وزارة التعليم العالي و البحث العلمي
المركز الجامعي صالحي أحمد بالنعامة

معهد الحقوق

قسم القانون:قانون خاص

مذكرة تخرج لنيل شهادة الماستر

تحت عنوان

جرائم الأعمال في البيئة الرقمية

من إعداد الطالبة:

-شريفي شيماء

تحت إشراف:

-الأستاذة : بوعزة أمينة

لجنة المناقشة:

إسم و لقب الأستاذ	الرتبة العلمية	الصفـة
أ.د مفتاح العيد	أستاذ تعليم عالي	رئيسا
د.برمضان حميد	أستاذ محاضر قسم ب	مناقشا
د. بوعزة أمينة	أستاذة محاضر قسم ب	مشرفة و مقررة

السنة الجامعية:
2025/2024

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
C.U.N
Centre Universitaire Salhi Ahmed de Naâma المركز الجامعي صالحي أحمد بالنعامة

النعامة في : 2025/06/17

معهدالحقوق

الإذن بالإيداع

أنا الممضي أسفله الأستاذ(ة)

..... بوعزة أمينة.....

الرتبة.....أستاذة محاضرة ب.....:...الجامعة.....أحمد صالحي النعامة.....

معهد :.....الحقوق:.....القســم.....القانون الخاص.....

المشرف على مذكرة الماستر للطالب (ة):

شريفي شيماء .....

تحت عنوان :

.....جرائم الأعمال في البيئة الرقمية.....

المقدمة لنيل شهادة الماستر في.....القانون الخاص.....

التخصص.....قانون أعمال.....

خلال الموسم الجامعي.....2025/2024.....

أشهد أن الطالب(ة) قد أتم(ت)تحرير المذكرة،وأخذ(ت) بعين الاعتبار مجمل التوجيهات المقدمة له(ها)،وعليه نوافق على طباعة العمل المذكور وفق المعهود في مذكرات والرسائل الجامعية ثم تقديمه للإدارة.

توقيع المشرف

إهداء

إلى نفسي، فخر أحتضنه بعد كل تعب، وامتنان عميق لما استطعت تجاوزه بعزيمة لاتلين

لروح والدي، التي لاتغيب عن قلبي لحظة ... طيفك كان رفيق خطواتي، والدعاء الذي لايغيب –رحمة الله عليك–

لأمي، من بها استقام الطريق وخفت الأعباء –أطال الله في عمرك–

لأخت كانت سندا لايعوض –فاطمة الزهراء– ، وأخ كان نسمة أمل كل اللحظات – علاء–

إلى توأمي ورفيقة الطفولة، مرآتي الأولى .. جيهان.

لصديقة كانت الدعم حين ثقلت الأحمال –دليلة–

إلى خالي مولاي جمال ، والأخ شريفي عبد الحق ... شكرا على مواقفكما الصادقة.

إلى من لم تجمعني بهم صلة دم ، لكن دعمهما فاق الروابط ... قادري هشام ، حركاتي بشير.

أختم كلامي ، وشكري الخاص إلى من آمن بي وفتح أمامي آفاق المعرفة بتشجيعه .. أستاذي تركي العيد . ومن لم يبخل عني بعلمه، ولم يتردد بمنحي دعمه وثقته .. الأستاذ المحامي رقايقية نور الدين

شكروعرفان

الحمد لله الذي ألهمني الصبر والعزم، ويسر لي السبل، وأعانني على إتمام هذا العمل ...

فالحمد لله حمدا كثيرا حتى يبلغ الحمد منتهاه.

من لا يشكر الناس لايشكر الله

بعيدا عن الإطراء، أتوجه بالشكر الجزيل إلى الأستاذة المشرفة "بوعزة امينة" على قبولها الإشراف على المذكرة وإخراجها بالشكل الذي عليه الآن ، وذلك بفضل جهودها وملاحظاتها السديدة والدقيقة

فلها مني كل التقدير والإحترام

كما لا يفوتني أن أتوجه بجزيل الشكر و الإمتنان لأعضاء لجنة المناقشة الأفاضل، الأستاذ "مفتاح العيد"، و الأستاذ "برمضان حميد" ، على قبولهم مناقشة هذا العمل المتواضع ، وعلى ما سيتفضلون به من ملاحظات قيمة تسهم في إثرائه والارتقاء به

قائمة المختصرات:

ج.ر.ج .ج : الجريدة الرسمية للجمهورية الجزائرية.

