تجريم التجسس حيث جاء فيها "الإستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات..."

وبالتالي فعبارة "بأية وسيلة كانت" توحي بإمكانية إرتكاب التجسس بوسيلة إلكترونية وبذلك يكون المشرع قد أشار ضمنيا إلى التجسس الإلكتروني، لكن ما ينبغي أن نشير إليه هو أنه وإن كان من الممكن حصر التجسس بالطرق التقليدية في المجال العسكري فقط وذلك صحيح ومقبول، لكن حينما يتعلق الأمر بالتجسس بوسائل تقنية فمن الصعب جدا حصره في ذلك المجال فقط، ويرجع ذلك إلى أن فعل الإعتراض غير القانوني للبيانات والمعلومات لا يقع فقط على المعلومات العسكرية بل يتعدى ذلك ليشمل حتى المعلومات التجارية وبشكل واسع، كون أن التنافس بين الشركات زادت حدته نتيجة التطورات التقنية التي يشهدها المجال التجاري.

كما أن المعلومات والوثائق السرية لم تعد حكرا على الدول فحسب وإنما تتعلق السرية بالمعلومة أو الوثيقة لا بأصحابها،[2] مما يعني أن شركات المساهمة كأشخاص معنوية تقف على قدم المساواة

[1] عزيزة رابحي ، مرجع سابق، ص 209.

[2] أسامة أحمد المناعسة، جلال محمد الزغبي، مرجع سابق، ص 300.

مع الدول فيما يتعلق بالتجريم والعقاب إذ يحدث أن تتعرض هذه الشركات إلى عملية إختراق سواء من قبل موظفيها أو أطراف خارجية من أجل الإطلاع على وثائقها وأسرارها.

وما تم إكتشافه مؤخرا في مجال التجسس هو أن هناك شركات متخصصة بحيث يرتكز نشاطها على تقديم مساعدات للشركات التجارية في مجال التجسس وذلك بطبيعة الحال بمقابل مادي، كما أن هناك العديد من الشركات التي تطلب هذا النوع من الخدمات وترتكز في تأدية خداماتها على توظيف الكوادر المختصة والمدربة،[1] ففي الولايات المتحدة الأمريكية قد خسرت إحدى الشركات البترولية جميع مناقصاتها لأشهر عدة متتالية حيث كانت ترسو تلك المناقصات لصالح شركة أخرى منافسة وذلك بسبب عملية التجسس التي قامت بها هذه الشركة على العروض التي كانت تقدمها الشركة الأخرى وذلك من خلال توصيلات سرية للحاسوب الآلي للشركة والذي كان يعطي إمكانية التعرف على العروض المقدمة.[2]

من جهة أخرى نجد المادة 65 من قانون العقوبات التي جاء فيها "الإضرار بمصالح الدفاع الوطني أو الاقتصاد الوطني" مما يعني بأن التجسس يمس بالمجال التجاري كون أن الاقتصاد الوطني قوامه الشركات الكبرى والتي هي في الأساس عبارة عن شركات مساهمة إذ أن التجسس عليها يشكل في الأساس إضرار بالإقتصاد الوطني كونها بمثابة العصب له والعماد الذي يقوم عليه.

أما بالنسبة للمحل الذي تنصب عليه جريمة التجسس الإلكتروني في إطار شركات المساهمة فإنها تستهدف الأسرار المتعلقة بخطط التسويق، الحسابات المالية الخاصة بها من خلال الإطلاع على عملية الحسابات المرتبطة بالتكلفة، كشوفات ميزانية الشركات، عناوين عملائها كما تستهدف إلى جانب ذلك أيضا الكشف على الأسرار الخاصة بالعملية الإنتاجية والقيام بتطويرها وذلك بهدف

---

[1] رواء زكي يونس الطويل، مرجع سابق، ص ص 9، 10.

[2] فايز محمد راجح غلاب، فايز محمد راجح غلاب، "الجرائم المعلوماتية في القانون الجزائري واليمني"، (أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2010-2011)، ص 17.

إختصار الوقت وتوفير المال الذي يضيع في عملية الأبحاث والنتيجة الحصول على أفضل منتوج دون تكلفة أو تحمل للأعباء المالية.[1]

فالقيمة الإستراتجية للمعلومات في إطار شركات المساهمة جعلها تمثل النموذج الجديد لرأس مالها الشيئ الذي زاد من قيمتها وجعلها محلا للتجسس، وهي لا تتمثل في المعلومات التقنية فقط وإنما تشمل جميع المعلومات ذات العلاقة بالشركة سواء كانت إقتصادية، مالية أو شخصية كبيانات الإنتاج، التسويق وكذا البيانات المتعلقة بالتنمية والتطوير، وهناك من يشبه التجسس على شركات المساهمة وكأنه بمثابة سرطان لإقتصاديات الدول إذ أن حماية أسرار أعمالها هو في الأساس حماية للتكنولوجيا ولمنصب عمل وحماية لإستثمارات كبيرة حساسة،[2] الأمر الذي يزيد من عملية التحفيز بين الشركات المتنافسة من أجل التجسس على أحدث وآخر التطورات والإبتكارات وبالتالي إحتكار الأسواق والسيطرة عليها وإزاحة الشركة المنافسة من الساحة.

ومن بين أشهر قضايا التجسس في إطار كبرى الشركات ما حدث سنة 2011 حين قام مخترقون صينيون بهدف التجسس من إختراق قواعد بيانات أجهزة الحواسيب الخاصة بخمسة شركات للنفط والغاز وصرح حينها " ديميتري ألبيروفيتش" نائب رئيس "MCAEE" لأبحاث التهديدات أن تلك المعلومات في غاية الحساسية وعلى درجة كبيرة من الأهمية ومن شأنها أن تحقق مبالغ هائلة للمنافسين، أيضا ما قامت شركة "هيتاشي" من أعمال التجسس على معلومات الحاسوب السرية الخاصة بشركة "IBM" من إرسالها إلى اليابان وكانت شركة "IBM" قد فازت بالقضية بعد أن أقرت الشركة الجانية "هيتاشي" بالتهمة المنسوبة إليها وتم على إثرها مقاضاة 22 من رجال الأعمال اليابانين وكان أغلبهم من كبار المسؤولين.[3]

---

[1] منذر عبد الرزاق العمايرة، "مدى الحماية الجنائية للمعلومات عبر الحاسوب والأنترنت دراسة مقارنة" (أطروحة دكتوراه، كلية القانون، جامعة عمان العربية، 2012)، ص 265.

[2] نادية سلامي، "آليات مكافحة التجسس الإلكتروني"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي تبسة، 2018-2019)، ص ص 57، 77.

[3] محمد حطاب، أشهر حالات التجسس الصناعي في العالم، مقال منشور بتاريخ 2020/04/1، أطلع عليه بتاريخ 07/15/ 2023 ، متاح على الرابط: https://abunawaf.com

أما على الساحة العربية فنذكر قضية "عزام عزام" وهو جاسوس قبض عليه في دولة مصر وذلك بهدف التجسس على الشركات المصرية وكذا نوعية المصانع والكيفية التي يتم بها إدارة أعمالهم وعلاقاتهم الاقتصادية، وكذا ما أعلنت عنه دولة الإمارات في يوليو 2001 حيث تم ضبط بريطانين يقومون بأعمال التجسس على الشركات الإماراتية.[1]

ثانيا: أركان جريمة التجسس الإلكتروني في إطار شركة المساهمة.

حتى تقوم جريمة التجسس الإلكتروني ضد شركة المساهمة لا بد من تحقق كل من ركنيها المادي وكذا المعنوي.

1-الركن المادي: مثلما سبقت الإشارة في المادة الثالثة من إتفاقية بودابست وكذا المادة السابعة من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات فإن فعل الإعتراض يمثل أساسا الركن المادي الذي تقوم عليه جريمة التجسس الإلكتروني، فحتى يمكن القول بأن شركة المساهمة قد تعرضت لجريمة تجسس إلكتروني لا بد أن يقوم الجاني بفعل الإعتراض دون وجه حق على بياناتها بوسائل تقنية غير علنية.

وفعل الإعتراض يعرف على أنه التنصت أو نقل للبيانات التي تتم داخل جهاز الحاسوب أو تلك التي تتم عبر جهازين عن بعد، وذلك من خلال الشبكات المعلوماتية المختلفة أو بترجمة الإنبعاثات الكهرومغناطسية التي تصدر من الحاسب أو التي تتم عبر الأجهزة اللاسلكية عن طريق أي من الوسائل الفنية غير العلنية،[2] كما يعرف على أنه رصد للإشارات الكهرومغناطسية وذلك في الأنظمة المعلوماتية ليتم بعدها تحليلها واسترجاع المعلومات وكذا المقروءة منها،[3] والإعتراض هو

---

[1]محمد بوبوش، التجسس الاقتصادي القوة الخفية للدول العظمى، مقال منشور بتاريخ 2009/04/26، أطلع عليه بتاريخ 2023/07/15 ، متاح على الرابط: https://www.hespress.com ›

[2]بهاء فهمي الكبيجي، "مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة"، (رسالة ماجستير، جامعة الشرق الأوسط، 2013)، ، ص 47.

[3]ضرغام جابر عطوش آل مواش، مرجع سابق، ص 202.

جمع للمعلومات عن بعد،[1] وذلك كله من أجل الوصول إلى المعلومات السرية غير المصرح بها والتي تخص شركات المساهمة.

أما بالنسبة للمشرع الجزائري فإنه لم يتطرق إلى فعل الإعتراض بموجب نص خاص وإنما نص على تجريم أفعال التلصص وذلك بموجب المادة 164 من القانون 18-04[2] والتي جاء فيها " يعاقب بالحبس من سنة (1) إلى خمسة (5) سنوات وبغرامة من 500.000دج إلى 1.000.000دج كل من ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها"

كما تم تعريف الاتصالات الإلكترونية في الفقرة "و" من المادة الثانية من القانون رقم 09-04 على أنها " أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية" فمصطلح "أي وسيلة إلكترونية" إستخدمه المشرع من أجل الدلالة على الوسائل التي يتم من خلالها إنتقال المعلومات وتداولها.

وفعل الإعتراض يتحقق عن طريق الإعتماد على الوسائل الفنية التي تؤدي إلى إعتراض جميع الأشكال التي يتم من خلالها النقل الإلكتروني للمعلومات،[3] كما ينبغي أن تكون تلك الوسائل الفنية غير علنية أي غير عمومية.

كما يشترط في فعل الإعتراض أن يتم بشكل غير مشروع أي دون وجه حق فجريمة التجسس الإلكتروني على شركة المساهمة يمكن أن تقع من طرف أي شخص بغض النظر عن صفته سواء كان يعمل في الأنظمة الحاسوبية لها أو لا علاقة له بذلك وإنما يجب أن يكون هذا الشخص من الأشخاص الذين ليس لهم حق الحصول على تلك المعلومات السرية.[4]

---

[1] نجاة عباوي، (الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات)، مجلة دفاتر السياسة والقانون، ع 16، الصادر في جانفي 2017، ص 285.

[2] القانون رقم 18-04 ،مرجع سابق.

[3] عزيزة رابحي ، مرجع سابق، ص 213.

[4] صورية بوربابة ، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 113.

2- الركن المعنوي: يتضح جليا من خلال النصوص السالفة الذكر بأن هذه الجريمة تعد من ضمن الجرائم العمدية والتي يتطلب قيامها تحقق القصد الجنائي العام بعنصريه العلم والإرادة.

بالنسبة لعنصر العلم يجب أن يكون الجاني عالما وقت إرتكابه للجريمة بأن حصوله على تلك المعلومات التي تخص شركات المساهمة قد تم بطريقة غير مشروعة وضد إرادتها باعتبار أنه لا يجوز الإطلاع عليها، فهي غير متاحة لعامة الناس و أن من شأن فعله أن يتسبب في إفشائها إلى جهة أخرى منافسة مما يترتب عليه إلحاق أضرار بهذه الشركات.

إلى جانب عنصر العلم يجب أن تتجه إرادة الجاني كذلك إلى تحقيق فعله الذي يعد مخالفا للقانون ودون أي إكراه.

الفرع الثاني:

جريمة التزوير الإلكتروني وخيانة الأمانة.

من خلال هذا الفرع نتعرف على كل من جرميتي التزوير الإلكتروني وخيانة الأمانة، والتي أصبحت شركات المساهمة تتعرض لهما بشكل واسع في ظل الأساليب التقنية التي سهلت من عملية إرتكابهما.

أولا: جريمة التزوير الإلكتروني.

يمكن إعتبار التزوير الإلكتروني نمط من أنماط الغش في المجال المعلوماتي والتي لم تعد شركة المساهمة بمنأى عنه نتيجة إعتمادها بشكل شبه كلي على الدعامات الإلكترونية وتخليها عن المستندات الورقية، ومن أجل توضيح هذه الجريمة بصورة أوضح نتطرق إلى تعريف التزوير الإكتروني أولا ثم نبين الأركان التي يقوم عليها.

1- تعريف التزوير الإلكتروني: يعرف التزوير الإلكتروني على أنه ذلك التغيير الذي يرتكب عمدا للبيانات التي يتضمنها المستند الإلكتروني بغية التضليل،[1] وهو أيضا التعديل الذي يمس بالبيانات

[1] Protéger contre la falsification de document, publié le 23/12/2019, consulté le 18/06/2023, sur le site : https://nec-itplatform.com

التي يتضمنها نظام المعلومات سواء كان ذلك من خلال إلغاء البيانات التي كانت موجودة فعلا أو من خلال إضافة بيانات جديدة لم تكن موجودة أصلا من قبل.[1]

كما ورد تعريفه في المادة السابعة من الإتفاقية المتعلقة بالجريمة الإلكترونية "بودابست" والتي جاء فيها بأنه على كل دولة طرف أن تعتمد ما يلزم من تدابير تشريعية وغيرها لتجريم الأفعال التالية في قانونها الوطني، إذا ما أرتكبت عمدا وبغير حق : إدخال، تغيير، حذف أو إتلاف بيانات كومبيوتر بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد إعتبارها أو إستخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا، ويجوز للدولة الطرف أن تشترط وجود نية الإحتيال أو نية غير صادقة مشابهة سابقة لإلحاق المسؤولية الجنائية.

في حين عرفته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال مادتها العاشرة التي جاء فيها بأنه إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه أن يحدث ضررا وذلك بنية إستعمالها كبيانات صحيحة.

أما إذا جئنا إلى المنظومة القانونية الجزائرية فنجد بأن المشرع الجزائري رغم التعديلات التي جاء بها من أجل مكافحة الجريمة الإلكترونية ، غير أنه لم يتطرق إلى جريمة التزوير الإلكتروني بصورة مستقلة فقط ما تم النص عليه في القانون رقم 24-02[2] يتعلق بمكافحة التزوير واستعمال المزور وذلك من المادة 1 إلى المادة 83 منه ، وعلى خلاف ذلك نجد بأن هناك العديد من التشريعات التي خصت جريمة التزوير الإلكتروني بنصوص مستقلة على غرار المشرع الفرنسي الذي تطرق إليها في المادة 441-1 من قانون العقوبات.[3]

2- أركان جريمة التزوير الإلكتروني: يتطلب قيام هذه الجريمة تحقق كل من ركنيها المادي والمعنوي شأنها في ذلك شأن بقية الجرائم.

---

[1] عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط 1، المملكة العربية السعودية، جامعة نايف العربية للعلوم الأمنية، ، 2015، ص 54.

[2] القانون رقم 24-02 مؤرخ في 26 فبراير 2024 يتعلق بمكافحة التزوير واستعمال المزور، ج ر ج ج، ع 15 الصادر في 29 فبراير 2924.

[3] Art: 441-1: Constitue un faux toute altération frauduleuse de la vérité, de nature à cause un préjudice et accomplie par quelque moyen que ce soit, dans un écrit au tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

أ-الركن المادي: حتى يمكن القول بأن شركات المساهمة قد تعرضت لجريمة التزوير الإلكتروني لا بد أن يقع ذلك على أحد مستنداتها الإلكترونية من خلال تغيير الحقيقة الواردة فيها بغية إلحاق الضرر بها، وبالتالي فالركن المادي لهذه الجريمة في إطار شركة المساهمة يقوم على ثلاث عناصر.

*وجود مستند إلكتروني: والذي يعتبر المحل الذي تقع جريمة التزوير الإلكتروني باعتباره محل حماية من أجل المحافظة على فحواه و الذي يعرف بأنه أية دعامة ذات طبيعة مادية يتم تهيأتها لإستقبال المعلومات وتسجيلها عليها وذلك عن طريق عملية المعالجة الآلية، والمستند الإلكتروني هو أيضا تلك الدعامة المادية التي يمكن أن تحول المعطيات التي يتم تسجيلها عليها إلى لغة الآلة،[1] كما أنه يتمثل في أي جسم منعزل أو من الممكن عزله عن النظام المعلوماتي قد سبق وتم تسجيل معطيات ما عليه، لذلك يمكن القول بوقوع جريمة التزوير الإلكتروني سواء كانت مخرجات الحاسب الآلي في شكل ورقي أو في شكل معطيات ذات طابع رقمي،[2] ويعود السبب في ظهور المستند الإلكتروني وإنشاره بشكل واسع إلى التطور الذي شهدته التجارة الإلكترونية، فوجدت شركة المساهمة نفسها مضطرة إلى إعتماده، وفي هذا الصدد نجد العلامة التجارية والتي تم إعتبارها من قبيل المستندات الإلكترونية بحث تتعرض شركة المساهمة إلى جريمة تزوير علامتها إلكترونيا بشكل كبير.

---

[1] حمزة بلحسيني، "الحماية الجزائية للمستند الإلكتروني"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة جيلالي اليابس سيدي بلعباس، 2019-2020)، ص 23.

[2] عبد الله بلقاسم، (الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية) مجلة الدراسات القانونية المقارنة،ع 2، مج 6، الصادر في ديسمبر 2020) ص 985.

بالنسبة للمشرع الجزائري وبتفحص جملة النصوص القانونية التي جاء بها نجد بأنه لم تتضمن أي تعريف للمستند الإلكتروني وإنما نص فقط على الإثبات بالكتابة الإلكترونية وذلك من خلال المادة 323 مكرر والتي أضافها بموجب القانون 05-10 المعدل والمتمم للقانون المدني حيث جاء فيها " ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها، كما نص في المادة 323 مكرر1 من نفس القانون على أنه " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها" وبذلك يكون المشرع الجزائري قد إنتقل من الإثبات بالكتابة الورقية إلى الإثبات بالكتابة الإلكترونية.

بحيث تعرف على أنها عبارة عن شكل مميز ينطوي على معنى معين يكون منسوبا إلى شخص محدد بذاته دون سواه وذلك بهدف تمييز منتوجاته أو بضائعه عن غيرها،[1] كما تعرف بأنها كل صورة مميزة تتشكل من أسماء أو كلمات أو إمضاءات أو حروف أو أرقام أو رسوم أو رموز أو عناوين أو دمغات أو أختام أو صور أو نقوش أو إعلانات،[2] ومع إنتشار العلامة التجارية على المواقع الإفتراضية أصبح من الممكن جدا تعرضها لجريمة التزوير الإلكتروني، من ذلك مثلا أن يتم نقل العلامة التجارية الخاصة بشركة المساهمة ووضعها على موقع آخر وذلك فقط من أجل تضليل عملائها.

-تغيير حقيقة المستند الإلكتروني لشركة المساهمة: ويعد تغيير الحقيقة الأساس الذي تستند إليه جريمة التزوير الإلكتروني في إطار شركات المساهمة كون أن ذلك التغيير يزعزع ثقتها ويمس بحقوقها.

وتغيير الحقيقة يعرف على أنه إحداث تغييرات على المستند الإلكتروني ما يؤدي إلى تغيير مضمونه أو شكله ولكن دون أن يترتب على ذلك إعدامه أو إهدار قيمته،[3] بمعنى أن تستبدل الحقيقة بحقيقة مخالفة لها يتم إنشاؤها من جديد،[4] ولا يشترط أن يتم تغيير الحقيقة بصفة كلية وإنما يمكن أن تتحقق جريمة التزوير الإلكتروني إذا ما تم تغيير تلك الحقيقة بصفة جزئية فقط والتي تمثل السلوك الإجرامي في هذه الجريمة وبدون هذا الفعل لا قيام لجريمة التزوير الإلكتروني في هذه الشركات.

وفي هذا الصدد يجب الإشارة أيضا إلى أن تغيير الحقيقة يكون بطريقة رقمية من خلال إستخدام النظام المعلوماتي لشركات المساهمة بصفة غير مشروعة وسواء كان ذلك التغيير ماديا أو

---

[1] عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، ط1، عمان، دار الثقافة للنشر والتوزيع، 2010 ، ص 191.

[2] المرجع نفسه، ص 164.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت دراسة متعمقة في جرائم الحاسب الآلي والأنترنت، د،ط، جمهورية مصر العربية، بهجات للطباعة والتجليد،2009، ص 144.

[4] عادل مستاري، زوليخة رواحنة ،(جريمة التزوير الإلكتروني)، مجلة العلوم الإنسانية، ع 46، الصادر في مارس 2017، ص 301.

معنويا، فإذا ما تم التزوير بطريقة مادية فإن ذلك يكون بصفة لاحقة أي يلي عملية إنشاء المستند الإلكتروني الأصلي ومن ذلك مثلا نجد:

-التزوير الإلكتروني بوضع إمضاءات مزورة ويتم بإدراج إمضاءات مزورة داخل الجهاز بواسطة الماسح الضوئي الذي يكون موصولا بجهاز الحاسوب، ليضاف ذلك الإمضاء على أحد مستندات الشركة بعد أن تمت معالجتها لتصبح ذات مضمون مزور، غير أنه بذلك الإمضاء ينسب المستند إلى الشركة رغم أنه لم يصدر عنها مما يخول الجاني التصرف باسمها كأن يتعلق المستند المزور بقائمة البضاعة وأسعارها المحددة،[1] وبنفس الطريقة يتم تزوير الأختام الخاصة بشركات المساهمة أيضا.

-التزوير الإلكتروني من خلال أفعال الإدخال، الإزالة والتعديل، حيث أن فعل الإدخال يتم من خلال إضافة معطيات سواء جديدة كإضافة رقم مثلا إلى مبلغ معين ومن ذلك ما قام به المشرف على تشغيل أجهزة الحاسوب الخاصة بإحدى البنوك في الولايات المتحدة الأمريكية حين أقدم على زيادة مبالغ إلى حسابات أصدقائه لترتفع بذلك قيمة أرصدتهم،[2] أما فعل الإزالة فيكون بحذف معطيات سواء تمثلت في كلمات أو أرقام أو رموز، في حين فعل التعديل يتجسد من خلال إستبدال المعطيات الموجودة بمعطيات أخرى سواء كانت صحيحة أو خاطئة، وما نلاحظه على هذه الطريقة في التزوير في إطار شركات المساهمة تكون أسهل بكثير من الطريقة التقليدية أين يخلف الجاني آثار تدل على عملية التزوير.

وقد سبق وأشرنا إلى هذه الأفعال حيت تطرقنا إلى جريمة التلاعب بمعطيات شركات المساهمة والتي تم تجريمها من قبل المشرع الجزائري في نص المادة 394 مكرر1، حيث أن التلاعب بمعطيات هذه الشركات يترتب عليه جريمة أخرى تتمثل في تزوير مستنداتها وبذلك يكون المشرع قد أشار إلى جريمة التزوير الإلكتروني من خلال هذه الأفعال، والتي تعد مستحدثة مقارنة بالأفعال المذكورة في جريمة التزوير التقليدية.

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص ص 183، 184.

[2] خدوجة الذهبي، "الحماية الجزائية للمعاملات الإلكترونية دراسة مقارنة"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2018-2019)، ص 70.

التزوير الإلكتروني بواسطة الإصطناع والتقليد، بالنسبة للإصطناع يعني خلق محرر إلكتروني بأكمله وفقا لرغبة الجاني لينسب بعدها إلى غير مصدره،[1] وكمثال على الإصطناع في إطار شركات المساهمة أن يعمد الجاني إلى إنشاء مواقع تكون وهمية وينسبها إلى هذه الشركة والتي لها مواقع على شبكة الأنترنت وذلك بغية الإستيلاء على البيانات المتعلقة بمستخدمي مواقعها الحقيقية كأرقام بطاقاتهم الإئتمانية.[2]

أما التقليد فهو أن يتم إنشاء مستند إلكتروني يكون مشابه تماما للمستند الأصلي،[3] ومن ذلك تقليد العلامة التجارية لشركات المساهمة أو دفاترها التجارية أو نسخ برامجها دون ترخيص منها.[4]

أما التزوير بطريقة معنوية والذي يترتب عليه تغيير في مضمون المستند لا في شكله ويقع هذا النوع من التزوير عند إنشاء المستند،[5] ويكون ذلك من خلال تدوين تصريحات لم تصدر عن أصحاب الشركة أو تكون مخالفة لإقرارهم أو من خلال جعل وقائع خاطئة في شكل صحيح أو بإسقاط معلومات صحيحة وردت ليتم إغفالها إو إيرادها بطريقة غير صحيحة.[6]

وإن كان هناك من يرى بعدم إمكانية تحقق التزوير الإلكتروني بطريقة معنوية باعتبار أن هذا التزوير لا يمكن وقوعه إلا خلال فترة التعبير عن الأفكار التي يتضمنها المستند وفي الأساس أن تلك الأفكار قد سبق التعبير عنها من قبل ذوي الشأن،[7] غير أننا لا نؤيد هذا القول ونرى عكس ذلك خاصة عندما يتعلق الأمر بشركات المساهمة فاعتمادها على تقنيات المعلومات في كل ما تقوم به من أعمال سواء تعلق الأمر بحجم أرباحها وخسائرها، كميات الإنتاج التي تقوم بها وكيفيات توزيعها

---

[1] إلهام بن خليفة، "الحماية الجنائية للمحررات الإلكترونية من التزوير"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2015-2016)، ص 104.

[2] صالح شنين، "الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة"،(أطروحة دكتوراه، كلية الحقوق جامعة أبو بكر بلقايد تلمسان، 2012-2013)، ، ص 61.

[3] عادل مستاري، زوليخة رواحنة ، مرجع سابق، ص 301.

[4] صالح شنين، مرجع سابق، ص 61.

[5] عبد الفتاح بيومي حجازي، مرجع سابق، ص 203.

[6] خدوجة الذهبي ، مرجع سابق، ص 70.

[7] فتيحة عمارة، (جريمة التزوير الإلكتروني)، مجلة القانون والمجتمع، ع 1، مج 7، الصادر في 2019، ص 179.

أو عدد عمالها والرواتب التي يتقاضونها أو إعداد ميزانيتها فأكيد أن هذه الأعمال تخولها لموظف ذو دراية وخبرة في المجال المعلوماتي من أجل القيام بمعالجتها آليا وبطبيعة الحال أثناء القيام بذلك يمكن للموظف كتابة بيانات غير تلك التي طلب منه رصدها في جهاز الحاسوب.[1] كما يمكن أن يتحقق في حالة إذا ما تعمد محاسب الشركة خلال عملية إعداده لرواتب عمالها من إسقاط دفعة الدين التي قام بتسديها أحد العمال من راتبه بمناسبة حصوله على قرض أو كامتناعه من التأشير على مديونيته لهذه الشركة،[2] حيث أن القيام بهذه الأعمال يتم وفق برنامج معين على أحد أجهزة حواسيب الشركة لذلك فنحن نقر بإمكانية وقوع التزوير الإلكتروني بهذه الطريقة ضمن شركات المساهمة خاصة مع تزايد إستعمالها للبيانات المعلوماتية في كافة أعمالها ومعاملاتها التجارية كما نقر أيضا بأنه حينما يتعلق الأمر بالتزوير الإلكتروني وفي إطار شركة بحجم شركات المساهمة فأكيد من الصعب جدا أن يتم حصر التزوير في طرق محددة كون أن التزوير الإلكتروني في إطار هذه الشركة يتطور بتطور التقنيات التي تعتمدها في القيام بأعمالها، لذلك فنحن نرى بأن المشرع الفرنسي أحسن ما فعل حينما أضاف عبارة " بأية طريقة كانت" فهي عبارة فضفاضة تتسع لتشمل كافة الطرق التي يتم بها التزوير سواء كانت مادية أو معنوية، لذلك حبذا لو أن المشرع الجزائري يحذو حذو نظيره الفرنسي خاصة وأن التزوير الإلكتروني أصبح يمس بشركات تمثل عصب الاقتصاد للبلاد.

-تعرض شركات المساهمة لعنصر الضرر: ويعرف الضرر عموما بأنه إنتهاك يمس بحق أو مصلحة محمية قانونا خشية تغيير حقيقتها،[3] ونظرا لأهمية هذا العنصر في تحقق جريمة التزوير هناك بعض فقهاء القانون الجنائي مثل الدكتور "محمود نجيب حسن" ذهبوا إلى القول بأن عنصر الضرر يمكن إعتباره بمثابة ركن مستقل بذاته ضمن هذه الجريمة،[4] وهذا ما يدل على أهمية تحقق هذا العنصر حتى تقوم جريمة التزوير وبدونه لا قيام لهذه الجريمة إذ تنتفي بانتفائه.

---

[1] إلهام بن خليفة، مرجع سابق، ص106.

[2] صالح شنين، مرجع سابق، ص63.

[3] عامر محمود الكسواني، مرجع سابق، ص 211.

[4] عبد الفتاح بيومي حجازي، مرجع سابق، ص 239.

كما تجب الإشارة إلى أنه لا يشترط تحقق ضرر محدد وإنما يكفي أن يكون هذا الضرر محتمل الوقوع،[1] كما يمكن أن يكون ضررا ماديا أو معنويا، أيضا لا يشترط أن يكون على درجة كبيرة من الجسامة فيكفي أن يتحقق ولو بدرجة بسيطة.[2]

وتعرض شركات المساهمة إلى جريمة التزوير الإلكتروني أكيد أنها ستترتب عنها أضرار قد تمس يذمتها المالية حيث أن هذا الضرر هو الأكثر شيوعا واستهدافا لهذه الشركة، كما أن هذا الضرر قد يمس سمعتها ويؤدي إلى زعزعة ثقة عملائها فيها وبالتالي فقدان العديد من زبائنها.

ففرضا في حالة تعرض هذه الشركات إلى جريمة التزوير مست علامتها التجارية فبطبيعة الحال أن ذلك سينجم عنه ضرر مادي يصيبها نظرا لتكاليف الدعاية التي أنفقتها من أجل الترويج لعلامتها، كما يترتب على ذلك إهتزاز الثقة العامة في تلك العلامة بسبب تعرض العملاء للغش والتضليل نتيجة التغيير الذي مس بحقيقتها وبالتالي تدني قيمتها وفقدان مصداقيتها.

ب-الركن المعنوي: جريمة التزوير الإلكتروني في إطار شركات المساهمة تعد من الجرائم العمدية إذ لا يمكن إرتكابها عن طريق الخطأ لذلك فالقصد الجنائي في هذه الجريمة يستند إلى أمرين يتمثلان في كل من القصد الجنائي العام والقصد الجنائي الخاص.

بالنسبة للقصد الجنائي العام والذي يقوم على عنصري العلم والإرادة، فالعلم هو أن يقدم الجاني على إرتكاب جريمته مع علمه وإدراكه بأن التغيير الذي يقوم به يمس حقيقة مستند إلكتروني يحظى بحماية قانونية وأن المساس به معاقب عليه،[3] كما أن عنصر العلم في هذه الجريمة مفترض إذ من غير الممكن دفع المسؤولية بجهله،[4] أما عنصر الإرادة فيتمثل في إتجاه إرادة الجاني إلى تغيير حقيقة المستند الإلكتروني رغم علمه بحقيقة فعله.

---

[1] أسامة أحمد المناعسة، جلال محمد الزغبي، مرجع سابق، ص 166.

[2] عامر محمود الكسواني، مرجع سابق، ص ص 212، 213.

[3] حورية قويقح ،" الجرائم الاقتصادية عبر الشبكة المعلوماتية دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري"، (أطروحة دكتوراه، كلية العلوم الإسلامية جامعة الجزائر 1، 2018-2019)، ص 206.

[4] عبد الله بلقاسم، مرجع سابق، ص 987.

في حين القصد الجنائي الخاص يتمثل في أن تكون لدى الجاني نية الغش،[1] إذ لا عبرة بالبواعث في هذه الجريمة كأن تكون لدى الجاني نية حسنة، وعليه فالقصد الجنائي الخاص في جريمة التزوير الإلكتروني في إطار شركات المساهمة هو أن تكون لدى الجاني نية تزوير مستنداتها من أجل إستعمالها في الغرض الذي زورت من أجله بهدف إلحاق أضرار بها سواء كانت محتملة الوقوع أو فعلية.

فمن يقدم على تزوير علامتها التجارية تكون له نية تضليل عملاء وزبائن هذه الشركات وذلك باستدراجهم إلى إقتناء منتجات أو الحصول على خدمات تحمل نفس علامة الشركة من خلال خداعهم بعلامة مزورة وبالتالي فقدان جزء من العملاء مما يتسبب في أضرار تلحق بهذه الشركات.

ثانيا: جريمة خيانة الأمانة.

تلجأ شركات المساهمة بحكم نشاطها التجاري الذي تقوم به إلى إبرام العديد من العقود على غرار عقود الأمانة، الشيئ الذي قد يترتب عليه خيانة الثقة أو النزاهة التي تودعها هذه الشركات في الطرف الذي تعاقدت معه بناءا على أحد العقود وبالتالي تكون قد تعرضت لجريمة خيانة الأمانة والتي لا تعتبر أقل ضررا عن باقي الجرائم الأخرى التي تتعرض لها.

وجريمة خيانة الأمانة لم تتوقف عند المعاملات التجارية التقليدية لهذه الشركات وإنما إمتدت لتمس حتى معاملاتها الإلكترونية، مثلها مثل بقية الجرائم التي سبق التطرق إليها وأيضا الجرائم التي سنتطرق إليها لاحقا، وذلك راجع بطبيعة الحال إلى التعاملات الإلكترونية التي أصبحت تعتمدها على نطاق واسع.

و تعرف جريمة خيانة الأمانة على أنها إعتداء يقوم به الجاني بهدف الإستيلاء على مال يكون عبارة عن منقول تعود ملكيته للغير، وقد تم تسليمه إلى الجاني بناءا على عقد من عقود الأمانة واستيلاؤه عليه يكون بنية إلحاق الضرر بالمالك الأصلي للمال،[2] وكان المشرع الجزائري قد تطرق إليها من خلال نص المادة 376 من قانون العقوبات والتي جاء فيها " كل من إختلس أو بدد بسوء

---

[1] فتيحة عمارة، مرجع سابق، ص 181.

[2] ناصر حمودي، مرجع سابق ، ص 162.

نية أوراقا تجارية أو نقودا أو بضائع أو أوراق مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت إلتزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الإستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لإستعمالها أو لإستخدامها في عمل معين وذلك إضرار بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة، ويعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 500 دج إلى 20.000دج"

بناءا على نص هذه المادة يتضح بأن هذه جريمة خيانة الأمانة في هذه الصورة تقوم بتحقق الركن المادي في فعل الإختلاس أو التبديد واللذان يمثلان السلوك الإجرامي الذي يرتكبه الجاني على محل الجريمة المتمثل في المال المنقول المملوك للغير، والذي يكون عبارة عن أوراق تجارية أو نقود أو بضائع أو أوراق مالية أو مخالصات أو أية محررات أخرى، ويجب أن يكون هناك أحد عقود الأمانة بين الجاني والمجني عليه والمتمثلة في:

-عقد الإيجار: هو عبارة عن عقد يلتزم فيه المؤجر بأن يمكن الطرف المستأجر أن ينتفع من شيئ يكون محدد وذلك لمدة معينة مقابل أجر يكون معلوم.[1]

-عقد الوديعة: وهو من العقود الرضائية التي يلتزم فيها الشخص بأن يستلم شيئا يكون منقولا أو عقارا شريطة أن يتولى حفظه والقيام برده عينا بحيث يتم إبرام العقد قبل تسليم الشيئ محل العقد.[2]

عقد الوكالة: وهو عقد يلتزم بمقتضاه الطرف الوكيل على أن يقوم بعمل لحساب وباسم طرف آخر هو الموكل.[3]

-عقد الرهن: هو عقد يلتزم فيه شخصا من أجل ضمان دين عليه أو على غيره بأن يسلم إلى الطرف الدائن أو إلى أجنبي يتم تعيينه من قبل المتعاقدان شيئ يرتب عليه للدائن حقا عينيا يمكنه من حبس

---

[1] حامد محمد شبيب الجبوري، أهمية الإلتزام بالعقود وضماناتها للحقوق التعاقدية وفقا للقوانين المدنية العربية، ط 1، عمان الأردن، شركة دار الأكاديميون للنشر والتوزيع، 2015، ص 384.

[2] أشرف أحمد عبد الوهاب، إبراهيم سيد أحمد، عقد الوديعة والحراسة في ضوء أراء الفقهاء والتشريع وأحكام القضاء، ط 1، القاهرة، دار العدالة للنشر والتوزيع، 2018، ص 7.

[3] محمد بن براك الفوزان، عبد الله بن أحمد زيتل علي رضا، أحكام نظام الوكالات التجارية السعودي دراسة مقارنة، ط1، الرياض ، مكتبة القانون والإقتصاد للنشر والتوزيع، ، 2012، ص 37.

الشيئ إلى غاية إستيفاء الدين، وأن يتقدم الدائنين العاديين والدائنين التالين له في المرتبة في أن يتقاضى حقه من ثمن هذا الشيئ وذلك في أي يد يكون.[1]

-عقد العارية: هو عقد يلتزم بمقتضاه الطرف المعير بأن يسلم للطرف الثاني وهو المستعير شيئا يكون غير قابل للإستهلاك من أجل إستعماله مجانا ودون عوض وذلك لمدة محددة ليتم رده بعد الإستعمال.[2]

-عقد أداء عمل: هو عبارة عن إتفاق بين طرفين يلتزم فيه أحدهما بأن يؤدي إلى الطرف الثاني عمل ما أو يمتنع عن القيام بعمل ما وذلك نظير أجر يتقاضاه.

وعقود الأمانة كان المشرع الجزائري قد ذكرها على سبيل الحصر لا المثال، بالإضافة إلى هذا كله يجب أن يكون لدى الجاني قصد جنائي بنية الإضرار هذا كلمحة عن جريمة الخيانة في صورتها التقليدية.

أما عن جريمة خيانة الأمانة بطريقة إلكترونية في إطار شركات المساهمة فنجد بأنها تعتبر من أحدث الجرائم التي تكون ناتجة عن إستعمال هذه الشركات للحاسوب حيث يعود ظهورها إلى وقت قريب وهي في تطور مستمر شأنها شأن بقية الجرائم الإلكترونية،[3] لكن ما يجب التنويه إليه هو إغفال المشرع الجزائري والتشريعات المقارنة عن تخصيص هذه الجريمة بأحكام خاصة في المجال المعلوماتي مما يقتضي ضرورة العودة إلى النصوص القانونية الخاصة بجريمة خيانة الأمانة في صورتها التقليدية، وحتى نتمكن من توضيح الصورة الإلكترونية لهذه الجريمة في إطار شركات المساهمة نناقش محل الإئتمان الذي تنصب عليه أولا ثم مدى تحقق ركنيها المادي والمعنوي.

---

[1] المادة 48 من الأمر 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، ج ر، ع 78، الصادر في 30 سبتمبر 1957، المعدل والمتمم.

[2] محمد عزمي البكري، موسوعة الفقه والقضاء والتشريع في القانون المدني الجديد، مج 8، د،ط، القاهرة، درا محمود للنشر والتوزيع، 2018، ص 4.

[3] صابرين يوسف عبد الله الحياني، مرجع سابق، ص 53.

1- محل الإئتمان لجريمة خيانة الأمانة في صورتها الإلكترونية في إطار شركات المساهمة: يثير محل الإئتمان لهذه الجريمة في صورتها الإلكترونية عدة عقبات كون أن نص المادة 376 من قانون العقوبات جاء صريح وحصر محل الإئتمان أن يكون عبارة عن مال مادي منقول يمكن إدراكه بالحواس (أوراق تجارية، نقود، بضائع، أوراق مالية، مخالصات أو أية محررات) فهو لم يشر إلى الأموال المعنوية، في حين أن محل الإئتمان في إطار شركات المساهمة بالنسبة لهذه الجريمة يتعلق بمال ذو طبيعة معنوية تكون في شكل بيانات إلكترونية، وهي تمثل الجوهر الذي تقوم عليه العلاقة التعاقدية التي تقوم بين شركات المساهمة وطرف آخر متعاقد معها.

غير أنه ورد في المادة 341 من قانون العقوبات المصري "أو غير ذلك"[1] وكذا المادة 314-1 من قانون العقوبات الفرنسي " مال أيا كان" UN BIEN QUELCONQUE"،[2] وبذلك حتى المحررات الإلكترونية تندرج تحت مفهوم "أية محررات أخرى" خاصة وأن المحررات الإلكترونية لشركات المساهمة تعتبر ذات قيمة مالية سواءت تعلقت بعملائها أو بأعمالها.

إضافة إلى ذلك فقد تضمنت المادة 376 مصطلح بضائع ، فالمشرع أورده دون أن يوضح أو يشير إلى الطبيعة التي تتميز بها هذه البضائع إن كانت ذات طبيعة مادية أو غير ذلك وهذا ما يدعوا إلى فتح المجال وإمكانية القول بإدراج المعلومات والبيانات ذات الطبيعة المعنوية ضمن مفهوم البضائع.

خاصة وأن القضاء الفرنسي كان قد وسع في تعريف هذا المصطلح ليشمل كذلك برامج الكمبيوتر وكذا المعلومات حتى وإن كانت لا تتضمن أي إلتزام أو إبراء من دين،[3] فنجد بأن محكمة النقض الفرنسية كانت قد قضت في أحد أحكامها بتحقق جريمة خيانة الأمانة في حق مدير بنك حين أقدم على إجراء تحويلات لمبالغ مالية من حسابات خاصة بأحد عملاء البنك إلى حسابه

---

[1] المادة 341 من قانون العقوبات المصري طبقا لأحدث التعديلات بالقانون 95 لسنة 2003 " كل من إختلس أو إستعمل أو بدد مبالغ أو أمتعة أو بضائع أو نقودا أو تذاكر أو كتابات أخرى مشتملة على تمسك أو مخالصة أو غير ذلك بماليكيها أو أصحابها..."

[2] Art: 314-1 " l'abus de confiance est le fait par une personne de tourner, au préjudice d'autrui des fonds, des valeurs au un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé l'abus de confiance est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende.

[3] صالح شنين: مرجع سابق، ص 21.

الشخصي، والمعنى من ذلك حسب القضاء الفرنسي أي جريمة خيانة الأمانة بإمكانها أن تتحقق حتى لو تم إرتكابها بأية وسيلة إلكترونية مثلها مثل أية وسيلة أخرى.[1]

وبالتالي فالشيئ الملاحظ هو إتجاه القضاء الفرنسي إلى توسيع دائرة محل هذه الجريمة لتشمل الأموال ذات الطبيعة المعنوية وذلك باعتبار أنها تترتب عنها قيمة مالية ذات طبيعة مادية، أما إذا كانت هذه الأموال المعنوية مقترنة بدعامة مادية كأن يتم إفراغها على أسطوانات ممغنطة ووقعت عليها جريمة خيانة الأمانة، ففي هذه الحالة تتحقق دون إثارة أي إشكال باعتبار أن تلك الأسطوانات تعد من قبيل الأموال المادية المنقولة.

وكل هذا إنما يدل على إمكانية تحقق جريمة خيانة الأمانة في صورتها الإلكترونية على الأموال المعنوية التي تعد محل إئتمان في إطار شركات المساهمة.

2- أركان جريمة خيانة الأمانة في صورتها الإلكترونية في إطار شركات المساهمة: بما أن الصورة الإلكترونية لهذه الجريمة لم يتم النص عليها بموجب نص خاص، لذلك فإن الحديث عن الأركان التي تقوم عليها يتطلب منا البحث عن مدى تحقق وانطباق الأحكام الخاصة بكل من الركن المادي والمعنوي في الصورة التقليدية لهذه الجريمة على صورتها الإلكترونية .

أ-الركن المادي: بالرجوع إلى نص المادة 376 من قانون العقوبات نجد بأن المشرع الجزائري قد أشار إلى أنه "كل من إختلس أو بدد" مما يعني أن السلوك الإجرامي الذي يقوم عليه الركن المادي يتمثل في كل من فعل الإختلاس والتبديد فما مدى تحقق هذين الفعلين على الأموال المعلوماتية ذات الطبيعة المعنوية الخاصة بشركات المساهمة؟

*فعل الإختلاس في جريمة خيانة الأمانة في صورتها الإلكترونية: المقصود بفعل الإختلاس في جريمة خيانة الأمانة هو أي فعل يمكن أن يفصح من خلاله الجاني -الأمين- عن إتجاه نيته إلى تحويل حيازة المال المعنوي لهذه الشركة بعد أن تسلمه بناءا على أحد عقود الأمانة إلى حيازته بصفة نهائية،[2] بمعنى أن الجاني تكون حيازته على ذلك المال حيازة مؤقتة باعتباره الطرف الأمين عليه

---

[1] خدوجة الذهبي ، مرجع سابق، ص 50.

[2] شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت دراسة مقارنة، د،ط، القاهرة، دار النهضة العربية، ، 2009 ، ص 207.

غير أنه يقوم بتحويل المال المعلوماتي لهذه الشركة إلى ملكيته ليحل محلها وكأنه المالك الأصلي له أي أنه يتصرف فيه تصرف المالك وليس تصرف الحائز.

في هولندا كان قد قضي بجريمة خيانة الأمانة على أحد الأشخاص كان قد تم تكليفه بمهمة صيانة برامج وذلك عن طريق قرص ممغنط يعود للشركة التي كان يعمل بها، حيث قام بنسخ ذلك القرض من أجل إنجاز مشروع له متجاوزا بذلك صلاحيته ومنتهكا الثقة التي وضعتها فيه الشركة،[1] كما أن فعل الإختلاس في هذه الجريمة يقع بأفعال الغش المحاسبية باستخدام جهاز الحاسوب ومن ذلك نذكر ما قام به عضو مجلس الإدارة والذي كان يقوم بصرف منح لنفسه دون أي حق من خلال حسابات غير منتظمة، أو كالذي يقوم بتزوير الحسابات المتعلقة بالتحصيل والمدفوعات التي تم تسجيلها في بطاقة الخزينة حتى يقوم باختلاس الرصيد،[2]ويشترط في فعل الإختلاس في جريمة خيانة الأمانة في صورتها الإلكترونية هو عدم خروج المال من حيازة الجاني وإلا أعتبر ذلك تبديدا.[3]

*فعل التبديد في جريمة خيانة الأمانة في صورتها الإلكترونية: يتحقق هذا الفعل عندما يقوم الأمين وهو الطرف الجاني بإعدام المال الذي أؤتمن عليه،[4] بمعنى أنه يستهلك ذلك المال ويتصرف فيه لغيره أو يتخلى له عن حيازته،[5]وفعل التبديد يتحقق سواء من خلال تصرفات قانونية كبيع ذلك المال أو هبته أو تصرفات مادية كإتلافه واستهلاكه،[6] وبالتالي فإن المجني عليه يفقد أمل إستعادة ذلك المال.

أما عن تحقق هذا الفعل في إطار شركات المساهمة فهو يحدث إذا ما قامت بتسليم الطرف الأمين بناءا على أحد عقود الأمانة، مجموعة من البرامج مثلا أو أسطوانات تحتوي معلومات تخص

---

[1]عبد الحليم بوقرين ، "الحماية الجنائية للمعاملات التجارية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2013-2014)، ، ص 190.

[2]لمقدم حمر العين ، (جريمة خيانة الأمانة المعلوماتية) مجلة دراسات وأبحاث، ع 15، مج 1، الصادر في 2009/09/15، ص 362.

[3]شمسان ناجي صالح الخيلي، مرجع سابق، ص 207.

[4]عبد الحليم بوقرين مرجع سابق ، ص 191.

[5]ناصر حمودي ، مرجع سابق، 168.

[6]شمسان ناجي صالح الخيلي، مرجع سابق، ص 208.

أعمالها ويقوم إستعمالها بطريقة تتسبب في تدميرها وتبديدها، ففعل التبديد قابل للتحقق في المجال المعلوماتي وإن كان هناك من يعارض ذلك ويرى بأنه من الصعب تحققه.

وينبغي الإشارة إلى أن هناك بعض التشريعات على غرار المشرع المصري قد أضافت مصطلح آخر والمتمثل في "الإستعمال" ليصبح كفعل ثالث يقوم عليه الركن المادي لجريمة خيانة الأمانة، فقد ورد في المادة 341 من قانون العقوبات المصري والتي سبق الإشارة إليها" كل من إختلس إو إستعمل أو بدد" والمقصود بفعل الإستعمال هو أن يقوم الجاني الذي تسلم المال محل الإئتمان باستخدامه بطريقة تؤدي إلى إستنزاف قيمته إما يصفة كلية أو جزء منه فقط،[1] مع بقاء مادة ذلك المال على حالها.

وهناك من يرى بأن فعل الإستعمال يتحقق في المجال المعلوماتي في حالة ما إذا تم إستخدام أجهزة الحاسوب والبرامج في تحقيق غير تلك الأهداف التي خصصت لها،[2] ففي حالة ما إذا قامت شركة المساهمة بتسليم الأمين جهاز الحاسوب بموجب عقد عارية الإستعمال مثلا وذلك من أجل تأدية أعمالها، غير أنه إنحرف عن تحقيق غرض الشركة واستعمله من أجل تحقيق مصالحه حيث يمكن القول في هذه الحالة بقيام جريمة خيانة الأمانة كون ذلك الجهاز تم إستعماله في تحقيق أغراض تعود بالنفع على الجاني بدلا من الشركة صاحبة الجهاز.

وحتى يتحقق إرتكاب هذه الأفعال على شركات المساهمة ويمكن القول بأنها قد تعرضت فعلا لجريمة خيانة الأمانة ضمن المجال المعلوماتي يتطلب الأمر أن يتم تسليم المال المعلوماتي بناءا على عقد من عقود الأمانة التي سبق الإشارة إليها والتي تم ذكرها على سبيل الحصر، حيث أن تلك العقود من الممكن جدا تصور تحققها ضمن مجال الأعمال الإلكترونية فهناك العديد من أنواع العقود التي تبرم بين هذه الشركات وأطراف أخرى سواء كانوا أشخاص طبيعية أو معنوية، وبناءا عليها تقوم بتسليمهم معلومات أو برامج تخص أعمالها أو أموال إلكترونية لتقوم تلك الأطراف باختلاسها أو تبديدها.

---

[1] خدوجة الذهبي ، مرجع سابق، ص 55.

[2] ناصر حمودي ، مرجع سابق، ص 169

والجدير بالذكر في هذه النقطة هو أن المشرع الفرنسي لم يقم بحصر عقود الأمانة كون أن المعاملات التجارية والإقتصادية في تطور دائم فقد يسفر المستقبل عن عدة عقود تصنف على أنها عقود أمانة،[1] وفي إعتقادنا بأنه عين الصواب ما فعله المشرع الفرنسي إذ أن توجهه يتماشى والتطورات التي يشهدها مجال التجارة الإلكترونية.

فمن خلال عملية البحث في هذا الموضوع إتضح لنا جليا بأن من أكثر العقود التي تعرض شركات المساهمة إلى جريمة خيانة الأمانة في المجال المعلوماتي هي عقود العمل، إذ تعد الغالبة في إرتكابها فمعضمها أرتكبت من طرف عمال وموظفين تربطهم علاقة عمل بها، وبحكم هذه العلاقة يقومون باستغلال الأموال المعلوماتية التي سلمت إليهم من طرف الشركة بناءا على ذلك العقد ويمارسون عليها أفعال الإختلاس والتبديد لتكون بذلك هذه الشركة ضحية في هذه الجريمة.

لكن من جهة أخرى هناك عقود أيضا تكون سبب في إرتكاب هذه الجريمة بنسب معتبرة مثل عقد الوكالة، في حالة ما إذا قام أحد مندوبي هذه الشركة كان قد عهد إليه أحد البرامج قصد تسويقها فقام بتبديدها أو إختلاسها، كذلك عقد عارية الإستعمال في حالة إمتناع أحد العملاء عن رد بطاقة الإئتمان التي سلمت إليه رغم إنتهاء فترة صلاحيتها أو في حالة قيام البنك بإلغائها إذ أن تلك البطاقة سلمت للعميل بموجب عقد عارية الإستعمال.[2]

إضافة إلى ذلك يجب أن يترتب عن هذه الجريمة ضررا بشركات المساهمة فقد ورد في المادة 376 من قانون العقوبات والتي سبق وأن أشرنا إليها " وذلك إضرارا بمالكيها أو واضعي اليد عليها.." إذ يعد الضرر عنصر جوهري لقيامها، وبطبيعة الحال هذا الضرر لا بد من رابطة سببية تربطه مع ذلك السلوك الإجرامي والمتمثل في فعلي الإختلاس والتبديد حتى يكتمل بذلك تحقق الركن المادي لهذه الجريمة.

---

[1] عبد الحليم بوقرين ، مرجع سابق، ص ص 192، 193.

[2] نسمة بطيحي ، مرجع سابق، ص 279.

ب–الركن المعنوي: لتحقق هذه الجريمة لا يكفي قيام الركن المادي فقط وإنما لا بد من تحقق الركن المعنوي أيضا إذ تعد من الجرائم العمدية التي يستوجب تحققها قيام القصد الجرمي، ومن خلال هذا سنناقش مدى توفر كل من القصد الجنائي العام والقصد الجنائي الخاص.

–القصد الجنائي العام: يقوم هذا القصد على عنصري العلم والإرادة، فالعلم هو أن يكون الجاني على علم بأن الأموال المعلوماتية التي تسلمها من شركات المساهمة إنما سلمت إليه على سبيل الأمانة لا أكثر وأم ملكيتها في الأساس تعود لتلك الشركة، بمعنى أن يكون مدركا بأن تلك المعلومات يحوزها فقط بصفة مؤقتة وأن ذلك التسليم لا يخوله تملكها.

وفي حالة إنتفاء علمه بذلك وكان معتقدا بأنه سلمت إليه بناءا على أحد العقود الناقلة للملكية كعقد الهبة مثلا فهنا ينتفي الجرم وذلك لإنتفاء علمه بحقيقة التسليم المؤقت،[1] كما يجب أن يعلم بأن من شأن فعله أن يلحق أضرارا بالشركة.

أما عنصر الإرادة هو أن تتجه إرادة الجاني إلى إختلاس أو تبديد تلك الأموال رغم علمه بحقيقة فعله الإجرامي فيتصرف فيها تصرف مالكها.

–القصد الجنائي الخاص: ويتمثل في نية التملك،[2] وإن كان هناك من يرى بأن هذه النية تتحقق في فعل الإختلاس فقط،[3] كون أن الجاني هنا يهدف إلى الإحتفاظ بذلك المال المعلوماتي والمُسلم له ويعمل على تغيير حيازته الناقصة له إلى حيازة كاملة،[4] أما في فعل التبديد والإستعمال فلا تظهر كون أن التبديد يؤدي إلى هلاك المال، أما الإستعمال فيترتب عليه إستنزاف قيمته لذلك ليس من الضروري أن تظهر لدى الجاني نية التملك أي ظهوره بمظهر المالك عند إرتكاب هذين الفعلين.[5]

---

[1] صابرين يوسف عبد الله الحياني، مرجع سابق، ص 57.

[2] عبد الحليم بوقرين ، مرجع سابق، ص 194.

[3] صابرين يوسف عبد الله الحياني، مرجع سابق، ص 57.

[4] خدوجة الذهبي، مرجع سابق، ص 57.

[5] صابرين يوسف عبد الله الحياني ، مرجع سابق، ص 57.

المطلب الثاني:

جريمة السرقة، الإحتيال، وغسل الأموال.

إضافة إلى الجرائم التي تم التطرق إليها في المطلب الأول قد تتعرض شركات المساهمة كذلك إلى مجموعة من الجرائم تضاف إلى سابقتها هذا والتي تتمثل في كل من جريمة السرقة الإلكترونية **(فرع أول)** جريمة الإحتيال وغسيل الأموال إلكترونيا **(فرع ثاني)** .

الفرع الأول:

جريمة السرقة الإلكترونية.

تعد السرقة الإلكترونية إحدى أنواع الجرائم الإلكترونية ومظهر من مظاهر الإجرام الرقمي ومن أكثر الجرائم إستهدافا لشركات المساهمة، حيث أنه قد يحدث الولوج إلى قاعدة البيانات الخاصة بها وارتكاب جريمة السرقة ضدها وذلك عن طريق الشبكة المعلوماتية.

والسرقة وفقا للقواعد العامة هي أخذ واختلاس المال المملوك للغير دون رضى من صاحبه الذي يعتبر مالكا له،[1] وهي إعتداء على مال الغير من خلال عملية إزالة حيازته من مالكه دون رضاه أو علمه وإدخال ذلك المال في حيازة الجاني دون وجه قانوني أو حق شرعي،[2] أما بالنسبة للمشرع الجزائري فقد عرفها بموجب نص المادة 350 من قانون العقوبات والتي جاء فيها" كل من إختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000دج إلى 500.000دج" وتقابلها في قانون العقوبات الفرنسي المادة 311-1[3] والتي عرفت السرقة على أنها إختلاس شيئ يملكه شخص آخر بطريقة إحتيالية.

وبالتالي حتى تتحقق جريمة السرقة مكتملة لا بد من القيام بفعل الإختلاس الذي يقع على مال الغير إضافة إلى عدم علم ورضا صاحب ذلك المال بفعل الجاني، لذلك يثور التساؤل عن معنى فعل الإختلاس ومحل الإختلاس.

---

[1] أسامة سمير حسن، مرجع سابق، ص 119.

[2] عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، ط1، الرياض، مكتبة القانون والإقتصاد، 2012 ، ص 127.

[3] Art: 311-1 Le vol est la soustraction frauduleuse de la chose d'autrui.

بالنسبة لفعل الإختلاس نجد بأنه رغم إستعماله في النصوص القانونية السالفة إلا أنها لم تورد تعريفا له، لذلك تم تعريفه من طرف الفقه وفق نظرتين:

بالنسبة للنظرية الأولى والتي تعد تقليدية حيث عرفته على أنه الفعل الذي يمكن من خلاله إنتزاع الشيئ بقصد تملكه دون رضى من صاحبه فلا يمكن للإختلاس أن يتحقق إذا لم تكن هناك أفعال إيجابية تأخذ شكل النقل أو الإنتزاع أو الأخذ.[1]

لكن أنتقدت كونها كانت قاصرة على تفسير الحالات التي يتحقق فيها فعل الإختلاس دون أن يتم ذلك عن طريق الإنتزاع أو الأخذ كمن يسلم شيئا للشخص بقصد فحصه فقط ولكن دون قصد تمليكه له فيحدث أن الجاني يفر فهنا يعد سارقا ،[2] وهذا مفاده نظرية التسليم الإضطراري والتي ظهرت قصد تصحيح النقص الذي يشوب النظيرية التقليدية.

أما بالنسبة للنظرية الثانية والتي جاء بها الأستاذ "جارسون"حيث تم تعريف فعل الإختلاس وفقا لها بأنه فعل يتم من خلاله سلب حيازة شيئ على الرغم من إرادة صاحبه أو حائزه الشرعي،[3] أي أن الإختلاس هو إخراج الشيئ من حيازة المالك –المجني عليه– إلى حيازة الجاني ولا يشترط في ذلك وسيلة محددة وإنما يتحقق الإختلاس بأية وسيلة كانت ،[4] وبذلك يمكننا أن نعرف بدورنا فعل الإختلاس بأنه ينصب على سلب حيازة المال من خلال إخراجها من دائرة المالك رغما عن إرادته ورضاه إلى دائرة من يقوم بارتكاب ذلك الفعل ويستوي في ذلك أن يظل محتفظا بالمال أو يتنازل عنه لغيره.

---

[1]توفيق غوالم، "السرقة المعلوماتية دراسة تأصيلية تحليلية مقارنة"، (رسالة ماجستير، كلية الحقوق، جامعة الجزائر1، 2012–2013)، ص 32.

[2]محمد عبد المحسن بن طريف، فيصل صالح العبادي، هبة عبد المطلب الفضلي،(جريمة السرقة المعلوماتية) مجلة الدراسات والبحوث القانونية، ع 2، مج 7، الصادر في 2022، ص 16.

[3]عبد القادر عمري ، (الشريعة والتشريع الجزائري)، مجلة الدراسات القانونية، ع 1، مج 3، الصادر في 2017/06/30، ص 7.

[4]توفيق غوالم ، مرجع سابق، ص ص 33، 34.

أما عن طبيعة المال المختلس في هذه الجريمة فهو عبارة عن مال منقول ملك للغير والمال كل شيئ يمكن أن يدخل في دائرة التعامل،[1] أي يكون ذو طبيعة مادية قابلا للتملك.[2]

وبطبيعة الحال ليست كل الأموال قابلة لأن تكون محلا للسرقة.[3] زيادة على ذلك يجب أن يكون هذا المال منقولا، بمعنى يمكن نقلها من مكان إلى آخر لذلك فمدلول المال في القانون الجنائي يعد أوسع عمّا هو عليه في القانون المدني،[4] فهناك أموال تعد من قبيل العقارات كالعقارات بالتخصيص من ذلك على سبيل المثال المعدات والآلات اللازمة لتشغيل المصانع وماكينات صرف النقود الملحقة بالبنوك،[5] فرغم أن القانون المدني يعتبرها من ضمن العقارات إلا أنها يمكن أن تقع عليها السرقة وإضافة إلى كل هذا لا بد من أن يكون هذا المال مملوك للغير، إذ من غير المعقول أن تقع السرقة على مال مملوك للسارق حتى لو تم ذلك بسوء نية كأن يعتقد مثلا بأنه مملوك لغيره وهو في الحقيقة مملوك لها، والنتيجة المترتبة عن جريمة السرقة هي إخراج المال من حيازة المالك وبالتالي إنهاء سلطاته المادية عليه إلى حيازة الجاني الذي يصبح وحده مخولا بممارسة تلك السلطات.

هذا كلمحة عن جريمة السرقة في صورتها التقليدية أما بالنسبة لجريمة السرقة الإلكترونية في إطار شركات المساهمة، فتعرف على أنها أخذ للمال المملوك للغير أو البرامج والمعلومات التي يمكن تقديرها مالا وذلك عن طريق إستخدام التقنيات الحديثة،[6] تعرف أيضا بأنها تلك الجريمة التي

---

[1]محمد عبد المحسن بن طريف، فيصل صالح العبادي، هبة عبد المطلب الفضلي، مرجع سابق، 17.

[2]ناصر حمودي ، مرجع سابق، ص 176.

[3]هناك أموال تدخل ضمن دائرة التعامل ومن ثم تصلح لأن تكون محلا للسرقة وطائفة أخرى تخرج عن دائرة التعامل ومن ثم لا تصلح لأن تكون محلا للسرقة، وهذه الطائفة تنقسم بدورها إلى قسمين:

القسم الأول: تخرج عن دائرة التعامل بحكم طبيعتها بحيث لا يمكن تملكها أو الإستحواذ عليها مثل الهواء والشمس.

القسم الثاني: يشمل الأموال التي تخرج عن دائرة التعامل بحكم القانون مثل الملك العام والوقف بالإضافة إلى الأشياء التي نص القانون على تجريمها مثل المخذرات. (محمد علي البدوي الأزهري، النظرية العامة للإلتزام مصادر الإلتزام، ج 1، ط1، ليبيا ، منشورات الجامعة المفتوحة، ، 1993، ص 140.

[4]ناصر حمودي، مرجع سابق، ص 146، 147.

[5]طارق عفيفي صادق أحمد، نظرية الحق، ط 1، القاهرة، المركز القومي للإصدارات القانونية، 2016 ، ص 363.

[6]محمد طيب عمور، (السرقة الإلكترونية تكييفها الشرعي وطرق إثباتها) مجلة الأحياء، ع 22، مج 19، الصادر في سبتمبر 2019)، ص 407.

تقع على المعلومات والبرامج التي تكون ذات قيمة مالية أو تتجسد في صورة أصول مالية داخل النظام المعلوماتي لشركات المساهمة،[1] وهي كذلك الإستخدام العمدي لوحدات الإدخال الخاصة بجهاز الحاسوب وذلك بهدف أخذ واستغلال البيانات والمعطيات المخزنة داخله أو على الأقراص الممغنطة، أو إستخدام تلك الأجهزة من أجل السيطرة على مال مملوك للغير ودون رضاه،[2]

وبالتالي يمكننا أن نعرف السرقة الإلكترونية في إطار شركات المساهمة بأنها إختلاس للمعلومات التي تعد هي مالكتها ونقل حيازتها إلى الغير ليسيطر عليها ويتصرف فيها، بحيث أن تلك المعلومات تكون لها قيمة إقتصادية أو تمثل أصول مالية، ومثلما سبقت الإشارة فإن جريمة السرقة في صورتها التقليدية تستهدف المال المنقول المملوك للغير وبما أن المشرع الجزائري لم يتطرق إلى جريمة السرقة الإلكنرونية بصورة مستقلة فما مدى تحقق إرتكابها في شركة المساهمة؟

من أجل توضيح سنقوم بالتطرق إلى كل من المحل الذي تنصب عليه السرقة الإلكترونية في شركة المساهمة ثم مدى تحقيق كل من الركن المادي والمعنوي.

أولا: محل السرقة الإلكترونية في إطار شركات المساهمة.

محل جريمة السرقة الإلكترونية في إطار شركات المساهمة هو المال المعلوماتي المملوك لها.

1-المال المعلوماتي: وينقسم إلى قسمين مال معلوماتي مادي سواء كان بحتا كأدوات النظام المعلوماتي مثل وحدات الإدخال والإخراج، أو كان ذلك المال المادي يحتوي مضمونا معنويا كالأسطوانات والذاكرة،[3] ولا يوجد هناك خلاف أو جدل في حالة تعرض هذا المال إلى السرقة باعتباره يعد من قبيل الأموال المادية الملموسة التي يمكن حيازتها وملكيتها وبالتالي تنطبق عليها جريمة السرقة العادية.

---

[1]أحمد محمد عبد الرؤوف المنيفي، السرقة الإلكترونية وحكمها في الإسلام، ط 2، لندن، E- KTUBLTD، 2018 ، ص 40.

[2]إسلام فوزي جمعة محسن، "السرقة الإلكترونية في التشريع الأردني"، (رسالة ماجستير، كلية القانون، جامعة عمان العربية، 2017)، ص 36.

[3]نسمة بطيحي ، مرجع سابق، ص 196.

وهناك أيضا المال المعلوماتي المنطقي أو المعنوي ويشمل المعلومات الخاصة بهذه الشركة ولكن توجد بمعزل عن دعامة مادية تحملها، وقد ثار خلاف بشأنها بين رأي مؤيد لأن تكون محلا للسرقة ورأي منكر لذلك وقد تم التفصيل في هذه النقطة وتوضيحها حيت تطرقنا إلى الأحكام الخاصة بمحل الجريمة الإلكترونية لذلك سنتجنب تكرار شرحها.

2-مدى إعتبار المال المعلوماتي لشركات المساهمة منقولا مملوكا لها: بالنسبة للمعلومات من حيث كونها تعد منقولا تقع عليه السرقة هناك من نفى هذه الصفة عنها وذلك على أساس أنه ليس لها كيان مادي محسوس بإمكانه أن يشغل حيزا في الفضاء الخارجي، وبالتالي تجريدها من صفة المحسوسية ينفي عنها صفة كونها تعد منقولا، غير أن الأجزاء المادية كالأسطوانات مثلا والتي تثبت عليها هذه المعلومات تكون محلا للسرقة نظرا لطابعا المادي،[1] إضافة إلى ذلك فإنه في جريمة السرقة يفترض أن تنتقل حيازة المنقول من الضحية إلى الجاني وهذا مالا نجده في المعلومات الخاصة بشركات المساهمة في حال سرقتها فإنها تبقى بحوزتها ولذلك فهي لا تحرم منها بشكل تام ونهائي.

من جهة أخرى وعلى خلاف الموقف الأول فإن الإعتداء الذي يطال معلومات شركات المساهمة والتي تكون منسوخة على دعامة مادية هو في الحقيقة إعتداء على تلك المعلومات بالدرجة الأولى والتي لا يمكن فصلها عن دعامتها بحيث أنه في حالة خلو الدعامة من أية معلومات فإنها أبدا لا تكون هدفا للجاني،[2] لذلك يمكن إعتبار معلومات هذه الشركات منقولا تقع عليه جريمة السرقة الإلكترونية.

ونجد بأن المشرع الفرنسي قد إعتبر المعلومة عبارة عن شيئ منقول وذلك وفقا للقانون رقم 82-652 الصادر في 26 يوليو 1982 والذي عرفها بأنه عبارة عن أصوات وصور ووثائق ومعطيات ورسائل أيا كانت طبيعتها،[3] وكانت محكمة النقض الفرنسية قد أكدت في حكم لها بأن

---

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، د،ط، عمان، دار الثقافة للنشر والتوزيع، 2005، ص 97.

[2] محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، ط 1، عمان، دار الثقافة للنشر والتوزيع، 2004، ص153.

[3] المرجع نفسه، ص 153.

الشيئ يعد منقولا ويكون قابلا للسرقة منذ إنفصاله عن أصله الذي كان لصيقا به،[1] أيضا القول بأن المعلومات هي منقول إنما يعد ذلك من قبيل الاتفاق مع التطور التكنولوجي بحيث أن هذه المعلومات وإن لم تكن ملموسة إلا أنها عبارة عن كيان مادي يتجسد من خلال إمكانية مشاهدتها على شاشة النظام المعلوماتي، كما أنها تنتقل عبر نبضات ورموز وشفرات أيضا يمكنها أن تنتقل من عقل إلى آخر إذا ما تم إلتقاطها عن طريق السمع أو المشاهدة، ومن ثمة وضعها ضمن حيز مادي سواء من خلال عملية تدوينها أو تسجيلها ليتم عرضها للبيع.[2]

وبالتالي فالشيئ الذي يترتب على هذه الحالة هو خروج المعلومات من الذمة المالية لشركة المساهمة إلى ذمة الجاني مما يجعل معلوماتها محلا لجريمة السرقة الإلكترونية ، كذلك أن تكون المعلومات عبارة عن منقول تفسيرا لمصطلح "شيئ" والتي وردت في كل من المادة 350 من قانون العقوبات الجزائري والمادة 311-1 من قانون العقوبات الفرنسي، حيث جاءت عامة تشمل كل الأشياء سواء كانت مادية أو غير مادية ، وبالتالي فإن المعلومات يمكن إدراجها ضمنها.[3]

أما فيما يتعلق بشرط أن تكون المعلومات ملكا لشركات المساهمة فبالنظر من زاوية أن هذه المعلومات هي نتاج فكري خالص لها، وبالتالي لها أن تستحوذ عليها وتتصرف فيها الشيئ الذي يؤكد ملكية هذه الشركات لمعلوماتها والتي تضاهي قيمتها الاقتصادية قيمة المال المادي، وبناءا على تلك المعلومات يمكن للشركة أن تحافظ على مكانتها في السوق فإذا ما تم الإستحواذ عليها من طرف شخص آخر يكون قد إختلس شيئا ليس من إنتاجه وهو الشيئ الذي يعد جوهر الإختلاس في السرقة لذلك فالمعلومات الخاصة بالشركة تعد وحدها صاحبة الحق فيها.

---

[1] يوسف زيدات حابس، مدة إستيعاب النصوص التقليدية للسرقة الإلكترونية دراسة مقارنة، مقال منشور بتاريخ 2019، تاريخ الدخول: 2023/05/31، متاح على الرابط: https://doi.org/10.5339/rolacc.2019.9

[2] بدرة عمارة، "الحماية الجنائية للمعلومات الإلكترونية"، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، 2011-2012)، ص 14.

[3] فايز محمد راجح غلاب، مرجع سابق، ص 92.

وفي هذا الصدد كان القضاء الفرنسي قد تعرض في قضية "HERBERTEAR" الذي كان يشتغل منصب مهندس تصاميم في إحدى الشركات، وحدث أن قدم إستقالته بها ليقوم مع بعض أصدقائه بتأسيس شركة منافسة تقوم بنفس النشاط وذلك بعد أن قام بسرقة تصاميم منتجات الشركة السابقة، والتي قامت برفع دعوى ضده بتهمة السرقة ورغم تبرئته من طرف المحكمة غير أن محكمة النقض قد جرمته وقضت بقيام جريمة السرقة كونه قام باختلاس مخططات دون رضى الشركة التي تعد مالكتها،[1] لذلك فالمعلومات والبرامج التي يتم تخزينها على جهاز الحاسوب أو أية دعامة مادية أخرى تخول لصاحبها الإستئثار بها وهذا إن دل فإنما يدل على أنها ملك لمخترعها.[2]

وعليه فالمعلومات مثلما تقبل التنقل تكون قابلة أيضا للحيازة والتملك إذ تعد ملكا لمبتكرها بحيث لا يمكن الإطلاع عليها إلا من خلال كلمة مرور تعتبر بمثابة مفتاح يمكن من خلاله لصاحبها أن يطلقها أو يحبسها وفقا لإرادته لذلك يمكن أن تكون محلا للملكية،[3] وفي قضية قام أحد العاملين في شركة "GULF OIL COMPANY" بسرقة مجموعة خرائط جيولوجية خاصة بتحديد مواقع إكتشاف البترول ليقوم ببيعها إلى شركة "LESTER" والتي تعد منافسة وعند إتهامه بجريمة السرقة كان محاميه قد دافع عنه بحجة أن تحقق قيام الجريمة المنسوبة لموكله لا بد من أن يكون هناك نقل لشيئ مملوك لشخص آخر وأن موكله لم يقم بنقل أي شيئ وإنما قام فقط بتصوير تلك الخرائط لذلك ليس هناك أي إستلاء على الملكية، غير أن المحكمة رفضت تلك الحجج وقضت بأن الملكية تتمثل أساسا في المعلومات السرية التي تتضمنها تلك الخرائط.[4]

ثانيا: أركان جريمة السرقة الإلكترونية في إطار شركات المساهمة.

لقيام هذه الجريمة لا بد من تحقق كل من ركنيها المادي والمعنوي واللذان سنوضحهما فيما يلي:

---

[1] سليمان النحوي، خالد شويرب، (حماية المعلومات والبرامج الإلكترونية في ظل جريمة السرقة)، مجلة دراسات وأبحاث، ع 29، الصادر في ديسمبر 2017، ص 265.

[2] علي سليمان البطوش، "التطبيقات المعاصرة لجريمة السرقة"، (رسالة ماجستير، جامعة مؤتة، 2005)، ص 78.

[3] أسامة سمير حسن، مرجع سابق، ص 122.

[4] المرجع نفسه، ص 124.

1-الركن المادي: كما أشرنا سابقا فإن السرقة التقليدية تقوم على فعل الإختلاس الذي يقوم عليه ركنها المادي من خلال قيام الجاني بحركات مادية كالخطف والسلب ونفس الفعل تقوم عليه السرقة الإلكترونية في إطار شركات المساهمة، حيث أن الإختلاس في السرقة الإلكترونية يتم بطرق تقنية ولا وجود للحركات المادية فيه.

ففي هذه الجريمة نجد بأن الجاني يقتصر دوره فقط في تهيئة الطرق والسبل الكفيلة يتسهيل عملية إنتقال المعلومات ولكن بعيدا عن أي سلوك مادي ملموس من ذلك مثلا أن يلجأ الجاني إلى إختراق النظام المعلوماتي لشركات المساهمة ليعطي بعدها أمرا بنسخ المعلومات السرية التي يحتويها ضمن دعامة يكون قد أعدها مسبقا لهذا الغرض، ليكون دوره مجرد مراقب فقط لعملية النسخ،[1] وبالتالي ففعل الإختلاس يختلف بين السرقة في صورتها التقليدية والسرقة الإلكترونية التي يتم فيها إرتكاب هذا الفعل بعيدا عن الكيان المادي كمحل لها، وهذا ما يقودنا إلى التساؤل عن الصور التي يتم من خلالها إختلاس المال المعلوماتي لشركات المساهمة بطريقة إلكترونية.

أ- النسخ غير المشروع لمعلومات شركات المساهمة: حيث يتم سرقة معلوماتها في هذه الصورة عن طريق عمل نسخ تكون مطابقة لتلك المعلومات أو البرامج،[2] ويتم ذلك بواسطة أوامر النسخ المختلفة[3]، وقد تم تكريس فعل الإختلاس عن طريق النسخ في القضية المعروفة باسم "بوركاين" حيث تتلخص وقائعها في قيام العاملان اللذان كانا يشتغلان ببوركاين والتي هي عبارة عن مطبعة حيث قاما بنسخ 47 قرص تضم أسماء أهم المتعاملين الأثرياء مع هذه المطبعة وذلك بغرض إنشاء مؤسسة منافسة، كما قاما بالإستيلاء على 70 قرص آخر، وكانت محكمة النقض الفرنسية قد أيدت الحكم السابق لمحكمة الإستئناف وذلك بإدانة العاملان بارتكاب جريمة سرقة 70 قرص من جهة وسرقة المحتوى

[1] محمد عبد المحسن بن طريف، فيصل صالح العبادي، هبة عبد المطلب الفضلي، مرجع سابق، ص ص 20،21.

[2] وليد البلتاجي السيد، (النسخ غير المشروع لبرامج الحاسب الآلي دراسة مقارنة)، مجلة كلية الشريعة والقانون بطنطا، ع 1، مج 36، الصادر في مارس 2021، ص 1459.

[3] أنسام سمير ظاهر،(جريمة السرقة الإلكترونية)، مجلة جامعة بابل للعلوم الإنسانية،ع 5، مج 27، الصادر في 2019، ص 136.

المعلوماتي ل 47 قرص عن طريق نسخها من جهة أخرى،[1] فاستعمال محكمة النقض لعبارة المال المعلوماتي إشارة إلى الإعتراف بوقوع جريمة السرقة على المعلومات.

فعملية النسخ تتم على البيانات والمعلومات السرية الخاصة بهذه الشركات التي تكون محفوظة ومخزنة وذلك بعد عملية إختراق أنظمة حمايتها حيث يتم نسخها إما عن طريق سحبها في نسخ ورقية مثلا، أو نسخها من الحاسوب الذي تحفظ به إلى حاسوب الجاني وذلك من خلال الإستعانة بشبكة تقوم بعملية الربط بينهما.

ب-الإلتقاط الذهني لمعلومات شركات المساهمة: والمقصود بالإلتقاط هنا هو أن يتم إلتقاط المعلومات الخاصة بها إما عن طريق البصر أو السمع بعيد عن الإعتماد عن أية وسيلة من الوسائل الإلكترونية، حيث أن الإلتقاط الذهني لهذه المعلومات يتم من خلال عملية حفظها في ذاكرة الجاني بقراءته لها على شاشة إحدى حواسيب الشركة أو بوصولها إلى سمعه في حالة ما إذا كانت في شكل صور صوتية تصدر عن الحاسوب.[2] فيترتب عن ذلك إنتقال المعلومات من الجهاز إلى ذهن الجاني الذي يصبح حائزا لها وبإمكانه الإستئثار بها وعرضها للبيع من ذلك مثلا الإطلاع على أحد المستندات الإلكترونية الخاصة بأعمال الشركة وحفظ فحواها ومن ثم إستغلالها مما يترتب عليه إلحاق أضرار بها.

ت-الإلتقاط الهوائي لمعلومات شركات المساهمة والتي يتم معالجتها أو نقلها إلكترونيا: في هذه الصورة يترتب عن إستعمال الحاسبات الإلكترونية وتوابعها صدور إشعاعات أو موجات تكون قابلة لإلتقاطها ثم ترجمتها في شكل بيانات مرئية على الشاشة[3]، ومن ذلك ما أقدم على إرتكابه أحد المهندسين في إدارة الخدمات البريدية والهاتفية والبرقية في هولندا حين أحضر معدات تتكون من جهاز تلفزيون وهوائي وكذا منظومة دارات كهربائية، وذلك بغية إلتقاط إشارات من الحواسيب الإلكترونية لعدد من المؤسسات الأوربية وفعلا نجح في ذلك حين إلتقط إشارات من حواسيب أحد

---

[1] سليمان النحوي، خالد شويرب، مرجع سابق، ص 265.

[2] فايز محمد راجح غلاب، مرجع سابق، ص 100.

[3] صبايحية خديجة دحمان ، "جرائم السرقة والإحتيال عبر الأنترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري"، (رسالة ماجستير، كلية العلوم الإسلامية، جامعة الجزائر، 2012-2013)، ص 52

البنوك[1]، ةعليه فإن صور الأفعال التي يتم من خلالها الإختلاس المعلوماتي لشركات المساهمة هي متعددة مثلما سبق شرحها ومن الصعب حصرها كونها دائمة التطور بتطور أنظمة المعلومات.

2-الركن المعنوي: السرقة الإلكترونية التي تستهدف شركات المساهمة تعد من الجرائم العمدية المقصودة إذ يتطلب قيامها تحقق القصد الجنائي بنوعيه العام والخاص وسنوضحهما على التوالي:

أ-القصد الجنائي العام: والذي يقوم على عنصري العلم والإرادة، فالعلم في هذه الجريمة هو أن يكون الجاني مدركا تماما بأن المال المعلوماتي الذي يقوم باختلاسه مملوك لهذه الشركات ووحدها تملك سلطة التصرف فيه، إلا أنه رغم ذلك تتجه إرادة الجاني إلى إخراجه من حيازة الشركة وإدخاله ضمن حيازته من أجل سيطرته عليه ويصبح يتصرف فيه وكأنه مالكه الأصلي وهذا كله ضد إرادة ورضا هذه الشركة.

ب-القصد الجنائي الخاص: يتمثل في نية التملك لدى الجاني، بمعنى أن تتجه نيته إلى تملك معلومات وبيانات وبرامج شركات المساهمة التي قام باختلاسها.

حيث كانت محكم النقض الفرنسية قد أيدت ذلك في القضية المعروفة بقضية "LAGBAX" حين أقدم موظف في الشركة على تصوير مستندات سرية تخص الشركة وذلك بغية تملك المستندات واستعمالها لمصلحته الشخصية.[2]

الفرع الثاني:

جريمة الإحتيال وغسل الأموال إلكترونيا.

بعد أن تطرقنا إلى جريمة السرقة الإلكترونية نتطرق في هذا المبحث إلى جريمتين أُخريَيْنِ بحيث لا تقل أضرارهما عن الجرائم التي تناولناها سابقا، والبداية تكون بجريمة الإحتيال الإلكتروني أولا ثم جريمة غسيل الأموال إلكترونيا.

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص 103.

[2] عزيزة رابحي ، مرجع سابق، ص 196.

أولا: جريمة الإحتيال الإلكتروني.

ويصطلح عليها كذلك بجريمة النصب في المجال المعلوماتي، إذ يعد الإحتيال الإلكتروني من أكثر وأخطر الجرائم التي شهدت إنتشارا واسعا وذلك نتيجة تأثر هذه الجريمة بالتطورات التكنولوجية ، حيث أن الوسائل التقنية التي أسفر عنها ذلك التطور فتحت الأبواب أمام مجرمي البيئة الرقمية من ممارسة أساليبهم الإحتيالية والتي أصبحت تتسم بالتقنية قصد ممارسة عمليات النصب التي أصبحت أكثر تعقيدا، فجناة الإحتيال الإلكتروني بعد أن كانوا يستهدفون النصب على الأشخاص الطبيعية إتجهت أنظارهم نحو كبرى الشركات والتي تعد شركات المساهمة واحدة منهم ومن خلال هذه النقطة سنقف على مدى إرتكاب الإحتيال الإلكتروني على شركات المساهمة.

يعرف الإحتيال الإلكتروني بأنه سلوك غير مشروع قصد الإستيلاء على مال الغير يتم إرتكابه من خلال الإعتماد على الأساليب الإحتالية التي تعمل على تضليل المجني عليه وتغليطه وذلك باستخدام الوسائل التكنولوجية،[1] كما يعرف على أنه الإعتداء الذي يرتكب عن طريق المعلوماتية وذلك بغية تحقيق أرباح مالية،[2] وهو أيضا الذي يقوم أساسا على جهاز الحاسوب بهدف الإستيلاء دون وجه حق على أموال وأصول الغير، وهو ذو طابع معقد ويرجع ذلك إلى الدلائل الإلكترونية التي تستخدم في إرتكابه،[3] وهو فعل إحتيالي ذو صلة بالحواسيب الآلية تتجه من خلاله نية الجاني إلى تحقيق أرباح مادية غير مشروعة.[4]

من خلال التعريفات يمكننا القول بأن الإحتيال الإلكتروني هو الفعل غير القانوني الذي يأتيه الجاني متعمدا من أجل الإستيلاء على أموال الطرف المجني عليه ويتم ذلك كله عبر الوسائل الإلكترونية، وكانت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قد عرفته من خلال المادة 11

---

[1] آسية بن بوعزيز ، ميلود بن عبد العزيز، (جريمة الإحتيال المالي في ظل تكنولوجيا المعلومات)، مجلة الدراسات المالية والمحاسبية والإدارية، ع 1، مج 9، الصادر في جوان 2022، ص 1368.

[2] مريم عبد الكافي ، صورية بوربابة ، (جريمة الإحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية)، مجلة القانون والعلوم السياسية، ع1، مج 8، الصادر في 2022، ص 414.

[3] حمد عبد الله حيي بوغانم السليطي، "تجريم الإحتيال الإلكتروني في القانون القطري والمقارن"، (رسالة ماجستير، كلية القانون، جامعة قطر، 2018)، ص 7.

[4] نسرين محسن نعمة الحسيني، محمد حسن مرعي، مرجع سابق، 98.

منها على أنه التسبب بإلحاق الضرر بالمستفدين والمستخدمين عن قصد وبدون وجه حق بنية الإحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير عن طريق:

-إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

-التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

-تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

كما نجد بعض الدول التي خصت جريمة الإحتيال الإلكتروني بتعريف خاص ضمن تشريعاتها مثل دولة الإمارات،[1] في حين هناك العديد من الدول التي لم تتعرض لها بموجب نصوص خاصة وإنما أخضعتها للأحكام العامة لهذه الجريمة في صورتها التقليدية، مثلما فعل المشرع الجزائري في المادة 372 من قانون العقوبات والتي جاء فيها، كل من توصل إلى إستيلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من إلتزامات أو الحصول على أي منها أو شرع في ذلك وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو إعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيئ أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيئ منها، يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000دج، ونفس الشيئ فعله المشرع الفرنسي إذ أنه لم ينص على هذه الجريمة ضمن نص خاص وإنما تطرق إلى صورتها التقليدية فقط وذلك في المادة 313-1[2] من قانون العقوبات.

---

[1] المادة 40 من القانون الإتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية" يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تزيد على مليون درهم، أو بإحدى هاتين العقوبتين كل من إستولى لنفسه أو لغيره بغير وجه حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالإستعانة بأي طريقة من الطرق الإحتيالية أو باتخاذ إسم كاذب أو إنتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات.

[2] Art: 313-1 "l'escroquerie est le fait, soit par l'usage d'un faux non ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou préjudice d'un tiers, à remettre des fonds des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.
l'escroquerie est punie de l'escroquerie cinq ans d'emprisonnement et de 375 00 euros d'amende"

فيمكن القول بأن الشيئ الذي نستشفه من خلال النص الذي جاء به المشرع الجزائري هو أنه لم يهتم ولم يركز على الوسائل التي يتم بواسطتها الإحتيال على أموال الغير سواء كان جهاز حاسوب أو وسيلة أخرى، بما أن هناك مناورات إحتيالية يلجأ إليها الطرف الجاني وهذا ما يدعوا إلى القول بإمكانية وقوع السلوك الإجرامي لفعل الإحتيال ضمن المجال الإلكتروني في حالة تحقق تلك المناورات الإحتيالية، كما أن المشرع لم يحدد الشخص المستهدف إن كان شخصا طبيعيا أو معنويا، وذلك على عكس المشرع الفرنسي الذي نص على إمكانية خداع كل منهما" DE TROPER UNE PERSONE PHYSIQUE OU MORALE" إضافة إلى ذلك فقد إستعمل مصطلح "قيما" "DES VALEURS" وبذلك فالمشرع الفرنسي لم يجعل من جريمة الإحتيال تنصب على الأموال المادية فحسب وإنما تشمل أيضا القيم المعنوية.

وعليه يمكن القول بأن التعريف الذي جاء به المشرع الفرنسي أعم وأشمل من تعريف المشرع الجزائري، حتى وإن كان مصطلح "الأموال" الذي ورد في المادة 372 من قانون العقوبات يمكن أن يشمل القيم المعنوية خاصة عندما يتعلق الأمر بقيم شركات المساهمة التي تتعلق بأعمالها والتي أصبحت تضاهي الأموال المادية، وبذلك يكون محل الإحتيال الإلكتروني القيم المتمثلة في المعلومات وكذا البيانات والتي تكون ذات قيمة إقتصادية أو مالية ضمن نظام معلوماتي، فمعظم الحالات التي تعتبر على أنها إحتيال إلكتروني تتم من خلال التلاعب بتلك المعلومات والبيانات سواء تعلقت بفواتير أو رصيد حسابي، أو كانت عبارة عن أرقام تمثل الأرباح الناتجة عن الصفقات التجارية خاصة وأن مجال الأعمال أصبح يعتمد بشكل واسع على أوامر تحويل الأموال.[1]

وبما أن شركات المساهمة تعد من الأشخاص الإعتبارية حسب القانون وأن حواسيبها وشبكات الإتصال الداخلية والخارجية الخاصة بها تعتبر من ضمن فروعها ومكوناتها لذلك تكون قابلة لإرتكاب أفعال الغش والتحايل عليها،[2] إذ أصبحت تلفت إنتباه العديد من الجناة ومحط أنظارهم من أجل

[1] خدوجة الذهبي ، مرجع سابق، ص ص 32، 33.

[2] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 73.

إرتكاب جرائم الإحتيال ضدها الشيئ الذي مكنهم من الحصول على أموال غير مشروعة بحجم مضاعف لتلك التي يتحصلوا عليها من الأشخاص الطبيعية.

ففي سنة 2019 كانت شركة :تويوتا بوشوكو" وهي مختصة في عملية توريد وتزويد سيارات "تويوتا" بالمعدات لعملية إحتيال تكبدت جرائها خسائر قدرت قيمتها ب 37 مليون دولار أمريكي، وذلك حين قام الجناة بالإحتيال على المدير المالي وإقناعه بتغيير المعلومات المتعلقة بمعلومات الحساب المصرفي الخاص بالمستلم الشيئ الذي مكنهم من الحصول على تلك الأموال.[1]

وحسب مكتب التحقيقات الأمريكي المعروف ب "أ ف بي آي" أن الإحتيال الإلكتروني ضد الشركات شهد إزدياد حاد خاصة ما يعرف باحتيال "الرئيس التنفيذي" والذي يعمل من خلاله الجاني على تقليد البريد الإلكتروني للرئيس التنفيذي للشركة ليوجه عبره دعوة إلى الموظفين بتحويل أموال بمبالغ معينة إلى حساب ما في دولة أخرى، ففي الفترة الممتدة بين شهر أكتوبر 2013 وشهر أوت 2015 خسرت هذه الشركات ما يقارب 1,2 مليار دولار وقد شهدت هذه الخسارة زيادة بنحو 800 مليون دولار في الستة أشهر الموالية،[2] ومن أجل التفصيل أكثر في جريمة الإحتيال الإلكتروني في إطار شركات المساهمة نقوم بتوضيح الأركان التي تقوم عليها:

1- الركن المادي: حتى يتحقق الركن المادي في جريمة الإحتيال الإلكتروني في إطار شركات المساهمة ينبغي أن يكون هناك سلوك إجرامي يتمكن من خلاله الجاني من تحقيق نتيجة وهي الإستيلاء على أموال هذه الشركات بالإضافة إلى علاقة سببية تربط بينهما.

أ-السلوك الإجرامي: وهو أول عنصر يقوم عليه الركن المادي في جريمة الإحتيال الإلكتروني في هذه الشركات، حيث يتمثل في الأساليب والمناورات الإحتيالية التي يعمد الجاني على إتيانها من أجل إيهام هذه الشركات بحقيقة الأفعال التي يقوم بها، وبالتالي الوصول إلى تحقيق غايته وهي إستيلام

---

[1] محمد بنهشوم، كيف تواجه الإحتيال الإلكتروني؟، مقال منشور بتاريخ 2021، تاريخ الدخول: 2023/07/28، متاح على الرابط: https://blog.khamsat.com/online-fraud

[2] رسائل الإحتيال تكلف الشركات ملياري دولار، مقال منشور بتاريخ 2016/02/25، على صفحة الجزيرة، تاريخ الدخول: 2023/07/28، متاح على الرابط: https://www.aljazeera.net

الأموال منها، وبالعودة إلى نص المادة 372 من قانون العقوبات نجدها قد حددت الطرق التي يتم من خلالها ممارسة الإحتيال والتي تتمثل في إتخاذ أسماء أو صفات كاذبة وكذا المناورات الإحتيالية.

وفيما يلي نتطرق إلى مدى تحقق هذه الأساليب لممارسة الإحتيال على شركات المساهمة بطريقة إلكترونية.

-إتخاذ أسماء أو صفات كاذبة: المقصود بذلك هو أن يلجأ الجاني إلى إستعمال إسم وهمي لا وجود له أساسا وقد يكون الإسم حقيقا موجود فعلا لكنه مملوك للغير،[1] أي أن الجاني ينتحل هوية أخرى وللإشارة فإن هذا الأسلوب وإن كان يعرف إنتشارا أوسع وتطبيقا أكثر في جريمة الإحتيال التقليدية ضد الأفراد، غير أن تطور الوسائل التقنية وشبكة الأنترنت أعطت للجناة إمكانية تطبيق ذلك أيضا في الصورة الإلكترونية لجريمة الإحتيال وليس ضد الأفراد بل حتى ضد الأشخاص المعنوية والتي تعد شركات المساهمة واحدة منهم، حيث أن إنتحال الهوية ضد هذه الشركات قد يكون من خلال عملية إنتحال شخصية أحد الأفراد مثلما سبقت الإشارة إلى الإحتيال الذي يتم تنفيذه ضد الشركات الأمريكية والذي عمد فيه الجاني إلى إنتحال صفة الرئيس التنفيذي للشركة من خلال تقليد بريده الإلكتروني.

وفي هذا الصدد نجد ما قام أحد موظفي شركات المساهمة الأردنية سنة 1994 حين أقدم على تسجيل عدد كبير من الأسهم بأسماء شركاء ولكنهم وهميين ضمن النظام المعلوماتي للشركة ليتم بعدها إستخراج الشهادات الخاصة بملكية تلك الأسهم لماليكيها الوهميين ليقوم ببيعها بمبلغ تجاوز مئة وتسعين ألف دينار أردني،[2] كما أن إنتحال الهوية يكون كذلك من خلال عملية إنشاء المواقع الإلكترونية المزيفة والمطابقة تماما لمواقع هذه الشركات ليقوم فيه المحتالين بإجراء جميع المعاملات التجارية التي يقدمها الموقع الأصلي للشركات مع عملائهم، ليتم بعد ذلك الإستيلاء على البيانات والمعلومات الخاصة بالعملاء،[3] ونظرا لخطورة هذا الفعل خاصة في ظل التنامي المتزايد للوسائل

---

[1] نسمة بطيحي ، مرجع سابق، ص 230.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 192.

[3] مريم عبد الكافي ، صورية بوربابة ، جريمة الإحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية مرجع سابق، ص 415.

التقنية وشبكات الأنترنت فقد أقدمت بعض الدول على تجريم هذا الأسلوب بموجب نص خاص مثلما فعل المشرع الكويتي في قانون مكافحة جرائم تقنية المعلومات.[1]

ب-الأساليب الإحتيالية ضمن المجال الإلكتروني: وتتمثل في المناورات التي يأتي بها الجاني من أجل تنفيذ جريمته حيث أن تلك الأساليب تكون مقترنة بعنصرين، أولهما الكذب وثانيهما السلوكات الخارجية التي يعتمد عليها الجاني من أجل الإيقاع بالمجني عليه في الغط، وبالتالي دفعه إلى تسليم المال له بكامل إرادته،[2] وما ينبغي الإشارة إليه هو أنه عندما يتعلق الأمر بالإحتيال الإلكتروني يكون من الصعب حصر تلك الأساليب وذلك راجع لإرتباطهما بالتطور التكنولوجي، فلا يمكن التنبؤ بما سيسفر عنه هذا التطور من أساليب في المستقبل.

لذلك نجد أنه وفقا لنص المادة 11 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أن الأساليب الإحتيالية ضمن المجال الإلكتروني تتنوع ويمكن إجمالها في التلاعب في البيانات والبرامج وكذا التلاعب في المكونات المادية للنظام المعلوماتي.

وبالتالي فإن ذلك التلاعب المعلوماتي إذا ما تم إرتكابه على شركات المساهمة يترتب عليه إيهامها بصحة تلك البيانات، الأمر الذي يدفعها إلى تسليم المال للجناة بالنسبة للتلاعب في البيانات وقد يقع ذلك في مرحلة الإخال أو الإخراج سواء من خلال إضافة معلومات أو تعديلها أو محوها وحتى حجبها، وللإشارة فإن هذه الأفعال سبقت الإشارة إليها في المادة 394 مكرر 1 والتي جاء نصها عاما بتجريمها سواء كان هدف الجاني هو الحصول على أموال هذه الشركات أم إستهداف معلوماتها فقط، على خلاف هذه الحالة التي يلجأ فيها الجاني إلى هذه الأفعال كأساليب إحتيالية من أجل النصب على هذه الشركات والحصول على أموالها.

---

[1] المادة 3-5 من القانون الكويتي رقم 63 لسنة 2015" يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف أو بإحدى هاتين العقوبتين كل من:

توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الإستيلاء لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند وذلك باستعمال طريقة إحتيالية أو باتخاذ إسم كاذب أو إنتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

[2] نسمة بطيحي، مرجع سابق، ص 231.

والإحتيال من خلال تلك الأفعال في مرحلة الإدخال يتم عن طريق تغذية النظام المعلوماتي للشركات بالمعلومات التي يقصد معالجتها ومن ثم يتم التلاعب بها، ليكون الإحتيال بهذه الطريقة من أكثر الحالات حدوثا وذلك نظرا لسهولة إرتكابه،[1] ونجد بأن القضاء الفرنسي قد إعتبر أن إدخال معلومات بعد إجراء تعديلات عليها أو إدخالها بصفة غير صحيحة إلى النظام المعلوماتي بغية تحقيق أرباح غير شرعية يعتبر من طرق الإحتيال التي تقوم بها جريمة الإحتيال.

أما التلاعب في مرحلة الإخراج فيفترض أن تلك المعلومات قد تم إدخالها بطريقة صحيحة إلى النظام المعلوماتي وأنه تم التلاعب بها في مرحلة لاحقة، أي قبل عملية إخراجها،[2] غير أنها تعتبر أقل حدوثا من سابقتها ومن ذلك ما أقدم عليه مدير أحد البنوك التجارية حين قام بالتلاعب ببعض البيانات خلال عملية إدخالها إلى النظام المعلوماتي لجهاز الحاسوب وذلك من أجل تغطية الإختلاسات التي فعلها، كما تلاعب أيضا في نظام الحاسوب من أجل عرقلة إستخراج تلك البيانات وذلك عند قيام المكلفون بالنظام باستخراج البيانات التي يتضمنها النظام كعملية روتينية، فالجاني خشية منه من أن يتم إكتشاف أمره تلاعب بالبيانات في مرحلتي الإدخال والإخراج.[3]

أما التلاعب بالبرامج فيعد من أخطر الأساليب الإحتيالية كونها تتطلب المعرفة الفنية الكافية ببرامج الحاسوب، حيث أن شركات المساهمة تعتمد عليها بشكل كبير في أعمالها كالبرامج المتعلقة بالرواتب والمحاسبة،[4] والتلاعب قد يكون من خلال إدخال تعديلات غير مسموح بها على البرنامج الذي تعتمده الشركة أو من خلال عملية الإستعانة بفيروسات لإحداث تلك التعديلات،[5] كما يتم التلاعب أيضا من خلال الإستعانة ببرامج إضافية يتم إعدادها وتطبيقها من قبل الجناة أو يكون قد تم إعدادها مسبقا مهمتها إجراء تعديلات على المعلومات التي يتضمنها الحاسوب،[6] ففي إحدى الشركات

---

[1] عبد اللطيف معتوق ، مرجع سابق، 41.

[2] محمد قدري، حسن عبد الرحمن، (جرائم الإحتيال الإلكتروني)، مجلة الفكر الشرطي، ع 79، مج 20، الصادر في 2011، ص 69.

[3] محمد قدري، حسن عبد الرحمن،مرجع سابق، ص 69.

[4] منذر عبد الرزاق العمايرة، مرجع سابق، ص 192.

[5] نسرين محسن نعمة، (جريمة الإحتيال المعلوماتي دراسة مقارنة)، مجلة الكوفة، ع 36، مج 2، د،ت،ص، ص 292

[6] نهلا عبد القادر المومني، مرجع سابق، ص 193.

بألمانيا قام أحد المبرمجين بإعداد برنامج مهيأ خصيصا للقيام بعملية الإحتيال وذلك بإدخال بيانات تتعلق بمرتبات أشخاص وهميين إلى النظام المعلوماتي إلى جانب ذلك يقوم بإجراء تعديل على البرامج المتعلقة بحسابات وميزانيات الشركة حتى يتم حجب البرنامج الأول وهذا ما رتب خسائر كبيرة على عاتق الشركة بسبب صرف تلك المرتبات الوهمية وقد حوكم الجاني بتهمة الإحتيال.[1]

في حين التلاعب في المكونات المادية للنظام المعلوماتي لا يقل تعقيدا عن الأسلوب الذي سبقه، حيث يتم اللجوء إلى الإستعانة بالمكونات المادية للنظام المعلوماتي حتى يتم تنفيذ عملية الإحتيال الإلكتروني.

ومن ذلك أن يتم التلاعب في الدوائر الإلكترونية للحاسوب وذلك بطريقة تؤدي إلى إخفاء عملية الإحتيال أو يتم ذلك بالضغط على مفتاح التوقيف الذي يوجد في لوحة المفاتيح باعتباره مكونا ماديا للحاسوب،[2] ومثال ذلك ما قام به أحد موظفي البنوك التجارية حين حجب عدد من المعاملات الخارجية التي كان يقوم بها البنك وذلك بواسطة ضغطة على مفتاح التوقيف الذي أعاق عملية تحويل البيانات إلى الحاسوب المركزي في حين أن تخزينها في السابق كان يتم عبر وحدة الحاسوب الثانوي الذي يقوم بتحويل البيانات إلى الحاسوب المركزي، وبالتالي فإن الجاني قد نجح في حصوله على تصديق للبيانات وتحويلها إلى الطرف المتعاقد معه ولكن من غير ظهور ذلك في الحاسوب المركزي.[3]

وعليه ما يمكننا قوله أن هذه الأساليب التي يرتكب بها الإحتيال الإلكتروني في إطار شركات المساهمة تنصب جميعا على التلاعب ببياناتها ، لكن رغم ذلك فإن هذه الجريمة لا تعتبر محققة الوقوع فعلا إلا إذا أوقعتها في الغلط ودفعتها إلى تسليم المال إلى الجناة والذي يعتبر النتيجة الإجرامية هذا ما ذكره المشرع في المادة 372 السالفة الذكر "كل من توصل إلى إستيلام أو تلقي".

ويثير الإحتيال الإلكتروني في إطار شركات المساهمة إشكالية تسليم الأموال إلكترونيا إذا ما كانت تتحقق فعلا أم لا؟

---

[1] نسرين محسن نعمة، جريمة الإحتيال المعلوماتي دراسة مقارنة، مرجع سابق، ص ص 292، 293.

[2] نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، مرجع سابق، ص 116.

[3] نسرين محسن نعمة، جريمة الإحتيال المعلوماتي دراسة مقارنة، مرجع سابق، ص 293.

باعتبار أن التسليم في الأصل يتم بشكل مادي من خلال المناولة اليدوية غير أن الأمر يختلف حينما يتعلق الأمر بالإحتيال الإلكتروني ، ففي هذه الحالة لا يجب أن ينظر إلى التسليم على أنه واقعة مادية وهي المناولة اليدوية وإنما ينظر إليه على أنه عمل قانوني،[1] يكون عنصره الأساسي هو إتجاه إرادة الطرف المجني عليه حتى يضع ذلك المال تحت تصرف الجاني وبالتالي يصبح تسليم الأموال إلكترونيا ممكننا،[2] وبذلك يكون التسليم قد تم بطريقة إلكترونية.

وفي هذا الصدد فقد أشارت المادة 11 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قد إستعملت مصطلحا واسعا وشاملا هو تحقيق مصالح ومنافع بطريقة غير مشروعة الشيئ الذي يترتب عليه إلحاق ضرر بالغير بصفة مقصودة، بمعنى أنه وفقا لهذه المادة هو أن أي شيئ يحقق من وراءه الجاني مصلحة أو منفعة عن طريق الإحتيال يكون محلا للتسليم وفي هذا إشارة إلى إمكانية التسليم المعنوي في إطار الإحتيال الإلكتروني.

وعليه نخلص إلى القول بأن النتيجة الإجرامية في الإحتيال الإلكتروني في إطار شركات المساهمة لا يختلف عن الإحتيال في صورته التقليدية وهي وضع المال تحت تصرف الجناة نتيجة ممارسة الأساليب الإحتيالية على نظامها المعلوماتي، بالإضافة إلى فعل الإحتيال الذي قام الجاني بارتكابه وتحقق فعل التسليم فإن ذلك لا يعد كافيا لتحقق الركن المادي وإنما لا بد من علاقة سببية تربط بينهما، بمعنى أن تسليم المال يكون كأثر قد ترتب نتيجة الأساليب الإحتيالية التي قام بها الجاني.

2- الركن المعنوي: تعد جريمة الإحتيال الإلكتروني من الجرائم العمدية شأنها في ذلك شأن جريمة الإحتيال التقليدية، إذ أن الركن المعنوي فيها يتخذ صورة القصد الجنائي العام والخاص.[3]

بالنسبة للقصد الجنائي العام يقوم على عنصري العلم والإرادة، فالعلم يعني أن يكون الجاني مدركا بأن تلاعبه ببيانات الشركة بعد من قبيل الأساليب الإحتيالية المجرمة والتي من شأنها أن تجعل النظام المعلوماتي للشركة يستجيب لها، وبالتالي تنفيذ ما يصبو إليه الجاني كما يجب أن يدرك

---

[1] خدوجة الذهبي ، مرجع سابق، 43.

[2] نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، مرجع سابق، ص 117.

[3] فايز محمد راجح غلاب، مرجع سابق، ص 136.

كذلك بأن المال الذي يهدف إلى السطو عليه هو ملك لهذه الشركة وعليه فالأرباح المحققة من وراء ذلك تعتبر غير مشروعة ودون وجه حق، أما عنصر الإرادة فهو أن تتجه إرادة الجاني إلى إتيان أفعاله الإحتيالية المشكلة للجريمة.

أما بالنسبة للقصد الجنائي الخاص فيتمثل في إتجاه نية الجاني إلى تحقيق مكاسب وأرباح غير مشروعة سواء لنفسه أو لغيره،[1] بمعنى إنصراف نية الجاني إلى تملك مال مملوك لهذه الشركة المجني عليها ليمارس بذلك عليه حقوق الملكية، لذلك فشركات المساهمة رغم أنها شخص معنوي إلا أنها لم تسلم من ممارسة جريمة الإحتيال عليها بطريقة إلكترونية وذلك من خلال نظامها المعلوماتي الذي يتخذه الجاني كوسيط ينفذ عبره أهدافه الإحتيالية.

ثانيا: جريمة غسل الأموال إلكترونيا.

ويصطلح عليها كذلك بتبييض الأموال،[2] غير أننا نفضل إستعمال مصطلح "غسل الأموال" في هذا الموضوع كونه الأقرب حين يكون هدف الجناة إضفاء المشروعية على أموالهم المتأتية من المصادر غير المشروعة ويتم ذلك عن طريق إستعمال شركات المساهمة كمغسلة لهذه العملية.

وقد أضحت هذه الجريمة من أخطر الجرائم التي تؤرق إقتصاديات الدول خاصة في ظل ما يعرف بالإقتصاد الرقمي، فالتطورات الهائلة التي تشهدها التكنولوجيا الحديثة مكنت الجناة من تطوير وتنويع الأساليب والقنوات التي يتم من خلالها إرتكاب هذه الجريمة متحاشين بذلك الطرق التقليدية التي كانت ترتكب بواسطتها، وتزداد خطورة هذه الجريمة كونها لا تقتصر على مرتكيبها فحسب بل تتعدى ذلك لإقحام أطراف أخرى ضمنها، حيث تعد شركات المساهمة أحد هذه الأطراف سواء كانت

---

[1] صورية بورباية ، قواعد الأمن المعلوماتي دراسة مقارنة، مرجع سابق، ص 150.

[2] مصطلح تبييض الأموال أول ما تم إستخدامه كان في الولايات المتحدة الأمريكية وذلك خلال الفترة الممتدة ما بين 1920-1930 حيث أطلقه أنذاك رجال الأمن على عصابات المافيا التي كانت تقوم باشتثمار الأموال غير المشروعة في أنشطة قانونية مثل المحلات التجارية وعلى رأسها محلات الغسلات الكهربائية كما طغى هذا المصطلح على صفحات الجرائد سنة 1973 فيما يعرف بفضيحة "Watergate" ليشاع إستعماله منذ ذلك الوقت ، (نادية عبد الرحيم، أمين بن سعيد، (جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية)، مجلة الدراسات الاقتصادية والمالية، ع 10 الصادر في 2017، ص 1973.

في شكل بنوك أو مؤسسات مالية وذلك نظرا للدور الذي تلعبه في هذه الجريمة، إذ تعد بمثابة بيئة خصبة لنموها خاصة في ظل رقمنة خداماتها وبذلك أصبحت تعاملاتها تتم بطريقة إلكترونية، الشيئ الذي إستغله الجناة ليستعملوا هذه الشركات كقنوات لتمرير أموالهم القذرة وإضفاء الصبغة القانونية عليها.

تعرف جريمة غسل الأموال على أنها عملية يتم من خلالها إخفاء وتمويه الطابع الحقيقي لتلك الأموال التي تم الحصول عليها بطرق غير قانونية وذلك بغية إضفاء الطابع الشرعي عليها،[1] وتعرف أيضا بأنها إحجاب الأصل غير الشرعي للأموال المحصلة من جرائم أخرى،[2] وهي عبارة عن عمليات تكون على تتابع وفي شكل مستمر ومتداخل من أجل إدخال الأموال القذرة التي تكون وليدة إقتصاد خفي ضمن الاقتصاد الرسمي القانوني وذلك عبر مختلف الأجهزة المالية،[3] هذا بالنسبة لجريمة غسل الأموال في صورتها التقليدية.

أما بالنسبة لهذه الجريمة التي أصبحت تنفذ بشكل إلكتروني فهي التي يلجأ فيها غاسلوا الأموال إلى إستخدام الوسائل التقنية الحديثة قصد تنفيذ صفقاتهم المشبوهة،[4] أي أنها الجريمة التي يتم فيها الإستعانة بالأجهزة الإلكترونية سواء جهاز حاسوب أو شبكة أنترنت كأداة لتنفيذها،[5] وبعد عرض هذه التعريفات نصل إلى القول بأن هذه الجريمة تهدف إلى وضع الأموال التي كانت نتيجة لجرائم سبقتها ضمن إطار قانوني وشرعي وذلك بالإعتماد على ما أسفرت عليه التكنولوجيا من أجهزة ووسائل مواكبة للتطور التقني الحاصل والذي سهل وأزاح العراقيل التي كانت تعترض الجناة من أجل القيام بغسل أموالهم، وبذلك فقد تم التخلي عن الأساليب والطرق التقليدية الشائعة.

---

[1] نعيم سلامة، أيمن أبو الحاج، موسى سعيد، مشهور هذلول، (البنوك وعمليات غسيل الأموال) مجلة كلية بغداد للعلوم الاقتصادية الجامعة، ع 33، الصادر في 2012، ص 354.

[2] عمرو عيسى الفقي، الجرائم المعلوماتية جرائم الحاسب الآلي والأنترنت في مصر والدول العربية، ط 1، الإسكندرية، المكتب الجامعي الحديث، 2006، ص 140.

[3] هشام بشير إبراهيم عبد ربه إبراهيم، غسيل الأموال بين النظرية والتطبيق، ط 1، القاهرة، المركز القومي للإصدارات القانونية، ، 2011، ص 9.

[4] المرجع نفسه، ص 31.

[5] حمدي محمد أحمد الجداوي، غسل الأموال عبر الأنترنت دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، ط1، مصر ،مركز الدراسات العربية للنشر والتوزيع، 2022، ص 87.

وفي التشريع الوطني نجد بأن المشرع الجزائري قد نص على هذه الجريمة ضمن المادة 389 مكرر من القانون رقم 04-15،[1] والتي جاء فيها "يتعبر تبييضا للأموال:

-تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في إرتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية؛

-إكتساب الممتلكات أو حيازتها أو إستخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية؛

-المشاركة في إرتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو التآمر على إرتكابها ومحاولة إرتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه، ونفس التعريف قد قام بإفراغه ضمن المادة الثانية من القانون 05-01[2] المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتمها، فما نلاحظه على هذه المادة والتي وردت ذاتها في القانونين أن المشرع الجزائري لم يعطي إهتماما ولم يركز على الأساليب والوسائل التي يتم من خلالها إرتكاب هذه الجريمة سواء كانت مادية أو إلكترونية وإنما ركز على الأفعال التي يعد إرتكابها تبييضا للأموال، لكن بالعودة إلى القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والذي نص في الفقرة الأولى من المادة الثانية منه على أن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية، وبالتالي فهذا النص يعد شاملا حتى لجريمة غسل الأموال إذا ما تمت بطريقة إلكترونية وذلك من خلال منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

---

[1] قانون رقم 04-15 ،مرجع سابق.

[2] القانون رقم 05-01 مؤرخ في 6 فيفري 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم بالقانون رقم 15-06 المؤرخ في 15 فبراير 2015، ج،ر، ع 8 الصادر في 15 فبراير 2015.

في حين أن القانون العربي النموذجي لمكافحة الجريمة المعلوماتية قد نص في المادة التاسعة منه على أنه، كل من قام بتحويل الأموال غير المشروعة أو أنه قام بنقلها أو تمويه مصدرها غير المشروع أو إخفائه أو أنه قام باستخدام تلك الأموال أو إكتسابها أو حيازتها مع علمه بمصدرها غير المشروع، وذلك من خلال إستعمال الحاسب الإلكتروني أو شبكة المعلومات الدولية قصد إضفاء صفة المشروعية عليها يعاقب، وتترك العقوبة وفقا لتقدير كل دولة.[1]

فمن خلال هذه النصوص القانونية فإن جريمة غسل الأموال تعتبر قائمة سواء تمت بطريقة تقليدية أو إلكترونية طالما تحققت الأفعال التي جرمها المشرع والتي تتمثل في تحويل الممتلكات أو نقلها أو إخفائها أو تمويه طبيعتها أو إكتسابها أو حيازتها أو المساهمة في إرتكاب هذه الأفعال، ففي ظل التطورات التكنولوجية الحاصلة قد إتجه الجناة من غاسلي الأموال إلى الإستعانة بمختلف الوسائط الإلكترونية التي تمكنهم من تطهير أموالهم من مصدرها غير المشروع وبالتالي إدخاله ضمن مجال الأموال القانونية حيث أن تلك الوسائط تمكنهم من تحريك أموالهم عن بعد في مختلف مراحل هذه الجريمة.[2]

---

[1]فيصل بدري ، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، (أطروحة دكتوراه، كلية الحقوق جامعة الجزائر1، 2017-2018)، ص 35.

[2]نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية والقعة على الأموال، مرجع سابق، ص 178. حيث أن عملية غسل الأموال تتم عبر ثلاثة مراحل وهي مترابطة فيما بينها وتتمثل في:

-مرحلة الإيداع: وتسمى بمرحلة الإحلال أو التوظيف، وهي تعتبر بمثابة القاعدة التي تبنى عليها باقي الخطوات وفيها يتم وضع الأموال غير المشروعة في مختلف المؤسسات المالية بطريقة غير ملفتة للإنتباه، (حمدي محمد أحمد الجداوي،مرجع سابق، ص 79)

مرحلة التمويه: وفيها يتم القيام بعمليات تتسم بالتعقيد قصد تمويه أصلها مثل إجراء عمليات مالية متتابعة ممزوجة بعمليات مالية أخرى قانونية من أجل تظليل الجهات الأمنية إذ يكون من الصعب جدا إكتشاف حقيقة تلك العمليات غير المشروعة (آمنة تازير، (جريمة تبييض الأموال في التشريع الجزائري بين القمع والوقاية)، مجلة دراسات إنسانية واجتماعية، ع 10، الصادر في جوان 2019، ص 294).

مرحلة الدمج والتكامل: وفيها يكون المال غير المشروع قد إنقطعت صلته تماما بأصله غير المشروع نتيجة دمجه بصفة نهائية بالأموال المشروعة لتظهر الأموال في شكل قانوني وذلك كونها دخلت ضمن الدورة المالية الاقتصادية وتعد هذه المرحلة الأكثر أمنا على الجناة، (صالح جزول، "جريمة تبييض الأموال في قانون العقوبات الجزائري والشريعة الإسلامية دراسة مقارنة"، (رسالة دكتوراه، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران 1، 2014-2015،)، ص ص 76، 77

وبما أننا في هذه النقطة بصدد البحث عن علاقة شركات المساهمة بجريمة غسل الأموال بطريقة إلكترونية فإننا سنتطرق أولا إلى دراسة مختلف الأساليب والوسائط الحديثة والتي مكنت الجناة من غسل أموالهم إلكترونيا والتي وسعت من دائرة إقحام هذه الشركات ضمن جريمة غسل الأموال نتطرق إلى الأركان الواجب توفرها حتى تقوم هذه الجريمة.

1- أساليب إرتكاب جريمة غسل الأموال إلكترونيا في إطار شركات المساهمة:

أ-التجارة الإلكترونية: وهي تلك التي يتم فيها الإعتماد على التقنيات الحديثة حتى يصبح القيام بالمعاملات التجارية يتم بطريقة تلقائية وسريعة من خلال الوسائط الإلكترونية، حيث أن تلك المعاملات منها ما تقوم به الشركات مع بعضها البعض أو مع عملائها أي أنها تقوم بإنجاز أعمالها عبر نظام المعلومات والإتصالات الحديثة،[1] وفي ظل هذه التجارة تقوم شركات المساهمة بإبرام العديد من الصفقات وتسويق منتاجاتها عبر الفضاء الإلكتروني دون لقاء طرفي العقد في مجلس واحد.

لذلك يلجأ غاسلي الأموال ممن يتعاقدون مع هذه الشركات إلى إستعمال أموالهم القذرة من أجل طمس مصدرها غير المشروع ضمن هذه الصفقات،[2] ونظرا لكون التجارة الإلكترونية سهلت عملية القيام بجميع مراحل المعاملات دةن الحاجة إلى أية مستندات ورقية،[3] كما سهلت من تسوية المدفوعات وبالتالي تقليص إستعمال النقود التقليدية،[4] فكل هذا أعطى الأمان للجناة في عملية غسل أموالهم من خلال التعاقد وإبرام الصفقات مع شركات المساهمة.

---

[1] مصطفى يوسف كافي، التجارة الإلكترونية، د،ط، سوريا، دار مؤسسة رسلان للطباعة والنشر والتوزيع، 2009 ، ص ص 10، 11.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة، ط 1، الإسكندرية، دار الفكر الجامعي، 2018)، ، ص 464.

[3] حمدي محمد أحمد الجداوي، مرجع سابق، ص 192.

[4] مهدي كمال، باخويا دريس، (دور الوسائط الإلكترونية في إنتشار جرائم الأموال وآليات مكافحتها)، المجلة الإفريقية للدراسات القانونية والسياسية، ع 2، مج 2، الصادر في ديسمبر 2018، ص 178.

ب-البورصة عبر الأنترنت: يمكن إعتبار البورصة ،[1] بأنها الأداة الأساسية من أجل تحريك إقتصاديات السوق كونها تمثل أكبر مساحة للنزاع الاقتصادي الذي يكون بين أكبر المؤسسات والشركات،[2] وفي ظل التطور التكنولوجي والتوجه نحو إعتماد الأعمال الإلكترونية فإن العمل في مباني البورصة قد تغير من الهاتف والشاشة العملاقة إلى إعتماد أجهزة الحاسوب التي تكون موصولة بشبكة الأنترنت، حيث أصبح بإمكان المستثمرين الدخول إلى شبكات الأنترنت وإجراء جميع معاملاتهم من خلال عملية التصفح، الشيئ الذي يغنيه عن التواجد بمقر البورصة،[3] ونتيجة لذلك أصبح هناك العديد من المواقع والتي تكون عبارة عن بورصات إفتراضية حيث يتم فيها القيام بعملية بيع السندات والأسهم، هذا ما شجع الجناة إلى التوجه إلى البورصة عبر الأنترنت لغسل أموالهم وذلك كون أن التعامل فيها سوف يتم عن بعد مع عدم إمكانية معرفة الشخص المتعامل بالإضافة إلى سرية عملية التداول فيها، ويتم غسل الأموال عن طريق هذه العملية بلجوء الجناة إلى شراء عدد كبير من الأسهم وذلك بطبيعة الحال باستخدام أموالهم القذرة ليتم بعدها تدوير ما قاموا بشرائه من خلال إعادة بيعها وشراءها مرة أخرى.[4]

خاصة وأن التداول الإلكتروني أصبح أداة مهمة وفعالة من أجل الوصول إلى كافة المستثمرين دون أن يكون لموقعهم الجغرافي أي معنى، حيث أن السمسار في هذا التداول ونيابة عن الشركة التي أصدرت أسهمها يقوم بعرض البيانات المتعلقة بالإكتتاب على شبكة الأنترنت، ليصبح بإمكان أي مشتري الحصول على صورة كاملة من بيان الإكتتاب واتخاذ قراره الإستثماري.[5]

---

[1]تعرف البورصة على أنها السوق الذي يتم فيع تداول مختلف الأوراق المالية، سندات أسهم التي تقوم الشركات بإصدارها وذلك بين السماسرة والوسطاء، وتعرف أيضا بأنها المكان الذي يجمع بين السماسرة والمصرفيون والتجار قصد إبرام الصفقات التجارية الخاصة بالأسهم والسندات، عبد القادر أحمد محمد صباغ، قيد الأوراق المالية في البورصة دراسة مقارنة، ط 1، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2018، ص 39.

[2]خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص 463.

[3] [3]مهدي كمال، باخويا دريس، مرجع سابق، ص 177.

[4]خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة ،مرجع سابق ص 463.

[5]أحمد إبراهيم محمد متولي دهشان، (إقتصاديات المعرفة وجه التنمية الاقتصادية الحديثة في ضوء بعض التجارب الدولية) مجلة كلية الشريعة والقانون بطنطا، ع 38، الصادر في 2023، ص 590.

كما تتم عملية غسل الأموال عن طريق إستعانة الجناة بشركات السمسرة والتي يتم تكليفها بالإكتتاب في شركات المساهمة التي هي تحت التأسيس، حيث تلجأ شركات السمسرة إلى الإكتتاب بمبالغ ضخمة وهي بطبيعة الحال أموال قذرة وذلك بأسماء أشخاص سبق تعاملها معهم، لتتحصل شركات السمسرة عند عملية التخصيص على أسهم الشركة التي تم الإكتتاب فيها، مع إعادة فائض التخصيص بشيكات تحمل أسماء المكتتبين ليتم بعدها إيداع ذلك الفائض من طرف شركات السمسرة في حسابها بناءا على توكيلات سابقة من قبل المكتتبين ثم إلى حسابات الجناة،[1] ليبرر بذلك الجناة مصدر أنوالهم كونهم إكتسبوها عن طريق البورصة عبر الأنترنت مستعملين شركات المساهمة كمغسلة لأموالهم التي تكون بهذه العملية قد إنقطعت صلتها تماما بمصدرها غير المشروع.

ت-التحويل الإلكتروني للأموال: ويسمى بالتحويل السلكي للأموال،[2] أو التحويل البرقي،[3] حيث أن هذا النظام ساعد كثيرا على حجب معالم جريمة غسل الأموال وصعب على رجال القانون مهمة تتبع مصادرها، ويفضل الجناة هذا الأسلوب من أجل غسل أموالهم بسبب الثغرات التي تعتريه حيث أنه يمكن إيداع الأموال في بنك أو مؤسسة مالية في الخارج دون أن يكون هناك داعي للكشف عن أسمائهم،[4] وتتم هذه الطريقة عن طريق قيام غاسلي الأموال بإيداع أموالهم في أحد البنوك أو المؤسسات المالية بصفة عادية وآمنة بعدها يقومون بتحويلها إلكترونيا أو برقيا إلى حسابات شركات وهمية تكون خارج دولهم،[5] وتكون تتسم بالسرية المطلقة في المجال المصرفي بحيث لا تتيح لأي أحد الكشف عن دفاترها أو حقيقة عملائها، وفي هذه الحالة فإن البنك الذي قام بتنفيذ عملية التحويل

---

[1] أحمد جمعة الخيلي، "غسل الأموال عبر الأنترنت دراسة مقارنة بين الأردن، مصر، الإمارات"، رسالة ماجستير، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، 2006)، ص ص 40، 41.