ق.إ.ج.ج: قانون الإجراءات الجزائية.

د.م.ن: دون مكان نشر.

د.س.ن: دون سنة نشر.

ص : صفحة .

ص.ص: من الصفحة إلى الصفحة

مقدمة

شهد العالم في الآونة الأخيرة تحولا جذريا بفعل التطور التكنولوجي، الذي غير مجرى جل المجالات والميادين، بما في ذلك النشاطات الإقتصادية والتجارية. حيث اصبحت المؤسسات والشركات تعتمد في معاملاتها على وسائل تقنية متطورة، والتي ساهمت في تسهيل وتسريع العمليات والنشاطات في قطاع الأعمال، وخلق جو من المنافسة بين الشركات التجارية أيضا.

إلا أن التطور الرقمي كان له وجه آخر، بحيث صاحبه بروز أشكال وأنماط جديدة تحمل بينها تهديدات لقطاع الأعمال. خاصة تلك المرتبطة بالجريمة الإلكترونية. والتي تتزايد في تنوعها وخطورتها، نظرا للتطور الرقمي المستمر.

ماجعل البيئة الرقمية للأعمال تواجه تحديات عديدة. ومن أهمها مسألة حماية وتأمين هذه العملية، ومن مختلف النشاطات الإجرامية التي تهدد المصالح المتعلقة بهذا المجال، خاصة تزايد الإعتماد على الخدمات والعمليات المالية الرقمية.

هذا ما أدى إلى ظهور نوع جديد من الجرائم، والتي تعرف ب" **جرائم الأعمال الرقمية** " . والتي تقوم على وسائل وأدوات تقنية، مايجعلها تتجاوز إقليم الدولة والحدود الجغرافية كونها من الجرائم العابرة للحدود. وبالتالي صعوبة مراقبة مرتكبيها، بحيث يصبح القانون هنا أمام تحديات معقدة من حيث نطاق تطبيقها.

كما نجد أن هذه الجرائم تتنوع وتتفاوت حسب طبيعة محلها. فمنها التي محلها الأموال، كالنصب والإحتيال الرقمي، تبييض الأموال باستعمال وسائل الدفع الإلكترونية، أو تلك الماسة بجرائم التجارة الإلكترونية.

إذ أن الجرائم الرقمية في قطاع الأعمال فرضت تحديات كبيرة على التشريع والقضاء. لأنه من الصعب تطبيق القواعد التقليدية لجرائم الأعمال التقليدية على هذا النوع من الجرائم المستحدثة. هذا ما يبرز خطورة جرائم الأعمال الرقمية و صعوبتها، لا من حيث تكييفها، إكتشافها أو إثباتها.

تبرز أهمية هذه الدراسة في أنها تتناول موضوعا مستجدا فرضته التحولات الرقمية على قطاع الأعمال وإبراز مدى استجابة التشريع الوطني للتحولات الرقمية. والذي أدى إلى ظهور

وتعدد جرائم جديدة في هذا المجال، والتي تهدد استقرار المؤسسات والشركات التجارية، وكذا المساس بالثقة العامة بين العملاء.

أما بالنسبة للأهداف المتوخاة من هاته الدراسة فتكمن في تسليط الضوء على هذا النوع من الجرائم، خاصة وأن مجال الأعمال من المجالات الحساسة والأكثر تعرضا للتهديدات بشتى أنواعها. لتحديد الإطار المفاهيمي لجرائم الأعمال الرقمية، و بهدف معرفة مدى نجاعة القانون في مكافحة جرائم الأعمال الرقمية، وكيفية تعامل المشرع الجزائري مع هذه الجرائم سواء في كيفية الكشف عنها، أو في إثباتها.

ولقد جاء اختيار موضوع **"جرائم الأعمال الرقمية"** نتيجة تقاطع نقاط من الدوافع الموضوعية والذاتية، التي أكدت لي أهمية التطرق إلى هذا النوع المستجد من الجرائم. إذ أن هذا الموضوع يعتبر من المواضيع المستجدة، والذي لا يزال يواجه قصورا من حيث التكييف القانوني. إضافة إلى ذلك أن جرائم الأعمال الرقمية من الجرائم الخطرة التي تهدد المؤسسات بصفة عامة، وتؤثر سلبا على الثقة في المعاملات التجارية إضافة إلى ذلك ، لاحظت غياب شبه منعدم لدراسات خاصة بهذا الموضوع.