[2] وهيبة عبد الرحيم، (دراسة غسيل الأموال عبر القنوات الإلكترونية) مجلة الحقوق والعلوم الإنسانية دراسات إقتصادية، ع 3، مج 1، الصادر في أكتوبر 2007، ص 61.

[3] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقيات العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة، د ط، الإسكندرية، دار الجامعة الجديدة، 2019، ص 207.

[4] ذهبية لعجال ، قاسي سي يوسف، (الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي)، مجلة الإجتهاد القضائي، ع خاص، مج 13، الصادر في جانفي 2021، ص 908.

[5] يزيد بوحليط، مرجع سابق، ص 207.

تقع عليه مسؤولية التحري ومحاولة فهم هدف العميل من إستخدام هذه الأموال،[1] ونجد بأن التحويلات التي تقوم بها البنوك الأجنبية أغلبها لا تذكر إسم العميل فقط يتم إدراج عبارة "إن عميلنا يرغب في تحويل...إلى عميلكم،[2] حيث أن الدول التي تنشأ فيها تسمى بدول الملاذ المصرفي مثل سويسرا.[3]

ث-الشيكات الإلكترونية: تعرف الشيكات الإلكترونية على أنها عبارة عن إلتزام قانوني بتسديد مبلغ معين لجهة ما أو شخص ما و الشيئ الذي يميزها أنها تقوم بإصدارها أجهزة الحاسوب،[4] وتمر بنفس مراحل الشيك الورقي العادي بدءا من إصداره إلى تسليمه ثم تحصيله وقيده في الحساب،[5] يتم تداوله عن طريق البريد الإلكتروني وذلك من الطرف الذي قام بإصداره لفائدة الطرف المستفيد وذلك بعد إمضاءه إلكترونيا ليسترجعه هذا الأخير -المستفيد- ليمضي عليه إلكترونيا ليقوم بإرساله عبر البريد وذلك رفقة إيداع إلكتروني أيضا في حسابه البنكي، ونجد بأن هذا النظام يمثل ما نسبته 85 % من حجم الشيكات التي يتم إصدارها في العالم،[6] أما إذا جئنا إلى البحث في علاقة الشيك الإلكتروني بجريمة غسل الأموال إلكترونيا فنجد بأنها علاقة جد وطيدة، كيف ذلك؟

طبعا أن هذا الشيك كل ما يعتمد عليه هو أن يكون للعميل -الشخص الذي قام بتحريك الشيك-حساب في بنك ما ليقوم بعدها بتداول الشيك من خلال شبكة الأنترنت وذلك بإبرامه لصفقات تجارية يكون هو أحد أطرافها، أما البنك فهو يأخذ دور الوسيط بين محرر الشيك والطرف المستفيد،[7] ففرضا أن الشخص "أ" له حساب في بنك ما بمليون دولار ومصدرها غير مشروع فحتى يتمكن من غسلها لا بد عليه من الدخول في علاقات تجارية مع أطراف أخرى "ب" ، "ج" وقد تكون تلك

---

[1] نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، مرجع سابق، ص 223.

[2] يزيد بوحليط، مرجع سابق، ص 207.

[3] صلاح الدين حسن السيسي، الموسوعة المصرفية والعملية، ج 2، ط 1، مصر، مجموعة النيل العربية، ، 2000، ص 584.

[4] مهدي كمال، باخويا دريس، مرجع سابق، ص 202.

[5] المرجع نفسه، ص 176.

[6] حمدي محمد أحمد الجداوي، مرجع سابق، ص 203.

[7] نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، مرجع سابق، ص 226.

المعاملات عبارة عن بيع أو إيجار، الشيئ الأهم فيها هو خروج تلك الأموال من ذمته إلى ذمة الأطراف وذلك عن طريق الشيك الإلكتروني من خلال الأموال المودعة لدى بنك العميل،[1] وبهذه العملية يكون قد تم تدوير الأموال القذرة وغسلها عن طريق إستعمال البنك كوسيط فيها كونه لا يسأل عن مصدرها.

ج-عن طريق الشركات الوهمية: وهي شركات يطلق عليها "شركات الدمى" كونها كيانات دون أي هدف تجاري،[2] أيضا تسمى بالشركات الورقية وذلك بسبب إستخدامها كواجهة أو كستار من أجل إخفاء الأموال غير المشروعة وهي مرخصة قانونا لذلك من الممكن إستعمال ذمتها المالية في إبرام مختلف الصفقات فهي مخولة بمختلف العمليات سواء كانت مالية أو مصرفية على المستوى المحلي أو الدولي،[3] من بين الأشكال التي يتم بها غسل الأموال عن طريق هذه الشركات هي الاتفاق مع غاسلي الأموال في بلده على أساس أنها مستثمر أجنبي ويتم إبرام عقود وصفقات معها ويكون لها الحصة الأكبر بينما في الواقع تلك الأموال كلها ملك للجناة ويتم تسوية الحسابات من خلال إجراء عملية تحويل وذلك من حساب هذه الشركة إلى حساب التاجر في أحد البنوك،[4]وبذلك تكون هذه الشركات حلقة مهمة في عملية غسل الأموال.

وللإشارة فإن هذه الأساليب ذكرناها على سبيل المثال لا الحصر وذلك راجع لإرتباطها بالمجال التقني والذي سيلجأ الجناة من خلاله إلى إكتشاف أساليب أخرى للإستعانة بها في عملية غسل أموالهم.

2- أركان جريمة غسل الأموال إلكتروني في إطار شركات المساهمة: بداية ينبغي علينا أن نشير إلى أن جريمة غسل الأموال إلكترونيا تتطلب تحقق جريمة سابقة تترتب عنها عائدات مالية غير مشروعة

[1] هبة نبيلة هروال ، مرجع سابق، ص 139.

[2] صالح جزول، مرجع سابق، ص 82.

[3] وهيبة عبد الرحيم، دراسة غسيل الأموال عبر القنوات الإلكترونية، مرجع سابق، ص 57.

[4] صلاح الدين حسن السيسي، مرجع سابق، ص 584.

تكون محلا لها وهذا ما يسمى بالركن المفترض،[1] بمعنى أن الجاني قبل أن يقدم على غسل أمواله إلكترونيا يفترض أنه قام قبل ذلك بارتكاب جريمة أخرى تبقها بغض النظر عما إذا كانت جناية أو جنحة، هذا بالإضافة إلى الركن المادي والمعنوي.

بالنسبة للركن المادي يتطلب توفر بيئة إفتراضية رقمية تكون موصولة بشبكة الأنترنت،[2] حتى يتمكن الجناة من إرتكاب نشاطهم الإجرامي والذي يتم من خلال القيام بسلسلة من العمليات المالية قد تكون بسيطة أو مركبة التي تسمح بإدخال المال غير المشروع ضمن الحركة المالية.[3]

فالنشاط الإجرامي لعملية غسل الأموال إلكترونيا يكون بإدخال الأموال المترتبة عن جريمة سابقة وتحويلها إلى مال إفتراضي وذلك بتداولها عبر الأنترنت سواء في التجارة أو عمليات البيع والشراء وغيرها من الأساليب الإلكترونية التي سبق التطرق إليها،[4] والتي تجعل من شركة المساهمة كوسيط في عملية الغسل بالإضافة إلى هذا السلوك الإجرامي يتطلب الركن المادي تحقق نتيجة والتي تتمثل في تحويل الأموال القذرة غير المشروعة إلى أموال نظيفة قانونية وإن كانت هذه النتيجة لا يمكن ملاحظتها من قبل كافة الأشخاص كون أن عملية التحويل غير ظاهرة للعيان كما هو الحال في باقي الجرائم كالسرقة مثلا،[5] فعملية غسل الأموال إلكترونيا تعتبر جريمة مادية لها نتيجة.

ومن أجل إكتمال الركن المادي يجب أن تكون هناك رابطة سببية تربط بين النتيجة المتحققة والسلوك الإجرامي، بمعنى أنه حتى تتم جريمة غسل الأموال إلكترونيا يجب أن تسند تلك النتيجة إلى فعل الجاني فهي ما كانت لتتحقق لولا فعله المتمثل في غسلها.

---

[1] آمنة تازير، (جريمة تبييض الأموال في التشريع الجزائري بين القمع والوقاية)، مجلة دراسات إنسانية واجتماعية، ع10، مج 2، الصادر في جوان 2019، ص 296.

[2] حمدي محمد أحمد الجداوي، مرجع سابق، ص 214.

[3] سفيان بن تقي ، (جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية) مجلة الأبحاث القانونية والسياسية، ع 2، مج 3، الصادر في 2021، ص 158.

[4] حمدي محمد أحمد الجداوي، مرجع سابق، ص 215.

[5] نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، مرجع سابق، ص 182.

أما بالنسبة للركن المعنوي ومن خلال المادة 389 من قانون العقوبات والتي سبق الإشارة إليها ورد فيها " ما علم الشخص على أنها تشكل عائدات إجرامية" وهذا إن دل فإنما يدل على أنها جريمة عمدية تتطلب توفر القصد الجنائي العام القائم على عنصري العلم والإرادة.

فعنصر العلم هو أن يكون الجاني عالما بالمصدر غير المشروع للأموال ومدركا بأن الفعل الذي يقوم به يعتبر مجرما ومعاقب عليه قانونا إلا أنه رغم ذلك تتجه إرادته إلى تحقيقه وإتمامه.

المبحث الثاني:

جرائم إلكترونية مستحدثة تستهدف شركات المساهمة في نظامها المعلوماتي.

باعتبار أن النظام المعلوماتي لشركات المساهمة هو مركز تخزين معطياتها المتعلقة بأسرارها التجارية مع قدرته على إسترجاعها في ظرف قياسي متى كانت الحاجة إليها وهذا ما لم يكن متاحا من قبل، لذلك فإن الإعتداء عليه يشكل خطرا حقيقيا قد يترتب عليه إنتهاء هذه الشركة، كونه ينتهك سرية وسلامة معطياتها، ومن خلال هذا المبحث سنتطرق إلى أنواع الجرائم التي تستهدف النظام المعلوماتي لشركات المساهمة وذلك بتقسيمه إلى مطلبين:

المطلب الأول: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركات المساهمة.

المطلب الثاني: الجرائم الواقعة على وظائف النظام المعلوماتي ومعطياته في شركات المساهمة.

المطلب الأول:

جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركات المساهمة.

ويطلق عليه كذلك باختراق النظام المعلوماتي لشركة المساهمة حيث تعد من اخطر الجرائم التي يمكن أن يتعرض لها النظام المعلوماتي لهذه الشركات، فيمكن إعتبارها بمثابة المرحلة التي تسبق باقي الجرائم والتي سنتكلم عنها لاحقا، بل أنها من أكثر الجرائم إنتشارا وتستهوي بشكل كبير جناة الفضاء الرقمي من أجل الإعتداء على شركة المساهمة، وفي هذا المطلب سنبين موقف التشريعات من هذه الجريمة **(الفرع الأول)** تم نتطرق إلى البنيان القانون لها **(فرع ثاني)**.

الفرع الأول:

موقف التشريعات من جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي.

رغم خطورة فعل الدخول أو البقاء غشا في النظام المعلوماتي إلا أنه ثار خلاف وجدل فيما يتعلق بمسألة تجريمهما، فهناك من رأى بأنه لا توجد ضرورة تستدعي تجريمهما طالما أن صاحبهما ليس له نية إرتكاب جريمة لاحقة،[1] وإنما يعتبر ذلك في الأساس مجرد إستعراض الجاني

[1] حفيظ بن قربة ، (جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري)، مجلة القانون والعلوم السياسية، ع 2، مج 3، الصادر في جوان 2017، ص 201.

للملكات الذهنية والفنية التي يتمتع بها،[1] وبالتالي فإن ذلك لا يعد جريمة قائمة بذاتها يترتب عليها معاقبة الفاعل.

فنجد بأن شركة "آبل" "APPLE" والتي بلغت قيمة إيرادتها سنة 2019 حوالي 260,2 مليار دولار وإجمالي أرباحها 55,3 مليار دولار وقدرت قيمة أصولها 338,5 مليار دولار، قد تعرضت لعملية إختراق في نظامها المعلوماتي من طرف مراهق أسترالي يبلغ من العمر 16 سنة، وعندما سألوه عن سبب الإختراق الذي قام به، رد بأن إعجابه الشديد بهاته الشركة وحلمه بأن يعمل بها هو الذي دفعه إلى ذلك،[2] وبما أن هذا الفعل لا يترتب عليه أي أثر فما الفائدة من تجريمه؟

من جهة أخرى هناك من يرى بأن فعل الدخول أو البقاء غير المشروع و إن لم تكن لدى صاحبه نية إرتكاب جريمة لاحقة إلا أنها قد تتولد لديه فيما بعد،[3] كما تترتب عليه خسائر نتيجة مجرد محاولة وقفه،[4] ففي الولايات المتحدة الأمريكية كانت الخسائر التي لحقت أحد المصانع 100,00 دولار وذلك كتكلفة أبحاث فقط من أجل منع أحد المخترقين من الدخول إلى النظام المعلوماتي بصفة متكررة.[5]

إضافة إلى ذلك فإن ترك فعل الدخول أو البقاء غير المشروع دون تجريم يشجع الجناة على إرتكابه، بل أن ذلك يدفعهم إلى التمادي أكثر وأكثر في الإعتداء على الأنظمة المعلوماتية، سيّما حين يستهدف شركة بحجم شركة المساهمة، إذ لا مجال لأحد في التباهي بعرض قدراته التقنية على إختراق حواجزها الإلكترونية وانتهاك سرية معطياتها.

---

[1] نجاة عباوي، مرجع سابق، ص 282.

[2] أكبر الشركات العالمية التي تعرضت للقرصنة، مقال منشور بتاريخ 31 جانفي 2021، تاريخ الدخول: 2023/02/15 ، متاح على الرابط:https://www.argaam.com

[3] بثينة حبيباتني،"الجرائم المتصلة بتكنولوجيات الإعلام والإتصال"، (أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر1، 2020) ، ص 15.

[4] نهلا عبد القادر المومني، مرجع سابق، ص 157.

[5] حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 51.

إلا أن التشريعات قد حسمت ذلك الجدل وسارعت إلى تجريم فعل الدخول أو البقاء غير المشروع، فعلى الصعيد الدولي نجد إتفاقية بودابست،[1] قد نصت في المادة الثانية[2] منها تحت عنوان "النفاذ غير المشروع" بأنه "يلزم على كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما أرتكب عمدا وبغير حق النفاذ الكامل أو الجزئي إلى نظام كومبيوتر، يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في إرتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

كما نجد قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها،[3] حيث نصت المادة الثالثة منه على أنه " كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس...والغرامة...أو بإحدى هاتين العقوبتين" أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،[4] فقد إعتبرت بأن الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء مت تقنية المعلومات أو الإستمرار فيه، يعد جريمة معاقب عليها وذلك بموجب المادة السادسة منها تحت عنوان "جريمة الدخول غير المشروع" والتي جاء فيها:

1-الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به.

2-تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمار بهذا الإتصال:

أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الإتصال وإلحاق الضرر بالمستخدمين والمستفدين.

ب-الحصول على معلومات حكومية سرية.

---

[1] إتفاقية بودابست لمكافحة جرائم تقنية المعلومات، مرجع سابق.

[2] Art: 2 –Accès illégal.

Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatique ou dans une autre intention délictuse , ou soit en relation avec un système informatique connecté à un autre système informatique.

[3] قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، إعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بموجب القرار رقم 417-د 21 في 2004.

[4] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق.

كما نجد العديد من الدول الغربية والعربية التي إعتبرت بأن فعل الدخول أو البقاء غير المشروع يعد جريمة قائمة بذاتها وجرمته في قوانينها الداخلية، ففي الولايات المتحدة الأمريكية نجد بأن أول تشريع صدر من أجل تجريم هذا الفعل كان عبارة عن مقترح على المستوى الفيدرالي سنة 1948، وذلك بإضافة نص تم من خلاله تجريم الإستخدام غير المصرح به لنظم المعلوماتية

غير أن هذا الإقتراح لم يتم أخذه بعين الإعتبار، ليصدر بعدها سنة 1996 تعديل القانون الفيدرالي،[1] فنجد بأن المادة 1030 (A-4)[2] من هذا القانون تنص على تجريم الدخول دون إذن إلى جهاز الحاسوب أو تجاوز الدخول المصرح به متى كان ذلك بنية الحصول على شيئ ذي قيمة تتجاوز 5000 دولا أمريكي.

أما المشرع الفرنسي فقد نص على تجريمه من خلال قانون العقوبات بموجب المادة 323 -1 المعدلة بموجب القانون رقم 2015-912،[3] والتي نصت على أنه يعاقب كل من دخل أو بقي بطريق الإحتيال في نظام المعالجة الآلية للبيانات أو في جزء منه بالحبس لمدة سنتين وغرامة مالية قدرها 60,000 يورو.

أيضا المشرع المصري الذي نص في المادة 14 من القانون 175 لسنة 2018 [4] بأنه" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي ويبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محضور الدخول عليه".

---

[1] عبد الله محمد الحضري، مرجع سابق، ص 13.

[2] 18USC 1030: Fraud and related activity in connection with computer, text contains those laws in effect on February 17, 2023.
(A-4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use computer and the value of such use is not more than $5,000 in any 1-year period.

[3] Art: 323-1 modifie par loi N^0 2015-912 du 24 juillet 2015, relative au renseignement échéancier d'application, art 4, J.O.R.F. N^0 0171 du 26 juillet 2015.
Le fait d'accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60,000€ d'amende.

[4] القانون المصري رقم 175 لسنة 2018 ، مرجع سابق.

أما بالنسبة للمشرع الجزائري ومن خلال جملة النصوص القانونية التي سارع إلى إصدارها بغية تدارك الفراغ القانوني فيما يتعلق بمكافحة الجريمة الإلكترونية، فقد نص على تجريم فعل الدخول أو البقاء غير المشروع بموجب القانون رقم 24-06[1] المعدل والمتمم لقانون العقوبات، حيث نصت المادة 394 مكرر منه على أنه " يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60,000 دج إلى 200,000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

فالمشرع الجزائري لم يشترط أن يكون نظام المعالجة الآلية للمعطيات محميا بشفرات إلكترونية أو غير محمي وإنما جاء النص عاما، وهذا ما يدل على إدراك المشرع لخطورة هذه الجريمة خاصة حينما يكون النظام المعلوماتي المستهدف يتعلق بشركة مساهمة.

الفرع الثاني:

أركان قيام جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركات المساهمة.

بما أن الدخول أو البقاء غشا في النظام المعلوماتي يعد جريمة قائمة بذاتها فبطبيعة الحال لها أركان تقوم عليها، هذا ما نوضحه في هذا الفرع من خلال التطرق إلى الركن المادي أولا ثم الركن المعنوي وللإشارة فقد تجنبنا الحديث عن الركن الشرعي كونه سبقت الإشارة إليه في معرض الحديث عن موقف التشريعات منه.

أولا: الركن المادي.

حتى تقوم هذه الجريمة وتتحقق يفترض أن يكون هناك سلوك يرتكبه الجاني، وبحسب ما ورد في نص المادة 394 مكرر فإن ذلك السلوك يتمثل في فعلين هما الدخول أو البقاء، كما أنه قد تترتب عنهما حذف أو تغيير للمعطيات أو تخريب النظام، لذلك فإن الركن المادي لهذه الجريمة يتخذ صورتينن صورة بسيطة وأخرى مشددة.

[1] قانون رقم 24-06 مؤرخ في 28 أفريل 2024 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج ر ج ج، ع 30 الصادر في 30 أفريل 2024.

1-الصورة البسيطة للدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة المساهمة: وتعد هذه الجريمة من جرائم السلوك التي لا يشترط أن تحدث نتيجة معينة وإنما تقوم بمجرد إرتكاب الفعلين اللذين نوضحهما فيما يلي:

أ-الدخول غير المشروع إلى النظام المعلوماتي لشركة المساهمة: بداية ينبغي التوضيح بأن الدخول في هذه الحالة لا يقصد به التواجد المادي للجاني، كتواجده بداخل أحد مكاتب هذه الشركة الذي يوجد به أجهزة حواسيبها، وإنما المقصود هو التواجد المنطقي المعنوي أي الدخول نظامها المعلوماتي والذي يمكن تشبيهه بالدخول إلى ذاكرة الإنسان.

ويعرف الدخول بأنه التواجد غير المشروع في نظام المعالجة الآلية للبيانات من خلال إنتهاك الإجراءات الأمنية له،[1] وهو أيضا الدخول غير المرخص به بأي طريقة تكون غير شرعية إلى النظام المعلوماتي أو المخالف لأحكام الترخيص،[2] كما انه جميع الأفعال التي يمكن من خلالها الولوج إلى النظام المعلوماتي والإحاطة به، أو السيطرة على المعلومات التي يحتويها أو الخدمات التي يقوم بتقديمها.[3]

وبالتالي يمكننا القول بأن مجرد الدخول إلى النظام المعلوماتي لشركات المساهمة لا يشكل جريمة في حد ذاته، وإنما يستمد صفة الجرم كونه تم بطريق الغش أو الإحتيال أي ضد إرادة المسؤول عن ذلك النظام في شركات المساهمة ودون أخذ تصريح منه، وعليه فالحالات التي يتم فيها الدخول بطريق غير مشروع هي:

*الدخول دون تصريح من المسؤول عن النظام: وهو المالك أو أي شخص آخر يتولى مهمة الإشراف على الحاسب الآلي بالشركة،[4] وتم تعريفه من خلال الأعمال التحضيرية لقانون الغش المعلوماتي الفرنسي سنة 1988 على أنه شخص طبيعي أو معنوي أو كل سلطة عامة أو مصلحة أو تنظيم،

---

[1] أيمن بن ناصر بن حمد العباد، مرجع سابق، ص 83.

[2] ليلى عبد المجيد، التنظيم التشريعي والقانوني للإعلام التقليدي والإلكتروني، ط 1، القاهرة، العربي للنشر والتوزيع، 2020، ص 140.

[3] عبد الإله محمد النوايسة، مرجع سابق، ص 217.

[4] المرجع نفسه، ص 221.

يكون مختصا بالتصرف في النظام أو إتخاذ القرار بشأن إنشائه، تنظيمه أو غاياته،[1] ويعرف أيضا على أنه كل شخص له كافة السلطات الممكنة على النظام المعلوماتي سواء من حيث إستعماله، إستغلاله وكذا التصرف فيه.[2]

أما التصريح فهو الإذن الذي يمنحه صاحب العلاقة إلى شخص آخر أو أكثر أو للجمهور قصد الدخول أو إستخدام النظام المعلوماتي أو الشبكة المعلوماتية أو موقع إلكتروني، بقصد الإطلاع أو إلغاء أو حذف إو إضافة أو تغيير إو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته.[3]

فالدخول غير المشروع يحدث حين يقوم شخص ما بالدخول إلى النظام المعلوماتي دون أن تكون له أية علاقة بالنظام ومن غير الحصول على ترخيص يسمح له بذلك، وهذا ما يحدث أيضا في شركات المساهمة فقد يكون ذلك الشخص أحد موظفيها دون أن تخول له وظيفته حق الإتصال بالنظام أو أن يكون أجنبي عن هذه الشركات ففي كلتا الحالتين يعتبر دخول غير مشروع.

واحيانا يكون الترخيص بالدخول مقترنا بشرط كتسديد مبلغ الإشتراك مثلا،[4] هذا ما نجده في حالة الشركات التي تقدم خدمات للجمهور عبر مواقع الأنترنت ويكون ذلك نظير مقابل مادي، فهنا تقوم جريمة الدخول غير المشروع بمجرد قيام الجاني باختراق النظام المعلوماتي وذلك بهدف إستبعاد ذلك المقابل وحرمان الشركة منه،[5] بالنسبة للمشرع الجزائري نجد بأن نص المادة 394 مكرر جاء عاما يشمل جميع الحالات دون أن ينص على أي شرط.

---

[1] نسمة بطيحي ، مرجع سابق، ص 52.

[2] حفيظ بن قربة ، مرجع سابق، ص 206.

[3] عبد الإله محمد الحضري، مرجع سابق، ص 56.

[4] بثينة حبيباتني ، مرجع سابق، ص 27.

[5] نسمة بطيحي ، مرجع سابق، ص 53.

-تجاوز حدود التصريح: في هذه الحالة الجاني يحوز على تصريح بالدخول غير أنه يتجاوز الحدود المسموح له بها في ذلك التصريح،[1] كأن يكون يملك حق الدخول إلى جزء فقط من النظام المعلوماتي فيقوم بالدخول إلى باقي الأجزاء الأخرى، والمشرع الجزائري عبر على هذا النوع من الدخول بعبارة "أو جزء من النظام" فهنا التصريح يشمل جزءا فقط وليس كل النظام.

فهذا النوع من الدخول يكون في الغالب من طرف الموظفين في الشركات، وذلك لكونهم يملكون تصريحا بالدخول بحكم وظيفتهم، إلا أنهم يتجاوزون حدود التصريح المخولة لهم ويطلعون على بيانات لا تعد من إختصاصهم الوظيفي،[2] ففي شركة المساهمة يتم تقسيم المهام على الموظفين بحسب الإختصاص فهناك المكلف بقائمة العملاء والزبائن، بحيث لا يجوز الإطلاع على ما يحويه النظام الخاص بتركبة المنتوج مثلا.

كما يتجلى هذا النوع من الدخول فيما إذا كان للموظفين الحق في الدخول إلى النظام المعلوماتي في الشركة بهدف القيام بغرض معين إلا أنه يحدث أن ينحرف عن الغرض المحدد ويحقق غرض آخر، لذلك فطبيعة الإعتداء على النظام المعلوماتي تتحدد بناءا على العلاقة بين الموظف والمسؤول عن ذلك النظام، ففي حالة ما إذا قام الموظف بالدخول دون يحترم الشروط التي رسمها المسؤول يكون قد خان ثقة المسؤول عن النظام.[3]

إلا أن المشرع الجزائري لم ينص على الحالة التي يكون فيها الجاني موظفا تابعا للشركة التي يعمل بها حتى تضاعف عقوبته،[4] كما أنه لم ينص على الإلتزام بالحدود المرسومة في التصريح أو تجاوزها بل تعتبر جريمة الدخول قائمة بذاتها متى تم الدخول بطريق غير مشروع لكل أو جزء من

---

[1] أشرف محمد نجيب السعيد الدريني، (جرائم الإعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات)، مجلة روح القوانين، ع 59، الصادر في يوليو 2021، ص 277.

[2] محمد بن أحمد ، مرجع سابق، ص 205.

[3] بثينة حبيباتني ، مرجع سابق، ص 28.

[4] على عكس ذلك نجد المشرع الأردني قد نص على تشديد العقوبة ومضاعفتها بحق كل من يرتكب الجرائم المنوص عليها في المواد 3 إلى 6 بمناسبة تأديته وظيفته أو عمله أو باستغلال أي منهما (المادة 8 من القانون رقم 27 لسنة 2015، ج،ر، ع 5343 الصادر في 06/01/ 2015).

النظام، ومهما كانت صفة فاعلها سواء كان من الموظفين في الشركة أو خارجا عنها مستعملا بذلك عبارة كل من يدخل والتي تشمل الكل.

ومن القضايا في هذا الشأن ما تعرض له القضاء الأمريكي حيث كان هناك موظف يدعى "ERIC LELAND" كان يحوز على كيفية الدخول إلى خطط العمل السرية للشركة التي كان يعمل بها وقبل أن يترك وظيفته بها قام بإرسال العديد من الأسرار التجارية والمعلومات الخاصة بتلك الشركة إلى شخص آخر، بعد عدة إغراءات وقد تم محاكمة هذا الموظف على أساس تعمد الدخول إلى النظام المعلوماتي للشركة إنتهاكا لتشريع الدخول غير المصرح به الفيدرالي، حيث تبنت المحكمة وجهة النظر القاضية بأن التصريح الذي يتم منحه للعاملين ينتهي متى كان يستهدف مصالح مضادة أو إخلال بالولاء للمسؤول عن النظام.[1]

أما بالنسة للطريقة التي يتم بها الدخول إلى النظام المعلوماتي باعتبار أن عملية الدخول تكتسي طابع تقني بحت فإنها تتم بواسطة:

– الإتصال المباشر بالنظام المعلوماتي، بمعنى أن الجاني في هذه الحالة موجود في نفس المكان الذي يوجد فيه النظام، فقط المطلوب منه القيام ببعض العمليات المادية مثل إدخال قرص مضغوط يتضمن برنامج فك الرموز من أجل الدخول إلى النظام المحمي تقنيا عن طرق شفرات، أو عمليات منطقية كالتلاعب في عين مكان النظام بمعطياته أو برامجه أو إجراء تعديلات فيها من أجل تسهيل عملية الدخول.[2]

–الإتصال المعنوي عن بعد بالنظام المعلوماتي: حيث أنه في هذه الحالة يتمكن من الجاني من الوصول إلى النظام المعلوماتي الخاص بالشركة الضحية عن طريق نظام آخر يكون متصل بنظامها من خلال شبكة الأنترنت،[3] وذلك من خلال إستعمال الوسائل المستحدثة للإتصال عن بعد كالشبكات المعلوماتية أو الإلكترونية السلكية واللاسلكية وهو يعكس النوع الأول، إذ يشترط أن يكون الجاني موجودا بنفس مكان وجود جهاز الحاسوب.

---

[1] بثينة حبيباتني ، مرجع سابق، ص 29.

[2] عفاف خذيري، مرجع سابق، ص 40.

[3] نسمة بطيحي ، مرجع سابق، ص 55.

وللإشارة فإن المشرع الجزائري لم ينص صراحة على الطرق التي يتم بها تنفيذ عملية الدخول غير المشروع، وإنما جاء نص المادة 394 مكرر عاما شاملا لكل الطرق التي يسلكها الجاني من أجل الوصول إلى النظام المعلوماتي، وبالتالي فإن دائرة التجريم تتسع لأي طريق.

أما فيما يتعلق بشرط أن يكون النظام المعلوماتي للشركة مشمولا بالحماية الأمنية والفنية حتى يحظى بالحماية الجنائية، فالمشرع الجزائري لم يشترط ذلك بل يعتبر دخولا غير مشروع متى تم ضد إرادة المسؤول عن النظام لهذه الشركة.

وهو نفس ما ذهب إليه المشرع الفرنسي من خلال قرار صادر عن مجلس قضاء باريس غرفة الجنح في 5 أفريل 1995، إذ إعتبر القاضي الجزائي بأن جريمة الدخول غير المشروع في النظام المعلوماتي قائمة بذاتها حتى في حالة غياب نظام الحماية للنظام.[1]

ب–البقاء غير المشروع في النظام المعلوماتي لشركة المساهمة: وهو السلوك الثاني الذي جرمه المشرع الجزائري بصفة مستقلة عن الدخول في المادة 394 مكرر، حيث يعرف بأنه التواجد داخل النظام المعلوماتي ضد إرادة من يملك الحق في السيطرة على ذلك النظام،[2] وهو أيضا عدم وضع حد للتشعب داخل النظام مع الإعتقاد بأن ذلك خطأ،[3] وهو التواجد غير العادي مثل الإتصال عن طريق الشبكة المعلوماتية بالنظام المعلوماتي، وبالتالي الدخول إليه والكشف عن كل ما يتضمنه من معلومات إلى غير ذلك من التصرفات التي يعتبر غير مسموح القيام بها والتي بدورها تشكل بقاء غير مشروع.[4]

كما يعني وصول الجاني إلى نظام الحاسوب مع إحتفاظه بالبقاء وعدم الخروج منه رغم معرفته بعدم مشروعية فعله كونه يتصرف بدون وجه حق في ذلك،[5] وعليه يجب على كل من دخل عن

---

[1] نسيم دردور، "جرائم المعلوماتية على ضوء القانون الجزائري والمقارن"، (رسالة ماجستير، كلية الحقوق، جامعة منتوري قسنطينة، 2012–2013)، ص 31.

[2] رشيدة بوكر ، (الدخول أو البقاء داخل نظم معلومات المؤسسة الاقتصادية بين عدم التصريح والحماية الجزائية)، مجلة قانون العمل والتشغيل، ع 1، مج 6، الصادر في جانفي 2021، ص 213.

[3] كريمة عباس ، (جرائم المساس بأنظمة المعالجة الآلية للمعطيات)، مجلة البيبان للدراسات القانونية والسياسية، (ع 4، الصادر في ديسمبر 2017، ص 123.

[4] Alain Bensoussan, internet, aspects juridique, 2 eme Ed, france, hermes science publication, juin 1996, p 109.

[5] Jean Pradel, (Les infraction relatives à l'informatique) , R. I. D. C, N02, vol 42, juin 1990, P 824 .

طريق الخطأ أو الصدفة قطع الإتصال بالنظام ومغادرته فورا، ففعل البقاء غير المشروع يندرج ضمن جرائم الإمتناع كون أن الجاني فيها يمتنع عن قطع الإتصال.

وفعل البقاء في النظام المعلوماتي لشركات المساهمة قد يرتكب مستقلا عن فعل الدخول كما يمكن أن يكون يقترن به.

ففي الحالة التي يستقل فيها عن فعل الدخول يتحقق ذلك في حالة ما إذا كان الدخول إلى نظامها المعلوماتي مرخص به ويتم بطريق مشروعة، كأن يتم ذلك صدفة أو سهوا إلا أن الجاني لا يقطع الإتصال ويستمر، أيضا إذا ما كان الدخول محدد بمدة معينة وتم إستهلاكها من طرف الشخص وزاد عنها فيعتبر دخوله غير مشروع كونه تجاوز المدة المسموح بها و المحددة،[1] كما يتحقق في حالة ما إذا تم السماح للإطلاع على معلومات تتعلق بالشركة من أجل مراجعتها غير أن الجاني يقوم بطباعتها،[2] كما يستقل فعل الدخول عن فعل البقاء كونهما مختلفين عن بعض، حيث يعتبر فعل البقاء من الأفعال المستمرة وذلك على خلاف فعل الدخول الذي يعتبر من قبيل الأفعال الوقتية.[3]

ومن القضايا التي أكدت على أن الفعلين مستقلين عن بعض ما قضت به محكمة النقض الفرنسية عن غرفتها الجنائية وذلك في قرارها الصادر في 20 ماي 2015، في قضية تتلخص وقائعها في أن الجاني تمكن من الوصول إلى النظام المعلوماتي للطرف الضحية عن طريق الخطأ ورغم معرفته وتأكده بأن بقاؤه يعتبر ضد إرادة مالك النظام إلا أنه واصل البقاء ولم يقطع الإتصال، إلا أن محكمة النقض قامت بتأييد الحكم المطعون فيه وأدانت الجاني على فعل البقاء فقط أما فعل الدخول فقد تم تبرئته منه.[4]

---

[1] محمد قسمية ، حمزة خضري ، (مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري)، مجلة صوت القانون، (المجلد 7، ع2، مج 7، الصادر في نوفمبر 2020، ص 133.

[2] عبد الوهاب ملياني ، "أمن المعلومات في بيئة الأعمال الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2016-2017)، ص 184.

[3] بهاء فهمي الكبيجي، مرجع سابق، ص 32.

الجريمة المستمرة هي التي يتكون ركنها المادي من تصرف أو حالة تحتمل الإستمرار لفترة زمنية غير محدد من الوقت.

الجريمة الوقتية هي التي يتكون ركنها المادي من تصرف يقع في وقت محدود أي فترة زمنية قصيرة، (نهلا عبد القادر المومني، مرجع سابق، ص ص 161،162).

[4] Cour de cassation, criminelle, chambre criminelle, 20 mai 2015, N^0 14. 81. 336. Publié ou bulletin.

أما بالنسبة للحالة التي يجتمع فيها فعل البقاء والدخول معا أي عكس الحالة الأولى، يتحقق ذلك عندما يقوم الجاني باختراق النظام المعلوماتي ويتم الدخول إليه بطريقة غير مشروعة متجاوزا بذلك إرادة صاحب النظام مع إستمراره في البقاء داخله، فالجاني في هذه الحالة لا يستهدف مجرد الدخول فقط وإنما المكوث داخله أيضا.

حيث أنه في هذه الحالة يمكن متابعة الجاني بتهمتين على أساس فكرة التعدد الجرمي،[1] الأولى تتمثل في جريمة الدخول إلى النظام المعلوماتي للشركة وهي جريمة وقتية، تعقبها جريمة مستمرة تتمثل في البقاء والمكوث به،[2] وكان المشرع قد أكد فكرة التعدد الفعلي للجرائم من خلال صياغته لنص المادة 349 مكرر من خلال إستعماله لعبارة "أو يبقى" فحرف "أو" يفيد التعدد كون أن هناك جريمتين مجتمعتين متتابعتين ولكن لكل جريمة سلوكها الخاص بها.

لكن السؤال الذي يطرح نفسه ماذا عن الزمن الذي يعتبر النقطة الفاصلة بين جريمة الدخول وجريمة البقاء؟

الواقع أنه لا يوجد نص صريح يحدد ذلك سواء في القانون الجزائري أو القوانين المقارنة، غير أن المنطق يقتضي بأن بداية جريمة البقاء داخل النظام المعلوماتي تكون من اللحظة التي يشرع فيها الجاني بالتجول فيه وتصفح معلوماته،[3] وفي هذا الصدد نجد القرار الصادر عن الغرفة الجزائية الثالثة بمجلس قضاء الجزائر، رقم الفهرس 16-09247 الصادر في 27 جوان 2016، بأن نيابة محكمة الحراش قامت بمتابعة المتهم المدعو (م.ل) بتهمة جريمة الدخول والبقاء غير المشروع في منظومة المعالجة الآلية للمعطيات لشركة إتصالات الجزائر، حيث قام المتهم بالدخول وتصفح مجموعة من الفواتير الخاصة بزبائن الهاتف الثابت حيث إعترف بذلك.

وبعد التحريات إتضح أنه تصفح تلك الفواتير لمدة 10 ساعات كاملة وقد قام بذلك دون الحصول على أي ترخيص من شركة إتصالات الجزائر، فبالنظر إلى مدة البقاء تبدو طويلة

---

[1] كريمة عباس ، مرجع سابق، ص 123.

[2] بثينة حبيباتني ، مرجع سابق، ص 37.

[3] محمد بن أحمد ، مرجع سابق، ص 220.

وتؤكد سوء نية الجاني وأنه لم يرتكب فعله بصفة عرضية أو عن طريق الخطأ، وكان المجلس قد أيد حكم المحكمة مبدئيا.[1]

2-الصورة المشددة للدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة المساهمة:

إذا كانت الصورة البسيطة لهذه الجريمة شكلية فإن الأمر يختلف في صورتها المشددة كونها تتحول إلى جريمة مادية تترتب عنها نتيجة تكون بمثابة ظرف مشددا تضاعف على أساسه العقوبة، فنجد بأن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قد نصت على هذا الظرف المشدد من خلال الفقرة الثانية من المادة السادة منها والتي جاء فيها " تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمار بهذا الإتصال:

-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الإتصال وإلحاق الضرر بالمستخدمين والمستفدين.

-الحصول على معلومات حكومية سرية".

كما نص على ذلك المشرع الفرنسي في المادة 323-2-1 من قانون العقوبات والمعدلة بموجب القانون رقم 2015-912 الصادر في 24 جويلية 2015.[2]

أما بالنسبة للمشرع الجزائري فقد نص على ظرفين لتشديد عقوبة جريمة الدخول أوالبقاء غير المشروع وذلك ما يتجلى في الفقرتين الثانية والثالثة من المادة 349 مكرر، والتي جاء فيها " تضاعف العقوبة إذ ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

-وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال إشتغال المنظومة تكون العقوبة الحبس من سنة إلى ثلاث سنوات والغرامة من 100.000 دج إلى 300.000دج"

وعليه يتم تشديد العقوبة في شركة المساهمة إذا ما ترتب عن الدخول أو البقاء في نظامها المعلوماتي حذف أو تغيير معطياته وكذا تخريب نظام إشتغاله.

---

[1] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات دراسة مقارنة، مرجع سابق، ص ص 164،165.

[2] Art: 323-1-2 modifié par loi N^0 2015-912 du 24 juillet 2015, op,cit.
Lorsqu' 'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100,000€ d'amende.
Lorsque les infractions prévue aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150,000€ d'amende.

أ-حذف أو تغيير معطيات النظام المعلوماتي لشركة المساهة: المقصود بعملية الحذف هو إزالة أو محو المعطيات التي يحويها نظامها المعلوماتي[1]، وتعد عملية الحذف هذه من أقصى أنواع الضرر الذي يمكن أن تتعرض له شركة المساهمة، كونه يزيل المعلومة بصفة نهائية من نظامها، بحث لا يشترط في عملية الحذف أن تشمل جميع المعلومات المدرجة في نظامها بل يكفي أن تحذف بعض أجزائها فقط.[2]

أما التغيير فمعناه إدخال تعديلات على معطياتها، كما يعني كذلك العبث بها من خلال التلاعب بها أو إخلال حدث بحيث يصبح معناها مختلف ومغاير تماما لما كانت عليه في السابق، وبالتالي الإنقاص من قيمتها الحقيقية وكذا أدائها لوظيفتها،[3] ومن ذلك نجد ما قامت به المجموعة الإرهابية الملقبة ب "ACTION DIRECT" من حذف ملفات خاصة بشركة "كبرس" وذلك لحساب مجموعة من الشركات المنافسة.[4]

ب-تخريب نظام إشتغال المنظومة المعلوماتية لشركة المساهمة: ويعني ذلك إرباك أو إعاقة عمل نظامها المعلوماتي،[5] وبالتالي تشويه أداء عمله بشكل طبيعي وعدم صلاحيته للإستعمال،[6] وسيتم التفصيل في هذه الجريمة أكثر في المطلب الموالي باعتبار أن هذه الجريمة سنتناولها بصورة مستقلة مثلما فعلت بعض التشريعات حين جرمتها بموجب نصوص مستقلة.

---

[1] محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ط 1، جمهورية مصر العربية، مركز الدراسات العربية للنشر والتوزيع، 2015، ص 74.

[2] دلال لطيف مطشر، (جريمة الإعتداء على المواقع الإلكترونية -دراسة مقارنة-)، مجلة جامعة بابل للعلوم الإنسانية، ع 9، مج 26، الصادر في 2018، ص 401.

[3] محمد بن أحمد ، مرجع سابق، ص 228.

[4] فيصل بدري ، مرجع سابق، 168.

[5] جمال زين العابدين أمين أحمد، (جرائم إختراق النظم الإلكترونية بين التشريع المصري والمغربي)، مجلة مستقبل العلوم الاجتماعية، ع 1، الصادر في أفريل 2020، ص 121.

[6] شول بن شهرة ، (آليات مكافحة الجريمة المعلوماتية مواقع التجارة الإلكترونية نموذجا)،مجلة دراسات الجزائر، ع 13، الصادر في مارس 2010، ص 209.

ثانيا: الركن المعنوي:

مثلما سبقت الإشارة فإن الركن المعنوي يعتبر ركيزة أساسية وهامة وعلى أساسها يتم تحديد السلوك المرتكب وتكييفه، فغياب هذا الركن يترتب عليه غياب وقوع الجريمة إذ لا يمكن قيام الجريمة على ركن واحد والمتثل في الركن المادي فقط.

وجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة المساهمة تأخذ صورة العمد لذلك فيتم تكييفها على أساس أنها جريمة عمدية، وقد أكدت على صفة العمد العديد من التشريعات وبعدة صيغ مختلفة رغم أنه لا حاجة إلى ذلك باعتبار أن الأصل فيها القصد واستثناءا يتم إرتكابها عن طريق الخطأ.[1]

من تلك التشريعات نجد المشرع الأردني، المشرع العماني وكذا المشرع القطري جميعهم إستعمل عبارة "كل من دخل عمدا"[2] كذلك المشرع الفرنسي الذي إستعمل عبارة " FRAUDULEUSEMENT" والتي تعني بطريق الغش وهي ذات العبارة التي إستعملها المشرع الجزائري، فهاته العبارة تحمل بين طياتها سوء نية الجاني وإنه أقدم على إرتكاب جريمته عمدا.

فجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة المساهمة تقوم على توفر القصد الجنائي لدى مرتكبها، لكن الإشكال الذي يمكن يطرح في هذه النقطة ماهو هذا القصد المطلوب، هل القصد الجنائي العام أم الخاص؟

1-القصد الجنائي العام:

المتعارف عليه أن هذا القصد يقوم على عنصرين هما العلم والإرادة، وفيما يلي نقوم بتوضيح مدى توفر هذين العنصرين في جريمة الدخول أوالبقاء في النظام المعلوماتي لشركة المساهمة.

---

[1] عبد الإله النوايسة، مرجع سابق، ص 265.

[2] خالد سليمان عبد الله الحمادي، "جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري –دراسة مقارنة–" (رسالة ماجستير، كلية القانون، جامعة قطر، 2019)، ص 79.

فعنصر العلم يتمثل في إدراك الجاني لخطورة الأفعال المرتكبة من طرفه كونه ينتهك خصوصية وسرية مصلحة يحميها القانون،[1] وكذا علمه بكافة العناصر التي يرتكز عليها كيان هذه الجريمة،[2] بمعنى أن الجاني يكون على علم ومدركا تماما إلى أن دخوله أو بقاؤه في النظام المعلوماتي لهذه الشركة غير مسموح به ولا يملك أي حق في ذلك وإنما يفعله بطريقة غير مشروعة وضد رغبة وإرادة المسؤول عن النظام في هذه الشركة.

وبمفهوم المخالفة أن إنتفاء علم الجاني بأن ما يقوم به يعتبر فعل محضور يترتب عليه عدم قيام الجريمة، كما لو حدث ودخل الجاني أو بقي داخل النظام بصفة عرضية كونها جريمة لا تقوم عن طريق الخطأ.

أما عنصر الإرادة فيعني أن تتجه إرادة الجاني إلى تحقيق فعل الدخول أو البقاء في النظام المعلوماتي والتجول داخله،[3] إذ لا يكفي علم الجاني بعدم مشروعية فعله وإنما أيضا أن تتجه إرادته إلى تحقيق ذلك، فالإرادة تقتصر على تحقيق السلوك الإجرامي فقط دون أن تتجه إلى تحقيق نتيجة معينة، بل أن المشرع جعل من تحقق النتيجة مجرد ظرف مشدد لا أكثر كما سبقت الإشارة إلى ذلك.

ما ينبغي أن نشير إليه كذلك هو أنه متى تحقق القصد العام بعنصريه العلم والإرادة تعتبر الجريمة قائمة بذاتها ولا عبرة للبواعث حينها كأن يكون الباعث على سبيل المثال الفضول وحب الإستطلاع، أو من أجل كشف هشاشة نظام الحماية من أجل إصلاحه.

فنجد بأنه في القانون القطري قد قضى بوقوع جريمة الدخول إلى النظام المعلوماتي لأحد البنوك من قبل أحد المهندسين الذي أراد أن يثبت للبنك الذي يشتغل فيه كموظف قدرته الفنية على

---

[1] عبد النور بشان"الجوانب الموضوعية لمعالجة الجريمة المعلوماتية"، (أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر1، 2017-2018) ص 333.

[2] إبراهيم محمد القاسمي، "جرائم الدخول والبقاء غير المشروع في نظم المعالجة الآلية للمعطيات الإلكترونية وفقا للمرسوم بقانون إتحادي رقم 5 لسنة 2012في شأن مكافحة جرائم تقنية المعلومات وتعديلاته"، (رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018)، ص 57.

[3] بهاء فهمي الكببجي، مرجع سابق، ص 34.

إختراق النظام المعلوماتي لهذا البنك، وهذا كله من أجل الحصول على عقد تدريب وتكوين لكوادر البنك.[1]

2-القصد الجاني الخاص: هناك بعض التشريعات التي جرمت الدخول أو البقاء غير المشروع قد تطلبت إلى جانب القصد الجنائي العام ضرورة توفر القصد الجنائي الخاص،[2] حيث تعتبرأن هذه الجريمة لا يمكن أن تقع مكتملة الأركان إلا إذا تحقق ذلك الهدف الذي قامت من أجله.

أما بالنسبة للمشرع الجزائري فكما سبقت الإشارة قد إستعمل في المادة 394 مكرر مصطلح "عن طريق الغش" وهو نفسه المصطلح المستعمل من قبل المشرع الفرنسي، حيث أن هناك من يعتبر بأن هذا المصطلح أستعمل كدلالة على القصد الجنائي الخاص وذلك لإختلافه عن مصطلحي "عمدا" أو "قصدا" اللذان يدلان على القصد الجنائي العام.[3]

لكن هناك إجماع على أن مصطلح " الغش" لا تعني نية الإضرار وذلك لكونها غير مطلوبة وإلا حصل تناقض بين ركن مادي لا يتطلب نتيجة وركن معنوي،[4] وبالتالي فإن الغش يتحقق عندما يكون الجاني على علم بغياب حقه في الدخول أو البقاء في النظام المعلوماتي لشركة المساهمة[5].

لذلك فإن القصد الخاص والذي يعني إنصراف علم الجاني وإرادته إلى وقائع خارجة عن عناصر الجريمة وأركانها،[6] في إعتقادنا لا نلمحه ضمن المادة 394 مكرر كون أن مصطلح

---

[1] خالد سليمان عبد الله الحمادي، مرجع سابق، ص 86.

[2] هذا ما قضى به قانون إساءة إستخدام الحاسبات الآلية في المملكة المتحدة والذي جرم في مادته الثانية الدخول غير المصرح به متى كان للجاني قصد خاص يتمثل في نية إرتكاب أو تسهيل إرتكاب جرائم أخرى (خالد سليمان عبد الله الحمادي ، المرجع نفسه، ص 88).

كما نص القانون البرتغالي في مادته السادسة على تجريم الدخول متى كان بهدف الحصول على فائدة أو ربح غير مشروع أيضا القانون الدنماركي الذي شدد من عقوبة الدخول غير المصرح به متى أرتكبت بنية الإطلاع والحصول على معلومات شخص أو أسرار الشركات التجارية (عبد الله محمد الحضري، مرجع سابق، ص 65).

[3] محمد بن أحمد ، مرجع سابق، ص 236.

[4] بثينة حبيباتني ، مرجع سابق، ص 50.

[5] صورية بورباية، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 94.

[6] محمد قسمية، حمزة خضري، مرجع سابق، ص 135.

الغش يقتصر على القصد العام ليس إلا وأن الجريمة عمدية لا أكثر، إضافة إلى ذلك فإن المشرع ومن خلال هذه المادة لم يشترط ضرورة أن يكون الجاني على علم بتلك الوقائع والتي تعتبر في ذاتها من أركان الجريمة، والدليل على ذلك إستعماله لعبارة "فإذا ترتب على ذلك حذف أو تغيير أو تخريب" فهاته النتيجة تتحقق عن طريق الخطأ ب والذي يعد كافيا لقيامها دون قصد جنائي خاص.

المطلب الثاني:

الجرائم الواقعة على وظائف النظام المعلوماتي ومعطياته في شركات المساهمة.

إضافة إلى جريمة الدخول و البقاء غشا في النظام المعلوماتي لشركات المساهمة هناك جرائم أخرى تترتب عن ذلك، منها ما يطال وظائف نظامها من خلال إرباك عملية سيره، ومنها ما يطال المعطيات والبيانات المخزنة فيه، ومن أجل توضيح ذلك نتطرق في هذا المطلب إلى جريمة الإعتداء على سير النظام المعلوماتي لشركة المساهمة **(فرع أول)** ثم جريمة الإعتداء على معطيات شركة المساهمة **(فرع ثاني)**.

الفرع الأول:

جريمة الإعتداء على سير النظام المعلوماتي لشركات المساهمة.

نشاط الجاني في هذه الجريمة يستهدف المساس بوظائف النظام المعلوماتي وإعاقته عن أداء عمله بصورة سليمة وعادية، الشيئ الذي يكلف شركة المساهمة خسائر فادحة جراء ذلك التعطيل، ورغم خطورة هذه الجريمة إلا أن المشرع الجزائري لم يتطرق إليه بصفة مستقلة مثلما فعل مع باقي الجرائم وإنما تمت الإشارة إليها من خلال الفقرة الثالثة من المادة 394 مكرر التي نصت على أنه " إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سوات والغرامة من 100,000 دج إلى 300,000 دج وتقابلها في قانون العقوبات الفرنسي المادة 323-2[1] التي نصت على أنه يعاقب كل من تسبب في إعاقة أو إفساد نظام المعالجة الآلية بالحبس لمدة خمسة (5) سنوات.

[1] Art: 323-2, modifié par loi N^0 2015-912 du 24 juillet 2015, art 4, op, cit

ونشير إلى محل الإعتداء في هذه الجريمة في إطار شركات المساهمة يتمركز على وظيفة نظامها المعلوماتي وذلك من خلال تعطيله بصفة كلية أو جزئية معينة منه فقط، غير أن المشرع الجزائري من خلال الفقرة الثالثة من المادة 394 مكرر لم يقم بإدراج عبارة كل أو جزء مثلما فعل ذلك في جريمة الدخول أو البقاء غشا، وبالتالي فإنه لم يتم تحديد مساحة الإعتداء وإنما العبرة في قيام هذه الجريمة هو جعل النظام المعلوماتي الخاص بشركة المساهمة غير قادرعلى القيام بوظائفه المعتادة، ولقيام هذه الجريمة يتطلب الأمر تحقق كل من الركن المادي والمعنوي.

أولا: الركن المادي.

مثلما سبقت الإشارة إلى ذلك فإن المشرع أشار إلى هذه الجريمة في الفقرة الثالثة من المادة 394 مكرر معبرا عن ذلك باستعمال مصطلح " تخريب" في حين نجد أن المشرع الفرنسي قد إعتمد على مصطلحي "الإعاقة والإفساد" لذلك فإن السلوك الإجرامي يتمثل في إعاقة وتعطيل النظام المعلوماتي لشركات المساهمة عن القيام بالنشاط المعتاد والمنتظر القيام به بصفة طبيعية، أو إفساد وظائفه وسواء كان ذلك التعطيل والإفساد قد تم بصورة كلية أو جزئية، [1] وبالتالي فإن الإعتداء على سير النظام المعلوماتي لشركة المساهمة يكون إما من خلال فعل الإعاقة أو فعل الإفساد.

1-فعل الإعاقة: إعاقة النظام المعلوماتي لشركات المساهمة تعني كل فعل من شأنه أن يؤدي إلى توقيف تشغيله عن طريق إحداث عطب أو خلل يؤثر على تأدية عمله بصورة طبيعية، كأن يجعله بطيئا وذلك بالحد من سرعته.[2]

كما أن فعل الإعاقة يكون الهدف من ورائه منع الحصول على نتائج المعالجة وشل النظام،[1] وذلك بتوقفه عن القيام بوظيفته فترة مؤقتة،[2] ولا يشترط في أن التوقف قد يشمل جميع عناصر النظام المعلوماتي، بل يتحقق أيضا إذ مس جزءا فقط من عناصره.[3]

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150, 000€ d'amende.

[1] فيصل بدري ، مرجع سابق، ص 24.

[2] صالح شنين، مرجع سابق، ص 80.

وحتى يمكننا القول بأن النظام المعلوماتي لشركات المساهمة قد تعرض لفعل الإعاقة حقا، يجب أن تكون قد تمت بدون وجه حق ويمكن أن تكون إيجابية كما يمكن أن تكون عن طريق الإمتناع، من ذلك مثلا كأن يمتنع الجاني عن القيام بفعل يفرضه عليه قانون الشركة بحكم علاقة العمل التي تربطه بها.

أما بالنسبة للوسيلة التي يتم من خلالها تنفيذ فعل الإعاقة فليست هناك وسيلة معينة لذلك، وإنما يمكن أن تتحق بأية وسيلة سواء كانت مادية أو معنوية.

بالنسبة للإعاقة المادية فهي أي عمل يعترض سير النظام المعلوماتي،[4] مثل ذلك أن يقوم الجاني بمنع العاملين على النظام المعلوماتي من الوصول إلى المكان الذي يوجد فيه، أو أي عمل تخريبي آخر كتحطيم الأجهزة أو سكب مادة عليها،[5] وفي هذا السياق يجب التنويه إلى أنه عندما يتعلق الأمر بالإعاقة المادية فإن الأمر لا يطرح أي إشكال كونها مشمولة بالحماية الجنائية ضمن نصوص قانون العقوبات كما سبقت الإشارة إلى ذلك في معرض حديثنا عن محل الجريمة الإلكترونية في شركة المساهمة.

أما الإعاقة المعنوية فما يميزها هو أن الجاني فيها لا يلجأ إلى العنف بل أن كل ما يستخدمه هو تقنيات تدمير ناعمة فقط،[6] ومن بين الأساليب الكفيلة بتحقيقها مثلا إدخال فيروسات على كلمة المرور[7] ، أو عن طريق اللجوء إلى إستخدام برامج مشفرة تسمى بالفيروسات[8]، وتواجه شركات المساهمة خطر الفيروسات التدميرية التي تتسبب في إعاقة نظامها المعلوماتي، ولعل من أشهر القضايا في هذا الموضوع قضية فيروس "ZOTOB".

---

[1] نسمة بطيحي ، مرجع سابق، ص 167.

[2] صورية بوربابة ، قواعد الأمن المعلوماتي –دراسة مقارنة، مرجع سابق، ص 98.

[3] صالح شنين، مرجع سابق، ص 80.

[4] حمزة بن عقون ، مرجع سابق، ص 151.

[5] ناصر حمودي ، مرجع سابق، ص 87.

[6] نسمة بطيحي ، مرجع سابق ص 171.

[7] جمال زين العابدين أمين أحمد، مرجع سابق، ص 119.

[8] دلال لطيف مطشر، مرجع سابق، ص 401.

حيث تتلخص وقائع هذه القضية في قيام طفل مغربي من تطوير هذا الفيروس وإرساله إلى أنظمة معلوماتية خاصة بكبرى الشركات العالمية المتواجدة بأمريكا، الأمر الذي تسبب في عرقلة أنظمتها إذ أصبحت غير قادرة على أداء وظائفها المعتادة فتكبدت جراء ذلك خسائر مالية ضخمة[1].

كما قد تتعرض هذه الشركات إلى إعاقة نظامها المعلوماتي من خلال إغراقه برسائل غير مرغوب فيها، وذلك عن طريق القيام بإرسال كم هائل منها لحواسيب الشركة المستهدفة الشيئ الذي يترتب عليه إمتلاء المساحة المحددة، وبالتالي عدم قدرة الجهاز على إستقبال ذلك الكم الأمر الذي يؤدي إلى توقف الأجهزة عن العمل وإعاقة نظامها المعلوماتي وانقطاع خدماتها،[2] وفي هذا الصدد كان القضاء الفرنسي قد أدان أحد الجناة بتهمة إعاقة خوادم الشركة الضحية لفترة تجاوزت عشرات الساعات وذلك بسبب إرسال 320 ألف رسالة طيلة يوم واحد فقط.[3]

2-فعل الإفساد: يتحقق إفساد النظام المعلوماتي لشركة المساهمة من خلال القيام بأي فعل يجعله غير قادر على الإشتغال بشكل سليم،[4] وبالتالي إعطاء نتائج غير تلك التي كان يجب الحصول عليها،[5] ففعل الإفساد يترتب عليه إعدام النظام وجعله غير صالح للإستعمال بصفة مطلقة كما أنه لا يشترط أن يقع على جميع عناصر النظام المعلوماتي وإنما يكفي إفساد جزء منه فقط.[6]

أما بالنسبة للوسائل التي يتم بواسطتها إفساد النظام المعلوماتي لشركات المساهمة فهي متعددة ومتنوعة مثل الديدان الإلكترونية، حصان طارودة، القنبلة المعلوماتية،[7] أما فيما يتعلق بالتميز بين

---

[1] علا عبد العزيز ، جرائم المس بنظم المعالجة الآلية للمعطيات –دراسة بين النص القانوني والعمل القضائي– بحث نهاية التدريب بالمعهد العالي للقضاء، المملكة المغربية، 2008-2010، ص 39.

[2] عبد اللطيف معتوق ، "مرجع سابق، ص 85.

[3] نسمة بطيحي ، مرجع سابق، ص 175.

[4]شول بن شهرة ،آليات مكافحة الجريمة المعلوماتية مواقع التجارة الإلكترونية نموذجا، مرجع سابق، ص 210.

[5] آمنة أمحمدي بوزينة" الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري دراسة تحليلية لقانوني العقوبات وحقوق المؤلف"، مجلة القانون والمجتمع، مج 3، ع2، الصادر في 2015 ، ص 104.

[6] صالح شنين، مرجع سابق، ص 81.

[7] تم التطرق إلى شرح هذه الوسائل في النقطة المتعلقة بالأساليب المستخدمة في إرتكاب الجرائم الإلكترونية على شركات المساهمة. راجع الصفحة 128.

فعل الإعاقة وفعل الإفساد فمن الصعب التميز بينهما باعتبار أن كلاهما يؤثر على النظام المعلوماتي لشركة المساهمة ويحدث فيه تغييرات وإن كانت متفاوتة في الدرجة، غير أن فعل الإعاقة يمكن إصلاح النظام المعلوماتي بعده في حين فعل الإفساد يعدم صلاحيته.

لكن ما ينبغي الإشارة إليه هو أنه رغم خطورة هذه الجريمة على النظام المعلوماتي لشركات المساهمة نظرا للأضرار التي يلحقها بها إلا أن المشرع الجزائري لم ينص عليها كجريمة مقصودة مستقلة، وإنما جعل منها مجرد ظرف مشدد على فعل الدخول أو البقاء غشا في النظام المعلوماتي مما يعني أن المساس به يقع بصفة عرضية ودون قصد، الأمر الذي يجعلنا نتساءل ماذا لو حدث المساس بالنظام المعلوماتي بصفة مقصودة أو كان نتيجة دخول مشروع فهل يفلت الجاني في هذه الحالة من العقاب ولا يمكن تطبيق الفقرة 3 من المادة 394 مكرر؟

إن كان هناك من يرى بأن المشرع الجزائري لم ينص عليها بصفة مستقلة كونها تتداخل وتتشابه إلى حد كبير مع جريمة التلاعب بمعطيات النظام المعلوماتي،[1] التي سنتناولها فيما بعد وبالتالي تفعيل أحكام المادة 394 مكرر 1 على هذه الجريمة، غير أننا نرى وإن كان هناك تشابه لكن ليس لدرجة تطبيق نفس المادة على نفس الجريمتين.

وبدورنا نؤيد الرأي الذي يذهب إلى القول بضرورة الفصل بين الجريمتين وذلك لإعتبارات عملية، فأحيانا يكون هناك إتلاف لمعطيات النظام المعلوماتي للشركة من خلال عملية الإدخال، التعديل أو المحو ولكن ذلك لا يؤدي إلى المساس بالسير العادي للنظام، وبخلاف ذلك يحدث أحيانا أن يتعرض النظام المعلوماتي إلى الإعاقة دون أن يترتب على ذلك إتلاف لمعطياته.[2]

لذلك نرى بأن المادة 394 مكرر 1 تتسم بالقصور ولا تتسع لإحتواء جريمة الإعتداء على سير النظام المعلوماتي، لذلك نرى بأنه من الضرورة النص على تجريم هذا الإعتداء خاصة عندما يتعلق

[1] بثينة حبيباتي ، مرجع سابق، ص 52.

[2] فايز محمد راجح غلاب، مرجع سابق، ص 241.

الأمر بنظام معلوماتي لشركة مساهمة التي تمثل الكيان الاقتصادي للدول فإعاقة سير نظامها المعلوماتي قد يكلف الدول خسائر إقتصادية بالغة.

ثانيا: الركن المعنوي:

تعد جريمة الإعتداء على سير النظام المعلوماتي لشركة المساهمة من خلال إعاقته أو إفساده من الجرائم العمدية، إذ يتطلب قيامها تحقق كل من الركن المادي والمعنوي.

إذ يجب أن يكون الجاني مدركا بأن أفعاله التي يقوم بها من شأنها تعطيل النظام المعلوماتي للشركة وبالتالي الإنتقاص من قيمته، الأمر الذي يؤدي إلى عدم صلاحيته[1]، ولكن رغم ذلك تتجه إرادته إلى إعاقة هذا النظام أو إفساده وذلك دون علم ورضا صاحب الشركة،[2] لذلك فإذا حدث عرقلة سير هذا النظام نتيجة خطأ ما فلا يتحقق قيام هذه الجريمة.

كذلك أن تحدث عرقلة النظام لسبب مشروع من ذلك مثلا الحالة التي يتم فيها إرسال رسائل بعدد ضخم إلى الشركة دون طلب منها كما في حالة الإشهار التجاري.[3]

الفرع الثاني:

جريمة الإعتداء على معطيات شركات المساهمة.

إمتدت الجرائم التي تستهدف شركة المساهمة لتمس أيضا بمعطياتها سواء كانت تلك المعطيات مخزنة داخل نظامها المعلوماتي عن طريق التلاعب فيها وإتلافها أو كانت خارجه من خلال إستغلالها والتعامل فيها بطريقة غير مشروعة .

أولا: جريمة التلاعب بمعطيات شركات المساهمة.

تم النص على هذه الجريمة من خلال المادة 394 مكرر 1 من القانون رقم 24-06 المعدل والمتمم لقانون العقوبات والتي جاء فيها" يعاقب بالحبس من سنة (1) أشهر إلى ثلاث (3) سنوات وبغرامة من 500,000 دج إلى 2,000,000 دج كل من أدخل بطريق الغش معطيات في نظام

---

[1] فايز محمد راجح غلاب، مرجع سابق ، ص 246.

[2] كمال حطاب، "الحماية الجزائية للتجارة الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، 2015-2016)، ص 86.

[3] نسمة بطيحي ، مرجع سابق، 184.

المعالجة الآلية أو أزال أو عدل بطريق بطريق الغش المعطيات التي يتضمنها" وتقابلها في قانون العقوبات الفرنسي المادة 323-3،[1] كما تم النص عليها كذلك ضمن إتفاقية بودابست ،[2] وكذا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.[3]

فما يستشف من نص المادة التي جاء بها المشرع الجزائري أنها جاءت شاملة لجميع أنواع المعطيات سواء كانت معلومات معالجة أو برامج، إلا أنه يخرج من دائرتها تلك المعطيات التي تتواجد خارج النظام المعلوماتي.

وبطبيعة الحال حتى يكتمل تحقق هذه الجريمة في إطار شركة المساهمة لا بد من قيام ركنيها المادي والمعنوي واللذان نوضحهما فيما يلي.

1-الركن المادي: حيث يتحقق فيه السلوك الإجرامي للجاني من خلال ثلاثة أفعال والمحددة في المادة 394 مكرر 1.

أ-إدخال معطيات إلى النظام المعلوماتي لشركة المساهمة: ويقصد بهذا الفعل بأن يتم إضافة معطيات حديدة على الدعامة الخاصة بالنظام المعلوماتي للشركة إذ يستوي في ذلك أن تكون تلك الدعامة خالية أو بها معطيات سابقة،[4] وتعتبر عملية إدراج معطيات غير معتمدة من ذي قبل في نظامها المعلوماتي من أكثر الأساليب شيوعا.[5]

---

[1] Art: 323-3, modifié par loi N^0 2015-912 du 24 juillet 2015, art 4, op, cit.
Le fait d'introduire frauduleusement des données dans un systéme de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150,000€ d'amende.

[2] المادة 4 من إتفاقية بودابست –التدخل في البيانات–

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما أرتكب عمدا إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها؛

يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

[3] المادة 8 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات –الإعتداء على سلامة البيانات

تدمير أو محو أو إعاقة أو تعديل أو حججب بيانات تقنية المعلومات قصدا وبدون وجه حق؛

للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة أن تتسبب بضرر جسيم.

[4] السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، ط 1، الإسكندرية، مكتبة الوفاء القانونية، ، 2018 ، ص 372.

[5] يزيد بوحليط، مرجع سابق، ص 133.

وفعل الإدخال يشمل جميع المعطيات سواء كانت صحيحة أو غير صحيحة،[1] كما يتحقق هذا الفعل أيضا من خلال عملية إدخال برامج غريبة يترتب عليها إضافة معطيات جديدة،[2] ومن بين الجرائم التي تم فيها إدانة مرتكبيها بسبب فعل الإدخال قضية "ميشال طومسون" " MICHAL THOMPSON" والتي تتلخص وقائعها في قيام هذا الشخص والذي كان يشغل منصب خبير في بنك الكويت التجاري، بإدخال برنامج يقوم بعملية التحويل وأثناء تواجده على الطائرة متجها إلى لندن بعد تركه لعمله في البنك، قام النظام بتحويل أموال من أرصدة المستثمرين بفروع البنك الكويتي إلى حساب آخر فتحه باسمه، وبعد وصوله إلى لندن قام بتحويل تلك الأموال من رصيده في البنك السابق إلى بنك آخر في لندن، وبعد إكتشاف أمره تمت محاكمته بتهمة إدخال بيانات إلى نظام المعالجة الآلية للمعطيات بخمسة عشر شهرا حبسا.[3]

كذلك ما تعرض له القضاء الفرنسي في قضية إدانة الجاني الذي كان موظف في شركة تجارية بعد أن قام بإدخال بعض المعلومات غير صحيحة تتعلق بنسب ضريبة المبيعات (TVA) إلى النظام المعلوماتي للشركة وتمت إدانته بتهمة إدخال معطيات إلى نظامها،[4] فما نلاحظه هو أن فعل الإدخال يرتكب من قبل الأشخاص الذين تكون لهم علاقة بشركات المساهمة كالموظفين فيها أو المسؤولين عن القسم المعلوماتي فيها باعتبار أن هؤلاء الأشخاص يكونون في وضع يؤهلهم لإرتكاب فعل الإدخال.

ب-إزالة معطيات من النظام المعلوماتي لشركات المساهمة: وتتحقق هذه الجريمة عن طريق محو المعطيات الموجودة في النظام المعلوماتي للشركة وذلك بإزالتها بصفة كلية أو جزئية،[5] كما يشمل هذا الفعل أيضا عملية تخزين أو نقل المعطيات إلى المنطقة الخاصة بالذاكرة، أي إخفائها دون أن

---

[1] نجاة عباوي ، مرجع سابق، ص 287.

[2] عبد الحليم بن بادة، محمد سعد بوحادة، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة –دراسة سياسية قانونية، مرجع سابق، ص 16.

[3] فايز محمد راجح غلاب، مرجع سابق، ص 213.

[4] نسمة بطيحي ، مرجع سابق، ص 120.

[5] شول بن شهرة ، آليات مكافحة الجريمة المعلوماتية مواقع التجارة الإلكترونية نموذجا، مرجع سابق، ص 213.

يتم محوها أي أنه يتم حجبها وبالتالي حرمان الشركة منها،[1] والإزالة تعني كذلك إقتطاع أجزاء تكون مسجلة على دعامة ممغنطة من خلال عملية محوها أو طمسها، أي يتم ضغط أجزاء جديدة فوقها وهذا مفاده أن الأجزاء الجديدة تقوم بطمس الأجزاء القديمة،[2] ويفترض أن عملية الإزالة تكون لاحقة لعملية الإدخال.

ومن بين القضايا في هذا الشأن قضية شركة " TRW COMPANY CREDIT DATA" حيث كان لها مجموعة من العملاء (بنوك، شركات، متاجر)، وعن طريق نظامها المعلوماتي حيث كانت تعمل على تزويدهم بالمعلومات الخاصة بالمراكز الإئتمانية لأفراد الجمهور وذلك مقابل نسبة من الإشتراك يدفعها العملاء، وكانت هذه الشركة تحوز على معلومات تتعلق بما يقارب 50 مليون شخص، فحدث أن قام أحد موظفي الشركة ببيع مراكز إئتمانية جديدة لأصحاب المراكز الإئتمانية الضعيفة وذلك عن طريق محو البيانات المتعلقة بهم واستبدالها ببيانات جديدة تحسن من مركزهم.[3]

ت–تعديل معطيات النظام المعلوماتي لشركة المساهمة: ويعني إستبدال المعطيات الموجودة داخل النظام النظام بمعطيات أخرى جديدة ،[4] كما يعني أيضا هذا الفعل التغيير في المعطيات سواء كان تغييرا كليا أو جزئيا الأمر الذي يترتب عليه تغيير المعنى،[5] ويشمل التعديل التلاعب في البرنامج من خلال عملية تزويده بمعطيات مختلفة يترتب عليها تحقيق نتائج مغايرة تماما لتلك التي تم تصميم البرنامج لأجل تحقيقها،[6] حيث يتم إرتكابه عن طريق المصيدة

---

[1] عبد الحليم بن بادة، محمد سعد بوحادة، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة –دراسة سياسية قانونية– مرجع سابق، ص ص 16،17.

[2] بثينة حبيباتني ، مرجع سابق، ص 57.

[3] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات –دراسة مقارنة، مرجع سابق، ص 196.

[4] محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها –دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، مرجع سابق، ص 449.

[5] إسمهان عون، (أركان جريمة الإتلاف المعلوماتي وعقوباتها –دراسة مقارنة–)، مجلة الدراسات الإفريقية وحوض النيل، ع 13، مج 4، الصادر في أكتوبر 2021، ص 363.

[6] شول بن شهرة ، آليات مكافحة الجريمة المعلوماتية مواقع التجارة الإلكترونية نموذجا، مرجع سابق، ص 214.

أو المنافذ المميزة والتي تعتبر ممرات خالية يسهل الولوج عبرها قصد التوصل إلى الشفرات والتعليمات.[1]

وقد أثيرت بشأن تعديل المعطيات قضية في أحد البنوك والتي قام فيها مسؤول النظام المعلوماتي بإضافة زيادة مالية إلى حسابات بعض أصدقائه وذلك وفق برنامج مساعد، وبعد أن يقوم المعنيين بسحب أموالهم يعمد الجاني إلى تمزيق إيصالات السحب، حيث أجبر على الإستمرار في هذه الزيادة من طرف أصدقائه إلى أن تم إكتشاف جريمته نتيجة حلول موعد المراجعة الدورية، وذلك عن طريق نظام أمن سري موجود في أحد الفروع التابعة للبنك، حيث كان يقوم بتسجيل كل العمليات على الحاسوب والجاني لم يكن لديه أي علم عن ذلك النظام الأمني.[2]

ومن خلال التطرق إلى الركن المادي لجريمة الإعتداء على معطيات شركات المساهمة يتضح لنا بأن الأفعال التي تشكل هذه الجريمة قد ذكرها المشرع الجزائري بصفة حصرية لا على سبيل المثال، وبالتالي فإذا ما تعرضت معطيات هذه الشركة إلى أي فعل آخر غير هذه الأفعال كنسخ معطياتها مثلا فإنها لا تندرج ضمن هذه الجريمة.

وما يجب التنويه إليه هو أنه من الصعب الفصل بين فعل التعديل، الإدخال وإزالة المعطيات، فحتى يتم تعديل معطيات ما لا بد من القيام بفل الإضافة أو الإزالة،[3] فرغم أن المشرع لم يشترط ضرورة إرتكابهم جميعا حتى يتحقق قيام الجريمة إلا أنهم قد يجتمعون في الجريمة الواحدة، ففي القضية التي قام فيها المدعو "و.خليل" من مواليد 1989 المنحدر من ولاية باتنة باختراق أكبر الشركات بالجزائر "ALGERIE TELECOM" في نظامها المعلوماتي خلال الفترة الممتدة من شهر جوان إلى نوفمبر 2017، حيث تمكن من تحميل جميع المعطيات وكذا ملفات الفوترة الخاصة بزبائن ومتعاملي الشركة، وكذا الدخول إلى الذاكرة المركزية لها وتغيير وتعديل وإضافة برامج ضارة

---

[1] بسمة مامن، (جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري)، مجلة الحقوق والعلوم السياسية، ع 1، مج 9، الصادر في 2022، ص 485.

[2] نسمة بطيحي ، مرجع سابق، ص 124.

[3] IBTISSEM MAALAOUI, "Les infraction portant atteinte à la sécurité du systéme informatique d'une entreprise", (mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit (L.L.M) option droit des affaires, université de montréal, septembre 2011), P 74.

تمكن من خلالها من تعطيل الشبكة على المستوى الوطني، وقد إعترف بذلك خلال رده على أسئلة العدالة وقد إلتمس ممثل الحق العام توقيع عقوبة 3 سنوات حبسا نافذا ضده مع 3 ملايين دينار جزائري غرامة نافذة.[1]

كذلك ما لاحظناه أن النتيجة المترتبة عن هذه الجريمة يمكن إعتبارها نفس الجريمة المترتبة عن الدخول أو البقاء غشا في النظام المعلوماتي لشركات المساهمة باعتبار أن كلاهما يغير من طبيعة معطيات هذه الشركة عما كانت عليه في السابق وإتلافها، غير أن الإختلاف الموجود بينهما هو الإتلاف الذي يلحق المعطيات في الجريمة الأولى يكون بعد أن يتم الدخول أو البقاء بطريق الغش وتحدث النتيجة بصفة عرضية غير عمدية، أما النتيجة في هذه الجريمة فيتم إرتكابها بصفة مقصودة سواء كان الدخول أو البقاء مصرح بهما أو عن طريق الغش.

فالإتلاف الذي يعتبر مجرد ظرف مشدد في الجريمة يختلف عن الإتلاف الذي يعد ركنا فيها، فالركن يعد من عناصر الجريمة ولا قيام لها دونه أما الظرف فهو عنصر إضافي لا أكثر، قد يتحقق وقد لا يتحقق فقط عملية تحققه تؤثر على جسامة الجريمة.[2]

2-الركن المعنوي: من خلال صياغة نص المادة 394 مكرر 1"كل من أدخل بطريق الغش...أو أزال أو عدل" يتضح بأن هذه الجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة.

بالنسبة لعنصر العلم يعني أن الجاني يقدم على إرتكاب الجريمة بأحد الأفعال المذكورة سابقا وهو يعلم أنه ليس له الحق نهائيا سواء في إدخال بيانات جديدة أو حذفها أو تعديلها،[3] بمعنى يكون مدركا بأن أفعاله تشكل إعتداء على معطيات الشركة والتي تعد وحدها صاحبة الحق في التصرف فيها، لذلك لا يتحقق قيام هذه الجريمة إذا ما أقدم الشخص على إدخال أو تعديل

---

[1] جميلة. ق، قمت بقرصنة أنظمة إتصالات الجزائر للتنبيه على وجود ثغرات خطيرة، مقال منشور على صفحة النهار Online، 06 ديسمبر 2017، أطلع عليه بتاريخ: 10 مارس 2023، متاح على الرابط: https://www.ennaharonline.com

[2] محمد حماد مرهج الهيتي، (مدى تطبيق نصوص جرائم الإتلاف والتخريب على الإتلاف الذي يتعرض له الحاسب الآلي – دراسة في نطاق التشريع البحريني والمقارن–)، مجلة الحقوق، د،ع، مج 6، الصادر في 2009، ص 181.

[3] IBTISSEM MAALAOUI, op-cit, p 74.

أو إزالة معطيات تابعة له،[1] كأن يقوم بهذه الأفعال مدير الشركة الذي له حق التصرف في تلك المعطيات،

إضافة إلى علم الجاني بعدم مشروعية سلوكه يجب أن تتجه إرادته إلى إرتكاب تلك الأفعال التي يقوم عليها سلوكه الإجرامي وليس بالضرورة أن تكون إرادته قاطعة في إحداث تغيير بتلك المعطيات وإنما يكفي تقبله لتلك النتيجة،[2] وفي هذه الجريمة لا يشترط الباعث الذي من أجله إتجهت إرادة الجاني إلى إرتكاب تلك الأفعال ضد معطيات الشركة سواء كان ذلك بدافع الإنتقام من صاحبها أو بدافع الربح وغيرها من البواعث.

أما بالنسبة للقصد الجنائي الخاص فلا نلمحه من خلال نص المادة 394 مكرر 1 وعبارة "بطريق الغش" الواردة فيها لا تدل سوى على أن الجريمة عمدية لا أكثر، لذلك فإن القصد الخاص غير مطلوب فيها كون أن المشرع لم يشترط نية الإضرار بالغير، وإن كان تحققه وارد وذلكنتيجة للسلوك الإدرامي غير أنه لا يعد من عناصر الجريمة.[3]

ثانيا: جريمة التعامل غير المشروع في معطيات شركات المساهمة.

إضافة إلى الجرائم السابقة التي تستهدف شركة المساهمة قد تتعرض هذه الشركة أيضا إلى مجموعة من الأفعال منها ما يسبق إرتكاب تلك الجرائم ومنها ما يعد لا حقا لها ليتم من خلالها التعامل في تلك المعطيات بصفة غير مشروعة، وسواء كانت في أقراص أو أشرطة أو قد تمت معالجتها بطريقة آلية أو قد تم إرسالها من نظام إلى آخر، إذ ليس بالضرورة أن تكون موجودة داخل النظام المعلوماتي فقد تكون في شكل منفصل عنه أي موجودة خارجه،[4] وحتى تحظى هذه المعطيات بالحماية فقد تم تجريم الأفعال المشكلة لهذه الجريمة نظرا لخطورتها.

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص 220.

[2] بثينة حبيباتني ، مرجع سابق، ص ص 62،63.

[3] كمال حطاب ، مرجع سابق، ص 91.

[4] أمال حابت ، "التجارة الإلكترونية في الجزائر"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2015)، ص 394.

فنجد بأن المشرع الجزائري قي نص في المادة 394 مكرر 2 على أنه " يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 1,000.000دج إلى 5,000,000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

وتقابلها المادة 323-3-1 في قانون العقوبات الفرنسي[1]، كما نجد إتفاقية بودابست قد جرمته في مادتها السادسة مجموعة من الأفعال،[2] وكذا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في

---

[1] Art: 323-3-1 modifié par loi N^0 2013-1168 du 18 décembre 2013, art 25,op,cit.
Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infraction prévues par les articles 323-1 à 323-3 puni des peines prévues respectivement pour l'infraction elle –même ou pour l'infraction la plus sévèrement réprimée.

[2] المادة 6 إساءة إستخدام الأجهزة،

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما أرتكبت عمدا وبغير حق:

أ.عملية إنتاج، بيع، شراء بغرض الإستخدام، إستيراد، توزيع أو إتاحة بأي طرق أخرى:

1.جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض إرتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛

2.كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض إرتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛

ب.حيازة إحدى المواد المشار إليها في الفقرة أ (1) أو (2) أعلاه، بغرض إرتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5، ويجوز للدولة الطرف أن تشترط بموجب القانون أن تكون حيازة عدد من هذه المواد سابقة لإلحاق المسؤولية الجنائية.

2.لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع، الشراء بغرض الإستخدام ، الإستيراد، التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها بالفقرة 1 من هذه المادة ليس الغرض منها إرتكاب جريمة من الجرائم المنصوص عليها في المواد من 2 إلى 5 من هذه الإتفاقية، بل بالأحرى للإستخدام المرخص لغرض إختيار أو حماية تظام الكمبيوتر.

3.يجوز لكل دولة طرف الإحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقا بعمليات بيع، توزيع أو إتاحة هذه المواد المشار إليها في الفقرة 1-أ (2) من هذه المادة.

المادة التاسعة منها[1]، ورغم أن هذه الأفعال منفصلة عن باقي الجرائم التي تمس شركات المساهمة في نظامها المعلوماتي والتي سبق توضيحها، إلا أنها لا تعد اقل خطورة أو أقل ضررا منها، نتيجة لما تتعرض له هذه الشركة جراء هذه الأفعال.

لذلك فالعبرة من تجريم التعامل غير المشروع في المعطيات هو أن هذه التعاملات تعتبر من قبيل جرائم الخطر وبالتالي تفادي ما قد ينجر عنها من أضرار فالهدف من تجريمها وقائي، وكذا القضاء من الآثار المترتبة عن الجرائم السابقة والتخفيف من حدتها في حالة ما إذا تعرضت شركات المساهمة لمثل هذه الأفعال،[2] وانطلاقا من كل هذا فإن هذه الجريمة كغيرها من الجرائم التي سبقتها إذ يتطلب الأمر لقيامها تحقق ركنيها المادي والمعنوي.

1-الركن المادي: من خلال ما ورد في المادة 394 مكرر 2 فإنه يتخذ صورتين باعتباره تضمن مجموعتين من الأفعال، المجموعة الأولى تكون سابقة للجرائم المذكورة آنفا وتساعد على إرتكابها في حين المجموعة الثانية تكون لاحقة لتلك الجرائم.

أ-التعامل غير المشروع في معطيات شركة المساهمة تصلح لإرتكاب إحدى الجرائم السابقة ضدها: هذه الصورة تمنتها الفقرة الأولى من المادة 394 مكرر2 والتي تنحصر أفعالها في :

-فعل التصميم: ويتم القيام به من طرف المختصون كالمبرمجين ومصممي البرامج[3]، حيث يقوم هؤلاء بتصميم برامج تمكنهم وتسهل عليهم الوصول إلى النظام المعلوماتي لشركة المساهمة، ومن خلال هذه البرامج يتم فك كلمات السر وشفرات الوصول الخاصة بنظامها.

ومن المصطلحات المرادفة لفعل التصميم نجد الإصطناع، التقليد، والإستنساخ،[4] فشركات المساهمة كثيرا ما تتعرض لمثل هذه الأفعال كتصميم مواقع وهمية تكون مشابهة لمواقعها الأصلية،

---

[1] محمد بن أحمد، مرجع سابق، ص 294.

[2] المرجع نفسه، ص 294.

[3] عبد الوهاب ملياني ، مرجع سابق، ص 197.

[4] الإصطناع: يعني إنشاء شيئ بحيث يعتقد كل من يطلع عليه أنه فعلا حقيقي وأنه صدر فعلا من صاحبه الحقيقي.

التقليد: هو إنشاء برامج تكون مشابهة تماما لبرامج أخرى صحيحة وتكون تابعة لنظام آخر.

الإستنساخ: ويعني إجراء نسخة تكون مطابقة للأصل أي نقل الملفات المخزنة في أية وسيلة تخزين سواء كانت أقراص صلبة أو مرتة...إلخ إلى جهاز آخر (محمد بن أحمد ، مرجع سابق، ص 299).

ومثالا على ذلك ما قضت به محكمة عنابة في حكمها رقم 10-05637 الصادر في 2010/06/28 ضد المتهم (ف.محمد) والذي قام بتصميم موقع مشابه بالموقع الرسمي لأحد البنوك وعندما قام زبائن ذلك البنك ببعض العمليات المصرفية بحساباتهم وجدوا أنفسهم في الموقع الخطأ للبنك الذي قام بتصميمه المتهم ما ترتب عنه إعطاء الأرقام السرية الخاصة بحساباتهم لمجهولين دون أن يدركوا ذلك.[1]

-فعل البحث: ويعني هنا البحث في الكيفية التي يتم بها خلق معطيات،[2] تمكن صاحبها من إرتكاب إحدى الجرائم التي سبق ذكرها ضد شركات المساهمة، فنجد بأن الجناة خلال عملية بحثهم عن كلمات المرور أو الشفرات الخاصة بشركات المساهمة يلجئون إلى نشر إعلانات عبر صفحات الأنترنت حيث يعرضون قدرتهم في الوصول إليها كما يعرضون على بعضهم إقتراح تبادل كلمات المرور.[3]

-فعل التجميع: وهو أن يتم تجميع العديد من المعطيات التي تتعلق بشركة المساهمة والتي تسهل من عملية إرتكاب إحدى الجرائم السابق ذكرها،[4] وتكون تلك المعلومات على درجة بالغة من الأهمية ومن ذلك مثلا تجميع برامج تمكن من تجاوز إجراءات الحماية الأمنية[5] ، الذي تعتمده هذه الشركة لحماية نظامها المعلوماتي، وتكمن خطورة هذا الفعل بالنسبة لها في الكم الهائل من المعلومات التي يتم تجميعها عنها وما إستعمال المشرع لمصطلح التجميع بصيغة الجمع إلا من أجل الرفع من درجة خطورة هذا الفعل.

---

[1] عبد الحليم بوقرين ، "الحماية الجنائية للمعاملات التجارية"، مرجع سابق، ص ص 146،147.

[2] بثينة حبيباتني ، مرجع سابق، ص 67.

[3] نسمة بطيحي ، مرجع سابق، ص 149.

[4] مراد يرمش ، مرجع سابق، ص 101.

[5] رشيدة بوكر، "الحماية الجزائية للتعاملات الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، 2017)، ص 56.

-فعل التوفير: ويعني الوضع تحت التصرف من خلال تقديم مجموعة من المعطيات وإتحاتها لمن يريدها،[1] ففي هذه الشركات كأن يتم منح شفرات الولوج إلى نظامها المعلوماتي إلى غيرها من الشركات المنافسة من أجل الإطلاع على معطياتها تمنافستها.

-فعل النشر: ويعني إذاعة المعطيات قصد تمكين الغير من الإطلاع عليها وذلك بأية وسيلة من وسائل النشر،[2] ولعل هذا الفعل يعتبر من أخطر الأفعال التي يمكن أن ترتكب بحق هذه الشركة قبل إرتكاب أية جريمة أخرى عليها، كونه يمكن من الإطلاع على معلوماتها لدى أكبر عدد ممكن من الأشخاص ويمكن أن يتم ذلك خلال ظرف وجيز جدا، ففعل النشر هو إنتهاك صارخ لسرية معلومات الشركة كأن يتم نشر كلمة السر الخاصة بأحد حوسيبها.

وقد ورد في منطوق حكم رقم 10-05272 الصادر في 2010/06/01 عن محكمة باتنة والذي جاء فيه" حيث أن نشر المعطيات الآلية المتحصل عليها من قبل المتهم والخاصة بمختلف الشركات ثابت بحقه باعترافه وإرساله تلك المعطيات إلى أحد القراصنة ووعده بعدم نشر صورة الشركة الأمريكية"[3]

-فعل الإتجار: وهو أن يتم تقديم المعطيات الخاصة بهذه الشركة إلى الغير نظير مقابل ولا يهم إن كان نقديا أو عينيا، أو أن يكون مجرد خدمات،[4] كأن يتم المتاجرة بشفرات الولوج إلى النظام المعلوماتي.

ومن خلال تجريم هذه المجموعة من الأفعال يكون بذلك المشرع الجزائري قد أوصد جميع الأبواب التي يمكن من خلالها التعامل بطريقة غير شرعية في معطيات هذه الشركة، والتي تمكن الجناة من إرتكاب عدة جرائم أخرى ضدها.

ب-التعامل غير المشروع في معطيات شركة المساهمة محصلة من إحدى الجرائم السابقة: وهي الصورة الثانية لجريمة التعامل غير المشروع في معطيات شركات المساهمة، حيث أن تعرض هذه

---

[1] عزيزة رابحي ، مرجع سابق، ص 171.

[2] نسيمة جدي ، مرجع سابق، ص 73.

[3] عبد الحليم بوقرين ، مرجع سابق، ص 147.

[4] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات -دراسة مقارنة، مرجع سابق، ص 216.

الشركة إلى مختلف الجرائم التي ترتكب ضد نظامها المعلوماتي ينتج عنه حصول الجناة على معطيات تخصها، الأمر الذي يشكل خطرا وتهديدا لها إذا ما تم التعامل فيها بموجب أفعال لاحقة لتلك الجرائم كونها معطيات سرية وقد تم الحصول عليها بطريقة غير شرعية، والمشرع الجزائري كان حريصا على منع التعامل في هذه المعطيات من خلال تجريمه لمجموعة من الأفعال والتي حددها في الفقرة الثانية من المادة 394 مكرر 2 على سبيل الحصر والمتمثلة في كل من فعل الحيازة، الإفشاء، النشر، الإستعمال وسنقوم بتوضيح خطورتها على شركة المساهمة كما يلي:

-حيازة المعطيات: حيث أن حيازة،[1] معطيات شركات المساهمة يلحق بها أضرارا خاصة وأنه يكون بإمكان الجاني السيطرة وأن يمارس عليها أي عمل كاستغلاله لها وانتفاعه بها، وتزداد خطورتها عندما تكون بين الشركات المتنافسة وتتحصل إحداها على معطيات شركة أخرى، كما يكون بإمكان الجاني إدخال تعديلات أو حتى إفنائها أو نقلها لجهات أخرى.

-إفشاء المعطيات: المقصود بالإفشاء في هذه الجريمة هو أن يتم نقل معطيات الشركة من حيازة الجاني الذي تحصل عليها بطريقة غير مشروعة إلى غيره من الأشخاص، وطبيعي أن يصدر منه هذا الفعل كونه لا يعد مؤتمنا عليها كما أنه غير ملزم بكتمانها،[2] فتتم إشاعتها ويترتب عن ذلك خروج تلك المعطيات من حيز الكتمان والسرية.

وبطبيعة الحال أن تعرض شركات المساهمة إلى إفشاء معطياتها له ماله من الأضرار عليها، فالمعطيات ذات الطابع الصناعي والتجاري تعد جزءا من رأسمالها والتكتم عليها يعد حماية لها من خطر المنافسة، ومن بين الأسرار التجارية نذكر الخلطة السرية لدجاج " كينتاكي"[3] فإفشاء هذه الأسرار قد يقضي على موقع الشركة في السوق.

---

[1] الحيازة وفقا للقانون الجنائي تعني بأن يسيطر شخص على مال منقول وتكون تلك السيطرة بنية التملك والإحتباس، وله أن يمارس أي عمل على المنقول دون رقابة من الشخص صاحب السلطة، وهي ليست حق وإنما مركز واقعي وتكون مشروعة من خلال إستنادها على سبب صحيح كما قد تكون غير مشروعة، أنظر عبد الوهاب ملياني، مرجع سابق، ص 200.

[2] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات دراسة مقارنة، مرجع سابق، ص 219.

[3] نسمة بطيحي ، مرجع سابق، ص 156.

-نشر المعطيات: يعد النشر الفعل الوحيد الذي تكرر ذكره في الفقرتين الأولى والثانية من المادة 394 مكرر 2، إذ يعتبر فعل مشترك بين صورتي جريمة التلاعب غير المشروع في معطيات الشركة وهذا إن دل على شيئ فإنما يدل على مدى خطورته، حيث يعني هذا الفعل إذاعة المعطيات وإطلاع الغير عليها وهو يقترب من فعل الإفشاء غير أنه يعتبر أشد خطورة وضررا منه باعتبار أن الأول يتم فيه إفشاء المعلومة لعدد محدد من الأشخاص أما النشر فيعني إذاعتها بين أكبر عدد ممكن من الأشخاص، أما بالنسبة للوسيلة التي يتم بها فلم يحددها المشرع الجزائري سواء تمت بوسائل تقليدية أو إلكترونية ، كما أنه لم يحدد إذا ما كان هذا الفعل يتم بمقابل أم لا.

-إستعمال المعطيات: والمقصود بهذا الفعل هو أن يتم توظيف معطيات الشركة التي يتم التحصل عليها بطريقة غير مشروعة من خلال إرتكاب إحدى الجرائم عليها، حيث يتحقق هذا الفعل مهما كان الغرض من توظيف واستعمال تلك المعطيات وبأية كيفية كانت،[1] كأن تقدم شركة على إستعمال المعطيات الخاصة بإحدى الشركات الأخرى المنافسة لها بعدما تحصلت عليها بطريقة غير مشروعة وذلك قصد الإضرار بها.[2]

وفي إعتقادنا بأن تجريم هذه الأفعال بعد تعرض شركة المساهمة لإحدى الجرائم الماسة بمعطياتها ما هو إلا من أجل التخفيف من حدة الأضرار التي تكون قد تعرضت لها، ووضع حد للتصرفات التي تمس تلك المعطيات بعد أن يتم الحصول عليها بطريقة غير مشروعة.

2-الركن المعنوي:

نجد بأنه قد ورد تفي المادة 394 مكرر 2 عبارة "عمدا" و "عن طريق الغش" ما يفيد بأن جريمة التعامل غير المشروع في معطيات هذه الشركة هي جريمة عمدية مقصودة، يتطلب قيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة لدى مرتكبها.

---

[1] عبد الحليم بن بادة، محمد سعد بوحادة، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة -دراسة سياسية قانونية- مرجع سابق، ص 20.

[2] نسمة بطيحي ، مرجع سابق، ص 157.

فالعلم يقتضي أن الجاني يكون مدركا تماما لحقيقة نشاطه الإجرامي وأن الأفعال التي يقوم بها من تصميم أو بحث أو تجميع أو توفير، أو نشر أو إتجار فيها خطورة على هذه الشركة،[1] باعتبار أنها تؤدي إرتكاب جرائم ضد سلامة معطياتها، وإلى جانب ذلك أن يكون على علم بأن المعطيات التي يتعامل بها تخص تلك الشركة وتم الحصول عليها عن طريق إحدى الجرائم السابقة،[2] وبالتالي تعامله بها يضاعف من حدة الأضرار التي تكون قد تعرضت لها الشركة.

أما بالنسبة لعنصر الإرادة فلا يكفي أن يكون الجاني عالما بحقيقة أفعاله وإنما لا بد من إنصراف إرادته إلى تحقيقها وتجسيدها، وباعتبار أن جريمة التعامل غير المشروع في معطيات شركات المساهمة جريمة شكلية لا تتطلب تحقق نتيجة معينة فإن إرادة الجاني تكون منصبة فقط على نشاطه ولا تتعدى إلى تحقيق النتيجة،هذا بالنسبة للقصد الجنائي العام فماذا عن القصد الجنائي الخاص في هذه الجريمة؟

بالنسبة لجريمة التعامل في معطيات تصلح لإرتكاب الجريمة يتضح من خلال الفقرة الأولى من المادة 394 مكرر 2 أن المشرع لم ينص صراحة على ضرورة توفر القصد الجنائي الخاص، إلا أنه لا بد من توفره في هذه الصورة وذلك باتجاه إرادة الجاني في التعامل بهذه المعطيات إلى الإعداد والتمهيد من أجل إستعمالها في إرتكاب أحد الجرائم التي تمس بالنظام المعلوماتي للشركة،[3] بمعنى أن هذه الجريمة تنتفي إذا ما تم إستعمال تلك المعطيات في أغراض أخرى مشروعة كالحماية مثلا من خطر الجرائم.[4]

على خلاف ذلك فإن الصورة الثانية والمتمثلة في جريمة التعامل في معطيات محصلة من جريمة فيكفي فيها القصد الجنائي العام، باعتبار أن تلك المعطيات هي في الأساس متحصل عليها بطريقة غير مشروعة أي من خلال جريمة، وبالتالي علم الجاني بطبيعة تلك المعطيات ينفي عنه القصد الجنائي الخاص.

---

[1] محمد بن أحمد ، مرجع سابق، ص 318.

[2] بثينة حبيباتني ، مرجع سابق، ص 77.

[3] رشيدة بوكر ، الحماية الجزائية للتعاملات الإلكترونية، مرجع سابق، ص 60.

[4] بثينة حبيباتني ، مرجع سابق، ص 78.

الفصل الثاني:

القواعد الإجرائية والأمنية للجرائم الإلكترونية الواقعة على شركات المساهمة.

الفصل الثاني:
القواعد الإجرائية والأمنية للجرائم الإلكترونية الواقعة على شركات المساهمة

رغم الطابع المعقد والغامض الذي تتميز به الجرائم الإلكترونية التي تستهدف شركات المساهمة إلا أن ذلك لا يعني العجز عن مواجهتها وعدم مكافحتها، فبطبيعة الحال لا بد من إتخاذ جملة من الإجراءات للحد من إستفحالها خاصة وأنها تشهد تنامي متزايد ضد هذه الشركات، وحتى يتم القيام بذلك بشكل ناجح ينبغي مراعاة الخصوصية التي تنفرد بها هذه الجرائم للقيام بالتحري عنها والتحقيق فيها وكذا إسنادها إلى الجهات القضائية المختصة بالنظر فيها، وخلال القيام بهذه الإجراءات فإن الأمر يتطلب البحث عن دليل يناسب طبيعتها التقنية يكون مستمد من مسرحها الإفتراضي حتى يتم إثباتها وللإشارة فإن هذه الإجراءات تتطلب كوادر مؤهلة لها خبرة ودراية بالمجال الإلكتروني.

ونظرا لخطورة الجرائم الإلكترونية فإن الأمر لا يتوقف عند إثباتها وإدانة مرتكبيها فقط، إذ لا بد من إيجاد آليات تقنية تشكل درعًا واقيًا لشركات المساهمة من خطرها حتى تحقق أمنها المعلوماتي الذي بات أولوية وضرورة لا يمكن أبدا الإستهانة بها سيما في ظل هذا العالم الإلكتروني، ومن خلال هذا الفصل سنقوم بتوضيح مختلف هذه الإجراءات وذلك بتقسيمه إلى مبحثين:

المبحث الأول: إجراءات التحري، التحقيق والمحاكمة في الجريمة الإلكترونية في إطار شركات المساهمة.

المبحث الثاني: إثبات الجرائم الواقعة في إطار شركات المساهمة وإجراءات الوقاية منها.

المبحث الأول:

إجراءات التحري، التحقيق والمحاكمة في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

نظرا لأن الجرائم الإلكترونية التي تتعرض لها شركات المساهمة تكون في بيئة ذات طبيعة خاصة ترتكز في الأساس على الوسائط الإلكترونية فهي بعيدة تماما عن الطابع المادي، وهذا ما يجعل من عملية متابعتها تتسم بالصعوبة والتعقيد، لذلك تثور عدة إشكالات سواء فيما يتعلق بعملية التحري عنها أو التحقيق فيها وحتى الجهة القضائية التي ستوكل لها مهمة الفصل فيها، هذا ما سنوضحه من خلال هذا المبحث وذلك بتقسيمه إلى مطلبين:

المطلب الأول: إجراءات التحري والتحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

المطلب الثاني: الجهة القضائية المختصة بالفصل في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة

المطلب الأول:

إجراءات التحري والتحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة

إذا كانت أعمال التحري والتحقيق في الجرائم التقليدية التي تتعرض لها شركات المساهمة لا تثير أي إشكال كونها تتم في عالم مادي محسوس، إلا أن الأمر يختلف بالنسبة لهاذين الإجرائين في حالة ما إذا تعرضت هذه الشركات لجرائم إلكترونية، حيث أن القيام بهما يتطلب تقنيات وأساليب حديثة تتناسب وبيئة الأعمال الإلكترونية التي أرتكبت فيها تلك الجرائم، لذلك في هذا المطلب سنناقش مدى إمكانية القيام بكل من إجراء التحري والتحقيق في البيئة الإفتراضية لشركات المساهمة من خلال التعرض لإجراء التحري **(فرع أول)** ثم إجراء التحقيق **(فرع ثاني)**.

الفرع الأول:

إجراء التحري.

يعد إجراء التحري والإستدلال عن الجرائم الإلكترونية في شركات المساهمة من أهم المراحل، إذ يعد الخطوة الأولى في عملية البحث التمهيدي من أجل كشفها وإزاحة الغموض عنها بغية الوصول

إلى حقيقة المعتدي على تلك الشركات، وما يميز إجراء التحري هنا هو أنه يتم بطريقة إلكترونية من خلال شبكة الأنترنت.

لذلك يطلق عليه التحري الإلكتروني والذي يعرف على أنه مجموع الإجراءات التي يقوم بها المتحري عبر شبكة الأنترنت بالإعتماد على تقنيات رقمية إلكترونية قصد الحصول على بيانات أو معلومات سواء تعلقت بالأشخاص أو الأماكن حتى يتم ضبط الجريمة الإلكترونية والحد منها،[1] كما يعرف أيضا بأنه الإجراء الذي يتم عن طريق الإستعانة بالوسائل التكنولوجية وذلك من أجل إسترجاع البيانات وجمعها وحفظها ليستخلص منها دليل يثبت وقوع الجريمة فعلا.[2]

وبما أن الجرائم الإلكترونية الواقعة على شركات المساهمة يَعمدُ فيها الجاني إلى طمس معالم جريمته وما يساعده على ذلك هو البيئة الإفتراضية التي ترتكب فيها، فالعديد من الشركات لا تكتشف هذه الجرائم إلا بعد مضي فترة من الزمن عليها، وباعتبار أن إجراء البحث والإستدلال يتم إنطلاقا بعد البلاغ أو الشكوى إلى الجهات القضائية المختصة،[3] الأمر الذي يجعل هذا الإجراء تعترضه بعض الإشكالات.

أولا: الإبلاغ عن الجرائم الإلكترونية الواقعة على شركات المساهمة.

المقصود بالإبلاغ عن الجريمة هو الإخبار عنها،[4] وهو بمثابة إشعار للسلطات المختصة بأن هناك جريمة قد أرتكبت أو أنه سيتم إرتكابها لاحقا من أجل مواجهتها،[5] كما يعني الإخطار عن الجريمة ويمكن أن يقوم به أي شخص حتى لو لم يتعرض إلى أي ضرر جراء تلك الجريمة.[6]

وعليه فإذا ما تعرضت شركات المساهمة إلى إحدى الجرائم الإلكترونية أو تبين لها بأن هناك جريمة من الممكن أن ترتكب ضدها عليها أن تخطر السلطات المختصة بذلك، والإبلاغ عن هذه

---

[1] مصطفى محمد موسى، دليل التحري عبر شبكة الأنترنت، د.ط، مصر، دار الكتب القانونية، 2005، ص 22.

[2] بثينة حبيباتني، مرجع سابق، ص 290.

[3] صالح شنين، مرجع سابق، ص 229.

[4] أدهم باسم نمر بغدادي، "وسائل البحث والتحري عن الجرائم الإلكترونية"، (رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، 2018)، ص 53.

[5] يزيد بوحليط، مرجع سابق، ص 222.

[6] عبد القادر عميمر، "آليات إثبات الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 205

الجرائم قد يكون ماديا كأن يتم كتابة أو شفويا كما يمكن أن يكون معنويا كما لو تم عن طريق الهاتف أو البريد،[1] بالإضافة إلى ذلك يمكن للتبليغ أن يكون إلكترونيا من خلال إرسال رسالة إلى البريد الإلكتروني للجهات المختصة أو من خلال القيام بملء إستمارة تكون في شكل إلكتروني في المواقع التي تخصص لتلقي البلاغات[2]، والمشرع الجزائري لم يشترط وسيلة محددة للقيام بالتبليغ، حيث نص في المادة 17 من الأمر 15-02[3] على أن ضباط الشرطة القضائية يباشرون السلطات الموضحة في المادتين 12 و 13 ويتلقون الشكاوى والبلاغات...، دون أن يحدد الوسيلة التي يتم بها التبليغ.

لكن ما ينبغي أن نشير إليه هو أنه في الجرائم الإلكترونية خاصة المتعلقة بشركات المساهمة من المستحب أن تكون الجهة المبلغة على دراية ومعرفة بتقنيات الحاسوب من أجل وصف المعلومات للجهة المختصة بشكل دقيق وواضح، كأن يصف أنواع البرامج واللغات والأجهزة التي يتم إستخدامها،[4] وهذا ما يسهل على هذه الجهات القيام بأعمال التحري وذات الشروط يستحسن أن تتوفر فيها أيضا.

لكن الإشكال الذي يثيره التبليغ عن الجرائم الإلكترونية في شركات المساهمة هي إحجام هذه الأخيرة عن التبليغ عن تلك الجرائم التي تتعرض لها، فالعديد من الشركات تتعمد التستر عنها وبالتالي لا تصل إلى علم السلطات المختصة مثل ما يحدث في الجرائم التقليدية،[5] وإذا جئنا إلى تفسير ذلك نجد بأن السبب يعود إلى خوف هذه الشركات على سمعتها التجارية وكذا حماية لمركزها المالي والمحافظة على ثقة عملائها بها، لذلك لا ترغب في الكشف عن الإختراقات التي تتعرض لها أجهزتها الحاسوبية ونظم معلوماتها حتى لا تصبح هناك نظرة على أن تدابير الحماية لديها ضعيفة وغير فعالة وبالتالي النتيجة المترتبة هي عزوف عملائها عن التعامل معها،[6] كما أن السبب يعود

---

[1] بثينة حبيباتني ، مرجع سابق، ص 276.

[2] صالح شنين، مرجع سابق، ص 227.

[3] الأمر رقم 15-02 مؤرخ في 23 يوليو 2015، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائرية، ج، ر، ع 40، الصادر في 23 يونيو 2015.

[4] بثينة حبيباتني ، مرجع سابق، ص 277.

[5] عبد الفتاح بيومي حجازي، مرجع سابق، ص 68.

[6] أسامة أحمد المناعسة، جلال محمد الزغبي، مرجع سابق، ص 82.

أيضا إلى خشية هذه الشركات من أن تؤدي أعمال التحري التي تقوم بها السلطات المختصة إلى حجز أجهزتها لفترة قد تطول وبالتالي النتيجة المترتبة عن ذلك تعطيل أعمالها، الأمر الذي يتسبب لها في خسائر مالية قد تفوق ويتجاوز حجمها حجم الخسائر التي تسببت فيها تلك الجرائم الإلكترونية.[1]

ففي إحدى الوقائع التي تعرض فيها بنك "MARCHANT BANK CITY" في بريطانيا إلى سرقة 8 مليون جنيه إسترليني من أحد أرصدته إلى رقم آخر في سويسرا وقد تم ضبط الجاني متلبسا بسحب المبلغ المسروق، ولكن بدلا من أن يقوم البنك بالإبلاغ عن هذه الجريمة قام بدفع مليون جنيه إلى الجاني مقابل إلتزامه بعدم إعلان جريمته وإطلاع البنك عن الآلية التي مكنته من إختراق نظام الأمن الخاص به.[2]

ففي غالب الأحيان لا يتم الإبلاغ عن الجرائم الإلكترونية التي تركب في إطار شركات المساهمة، فالفجوة بين العدد الحقيقي لهذه الجرائم والتي تم التبليغ عنها كبير جدا، فمجالس إدارة تلك الشركات في خوف دائم من الدعاية السلبية التي قد تترتب في حالة الإبلاغ عنها.[3]

ونظرا للدور السلبي لشركات المساهمة إزاء الجرائم الإلكترونية ومن أجل تفعيل عملية الإبلاغ عنها تم إقتراح في الولايات المتحدة الأمريكية بأن تتضمن النصوص المتعلقة بهذه الجرائم إلتزاما بفرض على موظفي تلك الشركات الإبلاغ عنها عند علمهم مع تقرير خبراء في حالة ما إذا تم الإخلال بالإلتزام،[4] ونحن بدورنا نحبذ لو يتم إقتراح مثل هذه الإلتزامات في القوانين الوطنية فكما سبقت الإشارة إلى أنواع الجرائم التي يمكن أن تتعرض هذه الشركات التي يقوم عليها الاقتصاد الوطني، فمثلا عندما يتعلق الأمر بجريمة غسل الأموال لا يمكن إحجام المؤسسات المالية عن

---

[1] عيدة بلعايد ، (خصوصية التحقيق في الجريمة المعلوماتية)، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، ع 6، الصادر في مارس 2021، ص، ص 138، 139.

[2] رجاء أومدور ، "خصوصية التحقيق في مواجهة الجرائم المعلوماتية" (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، 2020-2021)، ص 36.

[3] عبد المومن بن صغير، مرجع سابق، ص 75.

[4] صفيان بخدة ، ناصر وقاص ، مرجع سابق، ص 125.

الإبلاغ عنها حتى لو كان ذلك بداعي المحافظة على العملاء كون أن التكتم عن تلك الجرائم يترتب عليه تهديدا للإقتصاد الوطني والإضرار به.

إلا أن ما تم إقتراحه في الولايات المتحدة الأمريكية عندما تم عرضه على لجنة "خبراء مجلس أوربا" تم رفضه بسبب أن هذه الشركات تصبح هي الطرف المتهم بعد أن كانت الضحية لذلك تم تقديم إقتراحات بديلة كالإلتزام بإبلاغ هيئة إشرافية، مع تشكيل هيئات خاصة مهمتها تبادل المعلومات ومنح شهادة أمن خاصة يتم إصدارها بعد القيام بعملية المراجعة والتدقيق التي تقوم بها هيئة من المراجعين، والتي يتعين عليها الإبلاغ عما تكشفه من جرائم خلال عملية المراجعة،[1] وفي الدول العربية نجد دولة الإمارات العربية التي ألزمت بالإبلاغ عن هذه الجرائم ضمن نصوصها القانونية وفي حالة إخلال الضحية بذلك تفرض عليه عقوبات،[2] وبناء على ما سبق ذكره فإن الإبلاغ عن الجرائم الإلكتررونية في شركات المساهمة له قيمة قانونية من أجل مباشرة إجراء التحري عنها، كما له أهمية تتجلى في كونه جانب وقائي إذا ما تم الإبلاغ قبل وقوع تلك الجرائم كون أن الإجراءات التي يتم إتخاذها في هذه الحالة لا تعد من قبيل أعمال التحري وإنما هي إجراءات من أجل حماية تلك الشركات من جرائم في طريقها إلى التحقق.

ثانيا: كيفية تعامل الجهات المختصة مع بلاغ شركات المساهمة عن الجرائم الإلكترونية.

عند قيام هذه الشركات بالإبلاغ عن الجرائم الإلكترونية التي تعرضت لها تحرص على أن تقوم بإعداد قائمة تضم أسماء العاملين بها خاصة الذين تكون لهم علاقة بالأجهزة التي تم الإعتداء عليها، وكذا نسخة إحتياطية من بيانات تلك الأجهزة، بالإضافة إلى تكتمها وعدم إخطار أي طرف آخر بوقوع هذه الجرائم عليها، [3] لتقوم بعدها السلطات المختصة بإجراء البحث والتحري بضبط خطة عمل يتم وفقها التحري عن الجريمة الإلكترونية المرتكبة مع الأخذ بعين الإعتبار الظروف التي تكون محيطة بها حيث تمثل ركيزة لخطة عمل جهات التحري والتي منها:

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص ص 75، 76.

[2] بثينة حبيباتني ، مرجع سابق، ص 278.

[3] حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 218.

1-حجم أهمية أجهزة الحواسيب والشبكات المعلوماتية التي تم الإعتداء عليها في أداء عمل هذه الشركات؛

2-حجم أهمية وحساسية البيانات التي تم إختراقها؛

3-إمكانية إطلاع الرأي العام عن الجرائم التي تعرضت لها هذه الشركات أم لا خاصة إذا كانت الشركة الضحية من أهم الشركات في الدولة؛

4-حجم الإختراق الأمني الذي أحدثه الجاني وكذا حجم المهارة التقنية والفنية التي يتمتع بها.[1]

يتعين بعدها على جهات التحري الإنتقال قصد معاينة المسرح الإلكتروني وذلك باعتبار أن المعاينة مهمة وضرورية في عملية جمع الإستدلالات والتحري، وبطبيعة الحال تختلف المعاينة في هذه الجرائم عن تلك التي يتم إجراؤها في الجرائم التقليدية.

حيث أن معاينة مسرح الجرائم الإلكترونية يقصد بها معاينة تلك الآثار التي يخلفها مستعمل النظام المعلوماتي لشركات المساهمة وما يشتمله من رسائل سواء تلك التي تم إرسالها وكذا التي تم إستقبالها،[2] والمعاينة قد تتم ماديا بالإنتقال إلى مسرح الجريمة كما قد تتم إفتراضيا من خلال أي جهاز حاسوب،[3] حيث تتجلى أهميتها في الجرائم الإلكترونية أثناء عملية التحري وجمع الإستدلالات في أن الواقع العملي أثبت أثرها البالغ في كشفها عن طريق تتبعها في أي مكان كان وبغض النظر عن الزمان الذي تم إرتكابها فيه وإزاحة الغموض عنها.

وخلال عملية القيام بالمعاينة لا بد من إتباع ضوابط معينة قصد ضمان إجرائها كأن تكون بصورة متتابعة ومتسلسلة، بمعنى أن الجهات المكلفة بها تحدد بداية النقاط التي سيتم إجراء المعاينة عليها وعدم الإنتقال من مكان إلى آخر إلا بعد التأكد من معاينة المكان الأول وبشكل كامل، [4] وهذا التتابع والتسلسل لا بد من مراعاته سواء تمت المعاينة بشكل مادي أو إفتراضي كون أن النظام المعلوماتي يحوي العديد من الملفات التي يتوجب معاينتها.

---

[1] بثينة حبيباتني ، مرجع سابق، ص 284.

[2] نصيرة بوجزمة ، مرجع سابق، ص 351.

[3] خضرة شنتير ، مرجع سابق، ص 66.

[4] نصيرة بوجزمة ، مرجع سابق، ص 353.

بالإضافة إلى التحلي بالدقة وبذل العناية خلال عملية المعاينة كأن يتم تأمين جميع أجهزة حواسيب الشركة التي ستخضع لهذه العملية وإبعادها عن أي شخص آخر، كذلك القيام بتصويرها مع الأجهزة المتصلة بها وتدوين زمان ومكان إلتقاط الصورة،[1] وبمعاينة المسرح الإلكتروني للجرائم التي تتعرض لها شركات المساهمة يمكن فك شفراتها الغامضة كون أن ذلك المسرح هو مستودع أسرار هذه الجرائم، وإضافة إلى هذه الضوابط يتعين على الجهات المختصة التعجيل في إجراء عملية المعاينة وذلك خشية على إخفاء آثار تلك الجرائم بسهولة.

ثالثا: الأساليب المساعدة للقيام بعملية التحري عن الجرائم الإلكترونية الواقعة على شركات المساهمة.

في كثير من الأحيان تقف الجهات المكلفة بعملية البحث والتحري عن الجرائم الإلكترونية الماسة بهذه الشركات عاجزة عن إتمام عملها وذلك راجع إلى صعوبة البحث والتنقيب عن المعلومة التي من شأنها أن توصل إلى كشف تلك الجرائم لذلك بإمكان السلطات المختصة الإستعانة بالأساليب التي تراها مناسبة لإتمام عملية التحري.

1-أسلوب المراقبة الإلكترونية: ويعد من أهم الأساليب التي يستعين بها رجال التحري من أجل التقصي عن الجرائم الإلكترونية الواقعة على شركات المساهمة، وكانت لجنة خبراء البرلمان الأوربي قد عرفتها خلال إجتماعها المنعقد في أكتوبر 2006 بستراسبورغ على أنها عبارة عن مراقبة تكون في شكل سري للمراسلات السلكية واللاسلكية من أجل القيام بعملية البحث والتحري وتحصيل المعلومات عن الأشخاص الذين يشتبه فيهم إرتكاب جريمة أو مشاركتهم في إرتكابها[2].

ويعرف كذلك بأنه ذلك العمل الذي يتم عن طريق إستخدام الاتصالات الإلكترونية بغرض جمع معلومات عن المشتبه فيه في إرتكاب الجريمة سواء كان الخاضع لعملية المراقبة شخصا أو حتى مكانا،[3] لذلك يعتبر أسلوب المراقبة الإلكترونية إحدى وسائل التحري التي يمكن من خلالها للسلطات

---

[1] رجاء أومدور ، مرجع سابق، ص 157.

[2] عبد الحليم بن بادة ، (المراقبة الإلكترونية كإجراء لإستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني)، المجلة الأكاديمية للبحث القانوني، ع 3، مج 10، الصادر في 2019، ص 391.

[3] يزيد بوحليط، مرجع سابق، ص 307.

المختصة جمع بيانات ومعطيات عن الأطراف الذين تشتبه فيهم القيام بالإعتداء على الشركة المجني عليها باختراق حواسيبها حيث تتم عملية المراقبة بالإستعانة بالوسائل التقنية المناسبة لطابعها الإلكتروني.

ويرد أسلوب المراقبة الإلكترونية على الاتصالات فور القيام بها أو إجرائها باعتبار الأسلوب الذي يتناسب والطبيعة الحركية للبيانات التي يصعب تفتيشها وهذا عكس الاتصالات الإلكترونية التي تكون مخزنة والتي من الممكن إخضاعها للتفتيش، لذلك فهذا الأسلوب لا يعد تفتيشا وإنما هو إجراء يكون من لحظة إلتقاط الإتصال الإلكتروني وينتهي بتحصل الجهات المكلفة بالتحري عليه، وهذا ما تم التأكيد عليه خلال توصيات المجلس الأوربي والتي طالبت بالتمييز والتفريق بين البيانات الإلكترونية المتحركة والبيانات الساكنة،[1] وإجراء هذا الأسلوب على الأطراف المشتبه فيهم في الإعتداء على شركات المساهمة يعد من قبيل التحري عن الجرائم الإلكترونية التي تعرضت لها كون أن المراقبة ترد على بيانات متحركة والتي تتمثل في الاتصالات الإلكترونية مباشرة وقت القيام بها ولا ترد على تلك الاتصالات التي يكون قد تم إجراؤها وتخزينها، فتكون عبارة عن بيانات ساكنة وهذه الأخيرة تخضع لعملية التفتيش لا المراقبة وهذا ما سنوضحه لاحقا.

أما بالنسبة للمشرع الجزائري فنجد بأنه قد نص على إمكانية اللجوء إلى أسلوب المراقبة الإلكترونية حينما يتعلق الأمر بالجرائم الإلكترونية في القانون 06-22[2] وذلك في الفصل الرابع منه تحت عنوان "إعتراض المراسلات وتسجيل الأصوات والتقاط الصور" في المواد من 65 مكرر5 إلى 65 مكرر 10، ليتعزز النص على اللجوء إلى هذا الأسلوب مرة أخرى من خلال القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكتولوجيات الإعلام والإتصال من خلال المادة 3 منه التي جاء فيها "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضايات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية.."

---

[1] حمزة بلحسيني ، مرجع سابق، ص 401.

[2] القانون رقم 06-22 مؤرخ في 20 ديسمبر 2006-، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج،ر، ع 84، الصادر في 24 ديسمبر 2006.

ومن خلال هذه النصوص القانونية يتضح بأن المشرع الجزائري لم يقدم تعريفا للمراقبة الإلكترونية مكتفيا في ذلك بتعريف الاتصالات الإلكترونية فقط.[1]

كما نجد بأنه خصص الفصل الثاني من نفس القانون لأسلوب المراقبة الإلكترونية حيث حدد حالات اللجوء إليها في المادة 4 من هذا القانون والتي من بينها حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وبطبيعة الحال الإعتداء على شركات المساهمة هو في حقيقة الأمر إعتداء على إقتصاد الدولة وكأن المشرع أجاز أسلوب المراقبة الإلكترونية في حالة ما إذا كانت الجرائم على على درجة بالغة من الخطورة وتمس بالمجالات الحيوية التي يرتكز عليها الاقتصاد الوطني.

كما يتضح من نصوص القانون 09-04 السالف الذكر أنه لم يحدد الهيئة التي توكل إليها مهمة المراقبة الإلكترونية، غير أنه بصدور المرسوم الرئاسي رقم 20-183[2]نجد بأنه أوكل هذه المهمة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات والإتصال ومكافحتها، حيث جاء في المادة 22 منه على أنه "...تكلف الهيئة حصريا في مجال إختصاصها بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها" كذلك المادة 25 منه التي نصت على أنه "يتم تسجيل الاتصالات الإلكترونية التي تكون موضوع مراقبة وفقا للشروط المنصوص عليها في قانون الإجراءات الجزائية" ويتم حفظ المعلومات المتحصل عليها أثناء عملية المراقبة من طرف الهيئة وفقا للقواعد المطبقة على حماية المعلومات المصنفة هذا وفقا لنص المادة 24.

وعملية المراقبة الإلكترونية تتم بواسطة الإستعانة بمختلف الوسائل التقنية التي تكون على درجة من التطور، وفي هذا الصدد نص المشرع في المادة 17 من نفس المرسوم على أم مديرية المراقبة الوقائية واليقظة الإلكترونية تضع التجهيزات والوسائل والأجهزة التقنية اللازمة من أجل تنفيذ مهامها، فهناك العديد من الدول التي لجأت فيها جهات البحث والتحري إلى تصميم برامج إلكترونية وهي ذات

---

[1] المادة 2 فقرة و من القانون 09-04 "الاتصالات الإلكترونية أي تراسل أو إرسال أو إستقبال علامات إو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

[2] المرسوم الرئاسي رقم 20-183 مؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج،ر، ع 40، الصادر في 18 يوليو 2020.

تقنية عالية من أجل قيامها بعملية المراقبة عبر شبكة الأنترنت، حيث يتم إخضاعها لعدة تجارب واختبارات فنية وقضائية حتى يمكن إعتمادها كأسلوب لجمع المعلومات،[1] ومن تلك البرامج مثلا نجد:

أ-برامج التتبع المعلوماتية: والتي هي على شكل برنامج "HACK-TRACER" يتبع محاولات الإختراق ومن ثم التعرف على من قام بها، ليقوم بعدها بإشعار الجهة التي تعرضت إلى ضرر حيث أن هذه البرامج تكون ساكنة على خلفية المكتب وبمجرد أن تكون هناك محاولة إختراق أو قرصنة تقوم بصد المخترق من خلال غلق المنافذ أمامه مع مطاردته وتتبع أثره حتى يتم ضبط عنوانه الإلكتروني زمعلومات أخرى[2].

ب-تقنية البروكسي: وهو عبارة عن وسيط يعمل بين الشبكة ومستخدميها تكمن مهمته في تلقي طلبات المستخدمين قصد البحث عن صفحة ما، فيقوم هذا النظام بالتحقيق فيما إذا كان قد سبق وتم تنزيل الصفحة المطلوبة، فإذا كان ذلك قد تم فعلا فتكون جاهزة ضمن ذاكرته وهنا يقوم فقط بإعادة إرسالها إلى المستخدمين دون أن يكون هناك داعي إلى طلبها من الشبكة العالمية للمعلومات، ومن إيجابيات هذا البرنامج أنه يبقى محتفظا بكل تلك المعلومات والعمليات وبالتالي يمنح لرجال التحري تتبع آثار المتهم بمساعدة نزود الخدمات.[3]

2-أسلوب حفظ المعطيات المتعلقة بحركة السير: نجد بأن المشرع الجزائري قد نص على هذا الأسلوب ضمن الفصل الرابع من القانون 09-04 السالف الذكر تحت عنوان "إلتزامات مقدمي الخدمات" حيث جاء في المادة 10 منه على أنه يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بعملية التحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا لنص المادة 11 من نفس القانون، وهو ما تم النص عليه في الفصل الثاني من إتفاقية بودابست المتعلقة بالجريمة الإلكترونية تحت عنوان " التعجيل في حفظ بيانات الكمبيوتر المخزنة" وذلك في كل من المادة 16 و 17، وهو ما نصت عليه أيضا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ضمن موادها 23، 24 و ، وأسلوب حفظ المعطيات

---

[1] بثينة حبيباتني ، مرجع سابق، ص 304.

[2] حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، 229.

[3] نصيرة بوحزمة ، مرجع سابق، ص ص 140، 141.

المتعلقة بحركة السير يقتضي منا التطرق إلى تعريف مقدمو الخدمات وذلك كون أن هذه المعطيات هم من يخزنونها.

ومقدمي الخدمات وفقا للفقرة د من المادة 2 من القانون 09-04 هم:

-أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصالات؛

-وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد عرفت مزود الخدمة في الفقرة الثانية من المادة الثانية منها على أنه أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

فمن خلال هذه النصوص القانونية يتجلى لنا بأن مزود الخدمة يقوم بتخزين المعلومات والمعطيات الخاصة بالمشترك سواء تعلق الأمر بنوع الخدمة أو معلوماته الخاصة كعنوان بريده أو هويته مثلا، لذلك يكون بإمكانه معرفة جميع الخطوات التي قام بها المشترك وتتبعه ومراقبته من خلال الإطلاع على المواقع التي قام بزيارتها والمعلومات والمعطيات التي قام بحفظها أو تحويلها.

لذلك فأسلوب حفظ المعطيات معناه قيام مقدموا الخدمات بتجميع المعلومات والمعطيات التي تمكنهم من التعرف على المستخدمين ويتم حفظها وفق ترتيب ما في أرشيف حتى يمكن العودة إليها في حالة ما إذا كانت هناك حاجة قانونية إليها من قبل الجهات المختصة،[1] وعليه فإن مقدمي الخدمات يكون لهم دور مهم جدا في مساعدة رجال التحري في الكشف عن الجرائم الإلكترونية والتوصل إلى مرتكيبيها.

[1] عبد القادر فلاح ، (حجز وحفظ المعطيات في الجريمة الإلكترونية)، مجلة صوت القانون، ع 1، مج 8، الصادر في 2021، ص 183.

أما بالنسبة للمعلومات التي يجب حفظها من قبل مزودي الخدمات فتتمثل في تلك المتعلقة بخركة السير والتي عرفها المشرع في الفقر ه من المادة الثانية من القانون 09-04، وهي تلك المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة على أساس أنها جزء في حلقة إتصالات توضح مصدر الإتصال والوجهة التي ترسل إليها والطريق الذي تسلكه وكذا وقت وتاريخ وحجم ومدة الإتصال مع نوع الخدمة، وكان المشرع قد حصر طائفة هذه المعلومات بموجب المادة 11 من نفس القانون والتي تتمثل في:

-المعطيات التي يمكن من خلالها التعرف على مستعملي الخدمة؛

-المعطيات التي تتعلق بالتجهيزات الطرفية المستعملة للإتصال؛

-الخصائص التقنية وأيضا التاريخ والوقت والمدة الخاصة بكل إتصال؛

-المعطيات التي تتعلق بالخدمات التكميليةالمطلوبة أو المستعملة ومقدميها؛

-المعطيات التي تمكن من التعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

حيث يقع على عاتق مزودي الخدمات إلتزاما بمساعدة السلطات المختصة وكذا حفظ المعطيات المتعلقة بحركة السير، إلا أن حفظ هذه المعطيات يكون وقتي فقط وقد حددها المشرع في نص المادة 11 من القانون 09-04 "...مدة حفظ المعطيات المذكورة في هذه المادة سنة واحدة إبتداء من تاريخ التسجيل" كما أشارات نفس المادة إلى أنه في حالة إخلال مزودي الخدمات بالإلتزامات المفروضة عليهم يتعرضون إلى عقوبات جزائية إضافة إلى العقوبات الإدارية كون أن إخلالهم يمس بسير عملية التحريات.

وعليه فعملية حفظ هذه المعطيات يعد أسلوب تحري يعول عليه كونه يسمح بالتوصل إلى الاتصالات والتدخلات غير المشروعة التي يقوم بها الجاني على النظام المعلوماتي لشركات المساهمة، خاصة وأنه مثلما سبق ورأينا فإن معظم الجرائم الإلكترونية التي ترتكب على هذه الشركات تنفذ من خلال التظام المعلوماتي بواسطة الاتصالات المختلفة التي يقوم الجاني بإجرائها، لذلك فإن الإستعانة بمزودي الخدمات من شأنه أن يساعد على كشف الجاني خاصة إذا كان من بين موظفي الشركة، حيث يمكن كشف جميع الملفات التي قام بتخزينها وكذا الحوارات والإتصالات التي قام بها

وحركة فواتير الشراء والخدمات التي إشترك فيها،[1] لذلك فإن تكتم شركات المساهمة عن الجرائم الإلكترونية التي تتعرض لها يجعل من الصعب جدا أن تصل إلى الجاني لوحدها دون الإستعانة بأساليب التحري التي رأيناها.

الفرع الثاني:

إجراء التحقيق

يمكن إعتبار مرحلة التحقيق في الجرائم الإلكترونية في إطار شركات المساهمة ذات أهمية كبيرة نظرا للدور الذي تؤديه عملية التحقيق في التوصل إلى الأدلة التي من شأنها كشف حقيقة مرتكبي هذه الجرائم، وذلك بعد عملية البحث والتنقيب عنها.

والتحقيق عمل إجرائي يكون لاحقا لعملية البحث والتحري وسابقا لمرحلة المحاكمة، ونظرا للطابع المعقد الذي تتسم هذه الجرائم حيث أثبتت التجربة الواقعية صعوبة عملية التحقيق فيها بسبب طابعها التقني، فإجراء التحقيق فيها يختلف تماما عن التحقيق الذي يتم إجراؤه في الجرائم التقليدية، لذلك سنوضح من خلال هذا الفرع العوائق التي تعترضه سواء من حيث مواصفات الأشخاص المخول لهم القيام به أو من حيث الإجراءات التي يتم من خلالها.

أولا: تعريف التحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

التحقيق الذي يتم في هذه الحالة يتسم بطابع إلكتروني حتى يكون مناسبا للبيئة الإفتراضية التي تم فيها إرتكاب تلك الجرائم، حيث يعرف على أنه الأساليب الي يمكن إتباعها بغية معرفة وتقديم دليل ضمن وسيلة إلكترونية أمام الجهات القضائية،[2] وهو إجراء يكون الهدف منه الكشف والتنقيب عن دليل إلكتروني بشأن هذه الجرائم المرتكبة، ومدى كفاية ذلك الدليل من أجل إحالة الجاني إلى المحاكمة،[3] وهو أيضا الإستعانة بالطرق التي تكون مثبتة علميا قصد حفظ، جمع، تحليل، توثيق

---

[1] يزيد بوحليط، مرجع سابق، ص 319.

[2] الطيبي البركة، (إشكالات الإثبات في الجرائم الإلكترونية)، مجلة أفاق علمية، ع 1، مج 11، الصادر في 2019، ص 275.

[3] عبد القادر فلاح ، نادية آيت عبد المالك ، (التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري) مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 2، مج 4، الصادر في 2019، ص 1694.

والتحقق من صدق الأدلة التي تستخرج بطريقة إلكترونية من أجل المساعدة على بناء الأحداث الجنائية أو تسهيل إحباط العمليات غير القانونية المحتملة[1]، ومن خلال هذه التعريفات يمكننا أن نعرف بدورنا التحقيق الذي يتم في الجرائم الإلكترونية بأنه يعتمد على إستعمال وسائل مشروعة بطبيعة الحال، بالإضافة إلى تميزها بالطابع التقني الإلكتروني يتمكن من خلالها المحقق من رفع اللبس وكشف الغموض على هذه الجرائم، وبالتالي الوقوف على أدلتها وتحديد هوية مرتكبها.

ونظرا للطابع المعقد الذي تتسم به عملية التحقيق ضمن هذا النوع من الجرائم فإنه يستلزم أن توكل مهمة ذلك إلى أشخاص مختصين على مستوى من الكفاءة والخبرة، والشخص الذي يباشر عملية التحقيق يسمى بالمحقق الجنائي، وهو الذي تعهد إليه مهمة البحث عن الحقيقة في الجرائم الإلكترونية وتجميع أدلة الإدانة ضد الجناة وبالتالي إحالتهم أمام القضاء، كما أن المحقق شخص يتم تكليفه بتطبيق إجراءات القانون الساري كل حسب إختصاصه،[2] والمحقق هو من يتولى مباشرة التحقيق بالمعنى القانوني أي يكون من أعضاء النيابة العامة أو قضاة التحقيق إذ لا يمكن أن يطلق لفظ المحقق على الذين يتولون عملية جمع الإستدلالات،[3] وما يجب التأكيد عليه هو أن المحقق في هذا النوع من الجرائم لا يختلف عن المحقق الذي يباشر أعمال التحقيق في الجرائم التقليدية، فالعبرة بنوعية الجريمة لا بالمحقق رغم أن هناك بعض الصفات والمؤهلات التي يستلزم توفرها في المحقق في الجرائم الإلكترونية في إطار شركات المساهمة وهذا نظرا للطابع التقني المعقد الذي تتسم به ومن تلك الصفات:

1-الإلمام بالمعرفة في مجال الحاسوب وشبكات الأنترنت: بما أن الجرائم الإلكترونية والتي سبق الإشارة إليها ترتكب عن طريق أجهزة الحواسيب وشبكات الأنترنت، لذلك ينبغي أن يكون الشخص الذي يتولى مهمة التحقيق أن يكون مُلمًا بمعرفة جوانب هذه الأجهزة ومختلف مكوناتها المادية والمعنوية وكيفية عملها وطريقة التعامل معها وطريق التخزين في وسائطها.

---

[1] عزيزة رابحي ، مرجع سابق، ص 257.

[2] نصيرة بوحزمة ، مرجع سابق، ص 151.

[3] عزيزة رابحي ، مرجع سابق، ص 258.

كما يجب عليه أن يتقن الآلية التي تعمل بها شبكات الأنترنت، فإذا جئنا إلى الشبكة االدولية نجد بأن هناك ملايين الحواسيب التي تكون مرتبطة فيما بينها، فإتقان مبادئ الإتصال والطريقة التي يتم من خلالها إنتقال المعلومات والبيانات بين هذه الحواسيب يمكن المحقق من التوصل إلى الجاني في هذه الجرائم، وبالتالي فإن الإلمام بهذه التقنيات يكون لدى المحقق تصور عن الكيفية التي تم من خلالها الإعتداء على هذه الشركات نفي الفضاء الإلكتروني سواء باختراق شبكاتها وحواسيبها أو إعتراض بياناتها أثناء عملية إنتقالها ومن ثمة التجسس عليها وتغيير إتجاهها.[1]

وإلمام المحقق بالمعرفة في مجال الحاسوب وشبكات الأنترنت تفرض عليه الحرص على ضرورة عدم إدخال أي تعديلات أو تغييرات على الحالة التي تكون عليها حواسيب الشركة الضحية، وكذا عدم السماح باستخدامها أو إستخدام أي حاسب آخر يكون على إتصال بالشبكة وهذا ما يعرف بالقاعدتين الأساسسيتين في التحقيق الجنائي،[2] وبالتالي للمحقق دور في المحافظة على الدليل وعدم طمسه وإتلافه سيما وأن عملية التخلص منه بسيطة جدا إذ من الممكن أن تتحقق من خلال كبسة زر فقط في حالة ما إذا كان الجاني من بين موظفي الشركة مثلا وتم السماح بإعادة إستعمال أجهزة الحواسيب التي كانت محل إختراق، فهي موضوع الجريمة الإلكترونية.

2-المحقق في الجرائم الإلكترونية في إطار شركات المساهمة يجب أن يكون ذو خبرة واسعة: في عمليات التحقيق في مختلف القضايا المعقدة والشائكة، كون أن عملية التحقيق في هذه الجرائم تكون أكبر من أن يتولى التحقيق فيها شخص واحد بمفرده وإنما فريق، لذلك فالمحقق هنا يدير العمل كما يوجه باقي المحققين،[3] ولا تقتصر عملية التحقيق على عمل هؤلاء المحققين فقط وإنما ينبغي أن يكون هناك تعاون بينهم وبين الخبراء في مجال الحواسيب العاملين في الشركة المجني عليها،[4] ونظرا لكون أن بعض الجرائم الإلكترونية التي تستهدف شركات المساهمة تكون على درجة كبيرة من التعقيد

---

[1] عزيزة رابحي ، مرجع سابق، ص 261.

[2] علي جبار الحسيناوي، مرجع سابق، ص 107.

[3] المرجع نفسه، ص 107.

[4] عبد الصبور عبد القوي علي مصري، منال عبه اللاه عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، مرجع سابق ص 285.

خاصة وأنها تتجاوز الحدود الوطنية الأمر الذي يصعب من مهمة التحقيق، ففي مثل هذه الحالات من الممكن الإستعانة بالشركات العالمية التي تكون مختصة في هذه الجرائم من أجل التعاون مع المحققين فهناك العديد من هذه الجرائم التي حققت فيها نجاح من خلال الكشف عنها والتوصل إلى مرتكبيها.

3-المعرفة بتقنيات الأمن المعلوماتي: حيث أن إلمام المحقق بالتقنيات التي تستخدمها هذه الشركات من أجل تحقيق أمن حواسيبها وشبكاتها تشكل عاملا مهما في عملية التحقيق وذلك من خلال قراءة المحقق وفهمه لوظائفها والأسلوب التي تعمل به وطريقة إستخدامها، فعند مباشرة عملية التحقيق أو ما يسأل عنه المحقق القائمين على النظام المعلوماتي لهذه الشركات هو نوع برامج الحماية التي تستخدمها حتى يتمكن من معرفة الطريقة التي تم بها إختراقها،[1] ونظرا للتزايد الملحوظ في الجرائم الإلكترونية التي تستهدف شركات المساهمة وحتى لا يتم إفلات الجناة من قبضة العدالة وبالتالي تشجيع غيرهم على إختراق هذه الشركات يجب على الجهات الأمنية والقضائية تدعيم كوادرها بالمختصين ضمن مجال الحواسيب الآلية حتى يتسنى لهم القيام بعملية التحقيق على شكل جيد وبالتالي وضع حد لإنتشار هذه الجرائم من خلال التوصل إلى جناتها وردعهم.

إضافة إلى هذه الصفات يتطلب الأمر في المحقق في الجرائم الإلكترونية في إطار شركات المساهمة أن تتوفر فيه كذلك باقي الصفات المطلوب توفرها في أي محقق جنائي كأن يكون هدفه هو كشف الحقيقة والوصول إلى الجاني، وأن يكون محايدا خلال عملية التحقيق بالإضافة إلى محافظته على سرية التحقيق وعدم تأثره باتجاهات الرأي العام.

ثانيا: الإجراءات اللازمة لعملية التحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة:

بما أن التحقيق يهدف إلى كشف الحقيقة وحتى يتمكن المحقق من الوصول إلى ذلك ينبغي عليه اللجوء إلى مجموعة من الإجراءات، التي يلجأ إليها المحقق قصد القيام بعملية التحقيق والتي نتعرف عليها فيما يلي:

[1] نصيرة بوحزمة ، مرجع سابق، ص 163.

1-تفتيش النظام المعلوماتي لشركات المساهمة:

حيث يعرف التفتيش بأنه أحد إجراءات التحقيق يقوم بمباشرته موظف وذلك بهدف البحث عن أدلة ذات طبيعة مادية لجناية أو جنحة وقعت، ويتم وفقا للإجراءات التي قررها القانون،[1] كما يعرف على أنه عملية البحث عن الأشياء التي تتعلق بالجريمة قصد ضبطها وكل ما من شأنه أن يساعد على كشفها ويجب أن يستند إلى سند قانوني،[2] وبالتالي فإن التفتيش لا يعد من ضمن الإجراءات التي تكشف عن الجرائم قبل وقوعها وإنما هو إجراء للتحقيق فيها بعد أن يتم إرتكابها،[3] فمن خلال هذه التعريفات يتجلى لنا بأن الهدف من التفتيش هو الحصول على الدليل المادي، لذلك فهو يتناسب مع الجرائم التي تخلف آثار مادية كالجرائم التقليدية حيث أنه ليست هناك أية مشكلة تعيقه كونه إجراء تقليدي يلاءم الطبيعة المادية لتلك الجرائم، لكن إذا جئنا إلى تطبيق إجراء التفتيش على الجرائم الإلكترونية الواقعة على شركات المساهمة فإن الأمر يختلف كونه تعترضه مشكلات تعيق عملية تطبيقه، لذلك نتساءل عن مدى خضوع النظام المعلوماتي لشركات المساهمة لإجراء التفتيش؟

مثلما سبقت الإشارة فإن النظام المعلوماتي لشركات المساهمة يتكون من جزئين، كيان مادي وآخر منطقي وفي حالة وقوع جريمة إلكترونية فكلاهما يخضع لعملية التفتيش.

أ-تفتيش الكيان المادي للنظام المعلوماتي لشركات المساهمة: حينما يتعلق التفتيش بالمكونات المادية للنظام المعلوماتي لهذه الشركات فليس هناك إشكال يمكن إثارته ولا خلاف حول هذه المكونات في خضوعها لعملية التفتيش كونها ذات طبيعة مادية، وبالتالي فتفتيشها يتم وفقا لقواعد النصوص القانونية الإجرائية.

---

[1] سلمى مانع ، (التفتيش كإجراء للتحقيق في الجرائم المعلوماتية)، مجلة العلوم الإنسانية ، ع 22، الصادر في جوان 2011، ص 228.

[2] إدريس قرفي، (تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية بين إتفاقية بودابست والتشريع الجزائري) مجلة الحقوق والحريات، ع 2، الصادر في 2014، ص 100.

[3] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص 110.

فالمكونات المادية للنظام المعلوماتي كالشاشات، الذاكرات والطابعات يتم عن طريق الولوج إلى داخلها من أجل البحث عن أدلة تثبت الجريمة الإلكترونية التي تعرضت لها شركات المساهمة،[1] فمتى قامت أسباب ترجح إمكانية إحتواء هذه المكونات على أدلة تساعد على كشف الحقيقة يمكن إخضاعها لعملية التفتيش،[2] ولكن ما يجب التنويه إليه بخصوص تفتيش هذه المكونات هو الحرص على الجانب الفني خلال عملية تفتيشها نظرا لحساسيتها وإمكانية إتلافها لذلك وجب المحافظة عليها.[3]

كما أن القاعدة التي يجب مراعاتها في عملية تفتيش المكونات المادية للنظام المعلوماتي هو طبيعة المكان الذي تتواجد فيه إن كان عاما أو خاصا، حيث أن تحديد طبيعة هذا المكان أهمية خاصة في إجراء التفتيش،[4]لكن يجوز الخروج عن هذه القاعدة إذا ما تعلق الأمر بجريمة إلكترونية وهو الإستثناء الذي أورده المشرع الجزائري في الفقرة 3 من المادة 46 من القانون 06-22،[5] فما نستخلصه من أحكام هذه المادة التي أحالت إلى تطبيق أحكام المادتين 47 فقرة 3 و وكذا المادة 47 مكرر هو أنه يجوز إجراء عملية التفتيش في الجرائم الإلكترونية بما فيها تلك الواقعة على شركات المساهمة نهارا أو ليلا وفي أي مكان على إمتداد التراب الوطني.

ب-تفتيش الكيان المنطقي للنظام المعلوماتي لشركات المساهمة: إذا كان تفتيش الكيان المادي لا يثير أية صعوبات فإن الأمر يختلف بالنسبة للكيان المنطقي، حيث كان محل جدل فقهي كبير واعتبر الإشكالية الأكثر تعقيدا، فهذا الكيان يتعلق بالبيانات والبرامج الخاصة بأجهزة حواسيب هذه

---

[1]سلمى مانع ، مرجع سابق، ص 234.

[2]رابح الهوى، "الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2020-2021)، ص 173.

[3]ليندا بن طالب ، (التفتيش في الجريمة المعلوماتية)، مجلة العلوم القانونية والسياسية، ع 16، الصادر في جوان 2017، ص 490.

[4]خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص 195.

[5]الفقرة 3 من المادة 64: غير أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47 فقرة 3 من هذا القانون تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر).

الشركات حيث أن تفتيشها يستلزم الكشف عن كلمات المرور أو شفرات أو ترميز البيانات،[1] وهي ليست ذات طبيعة مادية محسوسة في الفضاء الخارجي،[2] ومن أجل حسم الخلاف والجدل حول صلاحية هذه المكونات لعملية التفتيش برز موقفين:

موقف يرى بإمكانية خضوع هذا الكيان لعملية التفتيش وذلك إستنادا إلى القوانين الإجرائية التي تنص على إمكانية تفتيش أي شيئ مما يوحي إلى تطبيق التفتيش على المكونات المادية وكذا غير المادية،[3] فنجد بأن الفقه اليوناني قد ذهب إلى التوسيع من عبارة "أي شيئ" والي وردت ضمن المادة 251 من قانون الإجراءات اليوناني لتشمل حتى المعلومات والبيانات التي يتم تخزينها بطريقة إلكترونية،[4] فهذه المعلومات وإن كانت على شكل ذبذبات إلكترونية أو عبارة عن نبضات غير أنه يمكن تسجيلها وتخزينها وحتى تحميلها وذلك في دعائم مادية، وبالتالي يصبح لها كيان مادي محسوس وعليه تصبح من الممكن إخضاعها للتفتيش.[5]

في حين هناك موقف آخر يرى عدم إمكانية إخضاع الكيان المنطقي لإجراء التفتيش وذلك بحجة عدم إنطباق المفهوم المادي على البيانات،[6] فالطبيعة الخاصة للكيان المنطقي تستلزم إحداث قواعد خاصة بها من أجل تفتيشها أو تعديل قواعد التفتيش الموجودة بحيث تصبح تتناسب مع هذه البيانات،[7] وفي هذا الصدد نجد المشرع الفرنسي قد قام بتعديل نصوص التفتيش حتى تتلاءم وطبيعة البيانات حيث أضاف عبارة المعطيات المعلوماتية بنص المادة 94 من قانون الإجراءات الجزائية

---

[1] لامية مجدوب، (إجراء التفتيش في التزوير الإلكتروني)، مجلة التواصل في الاقتصاد والإدارة والقانون، ع 3، مج 25، الصادر في سبتمبر 2019، ص 112.

[2] ليندا بن طالب ، "الدليل الإلكتروني ودوره في الإثبات الجنائي دراسة مقارنة"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2019)، ص 51.

[3] مراد يرمش ، مرجع سابق، ص 133.

[4] بثينة حبيباتني، مرجع سابق، ص 318.

[5] جمال براهيمي ، "التحقيق الجنائي في الجرائم الإلكترونية"، (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2018)، ص 18.

[6] أسامة بن غانم العبيدي، (لتفتيش عن الدليل في الجرائم المعلوماتية)، المجلة العربية للدراسات الأمنية والتدريب، ع 58، مج 29، د، ت، ص، ص 90.

[7] جمال براهيمي ، مرجع سابق، ص 19.

وذلك بموجب المادة 42 من القانون رقم 2004-575،[1] أيضا القانون الكندي الذي وسع من مفهوم المادة 487 من قانون العقوبات لتصبح تشمل تفتيش بيانات وبرامج الحاسوب.[2]

أما إذا جئنا إلى موقف المشرع الجزائري فنجد بأنه أقر بإمكانية تفتيش النظام المعلوماتي وذلك بموجب المادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث أجازت الدخول بغرض التفتيش ولو عن بعد إلى:

-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزمة فيها؛

-منظومة تخزين معلوماتية.

وبهذا يكون المشرع الجزائري قد إستحدث نصوص قانونية تجيز تفتيش الكيان المنطقي للنظام المعلوماتي، وهو ما أقرته أيضا الإتفاقية الأوربية المتعلقة بالجريمة الإلكترونية في الفقرة الأولى من المادة 19 منها وذلك حينما أجازت للدول الأطراف إنخاذ التدابير اللازمة التي تمكن من تفتيش نظام معلوماتي أو جزء منه والبيانات التي يتم تخزينها فيه، ومن خلال ما تم عرضه فإن هناك إمكانية تفتيش الكيان المنطقي للنظام المعلوماتي الخاص بشركات المساهمة، لكن رغم هذه الإمكانية إلا أنه يتم تنفيذه بصعوبة خاصة إذا ما كان هناك نقص خبرة لدى الفريق القائم بتنفيذه، وهنا تظهر أهمية وضرورة توفر الصفات الواجب توفرها في المحقق والتي سبق وأشرنا إليها.

وأمام صعوبات تفتيش الكيان المنطقي للنظام المعلوماتي لشركات المساهمة قد يثور إشكال آخر يتمثل فيما إذا كان هذا النظام المعلوماتي متصلا بنظام آخر موجود داخل الإقليم الوطني أو كان متصلا بنظام آخر ولكن موجود خارج الإقليم الوطني، ففي هذه الحالة تكون أمام عائق خطير كون أن البيانات المراد البحث عنها والتي قد تمكن من كشف الجريمة موجودة وموزعة عبر عدة أنظمة معلوماتية.

بالنسبة للحالة الأولى والتي تكون البيانات محل البحث موجودة في نظام معلوماتي آخر ويتم الولوج إليها من النظام المعلوماتي الأول المراد تفتيشه نجد بأن المشرع الجزائري قد أجاز تمديد إجراء

---

[1] لامية مجدوب، مرجع سابق، ص 112.

[2] صالح شنين، مرجع سابق، ص 242.

التفتيش إلى ذلك النظام المعلوماتي بعد إعلام السلطة القضائية المختصة بذلك، وهذا حسب ما ورد في الفقرة 2 من المادة 5 من القانون 09-04.

ومن التشريعات التي نادت أيضا بضرورة تمديد التفتيش نجد الفقه الألماني من خلال القسم 103 من قانون الإجراءات الجزائية وكذا التشريع الهولندي من خلال المادة 25 من مشروع قانون الحاسوب والذي إشترط أن تكون تلك المعلومات على درجة من الأهمية في إظهار الحقيقة.[1]

أما فيما يتعلق بالحالة الثانية التي تكون فيها المعلومات محل البحث موجودة في نظام معلوماتي يقع خارج إقليم الدولة، فكثيرا ما يلجأ الجناة خاصة إذا كانوا من موظفي الشركة إلى تخزين بياناتهم في نظام معلوماتي خارج الإقليم الذي توجد به الشركة التي يعملون بها وذلك بهدف طمس معالم الجريمة وإعاقة عملية التحقيق في حال إكتشافها،[2] ففي إحدى جرائم الإحتيال قام الجاني بتنفيذ الجريمة من الحاسوب المتواجد بألمانيا والذي كان متصلا بمجموعة من الحواسيب المتواجدة بسويسرا وذلك بتحريف المعلومات بهذه الحواسيب إنطلاقا من الحاسوب الأول، فلم يكن أمام السلطات القضائية الألمانية سوى طلب المساعدة المتبادلة حتى تتمكن من الحصول على تلك المعلومات.[3]

وفي هذا الصدد نجد بأن المشرع الجزائري ومن خلال الفقرة 3 من المادة 5 من القانون 09-04 قد أقر بإمكانية تفتيش النظام المعلوماتي المتصل حتى وإن كان خارج الإقليم الوطني، عن طريق مساعدة السلطات الأجنبية وذلك طبقا للإتفاقيات الدولية ذات الصلة، ففي الجرائم الإلكترونية في إطار شركات المساهمة لا يمكن التقيد بتفتيش الكيان المادي والمنطقي للنظام المعلوماتي فحسب، بل أن الطابع المعقد والشائك لهذه الجرائم تفرض إجراء تفتيش إلكتروني وإن كان عابرا للحدود الإقليمية حتى يتم كشفها والتوصل إلى مرتكبيها.

2-الضبط في الجريمة الإلكترونية في إطار شركات المساهمة: بعد إجراء التفتيش في الجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة النتيجة التي يفضي إليها هذا الإجراء هو ضبط أدلة تستخلص من عملية التفتيش، والضبط المقصود منه وضع اليد على كل شيئ يتصل بهذه

---

[1] خدوجة الذهبي ، مرجع سابق، ص ص 221، 222.

[2] لامية مجدوب، مرجع سابق، ص 113.

[3] خدوجة الذهبي ، مرجع سابق، ص 22.

الجريمة ويكون من شأنه كشف حقيقتها وحقيقة مرتكبها،[1] وهو المراد الأساسي من إجراء التفتيش وضبط الأشياء قد تكون أدوات أستعملت في إرتكابها أو أشياء ناتجة عنها أو غير ذلك مما يفيد في إظهار الجريمة،[2] وبالتالي فالضبط الذي يتم في الجرائم الإلكترونية في إطار هذه الشركات هو أن يتم وضع اليد على المكونات المادية والمنطقية للنظام المعلوماتي والتي قد تفيد في كشف هذه الجرائم، إلا أنه تعترضه هو الآخر صعوبات ومشكلات باعتبار أن الضبط لا يمكن أن يتم في الأصل إلا على الأشياء المادية،[3] وعليه فعملية ضبط الكيان المادي للنظام المعلوماتي لشركات المساهمة لا تثير أية إشكالات، إذ من الممكن جدا ضبط أجهزة حواسيبها بمختلف مكوناتها كوحدات الذاكرة الرئيسية وحدة المخرجات كالشاشة وحدات التخزين،[4] لكن الإشكال الذي يثار هو حينما يتعلق الضبط بالكيان المنطقي للنظام المعلوماتي.

حيث أن هناك من يرى بأنه من غير الممكن أن يكون هذا الكيان محلا للضبط إلا إذا تم إفراغه في كيان مادي ملموس،[5] وذلك من خلال التصوير الفتوغرافي أو عن طريق نقلها على دعامة أو غير ذلك من الوسائل المادية،[6] ويستند هذا الرأي إلى كون النصوص القانونية التي تتعلق بالضبط يكون محل تطبيقها الشيئ المادي الملموس فقط مثل الفقه الألماني واللوكسمبرجي،[7] لذلك حتى يتم حل هذا الإشكال يتطلب الأمر أن يكون هناك تدخل تشريعي حتى يتم التوسيع من دائرة الأشياء التي

---

[1] عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، ط 1، القاهرة، المركز القومي للإصدارات القانونية، 2012، ص 320.

[2] عادل بن عبد العزيز بن صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، ط 1، السعودية، دار كنوز إشبيليا للنشر والتوزيع، 2017، ص ص 127، 128.

[3] صالح شنين، مرجع سابق، ص 253.

[4] عبد الصبور عبد القوي علي مصري، منال عبه اللاه عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، مرجع سابق، ص ص 340، 341.

[5] عبد القادر فلاح ، "حجز وحفظ المعطيات في الجريمة الإلكترونية، مرجع سابق، ص 180.

[6] بثينة حبيباتني ، مرجع سابق، 333.

[7] فايز محمد راجح غلاب، مرجع سابق، 343.

يمكن إخضاعها لعملية الضبط،[1] لتشمل إلى جانب الأشياء المادية البرامج والبيانات والمعلومات التي تكون في الشكل الإلكتروني.

فنجد بأن التشريع الفرنسي وبموجب التعديلات التي قام بإدخالها على قانون الإجراءات الجزائية نص على إلزامية نسخ البيانات التي يتم التحصل عليها من تفتيش النظام المعلوماتي على دعامات وهو ما ذهب إليه أيضا المشرع البلجيكي،[2] كما تدخل المشرع الجزائري في هذا الشأن ومواجهة مشكلة ضبط الكيان المنطقي للنظام المعلوماتي وذلك بموجب القانون 09-04 في المادة 6 منه، حيث أجاز لسلطة التفتيش عند إكتشافها معطيات مخزنة في نظام معلوماتي وتكون ذات فائدة في الكشف عن الجرائم ومرتكبيها ولا يكون هناك داعي لحجز كافة النظام، يتم فقط نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز، وخلال عملية الضبط يجب الحرص على سلامة معطيات النظام المعلوماتي.

وفي حالة ما إذا إستحال القيام بإجراء الحجز يجب على السلطة التي تقوم بعملية التفتيش اللجوء إلى إستخدام التقنيات الملائمة قصد المنع من الوصول إلى المعطيات التي يتضمنها النظام المعلوماتي أو إلى نسخها التي تكون موضوعة تحت تصرف الأشخاص المخولين باستعمال ذلك النظام هذا وفقا لما ورد في المادة 7 من القانون 09-04، وبهذا يكون المشرع الجزائري حسم موقفه بخصوص هذه المسألة وأقر بإمكانية ضبط الكيان المنطقي عن طريق حجز معطياته، وذلك وفق طريقتين تتمثل الأولى في نسخ المعطيات محل البحث والثانية عن طريق إستعمال التقنيات اللازمة التي تمنع من الوصول إلى تلك المعطيات، كأن يتم مثلا تجميد التعامل مع أجهزة حواسيب الشركة أو أحد القطع التي تتكون منها كون أن الوصول إليها يشكل خطرا على الشركة.

3-الخبرة الفنية في الجرائم الإلكترونية في إطار شركات المساهمة: إن عملية تفتيش النظام المعلوماتي لشركات المساهمة وضبط الأدلة التي تفيد في كشف حقيقة الجرائم الإلكترونية التي تتعرض لها هذه الشركات، تتطلب في كثير من الأحيان الإستعانة بالخبرة الفنية وذلك راجع إلى

---

[1] صالح شنين، مرجع سابق، ص 255.

[2] ليندا بن طالب ، الدليل الإلكتروني ودوره في الإثبات الجنائي دراسة مقارنة، مرجع سابق، ص 66.

الجانب التقني والفني المعقد التي ترتكب به تلك الجرائم ومن خلال هذه النقطة نتعرف على القواعد التي تحكم إجراء الخبرة الفنية في مجال الجرائم الإلكترونية التي قد تتعرض لها.

تعد الخبرة من إجراءات التحقيق وهي تتعلق بوقائع تستوجب عملية البحث فيها وتقديرها الإستعانة بشخص مختص حتى يقدم رأيه الفني والتقني والذي لا يمكن للشخص العادي الوصول إليه،[1] أما في مجال الجريمة الإلكترونية فهي تلك التي يقوم شخص يدعى بالخبير وذلك عن طريق إستعانته بالمعلومات التقنية التي يحوزها والتي لا تتوفر لدى غيره من أجل الحصول على دليل إلكتروني لهذه الجرائم وكشف غموضها ،[2] حيث ترتبط الخبرة بالمهارات والمواهيب الخاصة في إستعمال الحاسوب والأنترنت وكذا معرفة التعامل مع التقنيات المعلوماتية.[3]

وللخبرة الفنية أهمية بالغة في الجريمة الإلكترونية في إطار شركات المساهمة حيث أن غيابها قد يترتب عليه فقدان الدليل أو التسبب في إتلافه وتدميره وذلك نتيجة عدم معرفة التعامل مع الجوانب التقنية لأجهزة الحواسيب،[4] وفي بعض الأحيان يتطلب الأمر الإستعانة بأكثر من خبير كون أن هناك بعض من هذه الجرائم في غاية التعقيد مما يستحيل على خبير واحد التعمق فيها والتعامل معها وبالتالي بدلا من مساعدته لجهة التحقيق قد يتسبب في فقدان الدليل،[5] حيث أنه من الصعب جدا أن يكون هناك خبير بإمكانه أن يتعامل مع كافة أنواع الجرائم التي تتعرض لها هذه الشركات وذلك لتعدد وتنوع أنماط الحواسيب والشبكات، كالجرائم التي تتعلق بنشر فيروسات التي تعمل على إتلاف الوحدات الرئيسية لحواسيب الشركة واختراق كلماتها المرورية قصد الإحتيال والحصول على الأموال،[6]

---

[1] خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، د، ط، الإسكندرية، دار الفكر الجامعي، 2020، ص 186.

[2] نبيهة قنفود، فوزي عمارة، (الخبرة التقنية في مجال إثبات الجريمة الإلكترونية)، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، ع 2، مج 36، الصادر في أكتوبر 2022، ص 408.

[3] مختار تابري، (الخبرة في الجريمة المعلوماتية)، مجلة الحوار المتوسطي، ع 3، مج 11، الصادر في ديسمبر 2020، ص 389.

[4] فراس نايف تايه، (دور الخبرة في جريمة التزوير المعلوماتية)، المجلة القانونية ، مجلة متخصصة في الدراسات والبحوث القانونية، ع 2، مج 14، الصادر في 2022، ص 677.

[5] فايز محمد راجح غلاب، مرجع سابق، ص، ص 362، 363.

[6] فراس نايف تايه، مرجع سابق، ص 677.

ومن ذلك ما وقع في إحدى الشركات حين قام أحد الأشخاص بزرع قنبلة منطقية بنظامها المعلوماتي فقامت الشركة بالإستعانة بخبير قصد التأكد من الجريمة وإزالة مفعول القنبلة قبل أن تقوم بإبلاغ السلطات المختصة عما تعرضت له، ورغم أن الخبير نجح في كشف القنبلة المنطقية وإزالتها لكن أثناء عملية التحقيق إتضح بأنه تسبب في إتلاف كل الأدلة على وجودها،[1] لذلك من الضروري جدا أن يكون الخبير في مجال الحواسيب الآلية ملما بالجانب التقني والفني لها، كما يتعين عليه مسايرة ومواكبة التطورات الحاصلة في مجال تكنولوجيات الإعلام والإتصال وإن كانت تطوراتها السريعة والمتلاحقة تصعب من عملية تتبعها واستيعابها.

ونظرا لأهمية الخبرة فقد سارعت معظم دول العالم إلى تنظيم الأعمال الخاصة بالخبرة بموجب نصوص ضمن القوانين المتعلقة بالجرائم الإلكترونية، ومن ذلك نجد القانون البلجيكي الصادر في 23 نوفمبر 2000 إذ نص في المادة 88 منه على أنه، بإمكان قاضي التحقيق وكذا الشرطة القضائية الإستعانة بخبير ذو إختصاص وذلك حتى يقدم المعلومات الواجبة التي توضح طريقة تشغيل النظام والولوج إليه وإلى البيانات المخزنة فيه والمعالجة والمنقولة من خلاله وذلك بشكل بسيط ومفهوم، كما يمنح هذا القانون أيضا الحق للسلطة المكلفة بالتحقيق في أن تطلب من الخبير بأن يشغل النظام أو يبحث فيه، أو حتى عمل نسخة عن البيانات المطلوبة في عملية التحقيق أو حتى سحب تلك البيانات التي تم تخزينها أو تحويلها أو نقلها وفقا للطريقة التي تحددها جهة التحقيق،[2] أيضا التشريع الفرنسي الذي نص هو الآخر على الإستعانة بالخبرة في مجال الجرائم الإلكترونية وذلك في المادة 60 من قانون الإجراءات العقابية حيث خول لوكيل الجمهورية وكذا ضبط الشرطة القضائية تسخير كل شخص أو مؤسسة أو تنظيم سواء كان خاص أو عام أو كل إدارة عامة تكون لهم معرفة بالنظام المعلوماتي ودراية بمعالجة المعطيات وذلك بغية تقديم معلوماتهم في شكل إلكتروني أي إرسالها عن طريق الحاسوب أو شبكات الإتصال.[3]

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص، 363.

[2] محمد بودالي ، مرجع سابق، ص 312.

[3] إلهام بن خليفة، مرجع سابق، ص 298.

وبطبيعة الحال المشرع الجزائري سارع هو الآخر إلى وضع نصوص قانونية تتعلق بالخبرة الفنية في مجال الجرائم الإلكترونية، وفي هذا نجد ما نصت عليه المادة 5 من القانون 09-04 في فقرتها الأخيرة حيث منحت للسلطات المكلفة بإجراء التحري تسخير كل شخص يكون على دراية بعمل النظام المعلوماتي الذي هو محل البحث، أو بالتدابير المتخذة قصد حماية المعطيات المعلوماتية التي يتضمنها من أجل مساعدتها وتزويدها بكافة المعلومات الضرورية التي تمكنها من إنجاز مهمتها.

كما نص في ذات القانون في المادة 13 منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ومن بين المهام المنوطة بالهيئة القيام بتجميع المعلومات وإنجاز الخبرات القضائية.

وما يجب التنويه إليه هنا هو أنه رغم أهمية الخبرة في هذا النوع من الجرائم غير أن السلطة غير ملزمة بأخذ رأي الخبير وإنما لها مطلق الحرية في تقديره، ولها أن تأمر بإجراء خبرة تكميلية كما أنه لا يحق لها أن تفند ما توصل إليه الخبير إلا بموجب سند فني،[1] ويتم تنفيذ الخبرة في الجرائم الإلكترونية التي ترتكب على شركات المساهمة من خلال فحص أجهزة حواسيبها التي كانت محلا لهذه الجرائم وذلك عبر مراحل بداية تكون بحجز البيانات،[2] التي قد يخلفها الجاني وراءه مثل الكلمات التي إستخدمها والمواقع التي أرسل إليها.

لتأتي بعدها مرحلة حفظ تلك البيانات من خلال عمل نسخ عليها وفي حالة ما إذا تم حذف تلك البيانات من طرف الجاني يكون على الخبير إستعادتها حتى يتمكن من إتمام تقرير الخبرة ثم يقوم بتقييم تلك البيانات حتى يتم تحديد وسائل هذه الجرائم بشكل دقيق، ليعاد بعد ذلك بناء القضية من جديد ومن خلال توضيح مجريات إرتكاب الجريمة على هذه الشركة،[3] وبعد الإنتهاء يقوم الخبير بإعداد تقرير خبرة يتضمن حوصلة عن النتائج التي توصل إليها من خلال عمله الفني والتقني.

---

[1] محمد بودالي ، مرجع سابق، ص 311.

[2] خدوجة الذهبي ، مرجع سابق، ص 237.

[3] المرجع نفسه، ص، ص 237، 238.

ومن كل ما تم عرضه تبقى الخبرة الفنية إجراء لا بد منه حتى يتم إزاحة اللبس عن هذه الجرائم التي تتعرض لها شركات المساهمة، إذ من الصعب جدا كشفها من قبل أشخاص عاديين دون الإستعانة بخبراء متخصصين.

المطلب الثاني:

الجهة القضائية المختصة بالفصل في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة

كون أن الجرائم الإلكترونية في إطار شركات المساهمة تتم في بيئة إلكترونية معقدة ومتشعبة متجاوزة بذلك الحدود الإقليمية إذ أن أثرها لا ينحصر في نطاق إقليمي محدد، كما لو أن إحدى الشركات الموجودة في الجزائر تعرضت لعملية إختراق في نظامها المعلوماتي من قبل جاني متواجد في دولة أخرى أو قد يحدث العكس، بأن يقوم الجناة المتواجدين على الإقليم الوطني باختراق شركة في دولة أجنبية، الأمر الذي يثير العديد من الإشكالات التي تتعلق بالإختصاص القضائي سواء على المستوى الوطني أو الدولي، هذا ما نوضحه من خلال هذا المطلب وذلك بالتعرض إلى القانون الواجب التطبيق على هذه الجرائم **(فرع أول)** ثم الجهة القضائية التي تكون مختصة إقليميا بالنظر فيها **(فرع ثاني)**.

الفرع الأول:

القانون الواجب التطبيق على الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

الإشكال الذي يطرح في هذه الحالة هو أن يكون تنازع في الإختصاص بين أكثر من دولة فقد يحدث أن تتعرض شركة مساهمة يوجد مقرها في دولة ما وذلك من قبل شخص أجنبي فأي القوانين يتم تطبيقها عندئذ؟ إذ من الممكن أن يتم إخضاع الجريمة لقانون الدولة الأولى كونها أرتكبت على إقليمها وذلك إستنادا إلى مبدأ الإقليمية، ويمكن إخضاعها لقانون دولة الجاني إستنادا لمبدأ الإختصاص الشخصي، كما يمكن بالنظر لأهمية هذه الشركة كون أن المساس بها يعد تهديدا ومساسا بالمصالح الأساسية الاقتصادية للدولة التابعة لها مما يعني إمكانية تطبيق قانون هذه الدولة على الجريمة هذا ما نوضحه فيما يلي:

أولا: القانون الواجب التطبيق على الجرائم الإلكترونية المرتكبة في الإقليم الوطني على شركات المساهمة إستنادا لمبدأ الإقليمية.

مبدأ الإقليمية يقتضي بأن تخضع الجرائم التي ترتكب في إقليم الدولة لقانونها الجنائي الوطني كما تكون محاكمها هي الجهة المخولة بنظر الدعوى،[1] فوفقا لهذا المبدأ فإن قوانين الدولة لا تمتد خارج إقليمها لتسري في نطاق دولة أخرى حتى لا تصطدم بسيادتها، وبتطبيق هذا المبدأ لا يكون لجنسية الجاني أي إعتبار سواء كان وطني أو أجنبي كون أن العبرة بمكان إرتكاب الجريمة.

وبالرجوع إلى قانون العقوبات الجزائري نجد بأن المشرع قد إعتمد على مبدأ الإقليمية من خلال نص المادة 3 في فقرتها الأولى والتي جاء فيها بأن قانون العقوبات يطبق على جميع الجرائم التي يتم إرتكابها في أراضي الجمهورية، وهو ما تم النص عليه أيضا في قانون العقوبات الفرنسي الذي نص في المادة 113-2 على أنه يتم تطبيق القانون الفرنسي إذا أرتكبت جريمة أو أحد العناصر المكونة لها على إقليمها،[2] كما نص المشرع الجزائري في المادة 586 من قانون الإجراءات الجزائية على أنه يمكن إعتبار الجريمة مرتكبة في الإقليم الجزائري عندما يكون عمل من أعمالها المميزة لأحد أركانها المذكورة لها قد تم في الجزائر، كما أكدت على هذا المبدأ الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي نصت في المادة 30 منها على أنه تلتزم كل دولة طرف بتبني الإجراءات اللازمة من أجل مد إختصاصها على أي جريمة منصوص عليها في الفصل الثاني من الإتفاقية إذا ما أرتكبت كليا أو جزئيا أو تحققت في إقليم الدولة الطرف.

ومن خلال ما سبق ذكره يتضح بأن المشرع الجزائري قد إعتبر بأن المحاكم الجزائرية تكون مختصة في نظر الجرائم إذا ما أرتكبت كامل أركانها أو أحد الأفعال المكونة لأركانها على الإقليم الوطني، لذلك فإنه في حالة إرتكاب جريمة إلكترونية فوق الإقليم الجزائري ضد شركات المساهمة فإن المحاكم الوطنية تكون هي صاحبة الولاية بنظر تلك الجرائم.

---

[1] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص 78.

[2] Art: 113-2: La loi pénale français est applicable aux infraction commises sur le territoire de la république.
L'infraction est réputée commise sur le territoire de la république des lors qu'un ses faits constitutifs a eu lieu sur ce territoire.

ثانيا: القانون الواجب التطبيق على الجرائم الإلكترونية المرتكبة خارج الإقليم الوطني على شركات المساهمة إستنادا لمبدأ الشخصية والعينية.

بالرجوع إلى المادة 3 من قانون العقوبات السالف ذكرها واستنادا على مبدأ الإقليمية فإن الأصل هو أن القانون الجزائري لا يسري على الجرائم التي ترتكب خارج الإقليم الوطني، غير أن المشرع الجزائري خرج عن هذه القاعدة وأورد إستثنائين يجوز بمقتضاهما تطبيق القانون الجزائري حتى لو كانت الجريمة قد أرتكبت في بلد أجنبي وذلك إستنادا على مبدأ الشخصية والعينية.

1-مبدأ الشخصية: يعرف هذا المبدأ بأنه سريان القانون الوطني على الجرائم التي ترتكب في الخارج من قبل أشخاص يحملون الجنسية الجزائرية، لذلك فهذا المبدأ يخاطب الجاني كما يعتبر مكملا لمبدأ الإقليمية كونه يطبق على الجناة الذين يرتكبون جرائمهم خارج الإقليم الوطني،[1] فحتى لا يتم إفلاتهم وملاحقتهم من جهة واتخاذ الوطن كملجأ للهروب من جرائمهم من جهة أخرى تم الإعتماد على هذا المبدأ والذي نص عليه المشرع الجزائري في المادة 582 من قانون الإجراءات الجزائية التي جاء فيها " كل واقعة موصوفة بأنها جناية معاقب عليها من القانون الجزائري، إرتكبها جزائري في خارج إقليم الجمهورية يجوز أن تتابع ويحكم فيها في الجزائر" وكذا المادة 583 التي نصت على أنه كل واقعة موصوفة بأنها جنحة سواء في نظر القانون الجزائري أم في نظر تشريع القطر الذي أرتكبت فيه يجوز المتابعة من أجلها والحكم فيها في الجزائر إذا كان مرتكبها شخص جزائري.

كما تم النص على هذا المبدأ في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك في المادة 30 فقرة د والتي جاء فيها " تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد إختصاصها على أي جريمة منصوص عليها في الفصل الثاني من هذه الإتفاقية إذا تم إرتكابها من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي لمكان إرتكابها".

فمن خلال جملة النصوص القانونية التي تم عرضها تكون المحاكم الجزائرية هي صاحبة الإختصاص في الجرائم الإلكترونية التي ترتكب ضد شركات المساهمة من طرف شخص يحمل

[1] عبد الرحمان خلفي ، بلال عثماني ، (حماية الرعايا الجزائرين بالخارج في إطار القانون الجنائي)، مجلة الدراسات حول فعلية القاعدة القانونية، ، ع 1، مج 3، الصادر في 2019، ص 222.

الجنسية الجزائرية خارج الإقليم الوطني كأن يقوم مثلا جزائري في بلد ما بالإعتداء على العلامة التجارية لهذه الشركات قصد الإحتيال على الأشخاص مما يسبب لها أضرار، حيث أنه في هذه الحالة تتولى الجهات القضائية الوطنية ملاحقة الجاني ومحاكمته، لكن ما تجدر الإشارة إليه هو أن تطبيق مبدأ الشخصية على الجرائم الإلكترونية التي يتم إرتكابها على شركات المساهمة تعترضه بعض الصعوبات والعوائق منها:

بما أن هذا المبدأ يقوم في الأساس على الطرف الجاني من أجل كشف هويته وبالتالي التعرف على جنسيته والحصول على هذه المعلومات أمر في غاية الصعوبة، كون أن الجاني في الجرائم الإلكترونية التي يرتكبها ضد شركات المساهمة يتجنب إستعمال إسمه الحقيقي وإنما يتخفى خلف أسماء مستعارة كما يعمد إلى التشفير،[1] أيضا نجد بأن عدد الدول التي قامت بالتوقيع على الإتفاقية المتعلقة بتسليم المجرمين يعد قليل جدا وذلك مقارنة مع الدول التي تشهد إنتشارا واسعا لشبكة الأنترنت،[2] كما أن محاكمة الجاني المقيم في بلد آخر فإن الأمر يتطلب جملة من الإجراءات الطويلة والمعقدة والمكلفة أيضا ونفس الشيئ بالنسبة للأحكام التي يتم إصدارها في الخارج،[3] وأمام هذه الإشكالات فإن الرأي الذي تم طرحه يتمحور حول إيجاد قانون دولي جنائي وذلك مثلما هو الحال في القانون الجنائي الدولي الخاص حتى يتم تطبيقه على الجرائم الإلكترونية،[4] خاصة وأنها باتت تستهدف شركات تمثل الدعائم التي يقوم إقتصاد العديد من الدول.

2-مبدأ العينية: يعني هذا المبدأ بأن يكون للدولة الحق في تطبيقها للقانون الوطني وذلك بصرف النظر عن المكان التي تم فيه إرتكاب الجريمة وأيا كانت جنسية مرتكبها، كون أن تلك الجريمة تمس

---

[1] أمال فكيري، (إشكالات الإثبات والإختصاص في جرائم تكنولوجيا الإعلام والإتصال العابرة للحدود)، مجلة العلوم القانونية والسياسية، ع 17، الصادر في جانفي 2018، ص 641.

[2] محمد بودالي ، مرجع سابق، ص 332.

[3] بثينة حبيباتني ، ص 376.

[4] فايز محمد راجح غلاب، مرجع سابق، ص 388.

بالمصالح الأساسية والجوهرية لتلك الدولة،[1] فهو مبدأ يكرس حق الدولة في حماية مصالحها من الإعتداء.

وتم تكريس هذا المبدأ في القانون 09-04 والذي نص في المادة 15 منه على أنه تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني عندما يرتكبها أجنبي وتكون تستهدف المؤسسات الجزائرية أو الدفاع الوطني أو المصالح الإستراتجية للإقتصاد الوطني، كما تم النص عليه أيضا في المادة 30 فقرة هـ من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي جاء فيها " تتبنى كل دولة طرف الإجراءات الضرورية لمد إختصاصها على أية جريمة منصوص عليها في الفصل الثاني من الإتفاقية إذا كانت تمس بأحد المصالح العليا للبلاد".

وبالرجوع إلى المادة 15 من القانون 09-04 نجد بأن من بين المصطلحات الواردة فيها "المصالح الإستراتجية للإقتصاد الوطني" وهذه من بين شروط تطبيق مبدأ العينية، وبمقابل ذلك فإن شركات المساهمة تمثل إحدى إستراتجيات الاقتصاد الوطني وأن المساس بها يعد مساس بالإقتصاد، وبذلك يكون المشرع الجزائري قد نص على إختصاص القضاء الوطني إذا ما تم إرتكاب جريمة إلكترونية خارج الإقليم الوطني من طرف أجنبي تستهدف إحدى شركات المساهمة كأن يتم الولوج إلى النظام المعلوماتي الخاص بها والتجسس عليها، كما نشير إلى أنه حتى يتم متابعة الجاني ومحاكمته وفقا للقانون الجزائري يجب أن يتم إلقاء القبض عليه في الجزائر أو أن الحكومة الجزائرية قد حصلت على تسليمه وفقا لإجراءات تسليم المجرمين، هذا حسب ما ورد في المادة 588 من قانون الإجراءات الجزائية.

وما نشير إليه أن الإستعانة بمبدأ العينية في الجرائم الإلكترونية إصطدم هو الآخر ببعض الإشكالات التي تعيق تطبيقه، والتي منها تعارض هذا المبدأ مع مبدأ الإقليمية وذلك عندما تكون الجريمة المرتكبة إستنادا إلى مبدأ العينية مجرمة كذلك في قانون البلد الذي أرتكبت فيه، وبالتالي

[1] أمال فكيري، مرجع سابق، ص 641.

نكون أمام نتيجة تنازع إختصاص بين هاتين الدولتين، [1] أيضا ما يزيد من صعوبة تطبيقه هو في حالة ما إذا كان الجاني حاملا لجنسية الدولة التي أرتكبت فيها جريمة الإعتداء على مصالح الدولة الأخرى، فبطبيعة الحال أن الدولة الأولى لا يمكنها أن تسلم رعاياها لدولة أخرى.[2]

لذلك من خلال ما تم التطرق إليه وإن كان لا يوجد ما يحول دون إعمال المبادئ الثلاثة السابقة والإعتماد عليها في الجرائم الإلكترونية المرتكبة في إطار شركات المساهمة، غير أنه قد تثار عدة إشكالات تعيق عملية تطبيقها مثلما سبق وتمت الإشارة إلى ذلك، وهذا ما يجعل من الإختصاص القضائي يتسم بنوع من التعقيد لذلك نرى بأن الأمر يتطلب أن يكون هناك إتفاق دولي ينظم المسألة وذلك عن طريق عقد إتفاقيات سواء كانت ثنائية أو جماعية.

الفرع الثاني:

الجهة القضائية المختصة إقليميا بنظر الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

بعد أن يتم إسناد الإختصاص إلى القضاء الوطني بنظر الجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة يتم بعدها تحديد الجهة القضائية التي يتم طرح الدعوى أمامها، الأمر الذي قد ينجم عنه إشكالية تتعلق بالإختصاص القضائي المحلي أو الإقليمي بمعنى يكون هناك تنازع بين أكثر من جهة قضائية على المستوى الوطني أي داخل إقليم الدولة.

والأصل أن الإختصاص المحلي للجهات القضائية يتحدد بناء إما على مكان وقوع الجريمة أو المكان الذي يمثل إقامة الشخص المشتبه فيه، أو المكان الذي يتم فيه إلقاء القبض على الجاني وهذا وفقا لما ورد في المواد 37، 40 و 329 من قانون الإجراءات الجزائية.

غير أن المشرع الجزائري وبمناسبة تعديله لقانون الإجراءات الجزائية بموجب القانون 04-14،[3] قام بتمديد نطاق الإختصاص المحلي لكل من وكيل الجمهورية، قاضي التحقيق وكذا قضاة الحكم

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص 391.

[2] دلال مولاي ملياني ، مرجع سابق، ص 258.

[3] قانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج، ر، ع 71 الصادر في 10 نوفمبر 2004.

إلى دائرة إختصاص محاكم أخرى في بعض الجرائم والتي منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك نظرا لخطورتها وتعقيدها متجها بذلك نحو فكرة التخصيص القضائي والتي تجسدت فعلا بصدور المرسوم التنفيذي رقم 06-348،[1] والذي نص في مواده 2، 3، 4، 5 على تمديد الإختصاص المحلي لأربعة محاكم على المستوى الوطني، ولم يتوقف عند هذه الأقطاب فقط بل عمد أيضا إلى إستحداث قطب جزائي وطني متخصص في المتابعة والتحقيق في هذه الجرائم بغية تعزيز وتكريس فكرة التخصص القضائي وكان ذلك بموجب الأمر رقم 21-11،[2] كما كان قد أنشأ سنة 2020 القطب الجزائي الاقتصادي والمالي وذلك بموجب الأمر رقم 20-04،[3] هذا ما سنوضحه من خلال هذا الفرع وذلك بالتطرق إلى الأقطاب الجزائية أولا ثن القطب الجزائي الوطني، بعدها القطب الجزائي الاقتصادي والمالي.

أولا: الأقطاب الجزائية المتخصصة.

كان هدف المشرع من وراء إنشائه لفكرة الأقطاب الجزائية المتخصصة هو سد العجز المسجل نتيجة غياب الهيئات القضائية المؤهلة والمتخصصة في مكافحة الجرائم الإلكترونية، خاصة وأن القضاء العادي أثبت عجزه في عدة مرات عجزه عن مواجهة هذا النوع من الجرائم نتيجة طابعها التقني المعقد التي تتسم به.

1-تعريف الأقطاب الجزائية المتخصصة: رغم أهمية هذه الأقطاب في مجابهة التطور الذي وصلت إليه الجرائم الإلكترونية غير أن المشرع لم يخصها بتعريف محدد، ولكن باستقراء النصوص القانونية المنظمة لها يمكن تعريفها بأنها تلك الجهات القضائية التي تكون متخصصة في نظر بعض الجرائم

---

[1] مرسوم تنفيذي رقم 06-348 مؤرخ في 5 أكتوبر 2006، يتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج، ر، ع 63 الصادر في 8 أكتوبر 2006.

[2] الأمر رقم 21-11 مؤرخ في 25 غشت 2021 يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج،ر، ع 51 الصادر في 26 غشت 2021.

[3] الأمر رقم 20-04 مؤرخ في 30 غشت 2020 يعدل ويتمم الأمر رقم 66-155 مؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج،ر، ع 51 الصادر في 31 غشت 2020.

المحددة في القانون،[1] والتي من بينها الجرائم الإلكترونية وبذلك فهي ليست أقطاب خاصة تخرج عن دائرة النظام القضائي الساري والمعمول بها،[2] كما أنها لا تنشط وفقا لإجراءات قانونية خاصة وإنما تخضع لذات الإجراءات القانونية التي تعمل بها الجهات القضائية العادية،[3] وفي هذا نجد بأن المادة 40 مكرر من قانون الإجراءات الجزائية قد نصت على أنه تطبق قواعد هذا القانون التي تتعلق بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع إختصاصها المحلي طبقا للمواد 37، 40 و 329 من هذا القانون.

وللإشارة فإن هذه الأقطاب قد بدأت في العمل بشكل فعلي سنة 2008 وكان ذلك بإعطاء إشارة إنطلاقها بشكل رسمي في كل من الجزائر العاصمة في 26 فيفري 2008، قسنطينة 3 مارس 2008، وهران 5 مارس 2008 في حين كان تدشين القطب الجزائي المتخصص لمحكمة ورقلة في 19 مارس 2008.[4]

2-نطاق إختصاص الأقطاب الجزائية المتخصصة: تعد مسألة تحديد نطاق إختصاص هذه الأقطاب مسألة جوهرية وفي غاية الأهمية حيث أن لها إختصاصين نوعي وإقليمي.

بالنسبة للإختصاص النوعي فهو أن تختص هذه الأقطاب فقط بنظر الجرائم التي تم تحديدها في المواد 37 فقرة 2، المادة 40 فقرة 2 والمادة 329 في فقرتها الأخيرة وتتمثل في ستة أنواع من الجرائم، جرائم المخذرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا الجرائم الماسة بأنظمة المعالجة الآلية

---

[1] جمال الدين بوقرة ، جمال الدين عنان ، (القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 1، مج 7، ، الصادر في جوان 2022، ص 1676.

[2] خديجة عميور ، (قواعد إختصاص الأقطاب الجزائية للنظر في جرائم الفساد)، مجلة الدراسات في الوظيفة العامة، ع 2، الصادر في 2014، ص 134.

[3] إيمان رتيبة شويطر، (الأقطاب الجزائية المتخصصة كتوجه لمكافحة جرائم الأعمال)، مجلة البحوث في العقود وقانون الأعمال، ع 1، مج 7، الصادر في 2022، ص 52.

[4] محمد بكرار شوش، (الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري)، مجلة دفاتر السياسة والقانون، ع 14، الصادر في 2016، ص 307.

للمعطيات و تعد من الجرائم الإلكترونية التي قد ترتكب في نطاق شركات المساهمة وقد تم ذكر هذه الجرائم على سبيل الحصر لا المثال.

لذلك فالأقطاب الجزائية المتخصصة تختص بنظر هذه الجرائم فقط، لكن ما ينبغي الإشارة إليه هو أن إختصاصها هذا لا يعتبر إختصاصا مانعا على غيرها من الجهات القضائية، وإنما يبقى الأمر متوقف على شرط المطالبة من طرف النائب العام والذي بعد تبليغه بملف القضية بإمكانه تركها تسير وفقا للإجراءات العادية أمام الهيئات القضائية العادية رغم أن الأمر في هذه الحالة يتعلق بإحدى أنواع الجرائم التي تكون من إختصاص تلك الأقطاب فنكون بذلك أمام إختصاص مشترك.[1]

أما بالنسبة للإختصاص الإقليمي لهذه الأقطاب فالمقصود منه هو الحدود التي وضحها المشرع الجزائري لقضاة النيابة العامة والتحقيق وكذا قضاة الحكم والتي يباشرون فيها ولايتهم في الدعوى التي يتم عرضها عليهم،[2] إذا ما تعلقت بإحدى الجرائم المحددة سابقا والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وبالرجوع إلى المرسوم التنفيذي رقم 06-348 السابق الإشارة إليه فقد تضمن تحديد أربعة محاكم تم توسيع إختصاصها المحلي ليشمل بذلك دوائر إختصاص محاكم أخرى وتتمثل تلك الأقطاب في:

-القطب الجزائي المتخصص لمحكم سيدي أمحمد (الجزائر) ويشمل محاكم المجالس القضائية لكل من الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، عين الدفلة مغطيا بذلك منطقة الوسط حسب المادة 2 من نفس المرسوم 06-348.

-القطب الجزائي المتخصص لمحكم قسنطينة ويشمل محاكم المجالس القضائية لكل من قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس، ميلة مغطيا بذلك نتطقة الشرق وهذا وفقا للمادة 3 من نفس المرسوم.

---

[1] إيمان رتيبة شويطر، مرجع سابق، ص 55.

[2] عبد الفتاح قادري، حيدرة سعدي، (آليات عمل الأقطاب الجزائية المتخصصة في جرائم الفساد)، مجلة العلوم الإنسانية لجامعة أم البواقي، ع 1، مج 8، الصادر في مارس 2021، ص 200.

-القطب الجزائي لمحكمة ورقلة ويشمل محاكم المجالس القضائية لكل من ورقة، أدرار تامنغست، إيليزي، تندوف، غرداية مغطيا بذلك منطقة الجنوب وفقا للمادة 4 من نفس المرسوم.

-القطب الجزائي لمحكمة وهران ويشمل محاكم المجالس القضائية لكل من وهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تيموشنت، غليزان مغطيا بذلك منطقة الغرب وفقا للمادة 5 من نفس المرسوم.

وما ينبغي أن نشير إليه هو أن تمديد الإختصاص المحلي بالنسبة لهذه الأقطاب هو من باب الجواز وليس من باب الجبر، فحينما نعود إلى المواد 37، 40، 329 من قانون الإجراءات الجزائية السالفة الذكر نجدها جميعا قد تضمنت عبارة " يجوز تمديد الإختصاص المحلي" لتكون بذلك كل من المحكمة الأصلية والمحكمة التي مدد إليها الإختصاص مخولتين بنظر الجريمة الإلكترونية، فعلى سبيل المثال أن هناك جريمة إلكترونية تم إرتكابها بولاية البويرة ضد إحدى شركات المساهمة بها، فالأصل في هذه الحالة أن محكمة البويرة هي التي تكون مختصة بنظر الدعوى، لكن بما أن الأمر بإحدى أنواع الجرائم التي تختص بها المحكمة التي مدد إليها الإختصاص وهي محكمة "سيدي أمحمد" بالجزائر العاصمة فيجوز لها أن تنظر فيها أيضا، فكلا المحكمتين مختصتين الأولى طبقا لقواعد الإختصاص المحلي العامة والثانية طبقا لنوع الجريمة المحددة قانونا.

3 الآليات الإجرائية لعمل الأقطاب الجزائية المتخصصة في الجرائم الإلكترونية الواقعة على شركات المساهمة: من خلال النصوص القانونية التي جاء بها المشرع الجزائري نجد بأنه لم يخص هذه الأقطاب بقواعد خاصة من أجل المتابعة وإنما تخضع الجرائم الإلكترونية التي تكون من إختصاص هذه الأقطاب لذات القواعد الإجرائية العامة التي تم النص عليها في قانون الإجراءات الجزائية والتي تطبق على باقي الجرائم.

فنجد بأن المادة 40 مكرر من القانون 04-14 بأنها نصت على أنه تطبق قواعد هذا القانون والتي تتعلق بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع إختصاصها المحلي طبقا للمواد 37، 40، 329 من هذا القانون، وذلك مع مراعاة أحكام المواد 40 مكرر1 إلى 40 مكرر5.

بمعنى أن نظام المحاكمة في الجرائم الإلكترونية أمام الأقطاب الجزائية المتخصصة يخضع لنفس القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، سواء تعلقت تلك القواعد بمبادئ المحاكمة كعلنية الجلسات مثلا شفافية المرافعات أو القواعد المتبعة لغاية إصدار الحكم، حيث أن القواعد الموضوعة من قبل المشرع هي قواعد عامة يكون على الجهات القضائية بغض النظر عن نوع ودرجة هذه الجهات الإلتزام بها كون أن هدفها هو حماية الحقوق وتكريس العدالة.[1]

لكن من جهة أخرى نجد بأن الأقطاب الجزائية المتخصصة تتمتع بنوع من الخصوصية تتعلق بالكيفية التي ينعقد بها إختصاصها، وطريقة إخطارها بالجرائم الإلكترونية التي تتعرض لها شركات المساهمة حتى تكون على إتصال بملف هذه الجرائم.

وبالعودة إلى قانون الإجراءات الجزائية نجده قد نص في مواده 40 مكرر1 إلى غاية 40 مكرر5 على الكيفية التي يتم من خلالها إخطار هذه الأقطاب، فحسب المادة 40 مكرر1 يجب على ضبط الشرطة القضائية أن يخبروا على الفور وكيل الجمهورية لدى المحكمة الواقع بها مكان إرتكاب الجريمة، وذلك من خلال تبليغه بأصل وكذا نسختين من إجراءات التحقيق ليقوم هذا الأخير بإرسال النسخة الثانية فورا إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة التي وسع إختصاصها.

أما المادة 40 مكرر2 فقد جعلت النائب العام وحده له صلاحية المطالبة بالإجراءات فورا وذلك إذا ما اتضح له بأن الجريمة الإلكترونية المرتكبة على هذه الشركة تندرج ضمن إختصاص المحكمة، ليتلقى بعدها ضباط الشرطة القضائية الذين يباشرون عملهم بدائرة إختصاص هذه المحكمة التعليمات مباشرة من وكيل الجمهورية لدى هذه الجهة القضائية.

كما يمكن للنائب العام لدى المجلس القضائي التابعة له المحكمة المختصة أن يطالب بالإجراءات وملف القضية في أي مرحلة من مراحل الدعوى، وإذا كان قد تم فتح تحقيق قضائي يقوم قاضي التحقيق بإصدار أمر بالتخلي عن الإجراءات وذلك لفائدة قاضي التحقيق لدى المحكمة التي وسع إليها الإختصاص هذا وفقا للمادة 40 مكرر3.

[1] إيمان رتيبة شويطر، مرجع سابق، ص 58.

فما نلاحظه هو أن المشرع قد أعطى للنائب العام لدى المجلس القضائي التابع له القطب الجزائي المتخصص السلطة التقديرية في التمسك بملف القضية والمطالبة بها، ودون أن يكون ملزما بمدة محددة في ذلك، كما أنه لم يتم وضع معايير معينة يستند إليها النائب العام حتى يطالب بملف القضية، وإن كان يمكن القول بأن خطورة الجرائم الإلكترونية ضد شركات المساهمة وخطورة مرتكبيها يمكن الإعتماد عليهما كمعيارين للمطالبة بملف القضية من جهة، ومن جهة أخرى فإن الإضرار بهذه الشركات هو إضرار بالإقتصاد الوطني.

أما بالنسبة للكيفية التي يمكن من خلالها للنائب العام المطالبة بملف القضية فيتم ذلك بموجب مراسلة وإن كان المشرع لم يضع نموذج أو شكل محدد لها، غير أن الواقع العملي أثبت البيانات الواجب توفرها فيها، كالجهة المرسلة –النيابة العامة لدى مجلس قضاء– الجهة المرسل إليها وهي التي بحوزتها ملف القضية، بالإضافة إلى البيانات المتعلقة بالمتهم وكذا وصف للجريمة الإلكترونية التي إرتكبها وأيضا توقيع النائب العام والتاريخ الذي تمت فيه،[1] ليترتب عن ذلك تخلي الجهة الأولى عن القضية ورفع يدها عنها لصالح الجهة القضائية ذات الإختصاص الموسع ويتم إصدار أمر بالتخلي.

ثانيا: القطب الجزائي الوطني المتخصص.

بالإضافة إلى الأقطاب الجزائية المتخصصة والتي سبق شرحها، نجد بأن المشرع الجزائري لم يتوقف عند ذلك بل سارع مرة أخرى إلى إنشاء هيئة قضائية أخرى تكون ذات إختصاص وطني، وهو ما أطلق عليها تسمية القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ولعل الدافع من وراء إنشاء هذا القطب هو أن الأقطاب المتخصصة غير قادرة على إستيعاب كافة الجرائم الإلكترونية، وإنما تختص فقط بتلك التي تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات في حين أن الجريمة الإلكترونية تشمل أية جريمة تكون ذات صلة بتكنولوجيات الإعلام والإتصال سواء كانت قديمة أو حديثة وحتى تلك التي سيسفر عنها مستقبلا.

[1] عبد الفتاح قادري، حيدرة سعدي، مرجع سابق، ص 210.

ومثلما سبقت الإشارة في الفصل الأول من هذا الباب هو أن شركات المساهمة تتعرض بالإضافة إلى الإعتداء على نظامها المعلوماتي إلى عدة جرائم أخرى ترتكب بطريقة إلكترونية، خاصة أمام التنامي اللا محدود لوسائل تكنولوجيا الإعلام والإتصال، وحتى لا يتم إسناد هذه الجرائم الإلكترونية المعقدة إلى الجهات القضائية العادية وبغية إزالة العراقيل التي تواجهها في مكافحة هذا النوع من الجرائم عمد المشرع إلى إنشاء قطب وطني متخصص وكان ذلك بموجب الأمر رقم 21-11،[1] المتمم لقانون الإجراءات الجزائية، ونجد بأن المشرع الجزائري لم يقم بتعريف القطب الوطني المتخصص في مكافحة الجرائم المتصة بتكنولوجيات الإعلام والإتصال وإنما إكتفى بتعريف هذه الجرائم فقط.

ويمكن تعربف هذا القطب على أنه عبارة عن جهة قضائية تم منح الإختصاص لها في هذا النوع من الجرائم وذلك عبر كامل الإقليم الوطني، وله نوعين من الإختصاص:

1-الإختصاص النوعي: ويمكن رصد الإختصاص النوعي لهذا القطب في إختصاص حصري واختصاص مشترك.

بالنسبة للإختصاص الحصري وهو أن يختص ببعض الجرائم بصفة منفردة دون إشراك أية جهة أخرى، ومن هذه الجرائم ما ورد في الفقرة الثانية من المادة 211 مكرر22 من الأمر 21-11 والتي جاء فيها"كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا" فالجنح التي يختص بها هذا القطب حددها المشرع على سبيل الحصر في المادة 211مكرر24[2] من نفس الأمر، ومن بين هذه الجنح التي تكون في شكل جريمة إلكترونية وتتعرض لها شركات

---

[1]أمر رقم 21-11 ، مرجع سابق.

[2]المادة 211 مكرر24 " مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصة بتكنولوجيات الإعلام والإتصال وقاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصة بتكنولوجيات الإعلام والإتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

-الجرائم التي تمس بأمن الدولة أو الدفاع الوطني؛

-جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو إستقرار المجتمع؛

-جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية؛

-جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية؛

-جرائم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين؛-جرائم التمييز وخطاب الكراهية.

المساهمة هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية .

فمن نوع المؤسسات العمومية هناك المؤسسات العمومية الاقتصادية والتي أعطاها المشرع شكل شركات تجارية،[1] وذلك لكونها تخضع من حيث الإنشاء والتنظيم والسير للأشكال التي تخضع لها شركات الأموال المنصوص عليها ضمن أحكام القانون التجاري هذا حسب ما ورد في الأمر 01-04، لذلك من بين الأشكال التي تتخذها المؤسسات العمومية الاقتصادية شكل شركات مساهمة.

وبالتالي فحتى يكون القطب الجزائي الوطني مختصا يجب أن تكون الجريمة الواقعة على شركات المساهمة في شكل جنحة المساس بأنظمة المعالجة الآلية لمعطياتها، وذلك في المراحل الثلاث، المتابعة، التحقيق وكذا المحاكمة.

كما يختص القطب الجزائي حصرا في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيدا والجرائم المرتبطة بها، وهذا حسب المادة 211 مكرر 25 فقرة 1[2] من الأمر 21-11، وقد تم هذه الجرائم في الفقرة 2 من نفس المادة[3]، وشركات المساهمة ليست بمنأى عن هذا النوع من الجرائم ففي العديد من الحالات قد تتعرض إلى جريمة إلكترونية في شكل جنحة ترتكب بتعاون عدة جناة، كما أنها قد ترتب آثار جسيمة لهذه الشركات بل أن أثرها لا ينحصر على الشركة فقط بل أنه يؤثر

---

[1] المؤسسات العمومية الاقتصادية هي شركات تجارية تحوز فيها الدولة أو أي شخص معنوي آخر خاضع للقانون العام، أغلبية رأس المال الاجتماعي مباشرة أو غير مباشرة وهي تخضع للقانون العام، (المادة 2 من الأمر رقم 01-04 مؤرخ في 20 غشت 2001، يتعلق بتنظيم المؤسسات العمومية الاقتصادية وتسييرها وخوصصتها، ج، ر،ج ،ج، ع 47، الصادر في 22 غشت 2001.

[2] المادة 211 مكرر 25 فقرة 1: مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وكذا قاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيدا والجرائم المرتبطة بها.

[3] المادة 211 مكرر 25 فقرة 2: يقصد بالجريمة المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيدا بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب إستعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي.

على إقتصاد الدولة التي تتبعها الشركة، لتكون بذلك هذه الشركة قد تعرضت إلى جريمة إلكترونية أكثر تعقيدا فيكون القطب الجزائي الوطني هو الجهة المختصة بنظرها .

أما بالنسبة للإختصاص المشترك فيعني أن يشترك هذا القطب مع الجهات القضائية ذات الإختصاص الموسع –الأقطاب الجزائية– والتي سلف شرحها، حيث أن المادة 211 مكرر27 من الأمر 21–11 نصت على أنه "بدون الإخلال بنص المادتين 211 مكرر24 و 211 مكرر25، يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب إختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37، 40 و 329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها.

وعليه من خلال ما تم التطرق إليه نجد بأن من أنواع الجرائم التي تتعرض لها شركات المساهمة ويكون الإختصاص بنظرها مشتركا بين القطب الجزائي الوطني والجهات القضائية ذات الإختصاص الموسع، الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات في حالة ما إذا لم تكن شركة المساهمة تندرج ضمن المؤسسات العمومية، باعتبار أنه في هذه الحالة يكون الإختصاص حصري للقطب الجزائي الوطني، وبالتالي يكون هناك تداخل في الإختصاص بين هذا القطب وباقي الأقطاب الجزائية.

وينبغي أن نشير كذلك إلى أن القطب الجزائي الوطني قد يتزامن إختصاصه مع إختصاص محكمة مقر مجلس قضاء الجزائر حيث أن الإختصاص في هذه الحالة يؤول وجوبا لهذه الأخيرة، وذلك طبقا لأحكام المادة 211 مكرر29 من الأمر 21–11.[1]

2–الإختصاص الإقليمي للقطب الجزائي الوطني: بالرجوع إلى المادة 211 مكرر23 من نفس الأمر نجده تنص على أنه يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل

[1] المادة 211 مكرر29: إذا تزامن إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مع إختصاص محكمة مقر مجلس قضاء الجزائر طبقا لأحكام المواد 211 مكرر 16 إلى 211 مكرر21 من هذا القانون يؤول الإختصاص وجوبا لهذه الأخيرة.

الإقليم الوطني، بمعنى أن إختصاص هذا القطب في كامل الجرائم التي تندرج ضمن إختصاصه النوعي بما فيها تلك التي ترتكب ضد شركات المساهمة يكون عبر كافة الإقليم الوطني دون أن يعاب عليه تجاوز الإختصاص، أما بالنسبة للقواعد المتبعة من أجل إتصال القطب الجزائي الوطني بملف القضية فنميز بين حالتين:

-في حالة الإختصاص الحصري للقطب تطبق حينها الإجراءات المنصوص عليها في المواد 211 مكرر19 إلى 211 مكرر21 من قانون الإجراءات الجزائية، هذا وفقا لما ورد في المادة 211 مكرر26.[1]

-في حالة الإختصاص المشترك مع الأقطاب الجزائية فإنه يتم تطبيق الإجراءات المنصوص عليها في المواد 211 مكرر4 إلى 211 مكرر15 من قانون الإجراءات الجزائية، هذا وفقا لما ورد في الفقرة 2 من المادة 211 مكرر27.[2]

ثالثا: القطب الجزائي اللإقتصادي والمالي:

تم إنشاء هذا القطب بموجب الأمر رقم 20-04،[3] حيث نصت المادة 3 منه على إضافة باب رابع تحت عنوان "القطب الجزائي الاقتصادي والمالي" وقد نصت المادة 211 مكرر منه على أنه " ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص لمكافحة الجريمة الاقتصادية والمالية".

وبالتالي فالأمر الملاحظ هو أن المشرع الجزائري لم يقدم تعريفا له، وما يستشف من نص المادة هو أن هذا القطب لا يمكن إعتباره بمثابة هيئة قضائية خاصة قائمة بذاتها، وإنما هو عبارة عن جهة قضائية يتم إنشاؤها بداخل محكمة مقر مجلس قضاء الجزائر تكون

---

[1] المادة 211 مكرر26: تطبق على الإختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، المنصوص عليه في المادتين 211 مكرر24 و 211 مكرر25 أعلاه، الإجراءات المنصوص عليها في المواد 211 مكرر19 إلى 211 مكرر21 من هذا القانون.

[2] المادة 211 مكرر27 فقرة 2: تطبق في هذه الحالة الإجراءات المنصوص عليها في المواد 211 مكرر4 إلى 211 مكرر15 من هذا القانون، أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

[3] أمر رقم 20-04 ،مرجع سابق.

متخصصة في مكافحة نوع من الجرائم التي حددها المشرع، وقد خصه المشرع بنوعين من الإختصاص:

1-الإختصاص النوعي: خص المشرع الجزائري القطب الجزائي الاقتصادي والمالي بنوع معين من الجرائم والتي تتمثل في الجرائم الاقتصادية والمالية الأكثر تعقيدا، وكأن المشرع إعتمد على معيارين من أجل تحديد الإختصاص النوعي لهذا القطب، يتمثل المعيار الأول في أن تكون الجريمة إما إقتصادية أو مالية، في حين يتمثل المعيار الثاني في أن تتسم هذه الجريمة بالتعقيد.[1]

وقد تم تحديد مجموع الجرائم الاقتصادية والمالية في المادة 211 مكرر2 من الأمر 20-04،[2] وقد تم تعريف الجريمة الاقتصادية الأكثر تعقيدا من خلال الفقرة 3 من المادة 211 مكرر3، حيث يقصد بهذه الجريمة تلك التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو جسامة الأضرار المترتبة عنها أو لطبيعتها المنظمة أو العابرة للحدود الوطنية أو لإستعمال تكنولوجيات الإعلام أو الإتصال في إرتكابها، تتطلب اللجوء إلى وسائل تحر خاصة أو خبرة فنية متخصصة أو تعاون قضائي دولي.

فمن بين أنواع الجرائم التي يختص بها هذا القطب هي جريمة تبييض الأموال المنصوص عليها في المواد 389 إلى 389 مكرر3 والتي يمكن إستعمال تكنولوجيات الإعلام والإتصال في إرتكابها لتكون بذلك أحد أنواع الجرائم التي ترتكب في إطار شركات المساهمة كما سبق

---

[1] حيدور جلول، (دور القطب الجزائي الاقتصادي والمالي في حماية المال العام من جرائم الفساد في ضوء التشريعات الجزائية)، مجلة الإجتهاد القضائي، ع 2، مج 13، الصادر في أكتوبر 2021، ص 914.

[2] المادة 211 مكرر2: يمارس وكيل الجمهورية لدى القطب الجزائي الاقتصادي والمالي وكذا قاضي التحقيق ورئيس ذات القطب إختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37، 40 و 329 من هذا القانون بالنسبة للجرائم المذكورة أدناه والجرائم المرتبطة بها:

-الجرائم المنصوص عليها في المواد 119 مكرر و 389 مكرر1 و 389 مكرر2 و 389 مكرر3 من قانون العقوبات.

-الجرائم المنصوص عليها في القانون 06-01 المؤرخ في 20 فبراير سنة 2006 والمتعلق بالوقاية من الفساد ومكافحته.

- الجرائم المنصوص عليها في الأمر 96-22 المؤرخ في 9 يوليو سنة 1966 والمتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من وإلى الخارج.

-الجرائم المنصوص عليها في المواد 11 و 12 و13 و14 و15 من الأمر 05-06 المؤرخ في 23 غشت سنة 200 والمتعلق بمكافحة التهريب.

توضيح ذلك في الفصل الأول من هذا الباب وبذلك يكون القطب الجزائي الاقتصادي والمالي هو المختص.

ونظرا لخطورة الجرائم التي يختص بها هذا القطب كجريمة تبييض الأموال التي تتعرض لها شركات المساهمة، فقد منحه المشرع الإختصاص وجوبا في حالة ما إذا تزامن إختصاصه مع إختصاص القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال،[1] ونشير أيضا إلى أنه في حالة ما إذا تزامن المطالبة بملف الجريمة بين وكيل الجمهورية لهذا القطب ووكيل الجمهورية لدى الجهات القضائية ذات الإختصاص الموسع فإنه يؤول الإختصاص وجوبا إلى القطب الجزائي الاقتصادي والمالي هذا حسب ما جاء في المادة 211 مكرر 11 في فقرتها الأولى، و يتولى مهمة البحث والتحري والمتابعة والتحقيق والحكم أيضا في الجرائم التي تندرج ضمن إختصاصه النوعي.[2]

2-الإختصاص الإقليمي: من خلال الأمر 20-04 فقد منح المشرع لهذا القطب إختصاصا وطنيا بالنسبة للجرائم التي يختص بها حيث نصت المادة 211 مكرر1 منه على أن وكيل الجمهورية لدى القطب الجزائي الاقتصادي والمالي وكذا قاضي التحقيق ورئيس ذات القطب يمارسون صلاحياتهم عبر كامل الإقليم الوطني.

وحتى يتمكن هذا القطب من التصدي للجرائم التي يختص بها والتي قد تتعرض لها شركات المساهمة مثل جريمة تبييض الأموال، ينبغي له أن يتصل بالقضية التي تتعلق بتلك الجريمة حيث يتم ذلك إما عن طريق إحالة المحاكم الجزائية لملف القضية المتعلقة الجريمة إلى هذا القطب إذا تبين لها بأنها تندرج ضمن إختصاصه،[3] ونجد بأن المادة 211 مكرر6 من الأمر رقم 20-04 نصت على أنه " يرسل وكلاء الجمهورية لدى الجهات القضائية المختصة إقليميا وفقا لأحكام المادة 37 من هذا القانون فورا، وبكل الطرق نسخا من التقارير الإخبارية وإجراءات التحقيق المنجزة من قبل الشرطة

---

[1] المادة 211 مكرر 28 من الأمر 21-11.

[2] المادة 211 مكرر3 فقرة 1 من 20-04.

[3] شهرزاد دراجي، نور الدين بن الشيخ، (القطب الجزائي الاقتصادي والمالي المستحدث قراءة في الأمر رقم 20-04 المؤرخ في 30-08-2020)، مجلة الدراسات القانونية والإقتصادية، ، ع 2، مج 5، الصادر في 2022، ص 822.

القضائية في إطار إحدى الجرائم المنصوص عليها في المادة 211 مكرر2 أعلاه، إلى وكيل الجمهورية لدى القطب الجزائي الاقتصادي والمالي.

وعليه نخلص إلى القول بأن الجرائم الإلكترونية التي تتعرض لها شركات المساهمة لا تختص بها جهة قضائية واحدة فقط، وإنما الجهات الثلاث التي سبق شرحها يمدد إختصاصها ليشمل هذه الجرائم وهذا ما يدل على صعوبة التعامل مع الطابع المعقد لها، وبالتي فحسن ما فعله المشرع الجزائري حين إتجه إلى فكرة التخصص القضائي.

المبحث الثاني:

إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة وإجراءات الوقاية منها.

أثبت الواقع العملي بأن الجرائم الإلكترونية الواقعة على شركات المساهمة تبقى مجهولة طالما أنه لم يتم تبليغ الجهات المعنية بها، كون أن هذه الجرائم من غير الممكن أن تصل إلى علم الجهات القضائية بطريقة معتادة مثلما يحصل في باقي الجرائم التقليدية التي تخلف آثار مادية الأمر الذي يترتب عليه صعوبة في إثباتها، فالتقنيات التكنولوجية المستخدمة من قبل الجناة قصد تنفيذ جرائمهم على شركات المساهمة تجعل من الأدلة المادية قاصرة على إثباتها كونها تفتقد للآثار المادية.

لذلك وحتى يتم كشف الأسرار المتعلقة بالجرائم الإلكترونية التي تتعرض لها شركات المساهمة يقتضي الأمر من الجهات المكلفة بعمليات التحري والتحقيق، البحث عن دليل يتناسب وبيئة الأعمال الإلكترونية التي تعتمدها تلك الشركات، وهو ما يعرف بالدليل الإلكتروني.

ومن جهة أخرى، ما أثبته الواقع العملي هو تضاعف الإعتداءات الموجهة من قبل جناة الفضاء الإلكتروني على شركات المساهمة واستهدافها بشكل واسع، وبما أن التطورات التكنولوجية تسفر بشكل يومي على تقنيات جديدة يتم تسخيرها من قبل أولئك الجناة في تخطي حواجز الحماية المعتمدة من قبل هذه الشركات الأمر الذي يتطلب منها إتخاذ إجراءات وقائية من خطر هذه الجرائم وتحقيق أمنها المعلوماتي، هذا ما سنوضحه من خلال هذه المبحث وذلك بتقسيمه إلى مطلبين:

المطلب الأول: إثبات الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

المطلب الثاني: إجراءات تحقيق الأمن المعلوماتي في شركات المساهمة.

المطلب الأول:

إثبات الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

الإثبات هو العملية التي يكون الهدف من ورائها التوصل إلى دليل يثبت الواقعة الإجرامية المرتكبة ويدين فاعله، وبما أن الدليل هو وليد الجريمة تتميز طبيعته بذات طبيعتها، لذلك فنتائج التحري والتحقيق في الجرائم الإلكترونية التي تستهدف شركات المساهمة تفضي إلى دليل في شكل

نبضات إلكترونية غير مرئية، الأمر الذي يثير مسألة القوة الثبوتية وحجية هذا الدليل في إثبات تلك الجرائم، لذلك من خلال هذا المطلب سنبحث في مفهوم الدليل الإلكتروني المستمد من إجراء التحري والتحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة **(فرع أول)** ثم حجية الدليل الإلكتروني في إثبات هذه الجرائم وسلطة الجهات القضائية المختصة في تقديره **(فرع ثاني)**.

الفرع الأول:

مفهوم الدليل الإلكتروني المستمد من إجراء التحري والتحقيق في الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

نظرا للطبيعة الإلكترونية للجرائم التي يشنها الجناة على شركات المساهمة مما يجعل مسألة الحصول على دليل يثبتها أمر في غاية الصعوبة كونه مسجل إلكترونيا ومشفر عبر وسائط تخزين يستحيل قراءتها، لذلك يبدو دليلا غامضا ومنفردا مقارنة بغيره من أدلة الإثبات وبالتالي فإن فهم هذا الدليل والوقوف على حقيقته يتطلب دراسة معمقة.

أولا: تعريف الدليل الإلكتروني:

رغم حداثة الدليل الإلكتروني إلا أن هناك العديد من التعريفات التي حظي بها وهذا إن دل فإنما يدل على أهميته في إثبات الجرائم التي يرتبط بها، حيث يعرف على أنه ذلك الدليل المستمد من جهاز الحاسوب وهو عبارة عن نبضات كهربائية أو مغناطسية قابلة للتجميع والتحليل عن طريق إستخدام البرامج والتطبيقات المخصصة لذلك، ليتم إخراج معلومات تكون في شكل نص مكتوب أو أشكال أو صور يتم الإعتماد عليها أمام الجهات القضائية قصد إثبات واقعة إجرامية ما،[1] وهو الذي يتم العثور عليه في البيئة الإفتراضية ويقود إلى الجريمة المرتكبة على مسرحها،[2] وهو أيضا تلك المعلومات الرقمية المقبولة من ناحية المنطق والعقل ويعتمدها العلم، يتم تحصيلها من خلال القيام بجملة من الإجراءات القانونية والعلمية وذلك بترجمة البيانات الحسابية التي تكون مخزنة على جهاز

[1] خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والأمنية، مرجع سابق، ص 37.

[2] يزيد بوحليط، مرجع سابق، ص282.

الحاسوب وملحقاته ليتم إستخدامها قصد إثبات حقيقة فعل وذلك في أي مرحلة من مراحل التحقيق أو المحاكمة.[1]

وبناء على جملة هذه التعريفات المقدمة يمكننا القول بأن الدليل الإلكتروني الذي يتم البحث عنه قصد إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة هو عبارة عن معلومات وبيانات يتم إستخلاصها من أجهزة حواسيبها والتي كانت محلا لتلك الجرائم، وذلك بعد عملية التحري والتحقيق، حيث يتم إفراغ تلك المعلومات والبيانات في شكل مادي سواء كانت في صورة مخرجات ورقية، أو من خلال تثبيتها على دعامات كالأقراص الصلبة مثلا، أو أية دعامة أخرى قابلة للعرض المرئي على الشاشات حيث يوصل الدليل الإلكتروني المتحصل عليه إلى مصدر الإعتداء الذي تعرضت له تلك الشركات، وبالتالي كشف الجناة وإيدانتهم وبذلك يكون الدليل الإلكتروني متناسب مع البيئة الإفتراضية شكلا ومضمونا.

ثانيا: خصائص الدليل الإلكتروني.

كون أن الدليل الإلكتروني يتم إستنباطه من بيئة إفتراضية ذات طابع تقني مما يجعله يتميز بعدة خصائص، البعض منها يشكل الجانب الإيجابي لهذا الدليل، فهي بمثابة مزايا تساعد على عملية إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة رغم ما تتسم به من صعوبة وتعقيد، في حين هناك خصائص أخرى يتميز بها ولكنها تمثل الجانب السلبي له حيث تمثل مشكلات وصعوبات تعيق عملية إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة، وفيما يلي نوضح كلا الجانبين:

1-مزايا الدليل الإلكتروني في إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة: يمكن إجمال هذه المزايا في النقاط التالية:

أ-قابلية الدليل الإلكتروني لعملية النسخ: وتعد هذه الخاصية من أهم المزايا التي يتميز بها والتي يستحيل أن تتميز بها الأدلة التقليدية، فالتقنية المعلوماتية تسمح بالحصول على عدة

[1] علي محمود إبراهيم أحمد، (الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية دراسة فقهية مقارنة)، مجلة كلية الشريعة والقانون بجامعة الأزهر، ع 32، الصادر في 2020، ص 1082.

نسخ للدليل الإلكتروني وتكون مطابقة تماما لأصلها،[1] فيمكن لهذا الدليل أن يخلف نسخ عديدة منه وذلك في عدة أماكن،[2] فقد يكون الجاني من بين موظفي شركة المساهمة التي يعمل بها ويقوم بإرسال محتوى سري يتعلق بنشاطها التجاري إلى جهة أخرى، ففي هذه الحالة هناك عدة نسخ للمحتوى الذي قام بإرساله، منها ما يوجد بذاكرة حاسوب الشركة الذي أرسل منه ومنها ما يوجد في مساحة الموقع الذي أرسل إليه، وأخرى في مساحة الموقع الذي تم إرسال المحتوى عبره.

حيث أن هذه النسخ تعتبر ذات أهمية فعالة تحول دون تلف أو فقد هذا الدليل أو العبث به وتغييره، وهذا ما يصعب مهمة التخلص منه، [3] بحيث أن المعطيات المتحصل عليها والتي تم إفراغها على دعامة تخزين إلكترونية تكون قابلة للحجز مثل الأقراص الصلبة وذلك بهدف تقديمها للجهات القضائية المختصة بنظر تلك الجرائم، هذا ما نص عليه المشرع الجزائري في المادة 6 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

ب-صعوبة التخلص من الدليل الإلكتروني: يتميز الدليل الإلكتروني بخاصية البقاء بحيث من غير الممكن إزالته بسهولة،[4] فمع التطورات التقنية أصبح من الممكن جدا الحصول على ذات الدليل الإلكتروني بعد عملية محوه وإظهاره بعد أن يتم إخفاؤه وذلك عن طريق مختلف برامج الحاسوب والتي يتم إعدادها خصيصا من أجل إسترجاع البيانات التي تم محوها أو إلغاؤها.[5]

---

[1] يزيد بوحليط، مرجع سابق، ص 285.

[2] رابح لهوى، "مرجع سابق، ص 42.

[3] علي محمود إبراهيم أحمد، مرجع سابق، ص 1087.

[4] نضال سالمي ، (الإطار التنظيمي للدليل الرقمي في الإثبات) مجلة القانون والمجتمع، العدد 1، الصادر في 2022، ص 337.

[5] عائشة عبد الحميد، (الدليل الرقمي كحجية للإثبات أمام القاضي الجزائي في المعاملات الإلكترونية)، مجلة صوت القانون، ع 1، مج، 7، الصادر في ماي 2020، ص 484.

ونظرا لهذه الخاصية فهناك من يشبهه بالدليل الجيني DNA، [1] بل الأكثر من هذا في حالة إعتداء الجاني على شركة مساهمة من خلال إرتكابه لإحدى الجرائم التي سبق التطرق إليها فإن الدليل على هذه الجرائم يكون قد تم تسجيله ضمن جهاز الحاسوب، وفي حالة ما إذا حاول التخلص من ذلك الدليل فإن محاولته تسجل وتصبح ضده كون أن جهات التحري والتحقيق سوف تكتشف فعل محاولة المحو، عن طريق إطلاعها على النسخة الأصلية للدليل الإلكتروني المسجل على جهاز الحاسوب وذلك ما يثبت التهمة ويؤكدها ضد الجاني.[2]

ت-الطبيعة الثنائية للدليل الإلكتروني: مضمون هذه الخاصية هو أن الدليل الإلكتروني يتكون في الأصل من عدد لا محدود من الأرقام التي تكون في شكل ثنائي موحدة في رقمي الواحد والصفر (1-0)، وبطبيعة الحال لا تكون متشابهة أبدا فيما بينها وذلك رغم وحدة الرقم الثنائي الذي تتألف منه،[3] وبذلك لا يكون للكتابة في البيئة الإفتراضية سواء كانت في شكل نصوص أو حروف أو صور الوجود المادي المعروف والموجود على الورق، بل تكون عبارة عن تشكيلة من الأرقام والتي تعود في الأصل إلى ذلك الرقم الثنائي،[4] فكل ما هو في البيئة الإفتراضية تكون تشكيلته عبارة عن معادلة ثنائية أساسها الرقمين (1) و (0) وهما عبارة عن نبضات وذبذبات تكون حيويتها وتفاعلها مستمدة من الطاقة، وتلك المعادلات تكون مختلفة حجما وموضوعا وكذا كمية وحجم الرقمين (1) و (0) وذلك حسب الملف الذي يختلف حجمه عن غيره من الملفات.[5]

وفي الحقيقة أن هذه الخاصية تعتبر إمتداد للخاصية العلمية التي تتميز بها كون أن الحصول على هذا الدليل لا يمكن أن يتم إلا عن طريق اللجوء إلى الأساليب العلمية المتعلقة بالبيئة

---

[1] محمد بن فردية ، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، مرجع سابق، ص 44.

[2] إلهام بن خليفة، مرجع سابق، ص 257.

[3] محمد علي سويلم، الإثبات الجنائي عبر الوسائل الإلكترونية دراسة مقارنة، د،ط، الإسكندرية، دار المطبوعات الجامعية، 2020، ص 257.

[4] إلهام بن خليفة، مرجع سابق، ص 257.

[5] محمد علي سويلم، مرجع سابق، ص 353.

الإفتراضية، إضافة إلى طابعه التقني المستمد من بيئة من ذات الطبيعة، كون أن التعامل معها لا يتوقف على رجال التحري والتحقيق وإنما يتطلب الأمر الإستعانة بخبراء وتقنيين لديهم دراية وخبرة في التعامل مع الأدلة الإلكترونية.

رغم هذه الجوانب الإيجابية للدليل الإلكتروني إلا أنه في مقابل ذلك يتسم ببعض الخصائص والتي يمكن إعتبارها بمثابة سلبيات أو مساوئ تحد من الوصول إليه واكتشافه، وبالتالي تصبح مسألة إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة عن طريق هذا الدليل ونسبتها إلى مرتكبيها تتسم بالنسبية:

2-مساوئ الدليل الإلكتروني في إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة: ويمكن إجمالها في النقاط التالية:

أ-تواجده بين كم ضخم من البيانات والمعطيات: إن المعطيات والبيانات التي يتم تداولها في النظام المعلوماتي لشركات المساهمة تشكل عددا ضخما تصعب عملية حصره، لذلك يصبح من العسير جدا الوصول إلى الدليل الإلكتروني إذا ما تعرضت لإحدى الجرائم الإلكترونية وذلك كونه يتواجد وسط كم هائل وضخم من الملفات التي يحتويها نظامها المعلوماتي، وبالتالي يتعذر على رجال التحري والتحقيق فحص ذلك الكم من البيانات والمعطيات كونها تستغرق وقتا طويلا وهذا ما يدفعهم إلى صرف النظر عن مواصلة عملية البحث إعتقادا منهم بأن هذه العملية ما هي إلا هدر للوقت والجهد خاصة في ظل عدم وجود آلية خاصة بالفرز الذاتي للملفات،[1] ففي إحدى الوقائع التي حدثت في ألمانيا سنة 1971 حين تعرضت شركة طلبيات بريدية إلى سرقة ما يقارب 300.000 عنوان لعملائها كانت على أشرطة ممغنطة، حيث قامت باستصدار أمر يسمى وقف الأعمال من أجل إسترجاع تلك العناوين التي أصبحت بحوزة شركة أخرى منافسة بعد أن تحصلت عليها من الجناة الذين قاموا بسرقتها، ومن أجل تنفيذ ذلك قامت الشركة المنافسة بالسماح لمساعد مأمور التنفيذ بالولوج إلى جهاز الحاسوب الخاص بها من أجل البحث على تلك العناوين

[1] موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مداخلة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون أكاديمية الدراسات العليا بطرابلس، المنعقد في 28، 29 أكتوبر، 2009، ص 6.

واسترجاعها، غير أنه وجد نفسه بين كم ضخم من الأشرطة والأقراص الممغنطة والتي إستحال عليه فحصها لعدم قدرته على ذلك فما كان عليه سوى مغادرة مقر الشركة دون أن يحصل على أية معلومات[1].

وفي حالة ما إذا أرادوا طباعة تلك الملفات قصد الإطلاع على ما تحويه من معطيات فإن ذلك يتطلب مئات الآلاف من الصفحات والتي ربما في نهاية المطاف لا تسفر عن أية نتيجة مفيدة لإثبات الجريمة المرتكبة،[2] إضافة إلى أن المجرم قد يعمد إلى خلط الملفات التي قام بالإعتداء عليها مع غيرها من الملفات السليمة، مثل الحالة التي يقوم فيها بإدخال بيانات غير مطلوبة أو محو جزء منها وعليه يصبح على رجال التحري والتحقيق فحص جميع الملفات تلك التي تم الإعتداء عليها وكذا السليمة،[3] الأمر الذي قد ينجر عليه الإطلاع على بعض الأسرار التجارية الخاصة بهذه الشركات والتي يحظر على على الغير الإطلاع عليها مثل التركيبة السرية للمواد المستعملة في صناعة مشروب "كوكاكولا" والتي تحتفظ به الشركة لفترة تزيد عن الربع قرن.

ب-إحاطة الدليل الإلكتروني بوسائل الحماية المعقدة: مثلما سبق وأشرنا فإن جناة الفضاء الإلكتروني على مستوى عال من الذكاء والدهاء إضافة إلى خبرتهم في مجال الحواسيب، لذلك فإذا ما أقدم أحدهم على الإعتداء على أحد شركات المساهمة فقبل تنفيذ جريمته يخطط لها سلفا خاصة إذا كان من بين أحد العاملين بها فحتى لا يتم إكتشاف أمره والوصول إلى دليل يثبت إدانته، فإنه يعمد إلى الإستعانة بأساليب الحماية الفنية والتي تكون على مستوى من التعقيد كاستخدام كلمات المرور وترميز البيانات، حيث أن هذه الأساليب تعيق مهمة التحقيق وتحول دون وصول الجهات المختصة إلى ذلك الدليل الذي يدين صاحبه،[4] إذ يمكن القول بأن هذه الجرائم يتم تسييجها أمنيا مثل حالة التشفير الذي يتم عن طريق فيروسات الحاسوب تكون مهمتها الحذف التلقائي عند

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 39.

[2] بشير عادل حامد ، مرجع سابق، ص 44.

[3] إلهام بن خليفة، مرجع سابق، ص 258.

[4] موسى مسعود أرحومة، مرجع سابق، ص 5.

محاولة الولوج إلى داخل النظام المعلوماتي للشركة،[1] وفي حالة ما إذا تم الإستعانة بالبرامج المخصصة لإسترجاع البيانات فقد يبرر الجاني فعله بوجود خطأ في نظام الحاسوب خاصة إذا كان من بين موظفي الشركة.

ت-الطبيعة غير المرئية للدليل الإلكتروني: تشكل خاصية الدليل الإلكتروني كونه ذو طبيعة غير مرئية عقبة في الوصول إليه، فهو دليل خفي لا يمكن رؤيته بالحواس الطبيعية للمحقق وهذا راجع إلى طبيعة النبضات الكهربائية والمغناطسية التي يتكون منها،[2] لذلك فهو يختلف تماما عن الأدلة التي تفرزها الجرائم التقليدية كآثار الدماء والبصمات والتي يمكن رؤيتها ولمسها.

ففي الجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة قد يجري الحاسب الآلي عمليات محاسبية من بين العمليات المالية التي يقوم بها دون أن تكون هناك حاجة إلى إدخال مثل إحتساب الفوائد في إطار الإيداعات البنكية، والتي تقيد بصفة آلية ضمن أرصدة العملاء وذلك وفقا للشروط التي تم الاتفاق عليها سلفا، لذلك تكون موجودة ضمن الحاسوب وخلال القيام بهذه العمليات قد ترتكب جريمة تزوير سواء بإدخال بيانات أو تعديلها، ففي هذه الحالة ليس هناك أي دليل يمكن رؤيته ويشير إلى الجريمة المرتكبة،[3] فعدم رؤية الدليل الإلكتروني يلقي بظلاله على الجريمة الإلكترونية المرتكبة في إطار شركات المساهمة ويعيق جهات التحقيق في الوصول إليه.

كما ينبغي الإشارة إلى أنه إضافة إلى هذه العوائق التي تحد من عملية الوصول إلى الدليل الإلكتروني إلا أنه هناك صعوبة أخرى حتى في حالة الوصول إليه كونه لا يفصح عن شخصية معينة ومحددة،[4] وبالتالي تكون هناك صعوبة في نسبة الجريمة المرتكبة إلى متهم معين خاصة إذا ما

---

[1] رابح لهوى، مرجع سابق، ص40.

[2] بندر عقاب جفين كميخ حطاب الدويش، (خصائص وأنواع الدليل الإلكتروني في الكويت والدول المقارنة)، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، ع 3، مج، 16، الصادر في ماي 2023، ص 826.

[3] فايز محمد راجح غلاب، مرجع سابق، ص 396.

[4] إلهام بن خليفة، مرجع سابق، ص 258.

لجأ إلى إرتكاب جريمته بأسماء وهمية مستعارة الأمر الذي يترتب عليه قطع الصلة تماما بين الجريمة وفاعلها.

وفي كثير من الأحيان يتم الإعتماد على البيانات والمصادر والعناوين التي يحتوي عليها نظام (IP) كونها تساعد على كشف مصدر الجهاز الذي تم إستخدامه في إرتكاب الجريمة، غير أن ذلك لا يعني بالضرورة الكشف عن المجرم والذي هو صاحب الجهاز كون أن الوصول إلى الجهاز من خلال تلك التقنية هو في الحقيقة وصول إلى عنوان إلكتروني للحاسب لا أكثر، وهذا لا يعتبر كافيا في إسناد الفعل إلى صاحب الجهاز إذ من الممكن جدا ليس هو مقترف الجريمة،[1] مثل الحالة التي يلجأ فيها الجاني إلى الدخول إلى النظام المعلوماتي الخاص بالشركة والإعتداء عليها من حاسوب مديرها التنفيذي منتحلا صفته كونه له حق الولوج إلى نظامها المعلوماتي حيث أنه في هذه الحالة تم تحديد الجهاز الذي تم تنفيذ الجريمة من خلاله ولكنه لم يتم تحديد الجاني.

كل هذه العوامل التي سلف شرحها تعيق عملية الوصول إلى الدليل الإلكتروني وبالتالي تحد من عملية إثبات الجرائم الإلكترونية التي ترتكب على شركات المساهمة.

الفرع الثاني:

حجية الدليل الإلكتروني في إثبات الجرائم الإلكترونية الواقعة في إطار شركات المساهمة وسلطة الجهة القضائية المختصة في تقديره.

كما سبقت الإشارة فإن الدليل الإلكتروني ذو طبيعة تقنية مميزة باعتباره وليد جريمته إذ يتميز بما تتميز به، لذلك فهو يختلف تماما عن الأدلة التقليدية الأمر الذي يقودنا إلى التساؤل عن مدى حجية هذا الدليل في إثبات الجرائم الإلكترونية التي قد تتعرض لها شركات المساهمة وإدانة فاعلها، وبالتالي تكون لهذا الدليل قيمة قانونية بحيث يمكن إعتبار هذه العملية بمثابة مرحلة أولى يمر بها من أجل إثبات الجرائم الإلكترونية الواقعة على تلك الشركات لتأتي بعدها مرحلة أخرى يمر بها هذا الدليل وهي خضوعه للسلطة التقديرية للجهة القضائية المختصة ومدى تقديرها وقبولها له هذا ما سنقوم بتوضيحه من خلال هذا الفرع.

[1] براهيمي جمال، مرجع سابق، ص 203.

أولا: حجية الدليل الإلكتروني في إثبات الجرائم الإلكترونية الواقعة على شركات المساهمة.

الحجية تعني القيمة والقوة التي يتمتع هذا الدليل في إثبات الجرائم الواقعة على شركات المساهمة ونسبتها إلى فاعلها والحديث عن حجية الدليل الإلكتروني يقودنا إلى الحديث عن موقف النظم القانونية إتجاه هذا الدليل بحيث تتباين وتختلف بينن موسع ومضيق وفيما يلي نتعرف على هذه الأنظمة.

1-حجية الدليل الإلكتروني في نظام الإثبات الحر: يسود هذا النظام في القوانين اللاتينية مثل القانون الفرنسي، السوري واللبناني وكذا القوانين التي تأثرت أيضا بالصيغة اللاتينية،[1] حيث يقوم على مبدأ حرية الإثبات، بمعنى أن المشرع لا يحدد الأدلة المعدة للإثبات أمام القضاء بل أنه يعطي للقاضي مطلق الحرية من أجل البحث عن الأدلة التي يراها مناسبة لعملية الإثبات وهو وحده يحدد قيمتها الثبوتية وفقا لقناعته،[2] فالقاضي وفقا لهذا غير ملزم بأن يستند إلى أي دليل لا يطمئن إليه وغير مقتنع به،[3] وبالتالي يكون بإمكان أطراف النزاع تقديم أية أدلة من شأنها أن تدعم موقفهم ليقوم بعدها القاضي بفهم تلك الأدلة وتقدير قيمتها دون أن يخضع في ذلك لرقابة قاضي النقض ولكن في مقابل ذلك يكون ملزم بفحص ومراقبة والتأكد من نزاهة تلك الأدلة كون أن إغفاله عن هذه العملية يترتب عليه هدر الأدلة،[4] ولعل غاية هذا النظام من منح السلطة التقديرية الواسعة للقاضي من أجل بناء قناعته وتقدير الأدلة هو تمكينه من كشف حقيقة غموض الواقعة الجرمية المطروحة أمامه وبالتالي تحقيق مبدأ العدالة.

وعليه وانطلاقا من المبادئ التي يقوم عليها هذا النظام فإن حجية الدليل الإلكتروني في الإثبات لا تثير أية صعوبة أو إشكال، باعتبار أن للقاضي مطلق الحرية في تقديرها واعتمادها كأدلة إثبات وذلك إستنادا للأصل الذي يقر بمشروعية أي دليل يطمئن إليه القاضي ويقتنع به.

---

[1] بشير عادل حامد ، مرجع سابق، ص 105

[2] محمد علي سويلم، مرجع سابق، 368.

[3] بشير عادل حامد ، مرجع سابق، ص 105.

[4] براهيمي جمال، ، مرجع سابق، ص 270.

غير أن هناك بعض الدول تشترط أن يكون الدليل الإلكتروني في شكل مقروء بعد عملية إستخراجه من جهاز الحاسوب وطبعه أو يكون مقروء عبر شاشة ذات الجهاز،[1] ويعتبر الأخذ بالدليل الإلكتروني إحدى نماذج تطبيقات الدليل العلمي وذلك نظرا لما يتصف به من صفات الحياد والموضوعية وكفاءة، لذلك على القاضي قبل بناء قناعته بهذا الدليل عليه أن يميز بين مسألتين، تتعلق الأولى بالقيمة العلمية التي يتمتع بها والثانية تتعلق بالظروف المحيطة به والتي وجد فيها، فالأولى ليس للقاضي أن يناقشها كونها تعتبر ضمن صميم عمله وتندرج في إطار تقديره الذاتي لها إذ بإمكانه أن يصرف النظر عن الدليل الإلكتروني إذا تبين له بأنه لا يتوافق وظروف الواقعة الإجرامية المطروحة أمامه وذلك رغم القطعية التي يتمتع بها من الناحية العلمية.[2]

وانطلاقا مما سبق ذكره فإنه يمكن القول بعملية إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة من خلال الإعتماد على الأدلة الإلكترونية التي خلفتها، وذلك بعد أن تخضع للسلطة التقديرية لقاضي الجهة القضائية المختصة بالفصل بهذه الجرائم حتى يبني إقتناعه بها واعتمادها كأدلة إثبات لتلك الجرائم.

2-حجية الدليل الإلكتروني في نظام الإثبات المقيد: وهو ما يعرف بنظام الأدلة القانونية،[3] وفي مقدمة القوانين التي إعتنقت هذا النظام نجد القانون الإنجلزي،[4] وفي هذا النظام يتم تحديد وحصر الأدلة المقبولة أما القضاء سلفا من قبل المشرع وما على القاضي سوى الإلتزام بها وعدم الخروج عليها بأية طريقة من الطرق،[5] والمشرع هو من يحدد القيمة الثبوتية والإقناعية لكل دليل،[6] وبالتالي

---

[1] يزيد بوحليط، مرجع سابق، ص 287.

[2] محمد بن فردية ، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، مرجع سابق، ص 248.

[3] محمد بودالي ، مرجع سابق، ص 342.

[4] بشير عادل حامد ، مرجع سابق، ص 107.

[5] أحمد رعد محمد الجيلاوي، التسجيل الصوتي وحجيته في الإثبات الجنائي، د،ط، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2017، ص 20.

[6] محمد كمال، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة، د،ط، الإمارات، دار كليم للطباعة والنشر، 2022، ص 84.

يقتصر دور القاضي في هذا النظام على فحص الأدلة والتحقق من مشروعيتها ومدى استيفاءها للشروط المحددة قانونا لأنه في حالة عدم توفرها على الشروط المطلوبة فإن القاضي يقوم باستبعادها حتى لو كانت لديه قناعة بيقينية تلك الأدلة،[1] ووفقا لمبادئ هذا النظام ثارت إشكالية إثبات الجريمة الإلكترونية وذلك لتعارض مبادئه مع الأدلة التي تخلفها.[2]

وفي ظل نظام الإثبات المقيد لا يكون للدليل الإلكتروني أية قيمة إثباتية ومن غير الممكن الإعتراف له بتلك القيمة إذا لم يتم التص على ذلك صراحة، وبالتالي النتيجة التي تترتب في هذه الحالة هو أن القاضي يجد نفسه مضطرا للحكم بما يتناقض والقناعة التي تكونت لديه.[3]

فمن خلال التمعن في المبادئ التي يقوم عليها هذا النظام يتضح لنا جليا بأنه تضمن مبدأين أحدهما إيجابي والآخر سلبي.

بالنسبة للمبدأ الأول فيتلخص في الدور الإيجابي الذي يقوم به المشرع كونه ينظم عملية الإثبات سواء بضبط الأدلة المقبولة، في هذه العملية مع إخضاع كل دليل لمجموعة من الشروط التي تحدد قيمتها الثبوتية من خلال منح الحجية الدامغة لبعض الأدلة والحجية النسبية للبعض الآخر، أما المبدأ الثاني فيتلخص في الدور السلبي للقاضي كونه يلتزم بالسير وفقا لما رسمه له المشرع، فقناعته متوقفة على قناعة المشرع،[4] لذلك تم إنتقاد هذا النظام وبشدة كونه يتعارض والوظيفة المعتادة والطبيعية للقاضي والمتمثلة في فحص الأدلة التي تعرض عليه ثم يبني عليها إقتناعه الشخصي بكل حرية ووفقا لما يمليه عليه ضميره المهني.

لذلك فإن عملية إثبات الجرائم الإلكترونية واجهتها العديد من الصعوبات في ظل هذا النظام، الأمر الذي إستلزم ضرورة البحث عن حلول خاصة في الدول التي تعتنق نظام الإثبات المقيد وتشهد إنتشارا واسعا لإستعمال التقنيات المعلوماتية بسبب التطور التكنولوجي الذي شهدته

---

[1] محمد علي سويلم، مرجع سابق، ص 366.

[2] بدري فيصل، مرجع سابق، ص 238.

[3] ربيعي حسين،آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 274.

[4] محمد علي سويلم، مرجع سابق، ص ص 366، 367.

والذي أدى بدوره إلى تفاقم إرتكاب الجرائم الإلكترونية والتي عجزت الأدلة التقليدية عن إثباتها بغية مكافحتها.

وفي هذا الصدد نجد بريطانيا والتي تعتبر مهدا لنظام الإثبات المقيد ومؤسسة له قد سارعت إلى الإعتراف بالدليل الإلكتروني ضمن أدلة الإثبات الجنائية وذلك بظهور القاعدة المعروفة ب "الإدانة دون أدنى شك" والتي بموجبها يكون بإمكان القاضي تكوين عقيدته بناء على أي دليل يكون قطعيا في دلالته،[1] وبذلك أصبح للقاضي الحرية في تقدير الأدلة ومعترفا له بذلك وفقا لإقتناعه الذاتي.

ومن بين القضايا التي تم فيها الإستناد إلى الدليل الإلكتروني المستخرج من جهاز الحاسوب ما قامت به المحكمة الجزائية ببريطانيا في قضية " R.V. PETTIGREW" والتي تتلخص وقائعها في ضبط المتهم الذي قام بالإعتداء على البنك وبحوزته أرقام لنقود كانت مسجلة على جهاز الحاسوب الخاص بالبنك الضحية، حيث قبلت المحكمة الأدلة التي تم إستخراجها من جهاز الحاسوب واعتبرتها بمثابة دليل مباشر.[2]

كذلك نجد الولايات المتحدة الأمريكية والتي تعد هي الأخرى من بين الدول المؤيدة لنظام الإثبات المقيد قد نصت بعض قوانينها على حجية الدليل الإلكتروني في الإثبات، فقانون الحاسوب تعتبر أدلة إثبات مقبولة بالنسبة للبيانات وكذا البرامج المخزنة داخله، أيضا صدر سنة 1983 ما يعرف بقانون الإثبات والذي تبين من خلاله بأن ما يتم إستخراجه من نسخ من تلك البيانات الموجودة بجهاز الحاسوب تعتبر كأفضل الأدلة لعملية إثبات تلك البيانات.[3]

وعليه حتى في ظل نظام الإثبات المقيد تم الإستناد إلى الدليل الإلكتروني ضمن أدلة الإثبات ومدلول ذلك يعود إلى الأهمية التي يكتسبها، خاصة بالنسبة للجرائم الإلكترونية التي تعتمد في إثباتها على دليل من نفس طبيعتها، وبذلك يكون لهذا الدليل حجية في إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة في ظل هذا النظام.

---

[1] محمد علي سويلم، مرجع سابق ، ص ص 367، 368.

[2] فايز محمد راجح غلاب، مرجع سابق، ص 404.

[3] بشير عادل حامد ، مرجع سابق، ص 109.

إضافة إلى هاذين النظامين هناك نظام آخر مختلط يتوسطهما والذي ظهر من أجل التوفيق بينهما، كون أن أحكامه تتراوح ما بين التقييد والإطلاق، ففي ظله يتم التخفيف من تعسف القاضي جراء حريته المطلقة في تقدير الأدلة في ظل نظام الإثبات الحر من جهة، ومن جهة أخرى يخفف من سلبية دور القاضي الذي تم تقييد حريته تماما في تقدير الأدلة في ظل نظام الإثبات المقيد،[1] ووفقا له يتم تحديد أدلة معينة من أجل إثبات مجموعة من الوقائع فقط دون غيرها من الوقائع أو أن يتم وضع جملة من الشروط في بعض الأدلة،[2] ومن ذلك نجد ما قام به المشرع الياباني حين إشترط في الأدلة التي تتعلق بجهاز الحاسوب والأنترنت حتى يتم إعتمادها كأدلة إثبات يجب أن تكون في شكل مرئي ومقروء من خلال طباعتها بعد أن كانت في صورة إلكترونية غير مرئية.[3]

3-حجية الدليل الإلكتروني في إثبات الجرائم الواقعة على شركات المساهمة في التشريع الجزائري:

من خلال عملية البحث يتضح لنا بأن الجزائر قد حذت حذو التشريعات التي تبنت نظام الإثبات الحر متأثرة في ذلك بالدول اللاتينية كفرنسا وسوريا، حيث أنه بالرجوع إلى قانون الإجراءات الجزائية نجد بأن المادة 212 منه قد كرست ذلك حين نصت على أنه "بجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكما تبعا لإقتناعد الخاص".

كما نجد المادة 307 من ذات القانون والتي جاء فيها "إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلو إلى تكوين إقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم.

هل لديكم إقتناع شخص؟

---

[1] يزيد بوحليط، مرجع سابق، ص 288.

[2] بشير عادل حامد ، مرجع سابق، ص 110.

[3] رجاء أومدور ، مرجع سابق، ص 66.

وبهذا يكون المشرع الجزائري قد منح للقاضي الحرية الواسعة من أجل تقدير الأدلة ويكون ذلك وفقا لإقتناعه الذاتي".

وعليه فإن القاضي يكون له دور جد إيجابي من أجل كشف الحقيقة بناء على الحرية المخولة له قانونا في قبول أي دليل أو أن يصرف النظر عنه بما في ذلك الدليل الإلكتروني، كما يكون له السلطة في توفير أدلة أخرى كونه غير مقيد بالأدلة التي يتم تقديمها من قبل أطراف الدعوى، فيمكن له أن يأمر باتخاذ أي إجراءات من شأنها إزاحة اللبس وكشف الغموض.[1]

وبناء على ما سبق ذكره فإن مبدأ حرية الإثبات الذي إعتمده المشرع الجزائري فإنه يمكن تطبيقه على الدليل الإلكتروني، من أجل إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة دون أي إشكال يعترضه، فقط ينبغي على قضاة الجهات القضائية المختصة بهذه الجرائم إخضاع الدليل الإلكتروني المحصل من تلك الجرائم لسلطتها التقديرية من أجل بناء قناعتها القضائية.

ونشير إلى أنه حتى تكون لدى القاضي قناعة قضائية موضوعية إتجاه الدليل الإلكتروني نؤيد ونؤكد على فكرة بناء تلك القناعة على مبدأي القيمة العلمية لهذا الدليل والتي ليس له مناقشة ما توصلت إليه التكنولوجيا المعلوماتية باعتبارها حقيقة علمية ثابتة، وكذا مبدأ الظروف التي تم فيها العثور على ذلك الدليل والتي بإمكانه تقديرها.

وما يؤكد حجية الدليل الإلكتروني في إثبات الجرائم الإلكترونية بما في ذلك تلك التي تتعرض لها شركات المساهمة ،هو نص المشرع الجزائري على الطريقة التي يتم من خلالها ضبط الأدلة الإلكترونية دون إتلافها والمحافظة على سلامتها وذلك في المادتين 6 و7 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وكأن بذلك المشرع يقر بمدى ملاءمة هذه الأدلة للجرائم الإلتكرونية.

[1] فيصل بدري ، مرجع سابق، ص ص 244، 245.

ثانيا: شروط قبول الدليل الإلكتروني وسلطة الجهة القضائية المختصة في تقديره من أجل إثبات الجرائم الإلكترونية الواقعة في إطار شركات المساهمة.

مثلما أسلفنا الذكر بأن مختلف التشريعات سواء تلك التي تتبنى نظام الإثبات الحر أو المقيد قد جعلت من الدليل الإلكتروني ضمن أدلة الإثبات، ورغم الخاصية العلمية التي يتمتع بها هذا الدليل التي تضاعف قيمته الإثباتية لتجعل شأنه في الإثبات شأن أي دليل علمي آخر، غير أن الطبيعة الفنية التي ترتكب بها الجرائم الإلكترونية في شركات المساهمة قد تعرض هذا الدليل للعبث به على نحو يحرف حقيقته، وبما أن عملية تقدير ذلك الدليل تكون من إختصاص القاضي بممارسة سلطته التقديرية، لذلك سنوضح من خلال هذه النقطة الشروط الواجب توفرها في الدليل الإلكتروني حتى يتم قبوله ثم سلطة الجهات القضائية المختصة في تقديره.

1-شروط قبول الدليل الإلكتروني: حتى يكون للدليل الإلكتروني يقين ومصداقية في عملية إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة جراء إمكانية تحريفه وتزييفه من قبل مرتكبي هذه الجرائم، فلا بد أن يتوفر على جملة من الشروط والتي نوردها في النقاط التالية:

أ- أن يكون للدليل الإلكتروني علاقة بموضوع الجريمة الإلكترونية المرتكبة: في هذا الصدد نجد المادة 407 من قانون الإثبات الفيديرالي الأمريكي قد تضمنت النص على ضرورة توفر هذا الشرط الذي أطلقت عليه تسمية مبدأ العلاقة الكاشفة "THE PRINCIPAL OF RELEVANCE" أي أنه وفقا لهذا القانون لا بد من أن يجمع بين الدليل والواقعة التي التي هي محل دعوى علاقة ما،[1] إضافة إلى أنه حتى يتم إثبات تلك العلاقة الكاشفة يستلزم توفر شرط آخر يتمثل في أن يكون ذلك الدليل الإلكتروني الذي تم إستخراجه من الحاسوب مطابقا للأصل الموجود داخل الجهاز، ولكي يتحقق هذا الشرط يجب أن لا يسجل أي إدعاء أو دفع بأن تلك البيانات ليست صحيحة والسبب في ذلك يعود لسوء دقة عمل الحاسوب.[2]

[1] حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 267.

[2] خضرة شنتير ، مرجع سابق، ص 52.

ب–أن يكون الدليل الإلكتروني المحصل من الجريمة الإلكترونية مشروعا: المشروعية تعني التقيد والإلتزام بأحكام القانون وذلك ضمن إطاره ومضمونه العام،[1] وطبقا لهذا الشرط فإنه يستلزم إتباع إجراءات شكلية وموضوعية من أجل الحصول عليه، فلا يمكن للقاضي أن يبني حكمه بناء على دليل تم التحصل عليه بطريقة غير مشروعة كالقيام بإفشاء سر مهنى أو خيانة أمانة، فمشروعية الأدلة حدا يمنع تجاوزه.[2]

ونجد بأن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات قد أوصى بهذا الشرط ضمن التوصية رقم 18 والتي أشارت إلى أنه ينبغي إحترام مبدأ المشروعية خلال عملية البحث عن دليل ضمن جرائم الحاسوب، وكذا الجرائم التقليدية التي ترتكب في بيئة تكنولوجيا المعلومات وفي حالة الإخلال بذلك يترتب بطلان الإجراء.[3]

لذلك يجب على الجهات المكلفة بالبحث عن الدليل الإلكتروني الإلتزام بالشروط التي يحددها القانون، ففي حكم صادر عن المحكمة الإستئنافية بالجيزة –مصر– سنة 2014 قضت من خلاله بصحة الدليل الإلكتروني المتحصل عليه من خلال عملية التفتيش لجهاز حاسوب تم ضبطه لدى المتهم في حالة تلبس، بمناسبة قيام أحد البنوك بالتبليغ ضد طرف مجهول متهم بسرقة أرقام البطاقات الإئتمانية المتعلقة بعملاء البنك، وكان المتهم قد إستخدمها في عملية الشراء عبر المواقع الإلكترونية، وبعد عملية تفتيش الحاسوب تم العثور على رسائل كان المتهم قد تبادلها مع مواقع التسوق، بالإضافة إلى كم هائل من البيانات خاصة ببطاقات إئتمانية مختلفة،[4] فرغم أن الإذن شرط جوهري للقيام بعملية التفتيش إلا أنه في هذه الحالة قد أعتبر الدليل الإلكتروني صحيحا رغم أن الحصول عليه تم دون إذن، لماذا ذلك؟

---

[1] خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، مرجع سابق، ص 47.

[2] ميرفت محمد حبابية، مرجع سابق، ص 243.

[3] بن فردية محمد، (الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، ع 1، مج، 9، الصادر في 2014، ص 281.

[4] خضرة شنتير ، مرجع سابق، ص ص 52، 53.

لأن القضاء والفقه في مصر يقر بجواز التفتيش دون الحصول على إذن في حالات التلبس، لذلك حتى يتم إثبات الجرائم الإلكترونية التي تتعرض لها شركات المساهمة يجب أن يكون الدليل الإلكتروني وليد إجراءات مشروعة وقانونية وإلا أعتبر باطلا وتم صرف النظر عنه.

ت–تمتع الدليل الإلكتروني باليقينية وعدم الشك: تعتبر النظم القانونية أن اليقين هو حالة ذهنية أو عقلية تجزم بوجود حقيقة، حيث يتم التوصل إليها من خلال ما يتم إستنتاجه بواسطة مختلف وسائل الإدراك التي يستعملها القاضي جراء ما يعرض عليه ضمن وقائع الدعوى وكذا ما يتبلور في ذهنه من إحتمالات وتصورات، تكون على مستوى عال من التأكيد ودرجة اليقين يتم التوصل إليها من خلال المعرفة التي تكون على نوعين، معرفة حسية يتم إدراكها بالحواس والأخرى يتم إدراكها بالعقل وذلك من خلال القيام بعملية التحليل والإستنتاج،[1] وعليه فإن الوصول إلى يقينية الدليل الإلكتروني يتطلب من القاضي الإلمام بالمعرفة التقنية في مجال تكنولوجيا المعلومات، حتى يتم الجزم بوقوع جريمة إلكترونية وهذا بطبيعة الحال يختلف عن يقينية الأدلة التقليدية والتي يمكن الوصول إليها من خلال الحواس والمعاينة وكذا عملية التحليل والإستنتاج.

ومن حيث يقينية الدليل الإلكتروني نجد بأن الفقه الكندي قد إعتبر بأن مخرجات جهاز الحاسوب تتمتع بدرجة كبيرة من اليقينية، بل أن القضاء الأمريكي قد ذهب إلى القول بأن النسخ التي يتم إستخراجها من البيانات التي يحتويها جهاز الحاسوب تعد أفضل أدلة الإثبات.[2]

لذلك ومن أجل إثبات الجرائم الإلكترونية يجب الإعتماد على دليل إلكتروني بعيد تماما عن الشك والظن، كون أن هذا يفسر لصالح المتهم ويتم الحكم عليه بالبراءة مما ينعكس بالسلب على الشركة الضحية.

ث–قابلية الدليل الإلكتروني للمناقشة: من المبادئ التي تقوم عليها شفوية المحاكمة هو أن يتم مناقشة الأدلة المعروضة وذلك بما فيها الأدلة الإلكترونية حتى يتم مواجهة الأطراف بها وإطلاعهم عليها.[3]

---

[1] حسين ربيعي ،آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 267.

[2] محمد بن فردية ، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي دراسة مقارنة، مرجع سابق، ص 281.

[3] دلال مولاي، مرجع سابق، ص 135.

وهذا الشرط نجد بأن المشرع الجزائري قد تطرق إليه في الفقرة الثانية من المادة 212 من قانون الإجراءات الجزائية والتي جاء فيها " ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت فيها المناقشة حضوريا أمامه".

وبالتالي فإن الأدلة الإلكترونية التي تخلفها الجرائم الإلكترونية التي ترتكب على شركات المساهمة سواء تم الحصول عليها من خلال أجهزة الحواسيب أو شبكات الأنترنت، وسواء كانت في شكل مطبوع أو كانت في صورة بيانات يتم عرضها على الشاشة أو مخزنة ضمن دعامة لا بد أن تخضع للمناقشة،[1] وباعتبار أن الدليل الإلكتروني من الناحية التطبيقية يكون على درجة من التعقيد ولا يكون للقاضي دراية في التعامل مع التعقيدات التقنية المعلوماتية فيمكن الإستعانة بخبير خلال الجلسة حتى يقوم بشرح هذا الدليل وتتم عملية مناقشته.[2]

وبهذا يكون الدليل الإلكتروني متساوي مع أدلة الإثبات الأخرى رغم طبيعته الخاصة التي لا تتوافق والجريمة الإلكترونية التي يتولد عنها، ولكن رغم توفره على جملة الشروط التي تم عرضها إلا أن مسألة تقديره من أجل إعتماده كدليل لإثبات تلك الجرائم تعود للقاضي هذا ما نوضحه في النقطة الموالية.

2-سلطة الجهة القضائية المختصة في تقدير الدليل الإلكتروني: مثلما سلف الذكر فإن المشرع الجزائري كان قد منح للقاضي الحرية في الأخذ بالأدلة التي يراها مناسبة وفقا لسلطته التقديرية في تقييم وتقدير تلك الأدلة حتى يقتنع بها ويستند إليها.

وبما أن الأدلة الإلكترونية التي تخلفها الجرائم الإلكترونية تلعب دورا مهما في عملية إثباتها غير أنه تطبيقا للمبدأ الذي أخذ به المشرع الجزائري في مجال الإثبات فإن ضبط الأدلة الإلكترونية مستوفية للشروط التي سبق شرحها لا يعد كافيا، ما لم يتم إخضاع هذه الأدلة للسلطة التقديرية لقاضي الجهة القضائية التي تكون مختصة بالفصل في الجرائم الإلكترونية التي تتعرض لها شركات

[1] حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص 268.

[2] دلال مولاي ملياني ، مرجع سابق، ص 316.

المساهمة، حيث تقوم السلطة التقديرية للقاضي على مبدأ الإقتناع الشخصي له، فما المقصود بهذا المبدأ؟

مبدأ الإقتناع الشخصي للقاضي يجد أساسه القانوني في المادتين 212 و 307 من قانون الإجراءات الجزائية واللتان نكتفي بذكر رقمهما فقط دون إعادة نصهما تفاديا للتكرار حيث سبقت الإشارة إليهما، أما أساسه القضائي فنجد بأن المحكمة العليا قد قضت به في عدة أحكام منها " من المقرر قانونا بأنه لا يمكن مطالبة قضاة محكمة الجنايات بتقديم حسابا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم الشخصي، ولا يرسم لهم بها قواعد يتعين عليهم أن يخضعوا على الأخص تقدير تمام أو كفاية دليل ما"[1]

ويعرف مبدأ الإقتناع الشخصي للقاضي من طرف الأستاذ "محمود نجيب حلمي" على أنه يتمثل في السلطة التقديرية التامة للقاضي من أجل وزن كل دليل لمعرفة قيمته وثقله ليكون له في النهاية سلطة إستخلاص نتيجة تكون منطقية، بناء على تلك الأدلة والتي تتمثل إما في تقرير الإدانة أو البراءة،[2] كما يعرف على أنه تلك الحرية التي يتمتع بها القاضي والتي تخوله أن يستمد قناعته من أي دليل من الأدلة المعروضة ضمن الدعوى يرى بأنه مطمئن إليه، دون أن يكون مقيدا بدليل معين.[3]

وبالتالي فهذان التعريفان يصبان في معنى واحد وهي بإمكان القاضي أن يستند إلى الدليل الذي يطمئن إليه أو أن يطرح أي دليل آخر لا يكون مقنعا بالنسبة له دون أن يفرض عليه في ذلك أي قيد إلا ما يمليه عليه ضميره والعدالة، ولا يكون مكلفا بتوضيح الأسباب التي بنى عليها إقتناعه الشخصي.

وانطلاقا مما سبق ذكره وحتى يتم إثبات الجرائم الإلكترونية التي تكون قد تعرضت لها شركات المساهمة ونسبتها إلى فاعلها وجب إخضاع الأدلة الإلكترونية المحصلة إلى السلطة التقديرية

---

[1] حفيظة عياشي ، (سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري)، مجلة القانون والعلوم السياسية، ع 1، مج، 9، الصادر في 2022، ص 557.

[2] فيصل بدري ، مرجع سابق، ص 247.

[3] دلال مولاي ملياني ، مرجع سابق، ص 318.

للقاضي، حتى يقوم بعملية تقييمها وتقديرها فيأخذ ما أقتنع به ويطرح ما لا يطمئن إليه بسبب ضعفها أو لوجود أدلة أقوى منها، لكن ينبغي أن نشير أيضا إلى أن سلطة القاضي في تقدير الدليل الإلكتروني لا تتم بطريقة عشوائية وإنما وفق ضوابط تعتبر بمثابة صمام أمان يمنع القاضي من الإنحراف عند القيام بعملية التقدير.

حيث أن تلك الضوابط منها ما يتعلق بشروط الدليل الإلكتروني والذي يعتبر مصدر إقتناع القاضي كأن يكون مشروعا، إذ من غير الممكن أن يصل القاضي إلى بناء إقتناعه الشخصي على أدلة تم التحصل عليها وفقا لإجراءات باطلة،[1] أو أدلة لم يتم مناقشتها كأن يقضي في الجرائم الإلكترونية المرتكبة إنطلاقا من رأي الغير فيها أو بناء على معلومات سابقة لديه،[2] إلى غير ذلك من الشروط التي سبق شرحها.

ومن الضوابط ما يتعلق بالإقتناع في حد ذاته، أي أن يكون القاضي قد وصل فعلا درجة اليقين الحقيقي بصحة تلك الجرائم المعروضة أمامه، كما يجب أن يتوافق ذلك الإقتناع مع مقتضيات العقل والمنطق أي أن إستخلاص وقائع الدعوى يكون معقولا وليس متعارض معها،[3] إضافة إلى كل هذا ينبغي على الجهة القضائية أن تسبب حكمها وذلك ببيان الواقعة الإجرامية التي تعرضت الشركة إليها والظروف والملابسات التي أرتكبت فيها وكذا الأساس القانوني الذي بموجبه تم إصدار الحكم.

المطلب الثاني:

إجراءات تحقيق الأمن المعلوماتي في شركات المساهمة

بعد أن تطرقنا إلى مختلف الجوانب الإجرائية من تحري وتحقيق ومحاكمة وإثبات الخاصة بالجرائم الإلكترونية التي ترتكب في إطار شركات المساهمة، ننتقل إلى جانب إجرائي آخر وهو لا يقل أهمية عما سبق التطرق إليه كونه يتعلق بالجانب الأمني والوقائي لهذه الشركات من خطر تلك الجرائم بعد أن أصبحت تشكل خطرا حقيقيا يهدد سلامتها ووجودها.

---

[1] يزيد بوحليط، مرجع سابق، ص 293.

[2] محمد بودالي ، مرجع سابق، ص ص 346، 347.

[3] يزيد بوحليط، مرجع سابق، ص 294.

فشركات المساهمة أضحت فعلا بحاجة ماسة إلى آليات كفيلة بتحقيق الحماية اللازمة لبياناتها ومعلوماتها وشبكاتها، أي تحقيق أمنها المعلوماتي، هذا ما سنعالجه من خلال هذا المطلب وذلك بالتعرض إلى مفهوم الأمن المعلوماتي **(فرع أول)** ثم الآليات التقنية للوقاية من الجرائم الإلكترونية وتحقيق الأمن المعلوماتي **(فرع ثاني)**.

الفرع الأول:

مفهوم الأمن المعلوماتي.

ما توصلنا إليه من خلال عملية البحث في هذا الموضوع هو أن شركات المساهمة لم تعد في معزل عن الجرائم الإلكترونية التي سبق التطرق إليها، لذلك فإن موضوع تحقيق الأمن المعلوماتي بات يؤرق عديد الشركات من أجل التصدي لتلك الجرائم ومنعها من التوغل أكثر حتى تحافظ على مكانتها وتواجدها في السوق.

أولا: تعريف الأمن المعلوماتي.

لقد أسال موضوع الأمن المعلوماتي الكثير من الحبر من أجل محاولة تعريفه، لذلك سنتطرق إلى أهم التعريفات التي قيلت بشأنه.

يعرف على أنه مجموع الأدوات التقنية وكذا الإجراءات التي يتم إستخدامها قصد حماية النظام من جميع الإستخدامات غير الشرعية، كالسرقة، التعديل أو الإضرار بالمعلومات أو قواعد البيانات،[1] كما عرفه الأستاذين "WHITMAN ET MOTTOD" في كتابهما تحت عنوان "مبادئ أمن المعلومات" على أنه المحافظة على سرية وسلامة المعلومات في مختلف مراحل المعالجة والحفظ والنقل، حيث يتحقق ذلك من خلال تطبيق السياسات الأمنية وكذا تعزيز الوعي والتدريب.[2]

كما عرفته لجنة أنظمة القومي الأمريكية (CNSS) بأنه حماية المعلومات وكذا عناصرها، بالإضافة إلى الأنظمة والأجهزة التي تستعمل في تخزين وإرسال تلك المعلومات، أما هيئة الاتصالات وتقنية المعلومات السعودية فترى على أنه، الحرص على إبقاء المعلومات تحت السيطرة المباشرة

---

[1] نوفيل حديد، كريبط حنان، (أمن المعلومات ودوره في مواجهة الإعتداءات الإلكترونية على نظام معلومات المؤسسة)، مجلة المؤسسة، ع 1، ، الصادر في 2014، ص 197.

[2] أسماء فيلالي ، عبد اللطيف شليل ، تهديدات أمن المعلومات وسبل التصدي لها، مرجع سابق، ص 164.

وعدم السماح بإمكانية الوصول إليها من قبل أشخاص آخرين دون إذن مع إدراك صاحب تلك المعلومات للمخاطر التي قد تلحق به عند السماح لشخص ما بالوصول إليها،[1] أما القانون الفرنسي فنجد بأنه قد تطرق إلى تعريفه ضمن القانون رقم 2004-575 المتعلق بالثقة في الاقتصاد الرقمي وذلك في المادة 29 منه.[2]

وانطلاقا من هذه التعريفات يمكننا أن نقدم بدورنا تعريفا للأمن المعلوماتي بالنسبة لشركات المساهمة على أنه، جملة التدابير والإجراءات التي تتخذها هذه الشركات بهدف توفير الوقاية والحماية لمنظومتها المعلوماتية ومنع الغير من الوصول إليها بطرق غير قانونية لتحريفها والعبث بها، وبالتالي تأمين بيئتها الإلكترونية وتعزيز مستوى الحماية لديها.

فيمكن القول بأن شركات المساهمة قد حققت الأمن المعلوماتي حين تضمن سلامة معلوماتها المتواجدة في فضائها الإلكتروني من خلال مختلف العمليات التي يقوم بها نظامها المعلوماتي من نقل ومعالجة وتخزين ضد مختلف التهديدات التي يمكن أن تلحقها وتسبب لها أضرار.[3]

ثانيا: أهداف الأمن المعلوماتي وعناصره:

تتجلى أهداف الأمن المعلوماتي بالنسبة لشركات المساهمة في ضمان الحماية الكاملة لنظامها المعلوماتي ومكوناته، وبالتالي ضمان نزاهة معلوماتها،[4] ومنع إدخال أية تعديلات أو تغييرات غير شرعية عليها، [5] كما أنه يضمن السيطرة على أي هجوم يستهدفها قصد الإستيلاء على سريتها أو تعطيل أجهزتها،[6] وعليه فالهدف الأساسي الذي يهدف إليه الأمن المعلوماتي هو حماية

---

[1] خالد حسن أحمد لطفي، الأمن المعلوماتي التهديدات والتدابير التشريعية والتقنية لحمايته، د،1، الإسكندرية، دار الفكر الجامعي، 2021، ص 79.

[2] Art: 29: de la loi N^0 2004-575 du 21 juin 2004 On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu il s'agisse d'information ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secréte.

[3] عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، د،ط1، الجزائر، دار الخلدونية، 2017، ص 68.

[4] يوسف خليل يوسف عبد الجابر، "مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية" (رسالة ماجستير، كلية الأعمال، جامعة الشرق الأوسط، 2013)، ص 22.

[5] نوفيل حديد، كريبط حنان، مرجع سابق، ص 198.

[6] خالد حسن أحمد لطفي، الأمن المعلوماتي التهديدات والتدابير التشريعية والتقنية لحمايته، مرجع سابق، ص 82.

شركات المساهمة من أي خطر قد ينجم عن تعرضها لإحدى الجرائم الإلكترونية التي سبق التطرق إليها.

خاصة وأن الأمن المعلوماتي أصبح قضية إستراتيجية كون أن نجاح هذه الشركات يتوقف عليه، لا سيما بعد سعيها نحو إعتماد تكنولوجيات الإعلام والإتصال في القيام بأعمالها التجارية التي أصبحت ذات طابع إلكتروني، وبهذا بات من الضروري تحقيق الأمن وضمان الحماية لمواقعها ومواردها الإلكترونية التي تعد الأساس الذي تقوم عليه أنشطتها التجارية، وحتى تتحقق أهداف الأمن المعلوماتي يجب عليها إتخاذ إستراتجية أمنية تطلع عليها الأفراد العاملين ضمن شبكاتها الداخلية ومواقع معلوماتها الحساسة وتلزمهم بها من خلال إتخاذ جملة من الخطوات منها:

-التفكير في المخاطر والجرائم التي يمكن أن تتعرض لها الشركة؛

- تحليل ومناقشة تلك المخاطر والجرائم التي كانت محل إحتمال من تعرض الشركة لها؛

-القيام بدراسة البدائل الأمنية التي تتوفر لديها؛

-القيام باختيار أحسن التقنيات الأمنية مع تحديد الخواص التي تتميز بها كل تقنية.[1]

وبالتالي توفير حمايتها وأمنها في جميع الأوقات،أما بالنسبة للعناصر التي يرتكز عليها الأمن المعلوماتي فتتمثل في:

1-السرية: وتعني المحافظة على المعلومات حيث أنه لا يمكن إستخدامها أو حتى الإطلاع عليها إلا بعد الحصول على إذن يسمح بذلك من طرف المسؤول عليها بالشركة، فالنظام الآمن هو ذلك النظام الذي يضمن سريتها بالإضافة إلى ضمان تأمين الطرق المناسبة التي تحميها من القراءة خلال عملية نقلها عبر شبكات الإتصال مع رسم حدود إستخدامها سواء كان إستخداما كليا أو جزئيا،[2] والسرية ضرورية جدا بالنسبة لشركات المساهمة حتى تتمكن من حماية أسرارها التجارية

[1] نادية لونيس ، "أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، مرجع سابق، ص 133.

[2] أسماء فيلالي ، "مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة، مرجع سابق، ص 63.

عن غيرها من الشركات المنافسة، كما أن السرية تتعلق من بالمعلومات الخاصة بعملائها والمتعاملين معها.[1]

2-التكاملية وضمان سلامة المحتوى: ويعني هذا العنصر بأن يتم التأكد من أن محتوى تلك المعلومات لا يزال صحيحا ولم يتعرض لأي تعديل أو عبث وبشكل خاص، وذلك في مختلف مراحل المعالجة سواء ضمن مرحلة التعامل الداخلي مع تلك المعلومات أو من خلال إعتداء غير مشروع.[2]

3-المراقبة: من أهم عناصر الأمن المعلوماتي هو أن يضمن ويوفر المراقبة المستمرة والدائمة التي يمكن من خلالها للقائمين على الأمن المعلوماتي لشركات المساهمة من معرفة الجناة الذين حاولوا الولوج إلى بياناتها، وكشف العمليات التي تمت بها من نقل أو تعديل أو حتى حذف، فمن خلال عنصر المراقبة تكون هناك سيطرة على قاعدة البيانات وتتيح إمكانية معرفة أي إختراق وإثباته في حينه.[3]

4-توفير البيانات: من الدلائل التي تؤكد على أن أمن النظام المعلوماتي للشركة هو أنه يقوم بتأدية عمله بكفاءة عالية، أي توفير المعلومة بصفة سليمة وكاملة ودون أيه أخطاء تتخللها وذلك في أي وقت يتم طلبها من قبل المسؤول عنها في تلك الشركة.[4]

5-الموثوقية: ويعني هذا العنصر التحقق من هوية المستخدم، بمعنى التأكد من صفة الجهة التي تتعامل معها هذه الشركة والتي ستقوم بإرسال معلومات لها،[5] حتى لا تكون ضحية لجناة ينتحلون صفة الجهة المتعاملة معها.

---

[1] بوزيد بن محمود، سهام عباسي، (الأمن المعلوماتي في ظل قانون التجارة الإلكترونية في الجزائر)، مجلة االبيبان للدراسات القانونية والسياسية، ع 13، مج، 3، الصادر في جوان 2018، ص 81.

[2] لمين علوطي، (تحديات الأمن الإلكتروني في المؤسسة)، مجلة أبحاث إقتصادية وإدارية، العدد 6، ، الصادر في 2009، ص ص 167، 168.

[3] محمد البغدادي، مفهوم أمن المعلومات وعناصره، مقال منشور في مارس 2021، أطلع عليه بتاريخ 2023/11/07. متاح على الرابط :https://mqall.org/concept-information-security/

[4] المرجع نفسه.

[5] نادية لونيس ، أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات –دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، مرجع سابق ص 128.

فهناك العديد من الشركات التي تقوم بتدعيم أجهزة معدات الإستخدام عن بعد خادم "RADIUS" في أجهزة الخادم للإتصال عن بعد وذلك بغية التأكد من هوية المستخدم، كذلك يتيح تبسيط إدارة الهوية وذلك عن طريق قاعدة البيانات المركزية لحقوق الإستخدام، فذلك الخادم بمقدرته التحقق من هوية أولئك المستخدمين الذين يتصلون بالشركة وذلك عن طريق قاعدة بيانات مشتركة وبناء على تلك المعطيات التي تحتويها هذه القاعدة يتم تحديد هوية المستخدمين والتأكد منها،[1] وبالتالي فإن الأمن المعلوماتي لشركات المساهمة يرتكز على مجموع هذه العناصر المحددة من قبل المختصين.

6-عدم إنكار التصرف: ويعني ذلك ضمان عدم إنكار الطرف الذي أقدم على إرتكاب تصرف ما متصل بالمعلومات أو مواقعها أنه هو من فعل ذلك، وهذا من خلال توفر القدرة على إثبات أن التصرف الذي أرتكب قد تم من طرف شخص ما في وقت محدد، وبذلك فإن الطرف الذي وصل إلى المعلومات الموجودة بالنظام المعلوماتي هو من يتحمل المسؤولية في حالة ما إذا طرأ عليها تغيير أو تعديل سواء كان ذلك الشخص موظف عادي أو كان مسؤولا عن النظام المعلوماتي بهذه الشركة أو أحد عملائها.[2]

الفرع الثاني :

الآليات التقنية للوقاية من الجرائم الإلكترونية في شركات المساهمة وتحقيق أمنها المعلوماتي.

بما أن الجرائم الإلكترونية أصبحت خطرا يهدد وجود واستمرارية شركات المساهمة لذالك فإن تحقيق أمنها المعلوماتي يتطلب أن تكون هناك منظومة حماية قادرة على تأمين نظامها المعلوماتي، من أي خطر يهدد معطياته وبياناته ولا يتحقق ذلك إلا من خلال جملة من الآليات والتدابير ذات الطابع التقني تعتمد عليها من أجل رسم سياسة وقائية تحميها من التعرض للجرائم الإلكترونية، ومن خلال هذا الفرع نوضح أهم هذه الآليات والتي نوردها على النحو التالي:

---

[1] لمين علوطي ، مرجع سابق، ص 173.

[2] بوزيد بن محمود، سهام عباسي، ص 81.

أولا: تقنية الجدار الناري.

1-تعريف الجدار الناري:[1] يعد من أنجع الحلول للشركات الكبرى وهي عبارة عن حل يقوم على مزيج من الأجهزة والبرامج تتوسط شبكة الشركة الداخلية وشبكة الأنترنت، حيث تتمثل مهمة هذا الجدار في منع المرور للأطراف غير المصرح لهم بذلك من جهة والسماح للأطراف المرخص لهم من جهة أخرى[2]، فهو بمثابة جسر إلكتروني أو عازل يفصل بين شبكة الأنترنت وشبكة الشركة.[3]

ويعرف على أنه برنامج أو جهاز يعمل على حماية أجهزة حواسيب الشركة من الهجمات خلال عملية إتصالها بشبكات الأنترنت، حيث يتولى مهمة فحص مجمل البيانات والمعلومات الواردة إليها عبر شبكة الأنترنت أو عبر أية شبكات أخرى، ففي حالة ما إذا توافقت تلك البيانات والمعلومات مع إعدادات جدار الحماية فإنه يسمح لها بالمرور إلى أجهزة حواسيب الشركة، أما في حالة ما إذا إكتشف أنها عبارة عن برامج تجسس مثلا أو فيروسات كونها لا تتوافق مع إعدادات جدار الحماية فيقوم بطردها ومنعها من الدخول،[4] كما يعمل هذا الجدار على تجزئة الشبكات إلى أجزاء وذلك بغية عزل وفصل الشبكات المصابة عن غيرها من الشبكات السليمة حتى تتم وقايتها.[5]

وبذلك تحمي شركات المساهمة بياناتها من خطر إتلافها جميعا، ففي عدة أحيان يتم الإعتداء عليها بغرض إتلاف جزء من منظومتها فيترتب عليه إتلاف كامل المنظومة المعلوماتية وتعطيلها، غير أنه بفضل السياسة الرقابية التي تمارسها تقنية الجدار الناري تمنع من تحقيق ذلك، وبالتالي

---

[1] مصطلح الجدار الناري يعود إلى أكثر من قرن حيث كان يتم بناء البيوت عن طريق طوب توضع في الجدار، وذلك من أجل وقف النيران التي قد تحدث فجأة ، حيث كانت تشكل حماية لها، (أسماء فيلالي ، مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة، مرجع سابق، ص 106.

[2] محمد حسن عمر، الإدارة والتقنية شركاء في مواجهة تحديات عصر الأنترنت، د، ط ، الرياض، مكتبة الملك فهد، 1997، ص 162.

[3] إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية دراسة مقارنة، د، ط ، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2019، ص 122.

[4] عيسى سليم داود الزيدي، مرجع سابق، ص 257.

[5] ضرغام جابر عطوش آل مواش، مرجع سابق، ص ص 74، 75.

يمكن القول بأن أهمية تقنية الجدار الناري كأسلوب حماية لشركات المساهمة تتجلى من خلال تحقيق المزايا التالية:

-يعتبر كمصفاة كونه يقوم بفحص جميع البيانات المراد تمريرها إلى النظام المعلوماتي للشركة عبر شبكة الأنترنت؛

-سد المنافذ والقنوات أمام جميع البيانات الغريبة والملوثة وعدم السماح لها لدخول؛

-يمثل دور برج المراقبة من خلال قيامه بعملية تتبع وتسجيل جميع الأنشطة التي قد تؤدي أخطار والتنبيه إليها.

2-أنواع الجدر النارية: يوجد الجدار الناري في عدة أنواع نوردها فيما يلي:

أ-جدار ترشيح الرزم: وهي أبسط أنواع الجدر حيث يتجلى دوره في فحص كل رزمة شبكية بصفة منفردة، دون أن يكون بإمكانه إدراك حالة الإتصال، وبالتالي فهو يقوم بالسماح بمرور الرزمة على ما تحويه بدايتها.[1]

ب-الجدار ذات الحالة: هذا النوع من الجدر تكون له القدرة وإمكانية على تحديد حالة إتصال الرزم وذلك بعكس النوع الأول، فهذا الجدار يقوم بالعمل عبر كافة الرزم الشبكية التي تكون مترابطة إلى أن يتمكن من ضبط حالة الإتصال وذلك قبل أن يتم تطبيق قواعد الجدار على البيانات المرسلة عبر الشبكة.[2]

ت-جدار التطبيقات: هذا النوع أكثر فاعلية من النوعين السابقين كونه يعمل على تحليل كافة البيانات المرسلة، وبالتالي يسمح بمطابقة هذه البيانات على قواعد الجدار الناري،[3] حيث يقدم درجة كبيرة من الأمان وأكثر ما تستعمله الشركات.

وينبغي أن نشير إلى أنه رغم المزايا التي تقدمها تقنية الجدار الناري، كونه هو المسؤول عن أية عملية دخول أو خروج تتم بين الشبكات، غير أن إستخدامه قد يترتب عنه بطء عملية التعامل مع شبكات الأنترنت كما أنه يرفض بعض البيانات التي تكون سليمة وآمنة والتي تكون الشركة بحاجتها،

---

[1] عيسى سليم داود الزيدي، مرجع سابق، ص 259

[2] عيسى سليم داود الزيدي ، ص 259.

[3] المرجع نفسه، ص 259.

كما أنه لا يصد الجاني الذي يكون من الداخل ويقدم على سرقة البيانات مثلا،[1] وهو الأمر الذي إستدعى البحث عن تقنية أخرى والمتمثلة في التشفير.

ثانيا: تقنية التشفير:

1-تعريف التشفير[2]:يعرف التشفير على أنه تلك العملية التي تقوم بتحويل البيانات والمعلومات إلى شفرات غير مقروءة حتى يتم منع الجهات غير المرخص لها من الإطلاع عليها وفهم محتواها، وتتم عملية تنفيذ التشفير عن طريق مفاتيح تكون عبارة عن صيغ رياضية معقدة[3]، كما يعرف على أنه آلية تحويل البيانات التي تمت معالجتها إلكترونيا إلى رموز وذلك للحفاظ على سريتها وعدم إنتهاكها إذ أن هذه الآلية تقوم بإجرائين، الإجراء الأول هو الذي يتم فيه تحويل المعلومات إلى رموز أما الإجراء الثاني فيكون بطريقة عكسية أي يتم تحويل الرموز إلى حقيقتها أي معلومات عن طريق فك الشفرة.[4]

ونجد أن بعض التشريعات قد نضمته ضمن نصوصها القانونية بشكل صريح ومن ذلك ما ذهب إليه المشرع التونسي الذي عرفه في المادة الثانية من القانون المتعلق بالمبادلات والتجارة الإلكترونية[5]، والتي جاء فيها "التشفير هو إستخدام رموز أو إشارات غير متداولة لتصبح بمقتضاها المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من طرف الغير، أو إستخدام رموز أو إشارات لا يمكن بدونها الوصول إلى المعلومات.

---

[1]ضرغام جابر عطوش آل مواش، مرجع سابق، ص 76.

[2]عرف التشفير منذ القدم فأول من إستعمله هو إمبراطور الرومان وذلك من أجل المحافظة على سرية الرسائل أنذاك، حيث كانت الرسائل السرية تستخدم تقنية أساسية في حلول المراسلة بين الحروف مثلا حرف A يصبح D وحرف B يصبح T وهكذا، وعند القيام بعكس المدخلات نتحصل على الرسالة الحقيقية ومع التطورات التكنولوجية التي حدثت تطورت تقنية التشفير إلى تشفير المعلومات، نادية لونيس، أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، ص 110.

[3]لونيس نادية،أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات، المرجع نفسه، ص 130.

[4]ضرغام جابر عطوش آل مواش، مرجع سابق، ص 65.

الشفرة هي عبارة عن مفاتيح سرية تكون خاصة بجهة معينة تستخدمها من أجل تشفير بياناتها الموجودة بالحاسوب بواسطة الأرقام أو الحروف أو الرموز وحتى بالبصامات، ميرفت محمد حبابية، مرجع سابق، ص 126.

[5]القانون التونسي رقم 83 مؤرخ في 9 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية.

وانطلاقا مما سبق يمكننا أن نعرف التشفير في إطار شركات المساهمة بأنه، تلك الآلية التقنية التي تستعملها من أجل إخفاء بياناتها ومعلوماتها التجارية بحث يستحيل على غير المخول بالإطلاع عليها وفهم مضمونها لتحافظ على سريتها.

ولهذه التقنية أهمية كبيرة في الوقاية من الجرائم الإلكترونية ، إذ أصبح من أكثر الآليات التقنية إستعمالا من أجل الوقاية من هذه الجرائم وتحقيق الأمن المعلوماتي وحماية مختلف الصفقات والعمليات التي تتم عبر شبكة الأنترنت، إذ أن الكتابة بطريقة مشفرة هي الضمانة الأساسية للمحافظة على سرية المعلومة في ظل هذا التطور التكنولوجي الذي يشهده العالم.[1]

حيث أنه هناك العديد من الشركات الكبرى التي باتت تلجأ إلى الإعتماد على تقنية التشفير حتى تحمي نفسها من خطر الإختراقات التي تستهدفها والوصول إلى أسرار أعمالها، فمن خلال هذه التقنية تحمي نظامها المعلوماتي من أي خطر.[2]

2-أنواع التشفير: يمكن تنفيذ تقنية التشفير من خلال النوعين التاليين.

أ-التشفير المتماثل: ويعتبر هذا النوع قديم حيث يقوم على إستخدام ذات المفتاح بين كل من مرسل البيانات ومستقبلها ،[3] ويتم تحديد المفتاح عن طريق الاتفاق عليه من كلا الطرفين في بداية الأمر، حيث تتضمن كلمة المرور المتفق عليها حروف بعضها صغير والبعض الآخر كبير، بالإضافة إلى رموز أو أرقام لتقوم بعد ذلك برمجيات التشفير بتحويلها إلى عدد ثنائي، حيث يشكل ذلك العدد الناتج مفتاح تشفير الرسالة وبعد أن يتم إستقبال الرسالة التي تكون مشفرة، يقوم الطرف المستقبل لها باستخدام ذات كلمة المرور حتى يتم فك شفرة النص وإعادته إلى أصله.[4]

---

[1] ميرفت محمد حبابية، مرجع سابق، ص 130.

[2] عيسى سليم داود الزيدي، مرجع سابق، ص 267.

[3] أسماء فيلالي ، "مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة، مرجع سابق، ص 111.

[4] ضرغام جابر عطوش آل مواش، مرجع سابق، ص 67.

لكن ما يعاب على هذا النوع من التشفير هو أنه فرضا في حالة ما إذا حصل طرف آخر على كلمة المرور كون أنه يتم تبادلها بين الطرفين بطريقة غير آمنة، فإنه يصبح بإمكان ذلك الطرف الثالث فك الشفرة والإطلاع على محتوى الرسالة وهذا ما يشكل خطرا على طرفيها فيمكن إعتبار هذا النوع أقل أمانا.

ب- التشفير اللاتماثلي: يعود إكتشاف هذا النوع من التشفير إلى ثلاث علماء في الرياضيات في الولايات المتحدة الأمريكية وذلك سنة 1978،[1] وكان بمثابة حل للإشكال الذي ترتب عن التشفير والذي أعتبر غير آمن بسبب إستخدامه لمفتاح واحد، فالتشفير اللاتماثلي بدلا من إعتماده على مفتاح واحد فإنه يعتمد على مفتاحين تجمعهما علاقة معقدة، حيث يطلق على هذان المفتاحان بالمفتاح العام والمفتاح الخاص[2].

-المفتاح العام: (CLE PUBLIQUE) ويتضح من خلال تسميته بأنه يكون معروف لدى أكثر من جهة ولا يقصد إبقاؤه سرا،[3] غير أنه يستحيل فك الشفرة وفتح البيانات المرسلة من خلال هذا المفتاح فقط وإنما ينبغي للمستقبل أن يحصل على رقم سري والذي يتمثل في المفتاح الخاص وبذلك تكتمل العملية الحسابية وتفك الشفرة ويتم الإطلاع على محتوى البيانات التي يتضمنها الملف المرسل.[4]

-المفتاح الخاص: (CLE PRIVEE) وهو على خلاف المفتاح الأول، فهو سري ويحظى بالحماية والسلامة من أجل تفادي إستعماله من قبل الآخرين،[5] وإذ يعتبر هوية إلكترونية بسمح لصاحبه بفك البيانات المشفرة التي يتم إرسالها له.[6]

---

[1] صورية بوربابة ، قواعد الأمن المعلوماتي دراسة مقارنة، مرجع سابق، ص 56.

[2] عيسى سليم داود الزيدي، مرجع سابق، ص 265.

[3] صورية بوربابة ، قواعد الأمن المعلوماتي دراسة مقارنة، مرجع سابق، ص 56.

[4] عيسى سليم داود الزيدي، مرجع سابق، ص 265.

[5] صورية بوربابة ، قواعد الأمن المعلوماتي دراسة مقارنة، مرجع سابق، ص 56.

[6] عيسى سليم داود الزيدي، مرجع سابق، ص 265.

ثالثا: تقنية البرامج المضادة للفيروسات.

حيث أن هذه البرامج تضاف إلى قائمة الآليات التقنية التي تلجأ إليها شركات المساهمة من أجل حماية نظامها المعلوماتي من الإعتداءات عن طريق الفيروسات، فقد تتعرض هذه الشركات إلى جريمة الإعتداء على سير نظامها المعلوماتي وذلك بإعاقته أو إفساده، وبالتالي عرقلته عن أداء وظائفه بالشكل الطبيعي والمعتاد وأشهر القضايا في ذلك قضية فيروس "ZOOTB".[1]

وحتى تقي الشركات نفسها من خطر مهاجمتها عن طريق هذه الفيروسات تلجأ إلى الإستعانة ببرامج مضادة لها، والتي تعرف على أنها، تلك البرامج المصنعة خصيصا لمنع دخول الفيروسات إلى النظام المعلوماتي والتخلص منها في حالة إكتشافها، ولها إمكانية على تحديث نفسها بطريقة آلية تلقائية من خلال شبكة الأنترنت وذلك لتحسين ومضاعفة قدرتها وكفاءتها على مطاردة تلك الفيروسات،[2] كما أن هذه البرامج تعتبر الرقيب على الملفات التي يتم إستخدامها في الأنظمة المعلوماتية وذلك من خلال القيام بعملية فحصه للتأكد من سلامته من الفيروسات قبل أن يتم إستخدامه[3].

وتقوم البرامج المضادة للفيروسات بمنح تحميل أي برنامج ضار على جهاز الحاسوب وذلك عن طريق أجهزته المحيطية للإدخال أو عن طريق الشبكات التي يكون مرتبط بها، فمن خلالها يتم إيقاف الإعتداءات التي قد تتعرض لها شركات المساهمة عن طريق مختلف الفيروسات،[4] حيث أن هذه البرامج توجد في عدة أنواع يتم تصنيعها من قبل شركات متخصصة في ذلك، حيث تقوم بتطويرها كلما إستدعت الضرورة إلى ذلك وظهرت أنواع جديدة من الفيروسات .

---

[1] تمت الإشارة إلى هذه القضية في المبحث الثاني من الفصل الأول من هذا الباب، أنظر ص 228 .

[2] عائشة بن قارة مصطفى، (إستراتجية تحقيق الأمن المعلوماتي للحكومة الإلكترونية)، مجلة دار ارافد، د، ع، مج 2، ، الصادر في يناير 2021، ص 32.

[3] عيسى سليم داود الزيدي، مرجع سابق، ص 270.

[4] لونيس نادية، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة دراسة حالة مؤسسة EMPLOITIC، مرجع سابق، ص 132.

وبخصوص هذه البرامج ينبغي الإشارة إلى أنه رغم الحماية التي تقدمها إلى شركات المساهمة من خطر البرامج الضارة والمحافظة على أمنها المعلوماتي، غير أنه في مقابل ذلك لا تتمتع بإمكانية سد المنافذ بجهاز الحاسوب والتي من خلالها يتمكن الجناة من الوصول إلى بياناتها السرية والإعتداء عليها.

بالإضافة إلى هذه الآليات هناك آلية أخرى تسمى بأنظمة كشف التدخل، والتي هي عبارة عن أدوات بتم وضعها في نقاط الدخول التي تعد أكثر المداخل أهمية وحساسية بالنسبة لشبكات الشركة وذلك حتى يتم كشف جميع التدخلات، وعندها يقوم النظام بإطلاق إنذار في حال وقوع إعتداء خطير.[1]

وبالتالي ما يمكن قوله عن هذه الآليات هو أنه حتى وإن كانت توفر جزء من الحماية لشركات المساهمة من خطر الهجمات الإلكترونية التي قد تتعرض لها، غير أنه ليس بإمكانها توفير الحماية بشكل مطلق وتام وهذا إن دل فإنما يدل على صعوبة تحقيق الأمن المعلوماتي في المجال الإفتراضي لهذه الشركات بصورة كاملة، وذلك راجع إلى الديناميكية والتطور الذي يشهده مجال تكنولوجيا الإعلام والإتصال، فكلما تطورت وسائل الحماية تطورت معها وسائل المهاجمة التي يستخدمها الجناة من أجل تنفيذ جرائمهم الإلكترونية.

وأمام عقبات تحقيق الأمن المعلوماتي بصورة مطلقة لهذه الشركات فإنه يتوجب عليها إلى جانب الآليات التقنية العمل كذلك على تأمين العنصر البشري لديها، وذلك من خلال مراقبتهم والتحري عنهم والتأكد من ضمان إخلاصهم لها وضمان عدم إغرائهم من قبل شركات أخرى ،[2] وبالتالي فحتى العنصر البشري يعد آلية بالغة الأهمية بالنسبة لشركات المساهمة من أجل تحقيق أمنها المعلوماتي خاصة وأن العديد من الجرائم الإلكترونية التي تتعرض لها ينفذها موظفين لديها إما بصفة مباشرة أو عن طريق تعاونهم وتواطؤهم مع أطراف أخرى.

---

[1] أسماء فيلالي ، مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة، مرجع سابق، ص 114.

[2] فتيحة ليتيم ، نادية ليتيم ، (الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة)، مجلة المفكر، ع 1، مج، 10، الصادر في مارس 2015، ص 247.

ونجد بأن من أهم الإكتشافات التي توصل إليها العلم مؤخرا من أجل حماية البيانات والمعلومات ضمن مجال البيئة الإلكترونية هو إستخدام الخصائص البيولوجية للشخص قصد تأمينها، وهي تعد أكثر حماية من الآليات التقنية كون أن هذه الخصائص يستحيل أن يشترك فيها شخصان، مثل إستخدام حدقة العين من أجل التمكن من الولوج إلى النظام المعلوماتي وذلك عن طريق جهاز يكون مزود بشرائح إلكترونية ويتم تدعيمه ببرنامج له السرعة والدقة العالية في تحديد هوية الشخص من خلال الوقوف بقربه، ليقوم الجهاز بالتقاط صورة لحدقة العين ومعالجتها بواسطة شريحة "شفرة إيرس" ثم مقارنتها مع الصورة المخزنة بداخله سابقا، وفي حالة التطابق يسمح للشخص باستخدام الجهاز والولوج إلى النظام المعلوماتي والإطلاع على بياناته ومعلوماته.[1]

[1] حمزة بلحسيني ، مرجع سابق، ص ص 131، 132.

خلاصة الباب الثاني.

بناء على ما تم التطرق إليه في هذا الباب نخلص إلى القول بأن الجرائم الإلكترونية التي إستهدفت شركات المساهمة كانت متنوعة ومتعددة وجمعيها تعتمد على الأساليب التقنية التي تتناسب والبيئة الإفتراضية، كما أنه لكل نوع من هذه الجرائم تقوم عليها حتى يتحقق وقوعها.

ورغم الغموض والتعقيد الذي تتسم به إلا أنه تم مواجهتها من خلال الإعتماد على إجراءات خاصة في عملية التحري عنها والتحقيق فيها، حتى لا يتم إستفحالها بشكل أوسع في إطار شركات المساهمة، التي لجأت إلى إعتماد آليات تقنية تحمي من خلالها نفسها من خطر هذه الجرائم.

خاتمة

خاتمة:

بعد قيامنا بالبحث والدراسة في موضوع الجرائم الإلكترونية المرتبطة بشركات المساهمة يتضح لنا جليا بأن هذه الجرائم لم تعد تقتصر فقط على الأشخاص، بل أصبحت تستهدف بشكل أوسع هذه الشركات حيث تشهد إنتشارا رهيبا، كما أنها تشهد تنوعا وتجددا بشكل مستمر وذلك راجع بطبيعة الحال إلى التطورات الحاصلة في مجال تقنيات المعلومات، هذا المجال الذي يعرف إكتشافات واختراعات متتالية ومتلاحقة.

وكون أن شركات المساهمة غيرت من نمط أعمالها لتتجه إلى التقنيات التي أسفر عليها التطور التكنولوجي، الأمر الذي يعرضها للجرائم الإلكترونية بصورة أكبر ويجعلها الوجهة الأكثر إستهدافا، فبعدما كانت هذه الشركات في ظل الجرائم التقليدية ترتكب ضدها في نطاق جغرافي محدد فإن الأمر في ظل الجرائم الإلكترونية مختلف كونها جرائم عالمية النطاق فهي عرضة لإختراقات الجناة عبر مختلف أرجاء العالم.

فالتطورات التكنولوجية التي أدت إلى التحول الرقمي في جميع المجالات وعلى رأسها المجال التجاري الذي شهد إزدهارا وتطورا ملحوظا في جميع المجالات وعلى رأسها المجال التجاري الذي شهد إزدهارا وتطورا ملحوظا خاصة بالنسبة لشركات المساهمة، كانت الجرائم الإلكترونية الإنعكاس السلبي والجانب المظلم لتلك التطورات إذ كلفها في عديد المرات خسائر فاذحة ما كانت لتتعرض لها في ظل البيئة التقليدية حيث أن تلك الخسائر لا تؤثر على هذه الشركات فحسب وإنما حتى على إقتصاد الدولة التابعة لها وهذا ما يدل على حجم خطر الجرائم الإلكترونية التي أضحت تهدد وجود كبرى الشركات التجارية.

من جهة أخرى فإن هذه الجرائم الإلكترونية التي إستهدفت شركات المساهمة لا تنحصر في نوع واحد فقط وإنما تعددت وتنوعت بين جرائم مستحدثة لم تكن معروفة من قبل وجرائم كانت موجودة في ظل البيئة التقليدية وأصبح يعتمد في إرتكابها على الوسائل التقنية فكانت أكثر دقة.

وبالتالي فإن تصدي شركات المساهمة لهذه الجرائم والإستعانة بوسائل الحماية منها أمر في غاية الأهمية وإن كان ليس بالأمر السهل واليسير غير أنه ضرورة لا بد منها وذلك حتى تتمكن من

المحافظة على تواجدها وتحقيق أمنها المعلوماتي، وبالتالي فإن جملة النتائج المتوصل إليها من خلال هذه الدراسة نوردها فيما يلي:

-تدارك المشرع الجزائري للفراغ القانوني الموجود ومبادرته إلى إصدار جملة من القوانين من أجل مجابهة الجرائم الإلكترونية، بداية بالقانون رقم 04-15 والذي تضمن القسم السابع مكرر منه لهذه الجرائم تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ثم القانون رقم 09-04 والذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، بالإضافة إلى نصوص قانونية أخرى مثل القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين وكذا القانون رقم 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، وكذا القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، كل هذا إنما يدل على إدراك المشرع لخطورة الجرائم الإلكترونية.

-الجرائم الإلكترونية المستحدثة التي تتعرض لها شركات المساهمة تمت مكافحتها بموجب نصوص قانونية خاصة، في حين أن تلك الجرائم التقليدية التي أصبحت ترتكب بطريقة إلكترونية لم تحظ بنصوص قانونية خاصة وذلك رغم أنها تعتبر أكثر خطورة وتعقيدا من صورتها التقليدية.

-تستهدف الجرائم الإلكترونية شركات المساهمة في مالها المعلوماتي والمتمثل في المعلومات والأسرار التجارية، باعتبارها تشكل ثروة مالية وذات قيمة إقتصادية عالية.

-الجرائم الإلكترونية التي تستهدف شركات المساهمة يصعب التمييز والفصل فيها بين العمل التحضيري والشروع في تنفيذ السلوك الإجرامي، لذلك فالأعمال التحضيرية تعتبر جريمة في حد ذاتها.

-كل الجرائم الإلكترونية التي تتعرض لها شركات المساهمة تحمل بين طياتها نتيجة حتى وإن لم تتجلى بشكل ظاهر، فمجرد الولوج إلى نظامها المعلوماتي له نتيجة تتمثل في الإطلاع على أسرارها ومعلوماتها، وتحقق النتيجة.

-الطابع المعقد للجرائم الإلكترونية التي تتعرض لها شركات المساهمة تجعل من أعمال التحقيق لا تقتصر على المحققين فقط، بل أن الأمر يستلزم أن يكون هناك تعاون بينهم وبين الخبراء في مجال الحواسيب العاملين بهذه الشركات، وهناك بعض الجرائم التي هي أشد تعقيدا وعابرة للحدود حيث تتطلب الإستعانة بالشركات العالمية المختصة في هذه الجرائم قصد التعاون مع المحققين.

-يكون القانون الوطني مختصا بنظر الجرائم الإلكترونية التي ترتكب على شركات المساهمة في الإقليم الوطني إستنادً لمبدأ الإقليمية، وكذا تلك التي ترتكب على هذه الشركات خارج الإقليم الوطني من قِبل أشخاص يحملون الجنسية الوطنية إستنادً لمبدأ الشخصية، كما أن شركات المساهمة باعتبار الإعتداء عليها من خلال هذه الجرائم يُعد مساسا بالمصالح الإستراتجية للإقتصاد الوطني، وعليه فالقانون الوطني هو المختص إستنادً لمبدأ العينية.

-إنشاء المشرع الجزائري للأقطاب الجزائية المتخصصة والقطب الجزائي الوطني المتخصص يدل على إهتمام المشرع الوطني بمكافحة هذه الجرائم.

أما التوصيات التي يمكن تقدمها من خلال هذه الدراسة فتتمثل في:

-تلعب شركات المساهمة دورا سلبيا في التكتم والتستر على الجرائم الإلكترونية التي تتعرض لها خوفا على سمعتها وثقة عملائها فيها، وهذا ما يشجع الجناة على التمادي أكثر في إختراقها وبما أنها تمثل دعائم للإقتصاد الوطني حيث أن المساس بها يعني المساس بهذا الاقتصاد، لذلك نحبذ لو يتم إضافة نصوص قانونية تفرض على هذه الشركات التبليغ عن أية جريمة إلكترونية تتعرض لها من أجل تسليط الجزاء على مرتكبيها وردعهم، ووضع حد للتكتم والتستر عنها بحجة الخوف على سمعة الشركة إذ أن الخوف على مكانة الاقتصاد الوطني أولى.

-بما أن الجرائم التقليدية التي أصبحت تستهدف شركات المساهمة بطريقة إلكترونية لا تقل خطرا عن تلك المستحدثة، حبذا لو يتم تخصيصهاليه بنصوص خاصة بها دون العودة إلى النصوص القانونية التي حظيت بها صورتها التقليدية وذلك لإختلافهما سواء من حيث المحل الذي تنصب عليه وكذا الطريقة التي تنفذ بها.

-الأساليب المستخدمة في إختراق شركات المساهمة متنوعة ومتطورة ويستحيل حصرها، إذ لا يمكن التنبؤ بما ستسفر عليه التطورات التكنولوجية من أساليب أخرى في المستقبل، لذلك ينبغي على شركات المساهمة مسايرة هذه التطورات حتى تُجدد أنظمة الحماية الخاصة بها بشكل يتناسب وما تم التوصل إليه من أساليب.

-تمديد الإختصاص المحلي للأقطاب الجزائية المتخصصة كان من باب الجواز، ولكن نظرا لما تتميز به الجرائم الماسة بالنظام المعلوماتي من تعقيد وغموض، وهي من بين الجرائم الإلكترونية التي قد تتعرض لها شركات المساهمة، نحبذ لو أن تمديد الإختصاص المحلي لهذه الأقطاب كان من باب الجبر وليس الجواز خاصة وأن القضاء العادي أثبت عجزه في العديد من الجرائم الإلكترونية وبالتالي تفادي الإختصاص المشترك بين الجهات القضائية العادية وهذه الأقطاب.

-باعتبار أنه من الصعب جدا على شركات المساهمة توفير الأمن المعلوماتي لها بصورة مطلقة مما يتطلب ضرورة تأمين العنصر البشري لديها، لذلك حبذا لو تضاعف عقوبة الجرائم الإلكترونية التي تتعرض لها في حالة ما إذا كان مرتكبها أحد موظفيها.

قائمة المصادر
والمراجع

قائمة المصادر والمراجع باللغة العربية:

أولا:قائمة المصادر.

-القوانين الوطنية:

أ-الدستور:

1- دستور الجمهورية الجزائرية الديمقراطية الشعبية المعدل في 2020، الصادر بموجب المرسوم رقم 20-442 مؤرخ في 30 ديسمبر 2020، ج، ر، ع 82 الصادر بتاريخ 2020/12/30.

ب-الإتفاقيات الدولية:

1- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الأمانة العامة لجامعة الدول العربية، صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014، ج،ر، ع 57، الصادر في 28 سبتمبر 2014.

2- إتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001، الموقعة في 23 نوفمبر 2001 بالعاصمة المجرية بودابست.

ت-النصوص التشريعية:

1-قانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج، ر، ع 71 الصادر في 10 نوفمبر 2004.

2-القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، ج،ر، ع 71، الصادر في 10 نوفمبر 2004.

3-القانون رقم 05-01 مؤرخ في 6 فيفري 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم بالقانون رقم 15-06 المؤرخ في 15 فبراير 2015، ج،ر، ع 8 الصادر في 15 فبراير 2015.

4-القانون رقم 05-10 المؤرخ في 20 يونيو 2005، يعدل ويتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني المعدل والمتمم، ج،ر، ع 44 الصادر في 26 يونيو 2005.

5-القانون رقم 06-22 مؤرخ في 20 ديسمبر 2006-، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج،ر، ع 84، الصادر في 24 ديسمبر 2006.

6-القانون رقم 09-04، المؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج،ر، ع 47، الصادر في 16 غشت 2009.

7-القانون رقم 15-04 مؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين، ج، ر، ع 6 الصادر في 10 فبراير 2015.

8-القانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، ج، ر، ع 27 الصادر في 13 ماي 2018.

9-القانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي، ج، ر ، ع 34، الصادر في 10 يونيو 2018.

10-القانون رقم 22-09 مؤرخ في 5 ماي 2022، يعدل ويتمم الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري، ج،ر، ع 32، الصادر في 14 ماي 2022.

11-القانون رقم 24-02 مؤرخ 26 فبراير 2024 يتعلق بمكافحة التزوير واستعمال المزور، ج ر،ع 15، الصادر في 29 فبراير 2024.

12-القانون رقم 24-06 مؤرخ في 28 أفريل 2024 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج ر، ع 30 الصادر في 30 أفريل 2024.

13-المرسوم التشريعي رقم 93-08 مؤرخ في 25 أفريل 1993، يعدل ويتمم الأمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري، ج،ر، ع 27، الصادر في 25 أفريل 1993.

14-الأمر 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، ج ر، ع 78، الصادر في 30 سبتمبر 1957، المعدل والمتمم.

15-الأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري،ج، ر، ع 101، الصادر في 19 ديسمبر 1975، المعدل والمتمم.

16-الأمر رقم 01-04 مؤرخ في 20 غشت 2001، يتعلق بتنظيم المؤسسات العمومية الاقتصادية وتسييرها وخوصصتها، ج، ر،ج ،ج، ع 47، الصادر في 22 غشت 2001.

17-الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج، ر، ع 44، الصادر في 23 يوليو 2003

18-الأمر رقم 15-02 مؤرخ في 23 يوليو 2015، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج،ر، ع 40، الصادر في 23 يونيو 2015.

19-الأمر رقم 20-04 مؤرخ في 30 غشت 2020 يعدل ويتمم الأمر رقم 66-155 مؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج،ر، ع 51 الصادر في 31 غشت 2020.

20-الأمر رقم 21-11 مؤرخ في 25 غشت 2021 يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج،ر، ع 51 الصادر في 26 غشت 2021.

ث-النصوص التنظيمية:

1-المرسوم الرئاسي رقم 20-183 مؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج،ر، ع 40، الصادر في 18 يوليو 2020.

2-مرسوم تنفيذي رقم 06-348 مؤرخ في 5 أكتوبر 2006، يتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج، ر، ع 63 الصادر في 8 أكتوبر 2006.

-القوانين العربية:

1- القانون رقم 2 لسنة 2002، يتعلق بالمعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة.

2-قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، إعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بموجب القرار رقم 417-د 21 في 2004.

3-القانون رقم 34 لسنة 2021، يتعلق بمكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة.

4- مرسوم بقانون إتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

5- قانون العقوبات المصري طبقا لأحدث التعديلات بالقانون 95 لسنة 2003.

6- قرار رقم 109 لسنة 2005 مؤرخ في 2005/05/15 يتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

7- القانون رقم 175 لسنة 2018، يتعلق بمكافحة جرائم تقنية المعلومات، ج،ر لجمهورية مصر العربية، رقم 32 مكرر (ج)، الصادر في أغسطس، 2018.

8- نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم 17 في بتاريخ 03/26/ 2007.

9- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، الصادر بموجب المرسوم التشريعي رقم 17 لسنة 2012.

10- القانون الكويتي رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

11- القانون رقم 14 الصادر بتاريخ 2014/09/15، يتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، ج،ر، لدولة قطر، ع 15 الصادر في 10/02/ 2014.

12- القانون الأردني رقم 27 لسنة 2015، ج،ر، ع 5343 الصادر في 06/01/ 2015.

13- القانون التونسي رقم 83 مؤرخ في 9 أوت 2000، يتعلق بالمبادلات والتجارة الإلكترونية.

ثانيا: قائمة المراجع:

أ-الكتب العامة:

1- العياشي زرزار، كريمة غياد، إستخدامات تكنولوجيا المعلومات والإتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية ، ط 1، عمان ، دار صفاء للنشر والتوزيع، 2016.

2- أيمن بن ناصر بن محمد العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي – دراسة مقارنة- ، ط 1، الرياض ، مكتبة القانون والإقتصاد، 2016.

3- أحمد رعد محمد الجيلاوي، التسجيل الصوتي وحجيته في الإثبات الجنائي، د،ط، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2017.

4- أشرف أحمد عبد الوهاب، إبراهيم سيد أحمد، عقد الوديعة والحراسة في ضوء أراء الفقهاء والتشريع وأحكام القضاء، ط 1، القاهرة، دار العدالة للنشر والتوزيع، 2018.

5- إيهاب خليفة، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، ط 1، القاهرة، العربي للنشر والتوزيع، 2019.

6- أحمد سلام عبد العاطي، التجارة الإلكترونية ، ط 1، القاهرة مؤسسة طيبة للنشر والتوزيع، 2021.

7- آمال حفناوي، الخامسة سايحي، التسويق الإلكتروني للخدمات، د، ط، الأردن ، دار اليازوردي العلمية للنشر والتوزيع، 2022.

8- حمدي القبيلات، قانون الإدارة العامة الإلكترونية، ط 1، الأردن، دار وائل للنشر والتوزيع، 2014.

9- حامد محمد شبيب الجبوري، أهمية الإلتزام بالعقود وضماناتها للحقوق التعاقدية وفقا للقوانين المدنية العربية، ط 1، عمان الأردن، شركة دار الأكاديميون للنشر والتوزيع، 2015.

10- حشمت توفيق عزيز عياد، الإعلام وقضايا التنمية، د، ط، عمان الأردن، دار غيداء للنشر والتوزيع، 2016.

11- حسام الدين خلفي، أحكام المسؤولية الجزائية لشركات المساهمة ، ط 1، جمهورية مصر العربية ، مركز الدراسات العربية للنشر والتوزيع، 2020.

12- خضر مصباح إسماعيل طيطي، إدارة المعرفة، التحديات والتقنيات والحلول، ط 1، عمان ، دار االحامد للنشر والتوزيع ، 2009.

13- رمزي محمود، النقود والبنوك والتجارة الإلكترونية ثورة نقدية تقرع أبواب القرن الحادي والعشرين وإعادة صياغة مستقبل الشعوب ، د، ط، الإسكندرية ، دار التعليم الجامعي، 2022.

- 14- سعد غالب ياسين، بشير عباس العلاق، التجارة الإلكترونية، د، ط، عمان الأردن، دار المناهج للنشر والتوزيع، 2015.

15- صلاح الدين حسن السيسي، الموسوعة المصرفية والعملية، ج 2، ط 1، مصر، مجموعة النيل العربية، ، 2000.

16- طارق عفيفي صادق أحمد، نظرية الحق، ط 1، القاهرة، المركز القومي للإصدارات القانونية، 2016 .

17- عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، ط1، الرياض، مكتبة القانون والإقتصاد، 2012.

18- عبد القادر أحمد محمد صباغ، قيد الأوراق المالية في البورصة دراسة مقارنة، ط 1، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2018.

19-عمار بوحوش، محمد محمود الذنيبات، مناهج البحث العلمي وطرق إعداد البحوث، ط 9، الجزائر، ديوان المطبوعات الجامعية، 2022.

20- غسان قاسم اللامي، تكنولوجيا المعلومات في منظمات الأعمال_، ط 1، الأردن ، دار الرواق للنشر والتوزيع، 2020.

21- ليلى عبد المجيد، التنظيم التشريعي والقانوني للإعلام التقليدي والإلكتروني، ط 1، القاهرة، العربي للنشر والتوزيع، 2020.

22- محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقها، ط 1 ، القاهرة، دار الشروق،1989.

23- محمد علي البدوي الأزهري، النظرية العامة للإلتزام مصادر الإلتزام، ج 1، ط1، ليبيا ، منشورات الجامعة المفتوحة، 1993.

24- مصطفى يوسف كافي، التجارة الإلكترونية، د،ط، سوريا، دار مؤسسة رسلان للطباعة والنشر والتوزيع،2009 .

25- محمد بن براك الفوزان، عبد الله بن أحمد زيتل علي رضا، أحكام نظام الوكالات التجارية السعودي دراسة مقارنة، ط1، الرياض ، مكتبة القانون والإقتصاد للنشر والتوزيع،2012 .

26- مزهر شعبان العاني، الأعمال الإلكترونية منظور إداري تكنولوجي ، ط 1، عمان ، دار الإعصار العلمي للنشر والتوزيع،2015.

27- محمد عزمي البكري، موسوعة الفقه والقضاء والتشريع في القانون المدني الجديد، مج 8، د،ط، القاهرة، درا محمود للنشر والتوزيع،2018.

28- نجم عبود نجم، الإدارة الإلكترونية الإستراتجية والوظائف والمشكلات ، د، ط، الرياض ، دار المريخ للنشر، 2004.

29- نادية فضيل، شركات الأموال في القانون الجزائري ، ط 3، بن عكون، الجزائر ، ديوان المطبوعات الجامعية،2008.

30- نجلاء محمد جابر، دراسة تحليلية في الإعلام الجماهيري، د، ط، د، ب، ن، دار المعتز للنشر والتوزيع،2015.

31- هاني شحادة الخوري، تكنولوجيا المعلومات على أعتاب القرن الحادي والعشرين، ج الأول مدخل تعريفي لتكنولوجيا المعلومات، ط 1، دمشق، مركز الرضا للكومبيوتر،1998.

32- هشام بشير إبراهيم عبد ربه إبراهيم، غسيل الأموال بين النظرية والتطبيق، ط 1، القاهرة، المركز القومي للإصدارات القانونية، 2011.

ب-الكتب المتخصصة:

1- أسامة سمير حسين، الإحتيال الإلكتروني -الأسباب والحلول- ط 1، الأردن، الجنادرية للنشر والتوزيع، ، 2011.

2- أسامة أحمد المناعسة، جلال محمد الزعبي ، جرائم تقنية المعلومات الإلكترونية دراسة مقارنة وفقا لقانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2012، ط 2 ، عمان الأردن، دار الثقافة للنشر والتوزيع، ، 2014.

3- أيمن عبد الله فكري ، الجرائم المعلوماتية -دراسة مقارنة في التشريعات العربية والأجنبية- ط 1، الرياض، مكتبة القانون والإقتصاد، ، 2014 .

4- السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، ط 1، الإسكندرية، مكتبة الوفاء القانونية، ، 2018.

5- أحمد محمد عبد الرؤوف المنيفي، السرقة الإلكترونية وحكمها في الإسلام، ط 2، لندن، E-KTUBLTD، 2018 .

6- إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية دراسة مقارنة، د، ط ، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2019.

7- بشرى حسين الحمداني ، القرصنة الإلكترونية -أسلحة الحرب الحديثة- ط 1، الأردن، دار أسامة للنشر والتوزيع، 2014.

8- بشير عادل حامد، الإثبات الجنائي للجريمة الإلكترونية، ط 1، القاهرة، دار النهضة العربية، 2021.

9- حمدي محمد أحمد الجداوي ، غسل الأموال عبر الأنترنت دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية، ط1، جمهورية مصر العربية، مركز الدراسات العربية للنشر والتوزيع، 2022.

10- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية دراسة مقارنة، ط 1، الإسكندرية، دار الفكر الجامعي،2018 .

11- خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، ط1، الإسكندرية، دار الفكر الجامعي، 2019.

12- خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، د، ط، الإسكندرية، دار الفكر الجامعي، 2020.

13- خالد حسن أحمد لطفي، الأمن المعلوماتي التهديدات والتدابير التشريعية والتقنية لحمايته، د،1، الإسكندرية، دار الفكر الجامعي، 2021.

14- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت د، ط ، الإسكندرية، دار الفكر الجامعي، 2007.

15- شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت دراسة مقارنة، د،ط، القاهرة، دار النهضة العربية، ، 2009 .

16- شيرين دبابنة ، جرائم الأنترنت في المجتمع من منظور إجتماعي، د،ط، الأردن، دار الحامد للنشر والتوزيع، 2018 .

17- ضرغام جابر عطوش آل مواش ، جريمة التجسس المعلوماتي –دراسة مقارنة– ط 1، جمهورية مصر العربية، المركز العربي للنشر والتوزيع، 2017.

18- طارق الخن، جرائم المعلوماتية، د،ط، الجمهورية العربية السورية، الجامعة الإفتراضية السورية، 2018.

19- عمرو عيسى الفقي، الجرائم المعلوماتية جرائم الحاسب الآلي والأنترنت في مصر والدول العربية، ط 1، الإسكندرية، المكتب الجامعي الحديث، 2006.

20- علي جبار الحسيناوي، جرائم الحاسوب والأنترنت، د، ط، عمان، دار اليازوردي العلمية، 2008.

21- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت دراسة متعمقة في جرائم الحاسب الآلي والأنترنت، د،ط، جمهورية مصر العربية، بهجات للطباعة والتجليد، 2009.

22- عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، ط1، عمان، دار الثقافة للنشر والتوزيع، 2010 .

23- علي عدنان الفيل ، الإجرام الإلكتروني، ط 1، بيروت، منشورات زين الحقوقية، 2011.

24- عبد القادر بن عبد الله الفنتوخ ، الجريمة في الأنترنت وطرق الحماية منها، ط 1، الرياض، مكتبة العبيكان، 2012.

25- عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية، ط 1، الرياض، مكتبة القانون والإقتصاد للنشر والتوزيع، ، 2012.

26- عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، ط 1، القاهرة، المركز القومي للإصدارات القانونية، 2012.

27- عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط 1، المملكة العربية السعودية، جامعة نايف العربية للعلوم الأمنية، ، 2015.

28- عبد الإله النوايسة ، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، الأردن، دار وائل للنشر والتوزيع، 2017.

29- عبد الوهاب جعيجع ، الأمن المعلوماتي وإدارة العلاقات الدولية، د،ط، الجزائر، منشورات دار الخلدونية، 2017.

30- عادل بن عبد العزيز بن صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، ط 1، السعودية، دار كنوز إشبيليا للنشر والتوزيع، 2017.

31- عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، د،ط1، الجزائر، دار الخلدونية، 2017.

32- عيسى سليم داود الزيدي ، جرائم القرصنة الإلكترونية –دراسة مقارنة- د، ط، مصر، دار الكتب القانونية، 2020.

33- عبد القادر عميمر ، التحديات القانونية لإثبات الجريمة المعلوماتية، د،ط، الجزائر، النشر الجامعي الجديد، 2021.

34- فارس محمد العمارات ، إبراهيم الحمامصة ، الأمن السيبراني المفهوم وتحديات العصر، ط 1، عمان، دار الخليج للنشر والتوزيع، 2022.

35- محمد حسن عمر، الإدارة والتقنية شركاء في مواجهة تحديات عصر الأنترنت، د، ط ، الرياض، مكتبة الملك فهد، 1997.

36- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، ط 1، عمان، دار الثقافة للنشر والتوزيع، 2004.

37- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، د،ط، عمان، دار الثقافة للنشر والتوزيع، 2005.

38- مصطفى محمد موسى، دليل التحري عبر شبكة الأنترنت، د.ط، مصر، دار الكتب القانونية، 2005.

39- محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د.ط ، الإسكندرية، دار الجامعة الجديدة للنشر، 2007.

40- مركز هردو لدعم التعبير الرقمي، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مصر، منشورات مركز هردو، ، 2014.

41- محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها –دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني- د ط، مصر، دار الكتب القانونية، 2014 .

42- محمد نصر محمد، الوسيط في الجرائم المعلوماتية، ط 1، جمهورية مصر العربية، مركز الدراسات العربية للنشر والتوزيع، 2015.

43- محمد علي سويلم، الإثبات الجنائي عبر الوسائل الإلكترونية دراسة مقارنة، د،ط، الإسكندرية، دار المطبوعات الجامعية، 2020.

44- ميرفت محمد حبابية، كتاب مكافحة الجريمة الإلكترونية –دراسة مقارنة في التشريع الجزائري والفلسطيني- د، ط، الأردن، دار اليازوردي العلمية، 2022 .

45- محمد كمال، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة، د،ط، الإمارات، دار كليم للطباعة والنشر، 2022.

46- نهلا عبد القادر المومني ، الجرائم المعلوماتية، ط 2 ، عمان، دار الثقافة للنشر والتوزيع، 2010.

47- نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال، د، ط ، الإسكندرية، دار المكتب الجامعي الحديث، 2020.

48- هبة علي زين عيدروس، سرقة برامج الحاسب في القانون المقارن، ط1، د.ب.ن، دار علام للإصدارات القانونية، 2022.

49- يعيش تمام شوقي، الجريمة المعلوماتية دراسة تأصيلية مقارنة، ط 1، الجزائر، مطبعة الرمال، 2019.

50- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقيات العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة، د ط، الإسكندرية، دار الجامعة الجديدة، 2019.

ت-المقالات:

1- أفنان عبد علي الأسدي، الإدارة الإلكترونية بين النظرية ومتطلبات التطبيق في بيئة منظمات الأعمال العراقية، مجلة دراسات الكوفة ، ع 15، الصادر في 2009.

2- إبراهيم لجلط، دور قاعدة بيانات الزبائن في تحليل الحصة السوقية –دراسة حالة شركة دال DELL، مجلة إقتصاديات شمال إفريقيا، ع 11، الصادر في 2013.

3- أحمد فتحي الحيت، محمد مفضي الكساسبة، تأثير وظائف الإدارة الإلكترونية في فاعلية وكفاءة البنوك في الأردن، المجلة العربية الدولية للمعلوماتية_ ع 4، مج 2 ، الصادر في يناير 2013.

4- إدريس قرفي، تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية بين إتفاقية بودابست والتشريع الجزائري، مجلة الحقوق والحريات، ع 2، الصادر في 2014.

5- آمنة أمحمدي بوزينة" الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري دراسة تحليلية لقانوني العقوبات وحقوق المؤلف"، مجلة القانون والمجتمع، مج 3، ع2، الصادر في 2015.

6- أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مجلة جامعة الأزهر، ع خاص بمؤتمر كلية الحقوق الخامس المحكم، مج 19، الصادر في 2017.

7- أحمد محمد براك بن حمد، المواجهة التشريعية للجريمة المعلوماتية بين الواقع والمأمول، مجلة جامعة الأزهر، ع خاص بمؤتمر كلية الحقوق الخامس، مج 19، الصادر في 2017.

8- إسراء جبريل رشاد مرعي ، الجرائم الإلكترونية، الأهداف، الأسباب، طرق الجريمة ومعالجتها، مجلة الدراسات الإعلامية، ع 1، الصادر في يناير 2018.

9- إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 11، الصادر في سبتمبر 2018.

10- أمال فكيري، إشكالات الإثبات والإختصاص في جرائم تكنولوجيا الإعلام والإتصال العابرة للحدود، مجلة العلوم القانونية والسياسية، ع 17، الصادر في جانفي 2018.

11- العيسى طلال ياسين، عناب محمد عدي ، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، ع 1، مج 19، الصادر في 2019.

12- آمنة زعيطي ، مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري دراسة مقارنة، مجلة حقوق الإنسان والحريات العامة، العدد 7، مج 4، الصادر في جوان 2019.

13- أسماء فيلالي ، عبد اللطيف شليل، تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر، ع 3، مج 4، الصادر في 2019.

14- أنسام سمير ظاهر، جريمة السرقة الإلكترونية، مجلة جامعة بابل للعلوم الإنسانية،ع 5، مج 27، الصادر في 2019.

15- آمنة تازير، جريمة تبييض الأموال في التشريع الجزائري بين القمع والوقاية، مجلة دراسات إنسانية واجتماعية، ع10، مج 2، الصادر في جوان 2019.

16- الطيبي البركة، إشكالات الإثبات في الجرائم الإلكترونية، مجلة أفاق علمية، ع 1، مج 11، الصادر في 2019.

17- أحمد علي محمود إبراهيم، الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية –دراسة فقهية مقارنة، مجلة كلية الشريعة والقانون، ع 32، الصادر في يونيو 2020.

18- أحمد برادي ، آليات مكافحة الجريمة الإلكترونية في ضوء قانون العقوبات الجزائري، مجلة وميض الفكر للبحوث، ع 7، الصادر في أيلول 2020.

19- أمال سلطان، صليحة عشبي، تكنولوجيا المعلومات والإتصال وأثرها على كفاءة أداء المؤسسة، دراسة حالة مؤسسة نقاوس للمصبرات باتنة، المجلة الجزائرية للأمن الإنساني، ع 1، مج 6، الصادر في جانفي 2021.

20- آمنة مخانشة، المؤسسات الناشئة في الجزائر الإطار المفاهيمي والقانوني، مجلة صوت القانون، ع 1، مج 8، الصادر في 2021.

21- أسامة سيد اللبان، الركن المادي للجريمة عناصره ومظاهره في الفقه الإسلامي ، مجلة مصر المعاصرة، ع 543، الصادر في يوليو 2021.

22- أشرف محمد نجيب السعيد الدريني، جرائم الإعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين، ع 59، الصادر في يوليو 2021.

23- إسمهان عون، أركان جريمة الإتلاف المعلوماتي وعقوباتها –دراسة مقارنة، مجلة الدراسات الإفريقية وحوض النيل، ع 13، مج 4، الصادر في أكتوبر 2021.

24- إسراء يونس هادي، أسامة أحمد النعيمي، جريمة التجسس الإلكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011، مجلة كلية القانون للعلوم القانونية والسياسية ، ع 36، مج 10، الصادر في 2021.

25- آسية بن بوعزيز ، ميلود بن عبد العزيز، جريمة الإحتيال المالي في ظل تكنولوجيا المعلومات، مجلة الدراسات المالية والمحاسبية والإدارية، ع 1، مج 9، الصادر في جوان 2022.

26- إيمان رتيبة شويطر، الأقطاب الجزائية المتخصصة كتوجه لمكافحة جرائم الأعمال، مجلة البحوث في العقود وقانون الأعمال، ع 1، مج 7، الصادر في 2022.

27-أحمد عبد الرحمان بن سالم، (التحول الإلزامي للشركة التجارية دراسة مقارنة)، مجلة الحقوق والعلوم الإنسانية ، ع 1، مج 15، الصادر في 2022.

28- أحمد لمين مناجلي، النظام القانوني لشركة المساهمة البسيطة وملاءمته للمؤسسات الناشئة ، مجلة العلوم القانونية والإجتماعية ع 3، مج 8، الصادر في سبتمبر 2023.

29- أحمد مسعود أسامة، فعالية الإدارة الإلكترونية في تطوير منظمات الأعمال دراسة ميدانية على بعض الشركات الخاصة بولاية البليدة، مجلة التنمية وإدارة الموارد البشرية بحوث ودراسات_ ، ع 1، مج 10، الصادر في 2023.

30- أحمد إبراهيم محمد متولي دهشان، إقتصاديات المعرفة وجه التنمية الاقتصادية الحديثة في ضوء بعض التجارب الدولية، مجلة كلية الشريعة والقانون بطنطا، ع 38، الصادر في 2023.

31- أسامة بن غانم العبيدي، لتفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، ع 58، مج 29، د، ت، ص.

32- بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي دراسة مقارنة، المجلة الأكاديمية للبحث القانوني، ع 1، مج، 9، الصادر في 2014.

33-بوعافية رشيد، يدو محمد، (التجارة الإلكترونية والإستثمار عبر شبكة الأنترنت الإطار النظري والتطبيقي)، مجلة الاقتصاد الجديد، ع 18، مج 1، الصادر في 2018.

34- بوزيد بن محمود، سهام عباسي، الأمن المعلوماتي في ظل قانون التجارة الإلكترونية في الجزائر، مجلة االبيبان للدراسات القانونية والسياسية، ع 13، مج، 3، الصادر في جوان 2018.

35- بشرى غربي ، خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، ع 2، مج 2، الصادر في 2021/06/01.

36- بسمة مامن، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، ع 1، مج 9، الصادر في 2022.

37- بندر عقاب جفين كميخ حطاب الدويش، خصائص وأنواع الدليل الإلكتروني في الكويت والدول المقارنة، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية، ع 3، مج، 16، الصادر في ماي 2023.

38- ثامر خالدي، شركة المساهمة البسيطة في ظل القانون التجاري رقم 22-09، المجلة الجزائرية للعلوم القانونية والسياسية، ع 3، مج 60، الصادر في 2023.

39- جميلة سلايمي، يوسف بوشي، التحول الرقمي بين الضرورة والمخاطر، مجلة العلوم القانونية والسياسية ، ع 2، مج 10، الصادر في سبتمبر 2019.

40- جمال زين العابدين أمين أحمد، جرائم إختراق النظم الإلكترونية بين التشريع المصري والمغربي، مجلة مستقبل العلوم الاجتماعية، ع 1، الصادر في أفريل 2020.

41- جمال الدين بوقرة ، جمال الدين عنان ، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 1، مج 7، ، الصادر في جوان 2022.

42- حنان أوشن ، عماد الدين وادي ، التجسس الإلكتروني وآليات مكافحته في التشريع الجنائي الجزائري، مجلة الحقوق والعلوم السياسية، ع 2 الصادر في جويلية 2014.

43- حسين ربيعي ، المجرم المعلوماتي، شخصيته وأصنافه، مجلة العلوم الإنسانية، ع 40، الصادر في جوان 2015.

44- حفيظ بن قربة ، جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري، مجلة القانون والعلوم السياسية، ع 2، مج 3، الصادر في جوان 2017.

45- حسين خليل مطر، التحقيق وجمع الأدلة في الجرائم الإلكترونية، مجلة الكوفة، ع 36، مج 1، الصادر في 2018.

46- حمزة خضري ، حمزة عشاش ، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، ع 2، مج 6، الصادر في جوان 2020.

47- حنان مسكين، واقع مكافحة الجرائم المعلوماتية وإتجهاتها التشريعية في الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية، ع 1، مج 4، الصادر في 2020.

48- حيدور جلول، دور القطب الجزائي الاقتصادي والمالي في حماية المال العام من جرائم الفساد في ضوء التشريعات الجزائية، مجلة الإجتهاد القضائي، ع 2، مج 13، الصادر في أكتوبر 2021.

49- حفيظة عياشي ، سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري، مجلة القانون والعلوم السياسية، ع 1، مج، 9، الصادر في 2022.

50- خلود عاصم ، دور تكنولوجيا المعلومات والإتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية، الصادر في 2013.

51- خديجة عميور ، قواعد إختصاص الأقطاب الجزائية للنظر في جرائم الفساد، مجلة الدراسات في الوظيفة العامة، ع 2، الصادر في 2014.

52- خليل يوسف جندي ، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، ع 36، مج 7، الصادر في 2018.

53- خالد رجم، خولة واصل، الويزة سعادة، (واقع الاقتصاد الرقمي في الجزائر دراسة تحليلية لقطاع تكنولوجيا المعلومات والإتصال)Journal of economic Growthand entrepreneurshp، ع 1، مج 1، الصادر في 2019/12/25

54- خالد ضو، التأصيل لمبدأ الشرعية الجنائية في الفقه الإسلامي والتشريعات الوضعية، مجلة الأبحاث القانونية والسياسية، ع 1، مج 3، الصادر في 2020.

55- دلال لطيف مطشر، جريمة الإعتداء على المواقع الإلكترونية –دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، ع 9، مج 26، الصادر في 2018.

56- داود عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية –دراسة تأصيلية مقارنة، مجلة الإجتهاد للدراسات القانونية والإقتصادية، ع 3، مج 9، الصادر في 2020.

57- ذهبية لعجال ، قاسي سي يوسف، الأساليب الحديثة لتبييض الأموال في ظل التطور التكنولوجي، مجلة الإجتهاد القضائي، ع خاص، مج 13، الصادر في جانفي 2021.

58- رواء زكي يونس الطويل، التجارة الإلكترونية والتجسس الاقتصادي، مجلة آداب الرافدين، ع 51، الصادر في 2008.

59- رمزي حوحو ، منيرة بلورغي، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق والحريات، ع 2، الصادر في 2014.

60- رشيد فراح، كريمة فرحي، متطلبات الأعمال الإلكترونية في العالم العربي بين الواقع وضرورة التحسين ، مجلة علوم الاقتصاد والتسيير والتجارة ع 32، الصادر في 2015.

61- رشيدة بوكر ، الدخول أو البقاء داخل نظم معلومات المؤسسة الاقتصادية بين عدم التصريح والحماية الجزائية، مجلة قانون العمل والتشغيل، ع 1، مج 6، الصادر في جانفي 2021.

62- زهية عزيزي، تداول الأسهم وعلاقته بالإعتبارين المالي والشخصي في شركة المساهمة، مجلة الدراسات الحقوقية ، ع 2، مج 09، الصادر في ديسمبر 2022.

63- سلمى مانع ، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية ، ع 22، الصادر في جوان 2011.

64- سمير بردال، خصوصية الجرائم المرتبطة بنظام الحاسب الآلي ومظاهر تمييزها عن الجرائم التقليدية، مجلة البحوث في الحقوق والعلوم السياسية، ، ع 4، مج 2، الصادر في أكتوبر 2016.

65- سليمان النحوي، خالد شويرب، حماية المعلومات والبرامج الإلكترونية في ظل جريمة السرقة، مجلة دراسات وأبحاث،ع 29، الصادر في ديسمبر 2017.

66- سهام خليلي، خصوصية المجرم الإلكتروني، مجلة المفكر، ع 15، الصادر في جوان 2017.

67- سميرة معاشي، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، ع 7، الصادر في جوان 2018.

68- سفيان بن تقي، جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية، مجلة الأبحاث القانونية والسياسية، ع 2، مج 3، الصادر في 2021.

69- سليمان قطاف ، عبد الحليم بوقرين، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، مج 6، ع 2، الصادر في 2022.

70- شول بن شهرة، آليات مكافحة الجريمة المعلوماتية مواقع التجارة الإلكترونية نموذجا، مجلة دراسات الجزائر، ع 13، الصادر في مارس 2010.

71- شريهان ممدوح، الجرائم المعلوماتية وسبل مواجهتها على المستووين الوطني والدولي، المجلة الإلكترونية الشاملة، ع 21، الصادر في 2020.

72- شول بن شهرة مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، ، ع 1، مج 4، الصادر في جوان 2020.

73- شهرزاد لكحل ، ميلود سلامي، الأسرار التجارية وأثرها على نقل التكنولوجيا، مجلة الإجتهاد القضائي، ع 28، مج 13، الصادر في نوفمبر 2021.

74- شهرزاد دراجي، نور الدين بن الشيخ، القطب الجزائي الاقتصادي والمالي المستحدث قراءة في الأمر رقم 20-04 المؤرخ في 30-08-2020، مجلة الدراسات القانونية والإقتصادية، ، ع 2، مج 5، الصادر في 2022.

75- صفيان بخدة ، ناصر وقاص، الطبيعة القانونية للجرائم المستحثة ووسائل إرتكابها جريمة الأنترنت كنموذج، مجلة البحوث القانونية والسياسية، ع 16، مج 3، الصادر في 2021.

76- صبرينة بوعمار، حمزة بوخروبة، الطبيعة القانونية لشركة المساهمة البسيطة ، شركة المؤسسات الناشئة، مجلة الدراسات والبحوث القانونية، ع 2، مج 8، الصادر في 2023.

77- عبد الله غالم، محمد قريشي، دور تكنولوجيا المعلومات في تدعيم وتفعيل علاقات الزبائن، مجلة أبحاث إقتصادية وإدارية، ع 10، الصادر في 2011.

78- عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، ع 2، الصادر في 2014.

79- عمر طه خليل ، عفاف بديع جميل ، التكييف الفقهي والقانوني لجرائم الأنترنت، مجلة كلية التراث الجامعة ،ع 17، الصادر في 2015.

80- عبد السلام زعرور، الإكتتاب في رأسمال شركة المساهمة بين العقد والإرادة المنفردة، مجلة الحقوق والعلوم السياسية ، ع 8، مج 02، الصادر في جوان 2017.

81- عادل مستاري، زوليخة رواحنة ، جريمة التزوير الإلكتروني، مجلة العلوم الإنسانية، ع 46، الصادر في مارس 2017.

82- عبد القادر عمري ، الشريعة والتشريع الجزائري، مجلة الدراسات القانونية، ع 1، مج 3، الصادر في 2017/06/30.

83- عبد القادر فلاح ، نادية آيت عبد المالك ، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 2، مج 4، الصادر في 2019.

84- عبد السلام محمد المايل ، عادل محمد الشربجي، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم الأسباب سبل المكافحة مع التعرض لحالة ليبيا، مجلة أفاق للبحوث والدراسات، ع 4، الصادر في جوان 2019.

85- عبد الحليم بن بادة ، المراقبة الإلكترونية كإجراء لإستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكاديمية للبحث القانوني، ع 3، مج 10، الصادر في 2019.

86- عبد الرحمان خلفي ، بلال عثماني، حماية الرعايا الجزائرين بالخارج في إطار القانون الجنائي، مجلة الدراسات حول فعلية القاعدة القانونية، ، ع 1، مج 3، الصادر في 2019.

87- عبد الباقي خلفاوي، حرية تداول الأسهم في شركات المساهمة في التشريع الجزائري، مجلة العلوم الإنسانية ، ع 2، مج 31، الصادر في جوان 2020.

88- عبد القادر حمر العين، المركز القانوني للشريك المؤسس في شركة المساهمة قيد التأسيس، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة الجزائر ، ع 3، مج 34، الصادر في 2020.

89- علي محمود إبراهيم أحمد، الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية دراسة فقهية مقارنة، مجلة كلية الشريعة والقانون بجامعة الأزهر، ع 32، الصادر في 2020.

90- عائشة عبد الحميد، الدليل الرقمي كحجية للإثبات أمام القاضي الجزائي في المعاملات الإلكترونية، مجلة صوت القانون، ع 1، مج، 7، الصادر في ماي 2020.

91- عبد الله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية، مجلة الدراسات القانونية المقارنة،ع 2، مج 6، الصادر في ديسمبر 2020.

92- عبد العزيز زردازي، الأسرار التجارية في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ع 2، مج 6، الصادر في ديسمبر 2021.

93- عيدة بلعايد ، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، ع 6، الصادر في مارس 2021.

94- عبد القادر فلاح ، حجز وحفظ المعطيات في الجريمة الإلكترونية، مجلة صوت القانون، ع 1، مج 8، الصادر في 2021.

95- عبد الفتاح قادري، حيدرة سعدي، آليات عمل الأقطاب الجزائية المتخصصة في جرائم الفساد، مجلة العلوم الإنسانية لجامعة أم البواقي، ع 1، مج 8، الصادر في مارس 2021.

96- عائشة بن قارة مصطفى، إستراتجية تحقيق الأمن المعلوماتي للحكومة الإلكترونية، مجلة دار ارافد، د، ع، مج 2، ، الصادر في يناير 2021.

97- غسان كوريل إبراهيم، آراس قادر خوشناو، دور إستخدام الأعمال الإلكترونية في إعداد الميزانية العمومية للشركات للحد من التهرب الضريبي، مجلة يوليتكنيك للعلوم الإنسانية والإجتماعية ، ع 2، مج 4، الصادر في 2023 .

98-فاديا سليمان، الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، مجلة الدراسات المالية والمصرفية، ع 1 ، الصادر في 2015.

99- فتيحة ليتيم ، نادية ليتيم ، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، ع 1، مج، 10، الصادر في مارس 2015.

100- فتيحة عمارة، جريمة التزوير الإلكتروني، مجلة القانون والمجتمع، ع 1، مج 7، الصادر في 2019.

101- فطيمة الزهرة المفيدة ، نجاح عصام بن أوجيت ، إستراتجيات التحول من الإدارة التقليدية إلى الإدارة الإلكترونية في ظل الأزمات، أزمة كورونا COVID 19، مجلة التنمية البشرية والتعليم للأبحاث التخصصية ، ع 3، مج 7 ، الصادر في 2021.

102- فراس نايف تايه، دور الخبرة في جريمة التزوير المعلوماتية، المجلة القانونية ، مجلة متخصصة في الدراسات والبحوث القانونية، ع 2، مج 14، الصادر في 2022.

103- كريمة عباس، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيبان للدراسات القانونية والسياسية، ع 4، الصادر في ديسمبر 2017.

104- لمقدم حمر العين ، جريمة خيانة الأمانة المعلوماتية، مجلة دراسات وأبحاث، ع 15، مج 1، الصادر في 2009/09/15.

105- لمين علوطي، تحديات الأمن الإلكتروني في المؤسسة، مجلة أبحاث إقتصادية وإدارية، العدد 6، ، الصادر في 2009.

106- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها –دراسة مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، د ع، الصادر في 2017.

107- ليندا بن طالب ، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، ع 16، الصادر في جوان 2017.

108- لامية مجدوب، إجراء التفتيش في التزوير الإلكتروني، مجلة التواصل في الاقتصاد والإدارة والقانون، ع 3، مج 25، الصادر في سبتمبر 2019.

109- لامية طالة ، كهينة سلام ، الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الإحتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، ع 2، مج 6، الصادر في ديسمبر 2020.

110- ليلى بن عودة، خصائص شركة المساهمة البسيطة الأكثر ملاءمة للمؤسسات الناشئة، مجلة الدراسات القانونية المقارنة، ع 1، مج 9، الصادر في 2023.

111- محمد حماد مرهج الهيتي، مدى تطبيق نصوص جرائم الإتلاف والتخريب على الإتلاف الذي يتعرض له الحاسب الآلي –دراسة في نطاق التشريع البحريني والمقارن، مجلة الحقوق، د،ع، مج 6، الصادر في 2009.

112- محمد قدري، حسن عبد الرحمن، جرائم الإحتيال الإلكتروني، مجلة الفكر الشرطي، ع 79، مج 20، الصادر في 2011.

113- محمد محسن حسينات، جرائم الحاسوب والأنترنت، مجلة جامعة فلسطين للأبحاث والدراسات، ع 2، الصادر في يناير 2012.

114- مسعود خثير، الإمتناع كعنصر لقيام الركن المادي في الجريمة السلبية، مجلة القانون والمجتمع، ع 2، مج 1، الصادر في 2013/12/01.

115- مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب في ارتكابها، مجلة العلوم القانونية والسياسية، ع 1، مج 3، الصادر في 2014.

116- محمد هشام فريجة، ضرورة التعامل بأسلوب الإدارة بالأهداف كأداة للإدارة الإلكترونية، مجلة الاقتصاد الخليجي ، ع 28، الصادر في حزيران 2016.

117- محمد بكرار شوش، الإختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة والقانون، ع 14، الصادر في 2016.

118- محمود بوزيدين، سهام عباسي، الأمن المعلوماتي في ظل قانون التجارة الإلكترونية في الجزائر ، مجلة البيبان للدراسات القانونية والسياسية ع 1، مج 3، الصادر في جوان 2018.

119-مهدي كمال، باخويا دريس، دور الوسائط الإلكترونية في إنتشار جرائم الأموال وآليات مكافحتها، المجلة الإفريقية للدراسات القانونية والسياسية، ع 2، مج 2، الصادر في ديسمبر 2018.

120- محمد طيب عمور، السرقة الإلكترونية تكييفها الشرعي وطرق إثباتها، مجلة الأحياء، ع 22، مج 19، الصادر في سبتمبر 2019.

121- ماء العينين سعداني، حماية التجارة الإلكترونية في ضوء المستجدات التشريعية، المجلة الإلكترونية للأبحاث القانونية ع 5، الصادر في 2020.

122- محمد قسمية ، حمزة خضري، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، ع2، مج 7، الصادر في نوفمبر 2020.

123- مختار تابري، الخبرة في الجريمة المعلوماتية، مجلة الحوار المتوسطي، ع 3، مج 11، الصادر في ديسمبر 2020.

124- محمد مكاوي محمد، دينا عبد الله صالح ، الجرائم ذات التقنية العالية والحماية من الهجمات الإلكترونية في النظام السعودي، مجلة الإجتهاد القضائي ع 1،، مج 13، الصادر في مارس 2021.

125- مونة مقلاتي، راضية مشري، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، ع 1، مج 6، الصادر في جوان 2021.

126- محمد أمين بكوش ، هبة نبيلة هروال، خصوصية المجرم الإلكتروني–مجرم الأنترنت نموذجا–، مجلة البحوث في الحقوق والعلوم السياسية، ع 1، مج 7، الصادر في جوان 2021.

127- مخلد إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية دراسة مقارنة، المجلة العربية للنشر والتوزيع، ع 37، الصادر في تشرين الثاني 2021.

128- محمد عبد المحسن بن طريف، فيصل صالح العبادي، هبة عبد المطلب الفضلي، جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، ع 2، مج 7، الصادر في 2022.

129- مريم عبد الكافي ، صورية بورباية، جريمة الإحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية، مجلة القانون والعلوم السياسية، ع1، مج 8، الصادر في 2022.

130- مريم مالكي، أهمية التجارة الإلكترونية في تحسين مستويات التنمية المستدامة في الدول العربية ، مجلة الناقد للدراسات السياسية_، ع 1، مج 7 ، الصادر في 2023.

131- محمد رحموني، خصائص الجريمة الإلكترونية ومجالات إستخدامها، مجلة الحقيقة، ع 41، د،ت،ص.

132- نوفيل حديد، كريبط حنان، أمن المعلومات ودوره في مواجهة الإعتداءات الإلكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، ع 1، ، الصادر في 2014.

133- نعيم سلامة، أيمن أبو الحاج، موسى سعيد، مشهور هذلول، البنوك وعمليات غسيل الأموال مجلة كلية بغداد للعلوم الاقتصادية الجامعة، ع 33، الصادر في 2012.

134- نعيمة يحياوي، مريم يوسف، التجارة الإلكترونية وآثارها على إقتصاديات الأعمال العربية، المجلة الجزائرية للتنمية الإقتصادية_، ع 6، الصادر في جوان 2017.

135- نبيل دريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر نموذجا، مجلة القانون والمجتمع، ع 2، مج 5، الصادر في 2017/12/01.

136- نجاة عباوي، الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، ع 16، الصادر في جانفي 2017.

137- نادية عبد الرحيم، أمين بن سعيد، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية، مجلة الدراسات الاقتصادية والمالية، ع 10 الصادر في 2017.

138- نبيهة قنفود، فوزي عمارة، الخبرة التقنية في مجال إثبات الجريمة الإلكترونية، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، ع 2، مج 36، الصادر في أكتوبر 2022.

139- نضال سالمي، الإطار التنظيمي للدليل الرقمي في الإثبات، مجلة القانون والمجتمع، العدد 1، الصادر في 2022.

140- نادية بوخرص، الأحكام القانونية الخاصة الناظمة لشركة المساهمة البسيطة وفق للقانون رقم 22-09، مجلة الدراسات القانونية، ع 1، مج 9، الصادر في جانفي 2023.

141- نسرين محسن نعمة، جريمة الإحتيال المعلوماتي دراسة مقارنة، مجلة الكوفة، ع 36، مج 2، د،ت،ص.

142- وهيبة عبد الرحيم، دراسة غسيل الأموال عبر القنوات الإلكترونية، مجلة الحقوق والعلوم الإنسانية دراسات إقتصادية، ع 3، مج 1، الصادر في أكتوبر 2007.

143- وهيبة عبد الرحيم ، أمين بن سعيد ، نادية عبد الرحيم ، الجريمة الإلكترونية من خلال مؤشرات عالمية وآثارها على المؤسسات، مجلة دراسات، ع 1، مج 16، الصادر في جانفي 2019.

144- وهيبة بوعنينيبة، زهرة سعد قرمش، وفاء سلامة، متطلبات التحول من الإدارة التقليدية إلى الإدارة الإلكترونية ومعوقاتها، مجلة الحدث للدراسات المالية والإقتصادية ، ع 7، الصادر في ديسمبر 2021.

145- وليد البلتاجي السيد، النسخ غير المشروع لبرامج الحاسب الآلي دراسة مقارنة، مجلة كلية الشريعة والقانون بطنطا، ع 1، مج 36، الصادر في مارس 2021.

146- ياسمينة بونعارة ، الجريمة الإلكترونية، مجلة المعيار، ع 39، مج 20، الصادر في 2015/06/19.

ث-أطروحات الدكتوراه:

1- أديب محمد حسن هزايمه، أثر تطبيق تكنولوجيا المعلومات على تحسين الميزة التنافسية في شركات المساهمة العامة، أطروحة دكتوراه، كلية الأعمال، جامعة عمان العربية، 2011.

2- آمال حابت، التجارة الإلكترونية في الجزائر، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2015.

3- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2015-2016.

4- الميلود سحانين، مساهمة تكنولوجيا المعلومات والإتصال في تحقيق أبعاد التنمية المستدامة دراسة حالة الجزائر، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجيلالي اليابس سيدي بلعباس، 2016-2017.

5- أسماء فيلالي، مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة، أطروحة دكتوراه، كلية العلوم الإقتصادية والعلوم التجارية جامعة أبو بكر بلقايد، 2018-2019.

6- إسماعيل بن يحي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2020-2021.

7- الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020-2021.

8- بثينة حبيباتني، الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2020.

9- جمال براهيمي ، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2018.

10- جميلة مقدم ، قيام الرابطة السببية في الجرائم الطبية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم الساسية جامعة الجيلالي اليابس سيدي بلعباس، 2018-2019.

11- حفصي عباس، جرائم التزوير الإلكترونية"، (أطروحة دكتوراه، كلية العلوم الإنسانية والعلوم الإسلامية جامعة وهران 1، 2014-2015.

12- حسين ربيعي ، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016.

13- حورية قويقح ، الجرائم الاقتصادية عبر الشبكة المعلوماتية دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، أطروحة دكتوراه، كلية العلوم الإسلامية جامعة الجزائر 1، 2018-2019.

14- حمزة بلحسيني، الحماية الجزائية للمستند الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة جيلالي اليابس سيدي بلعباس، 2019-2020.

15- خدوجة الذهبي، الحماية الجزائية للمعاملات الإلكترونية دراسة مقارنة، أطروحة دكتوراه ، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2018-2019.

16- خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية –دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أحمد درارية، 2020-2021.

17- دلال مولاي ملياني ، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2017-2018.

18- رشيدة بوكر، الحماية الجزائية للتعاملات الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، 2017.

19- رجاء أومدور ، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، 2020-2021.

20- رابح الهوى، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2020-2021.

21- سهام دربال، شركة المساهمة ومبادئ الحوكمة الرشيدة ، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2018-2019.

22- سميرة حمادوش، دور تكنولوجيا المعلومات والإتصالات في تعزيز الميزة التنافسية لشركات التأمين في الجزائر ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة حسيبة بن بوعلي الشلف، 2019-2020.

23- صباح بلقيدوم، أثر تكنولوجيا المعلومات والإتصالات الحديثة، NTIC، على التسيير الإستراتيجي للمؤسسات الاقتصادية، أطروحة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة قسنطينة 2، 2012-2013.

24- صالح شنين، الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، كلية الحقوق جامعة أبو بكر بلقايد تلمسان، 2012-2013.

25- صالح جزول، جريمة تبييض الأموال في قانون العقوبات الجزائري والشريعة الإسلامية دراسة مقارنة، رسالة دكتوراه، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران 1، 2014-2015.

26- صورية بورباية، قواعد الأمن المعلوماتي دراسة مقارنة ، أطروحة مقدة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس، 2015-2016.

27- عبد الحليم بوقرين ، الحماية الجنائية للمعاملات التجارية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2013-2014.

28- عبد الوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2016-2017.

29- عزيزة رابحي ، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد، 2017-2018.

30- عفاف خذيري ، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، 2017-2018.

31- عبد النور بشان، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2017-2018.

32- عبد القادر عميمر ، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري دراسة مقارنة أطروحة دكتوراه، كلية الحقوق ، جامعة الجزائر 1، 2019-2020.

33- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2010-2011.

34- فاطمة مصفح، حماية برامج الحاسوب في ظل التشريعات الوطنية والإتفاقيات الدولية، رسالة الدكتوراه، كلية الحقوق جامعة الجزائر 1، 2017-2018.

35- كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، 2015-2016.

36- ليندا بن طالب ، الدليل الإلكتروني ودوره في الإثبات الجنائي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2019.

37- منذر عبد الرزاق العمايرة، مدى الحماية الجنائية للمعلومات عبر الحاسوب والأنترنت دراسة مقارنة، أطروحة دكتوراه، كلية القانون، جامعة عمان العربية، 2012.

38- محمد بن فردية، لإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2015.

39- محمد بودالي، الحماية الجزائية للتجارة الإلكترونية ، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، 2015-2016.

40- مشري محمد الناصر، سبل تفعيل دور تكنولوجيا المعلومات والإتصال في دعم التنمية المستدامة في المؤسسات الصناعية الجزائرية دراسة عدد من المؤسسات في الشرق الجزائري، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة فرحات عباس سطيف 1، 2016-2017.

41- مصطفى هنشور وسيمة، النظام القانوني للتجارة الإلكترونية في التشريع الجزائري والمقارن أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2016-2017.

42- محمد ياسين بوزوينة، الآليات القانونية لمكافحة الجريمة الاقتصادية في القانون الجنائي الجزائري، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2018-2019.

43- مراد يرمش ، خصوصية الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق جامعة الجزائر 1، 2020-2021.

44- محمد بن أحمد ، المسؤولية الجنائية للمجرم المعلوماتي دراسة تأصيلية موضوعية في التشريع الجزائري والمقران، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس مستغانم، 2021-2022.

45-- نادية لونيس، الأعمال الإلكترونية ودورها في الإبداع والتميز بالمؤسسة دراسة حالة مؤسسة EMPLOITIC، أطروحة دكتوراه، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2017-2018.

46- نادية سلامي، آليات مكافحة التجسس الإلكتروني، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي تبسة، 2018-2019.

47- نسمة بطيحي، الإعتداءات ذات الصلة بالنظام المعلوماتي، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر 1، 2019-2020.

48- نصيرة بوحزمة ، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة الجيلالي اليابس، 2021-2022.

49- هبة نبيلة هروال، جرائم الأنترنت –دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد، 2013-2014.

50- وسيلة هني، أثر إستخدام تكنولوجيا المعلومات على أداء المؤسسة الاقتصادية دراسة نماذج بعض البلدان العربية، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجيلالي اليابس سيدي بلعباس، 2017-2018.

ج-رسائل الماجستير:

1- أحمد جمعة الخيلي، غسل الأموال عبر الأنترنت دراسة مقارنة بين الأردن، مصر، الإمارات، رسالة ماجستير، كلية الدراسات القانونية العليا، جامعة عمان العربية للدراسات العليا، 2006.

2- إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظم المعالجة الآلية للمعطيات الإلكترونية وفقا للمرسوم بقانون إتحادي رقم 5 لسنة 2012في شأن مكافحة جرائم تقنية المعلومات وتعديلاته، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، 2018.

3- إسلام فوزي جمعة محسن، السرقة الإلكترونية في التشريع الأردني، رسالة ماجستير، كلية القانون، جامعة عمان العربية، 2017.

4- إبراهيم محمد بن حمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني دراسة مقارنة، رسالة ماجستير، قسم الدراسات الإسلامية، جامعة فطاني، 2018.

5- أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، 2018.

6- بالضياف خزاني، مبدأ الشرعية الجزائية وأثره على السلطة التقديرية للقاضي الجزائي، رسالة ماجستير، معهد العلوم القانونية والإدارية، المركز الجامعي العربي بن مهيدي بأم البواقي، 2007-2008.

7- بدرة عمارة، "الحماية الجنائية للمعلومات الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، 2011-2012.

8- بهاء فهمي الكبجي، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير، جامعة الشرق الأوسط، 2013.

9- توفيق غوالم، السرقة المعلوماتية دراسة تأصيلية تحليلية مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الجزائر1، 2012-2013.

10- ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية -دراسة تأصيلية تطبيقية، رسالة ماجستير، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، 2012.

11- حورية بولعويدات ، إستخدام تكنولوجيا الإتصال الحديثة في المؤسسة الاقتصادية الجزائريةدراسة ميدانية بمؤسسة سونلغاز فرع تسيير شبكة نقل الغاز بالشرق GRTG قسنطينة، رسالة ماجستير، كلية العلوم الإنسانية والعلوم الإجتماعية، جامعة منتوري قسنطينة، 2007-2008.

12- حمزة بن عقون لسلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011-2012.

13- حمد عبد الله حيي بوغانم السليطي، تجريم الإحتيال الإلكتروني في القانون القطري والمقارن، رسالة ماجستير، كلية القانون، جامعة قطر، 2018.

14- خالد سليمان عبد الله الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019.

15- سفيان سوير ، جرائم المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة أو بكر بلقايد، 2010-2011.

16- سراج طلعت عبد النبي الوحيدي، أثر إستخدام تكنولوجيا المعلومات على كفاءة أساليب المحاسبة الإدارية الحديثة في الشركات الصناعية في قطاع غزة رسالة ماجستير، كلية التجارة، الجامعة الإسلامية غزة، 2017.

17- صبايحية خديجة دحمان ، جرائم السرقة والإحتيال عبر الأنترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، رسالة ماجستير، كلية العلوم الإسلامية، جامعة الجزائر، 2012-2013.

18- صابرين يوسف عبد الله الحياني، جرائم الأموال الناجمة عن إستعمال الحاسوب دراسة مقارنة، رسالة ماجستير، كلية الحقوق جامعة النهرين، 2014.

19- صليحة يحياوي ، السلطة التقديرية للقاضي الجنائي، رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2015-2016.

20- علي سليمان البطوش، التطبيقات المعاصرة لجريمة السرقة، رسالة ماجستير، جامعة مؤتة، 2005.

21- علي جقريب، أثر إستخدام تكنولوجيا المعلومات على أداء بورصة عمان للأوراق المالية، رسالة ماجستير، كلية إدارة المال والأعمال، جامعة آل بيت، 2010.

22- عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة، 2011-2012.

23- عبد العزيز بوذراع، خصوصية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، كلية الحقوق جامعة الجزائر 1، 2011-2012.

24- عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير، جامعة وهران، 2012-2013.

25- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، 2014.

26- عبد الله محمد الحضري، جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري دراسة تحليلية مقارنة، رسالة ماجستير، كلية الحقوق، جامعة قطر 2020.

27- عماد الدين رضا علي لدادوه، مدى ملائمة نصوص قانون الجرائم الإلكترونية الأردني للأحكام العامة لقانون العقوبات، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2021.

28- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2011-2012.

29- ليلى هيكل، أثر إستخدام تكنولوجيا المعلومات في أداء المنظمات دراسة تطبيقية على شركة الأمل لصناعة الأدوية، رسالة ماجستير، الجامعة الإفتراضية السورية، 2015.

30- مريم زلماط ، دور تكنولوجيا الإعلام والإتصال في إدارة المعرفة داخل المؤسسة الجزائرية دراسة حال بسوناطراك فرع STH ، رسالة ماجستير، كلية العلوم الاقتصادية والتسيير، جامعة أبو بكر بلقايد تلمسان، 2009-2010.

31- مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 09-04، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح، 2012-2013.

32- نادية لونيس، أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات دراسة حالة التذاكر الإلكترونية في مؤسسة الخطوط الجوية الجزائرية، رسالة ماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، 2010-2011.

33- نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق، جامعة منتوري قسنطينة، 2012-2013.

34- نعيم سعيداني ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر، 2012-2013.

35- نسيمة جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، كلية الحقوق جامعة وهران، 2013-2014 .

36- ناصر حمودي، الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2015.

37- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية جامعة مولود معمري، 2013.

38- يوسف خليل يوسف عبد الجابر، مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، رسالة ماجستير، كلية الأعمال، جامعة الشرق الأوسط، 2013.

ح-المداخلات:

1-رحيمة نمدلي ، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، مداخلة مقدمة إلى المؤتمر الدولي الرابع عشر -الجرائم الإلكترونية، المنعقد في 24و 25 مارس 2017، بطرابلس.

2-عبد الحليم بن بادة، محمد سعد بوحادة، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة -دراسة سياسية قانونية- مداخلة مقدمة إلى" الملتقى الدولي الأول ، أمن المعلومات في الفضاء الإلكتروني الرهانات والتحديات في شمال إفريقيا" ،كلية الحقوق والعلوم السياسية، جامعة غرداية، المنعقد في 17 و 18 فيفري 2020، الجزائر.

3-إيمان بومدين، حنان مزيان، الجريمة الإلكترونية بين دوافع إرتكابها وآليات مواجهتها -الإستراتجية الأمنية للدولة الجزائرية في مكافحة الجرائم الإلكترونية نموذجا- مداخلة مقدمة إلى: المؤتمر الدولي الإفتراضي المنعقد في14و 15 ماي 2022، بألمانيا.

4-موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مداخلة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون ، أكاديمية الدراسات العليا، المعقد في 28 و 29 أكتوبر، 2009، طرابلس.

5-يونس عرب، جرائم الكمبيوتر والأنترنت، مداخلة مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، المنعقد في 2002/12/10، أبو ظبي.

خ-المواقع الإلكترونية:

1- خالد ممدوح إبراهيم ، الجرائم المعلوماتية، مقال منشور بتاريخ 26 نوفمبر 2008، تاريخ الدخول: 2022/08/13، متاح على الرابط: https://kenanaonline.com_

2-محمد بوبوش، التجسس الاقتصادي القوة الخفية للدول العظمى، مقال منشور بتاريخ2009/04/26، أطلع عليه بتاريخ 2023/07/15 ، متاح على الرابط: https://www.hespress.com ›

3-كيف تحقق الشركات الإستراتجية المعلوماتية من أنظمة البرمجيات الذكية، جريدة العرب الاقتصادية الدولية، مقال منشور بتاريخ 1 ماي 2009، تاريخ الدخول 2022/12/04، متاح على الرابط: https://www.aleqt.com

4-نايلة الصليبي، أسلوب تجسس واختراق يهدد ملايين شاشات الكمبيوتر، مقال منشور بتاريخ 2016/08/19، تاريخ الدخول: 2023/01/01، متاح على الرابط: https://www.mc-doualiya.com

5-رسائل الإحتيال تكلف الشركات ملياري دولار، مقال منشور بتاريخ 2016/02/25، على صفحة الجزيرة، تاريخ الدخول: 2023/07/28، متاح على الرابط: https://www.aljazeera.net

6-شيماء عزت، كيف يمكنكم حماية حواسيبكم من فيروس الفدية الخطير، France 24، مقال منشور بتاريخ: 2017/05/15، تاريخ الدخول: 2022/12/31، متاح على الرابط: https://www.france24.com ›

7-فاضل عواد محمد الدليمي، نتائج مبدأ الشرعية الجنائية ودورها في تحديد ذاتية القواعد الجنائية الموضوعية، مقال منشور في 2017/04/18، تاريخ الدخول: 2022/10/27، متاح على الرابط: https://almerja.com ›

8-جميلة. ق، قمت بقرصنة أنظمة إتصالات الجزائر للتنبيه على وجود ثغرات خطيرة، مقال منشور على صفحة النهار Online، 06 ديسمبر 2017، أطلع عليه بتاريخ: 10 مارس 2023، متاح على الرابط: https://www.ennaharonline.com

9-مروة أبو العلا ، خصوصية الجرائم الإلكترونية في التشريع الجزائري والتشريعات المقارنة، مقال منشور بتاريخ 20 أفريل 2018، تاريخ الدخول: 2022/09/02، متاح على الرابط: *https://www.mohamah.net*

10-يوسف زيدات حابس، مدة إستيعاب النصوص التقليدية للسرقة الإلكترونية دراسة مقارنة، مقال منشور بتاريخ 2019، تاريخ الدخول 2023/05/31، متاح على الرابط https://doi.org/10.5339/rolacc.2019.9

11-أبقال عبد المنعم، الإطار القانوني لمكافحة الجريمة الإلكترونية –دراسة مقارنة–، مقال منشور بتاريخ،01 نوفمبر 2020، تاريخ الدخول: 2022/08/25، متاح على الرابط: *https://revuealmanara.com*

12-عبد الغفور الوازني ، تصنيفات المجرم المعلوماتي بين تباين الدوافع واختلاف الأهداف، مقال منشور بتاريخ 2020/04/17، تاريخ الدخول: 2022/09/26متاح على الرابط: *https://revuealmanara.com*

13-الشرعية الجنائية الجزء الثاني، مقال منشور بتاريخ، 2020/09/05،: تاريخ الدخول: 10/15/ 2020 متاح على الربط: https://www.academia.edu

14-عبد القادر غالب ، المجرم الإلكتروني، مقال منشور بتاريخ 2021/12/16، تاريخ الدخول: 2022/09/16، متاح على الرابط" https://www.africanewsanalysis.com

15-عبد الرحمن عايش، أحدث إحصائيات الجرائم الإلكترونية لعام 2023، مقال منشور على صفحة تكنولوجيا اليوم بتاريخ 2023/05/19، تاريخ الدخول: 2024/06/29، متاح على الرابط: https://today-tech.net.

16-عوني الداوود، الجرائم الإلكترونية آثار مدمرة على إقتصادات الدول والشركات والبنوك والأفراد، مقال منشور على صفحة مركز الدستور للدراسات الاقتصادية، بتاريخ يوليو 2023، تاريخ الدخول 2024/06/29، متاح على الراط: https://www.addustour.com

17-أكبر الشركات العالمية التي تعرضت للقرصنة، مقال منشور بتاريخ 31 جانفي 2021، تاريخ الدخول: 2023/02/15 ، متاح على الرابط:*https://www.argaam.com*

18-محمد البغدادي، مفهوم أمن المعلومات وعناصره، مقال منشور في مارس 2021، أطلع عليه بتاريخ 2023/11/07. متاح على الرابط: https://mqall.org/concept-information-security/

19-محمد بنهشوم، كيف تواجه الإحتيال الإلكتروني؟، مقال منشور بتاريخ 2021، تاريخ الدخول: 2023/07/28، متاح على الرابط: https://blog.khamsat.com/online-fraud

20-مها دحام ، تعريف الشخصية القانونية، مقال منشور في 8 أغسطس 2022، تاريخ الدخول: 2022/09/30، متاح على الرابط: *https://mawdoo3.com*

21-إبراهيم علوني ، جرائم اللياقات البيضاء، مقال منشور بتاريخ 24 يوليو 2020، تاريخ الدخول: 2022/09/16، متاح على الرابط: *https://www.okaz.com.sa*

22-مي مجدي، أخطر هجمات سيبرانية تستهدف شركات الطاقة...إبتزاز أرامكو أشهرها، مقال منشور بتاريخ، 2022/03/06، تاريخ الدخول: 2022/12/31، متاح على الرابط: *https://attaqa.net*

23-محمد حطاب، أشهر حالات التجسس الصناعي في العالم، مقال منشور بتاريخ 2020/04/1، أطلع عليه بتاريخ 07/15/ 2023 ، متاح على الرابط: *https://abunawaf.com*

قائمة المصادر والمراجع باللغة الفرنسية:

A-les lois:

1- la déclaration des droits de l'homme et du citoyen de 1789.

2- la déclaration universelle des droits de l'homme de 1948.

3- Loi N°88-19 du 5 janvier 1988, relative à la Froude informatique, J,O,R,F, du 6 janvier 1988.

4- Loi N° 92-683 du 22 juillet 1992 portant reforme du code pénale, J,O,R,F, du 23 juillet 1992.

5- Loi N^0 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J,O,R,F du 22 juin 2004

6- Loi N° 2009-1311 du 28 octobre 2009, relative à la protection pénale de la propriété littéraire et artistique sur internet, J,O,R,F, du 29octobre 2009.

7- Loi N°2012-287 du 1er mars 2012, relative à l'exploitation numérique des livres indisponible du xxe siécle, J,O,R,F, du 2 mars 2012.

8- Loi N° 2013-1168 du 18 décembre 2013, relative à la programmation militaire pour les années 2014 à 2019 et portant diverses disposition concernant la défense et la sécurité nationale, J,O,R,F, du 19 décembre 2013.
9- Loi N° 2014-1353 du 13 novembre 2014, renforçant les dispositions relative à la lutte contre le terrorisme, J,O,R,F, du 14 novembre 2014.
10- loi N^0 2015-912 du 24 juillet 2015, relative au renseignement échéancier d'application, art 4, J.O.R.F. N^0 0171 du 26 juillet 2015.

B-Les décisions judiciaires:

1- Cour de cassation, criminelle, chambre criminelle, 20 mai 2015, N^0 14. 81. 336. Publié ou bulletin.

C-les ouvrage:

-Alain Bensoussan, internet, aspects juridique, 2 eme Ed, france, hermes science publication, juin 1999.

D-les articles:

1- Jean Pradel, Les infraction relatives à l'informatique , R. I. D. C, N^{0}2, vol 42, juin 1990.
2- Nassima Azizi , Ibtissem Khedri, Cybercriminalité un fléau planétaire, R D E J, N° 1, VOL 1, 2020.

E-Les thèses:

1- Ibtissem Maalaoui, Les infraction portant atteinte à la sécurité du systéme informatique d'une entreprise**,** mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit (L.L.M) option droit des affaires, université de montréal, septembre 2011.

F-Les sites électroniques:

1- Mohamed Chawki, Essai sur la notion de cybercriminalité, juillet 2006, consulté le 01/09/2022, sur le site: http://www.iehei.org .
2- Leila Marchand, La cybercriminalité coute 600 milliard de dollars par an, publie le 21/02/2018, consulté le 08/09/2022, sur le site: https://lesechos.fr.
3- Protéger contre la falsification de document, publié le 23/12/2019, consulté le 18/06/2023, sur le site : https://nec-itplatform.com.

قائمة المراجع باللغة الإنجليزية:

A-Articles:

1-Rezki Kettaf, Cyberspace and cyber crime-towards modeling behavior and controlling action- J H S, (N°2, VOL 09, JUIN, 2022.

2- Seffari Asma, information security and the need to move towards the application of standard specification in Algerian institutions, J. H. S, VOL 9, N^{O} 2, JUIN 2022.

الفهرس

شكر وتقدير

إهداء

قائمة المختصرات

الملخص

دفعت التطورات الحاصلة في مجال تقنية المعلومات شركات المساهمة إلى التغيير من نمط أعمالها حتى تواكب تلك التطورات، الشيئ الذي عرضها إلى نوع مستحدث من الجرائم والتي تتمثل في الجرائم الإلكترونية التي إتخذت من البيئة الإفتراضية مسرحا لها.

حيث تعتبر الجرائم الإلكترونية أكثر خطورة على شركات المساهمة من نظيرتها التقليدية خاصة وأنها تستهدف معلوماتها وأسرارها التجارية، فالمساس بها قد يؤدي إلى إزاحة هذه الشركات من الساحة التجارية، الأمر الذي يتطلب منها إتخاذ إجراءات وقائية قصد تحقيق الأمن المعلوماتي والوقاية منها.

الكلمات المفتاحية:

شركات مساهمة، جرائم إلكترونية، بيئة إفتراضية، نظام معلوماتي، إختراق.

Résumé

Les progrès des technologies de l'information ont mené les sociétés par action, changer son style d'affaires pour suivre le rythme de ces développements, Ce qui l'a influencé à un nouveau type de crime, c'est la cybercriminalité, prise de l'environnement virtuel comme sa scène.

La cybercriminalité est plus grave pour aux sociétés anonymes de son homologue traditionnel d'autant plus qu'il cible ses informations et secrets commerciaux, les endommager pourrait déloger ces entreprises de l'arène commerciale, Cela nécessite une action préventive pour atteindre et prévenir la sécurité de l'information.

Mots clés : : sociétés par actions, cybercriminalité, l'environnement virtuel , système informatique, piratage.

Abstract:

Advances in information technology have led joint-stock companies to change their business methods so as to keep pace with these new developments. However, this has exposed them to a new type of crime--electronic crimes, which operate in the virtual space.

These crimes are particularly risky for joint-stock companies because they target sensitive information and trade secrets. If such information is compromised, the companies may be pushed out of the market, thereby calling for pre-emptive measures to ensure cybersecurity and protection

Keywords: joint-stock companies, cybercrime; virtual environment; computer system, hacking