أما من الناحية الذاتية، فإنه في الأصل تتجه ميولاتي إلى كل من القانون الجزائي وكذا قانون الأعمال. وقد جاء هذا الموضوع كفرصة تحفيزية للغوص في كلا المجالين، وكإنطلاقة أولى نحو أهدافي المستقبلية في هذا المجال. إذ لطالما استوقفتني التحديات الجديدة التي تواجهه المؤسسات والشركات في البيئة الرقمية من جهة، وعدم اهتمام التشريعات الوطنية والدولية بصفة خاصة بهذا النوع من الجرائم من جهة أخرى.

ومن هنا تبرز الإشكالية المحورية التي تسعى هذه الدراسة إلى معالجتها، والمتمثلة في:

ما مدى نجاعة النصوص القانونية التي وضعها المشرع الجزائري للحد من جرائم الأعمال في البيئة الرقمية؟

و التي تتفرع منها الإشكالات التالية:

ماهو مفهوم جرائم الأعمال الرقمية؟

ماهي الخصائص التي تميز جرائم الأعمال الرقمية عن غيرها من الجرائم؟

فيما تتمثل أبرز صور الجرائم الرقمية في مجال الأعمال؟

وطبقا للقاعدة شبه الراسخة في البحث العلمي والتي مفادها أن موضوع الدراسة هو من يحدد المنهج المتبع، فقد اتبعت المنهج الوصفي في دراسة المفاهيم الأساسية التي يقوم عليها الموضوع محل الدراسة، وتصنيف أنواعها، مع تحليل التشريعات الوطنية لرؤية مدى جهودها في مكافحة هذه الجرائم، وإرائها للإجراءات للكشف عن ملابساتها وضبط الدليل الرقمي. والذي تخلله المنهج المقارن في دراسة الجهود الإقليمية وكذا الدولية في مجابهة هذه الجرائم.

ولقد واجه إعداد هذه المذكرة الكثير من الصعوبات، نذكر منها على سبيل المثال لا الحصر غياب المرجع والنصوص القانونية الخاصة به، وكذا الاجتهادات القضائية حوله، إلا أن هذا لم يشكل عائقا لي طوال كل مراحل إنجاز بحثي هذا، بحيث حرصت على تقديم جهدي الشخصي لدراسة كل من الجانب النظري وكذا التطبيقي والربط بينهما، ومواجة التحديات والصعوبات للتوصل إلى نتائج تتوافق مع الهدف الرئيسي لهذه الدراسة بما يتوافق مع البحث العلمي الصحيح.

كما ذكرت سابقا أن هذا الموضوع من الجرائم المستحدثة، والتي لم تلق دراسة خاصة من حيث مفاهيمها، ولا إجراءات الكشف عنها بشكل خاص. إلا أنه هناك دراسات لها علاقة بشكل غير مباشر بهذا الموضوع. ونذكر منها:

_ صالح شنين، الحماية الجنائية للتجارة الإكترونية-دراسة مقارنة-، مذكرة لنيل شهادة دكتوراه.

_بورنان فاطمة الزهراء، عوادي بشينة، خصوصية المسؤولية الجزائية في جرائم الأعمال، مذكرة لنيل شهادة ماستر.

_ محمد الشريف بولعراس، أسامة طلحي، جريمة التزوير المعلوماتية، مذكرة مقدمة لنيل شهادة ماستر.

_يحي ثنهنان، بن مسعود فاطمة، جرائم الأعمال في قانون التجارة الإلكترونية، مذكرة لنيل شهادة ماستر قانون أعمال.

_لبيض عادل، نزلي بشرى، إثبات الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر.

وقد تم تقسيم هذه الدراسة وفقا للخطة التالية:

الفصل الأول: ماهية جرائم الأعمال الرقمية.

المبحث الأول: مفهوم جرائم الأعمال الرقمية.

المبحث الثاني: الجهود الدولية والوطنية لمكافحة جرائم الأعمال الرقمية.

الفصل الثاني: صور جرائم الأعمال الرقمية والآليات الإجرائية للكشف عنها.

المبحث الأول: صور جرائم الأعمال الرقمية

المبحث الثاني: الآليات الإجرائية للكشف عن جرائم الأعمال الرقمية وإثباتها.

الفصل الأول: ماهية جرائم الأعمال الرقمية

مع التطور التكنولوجي الذي شهدته كل المجالات، أصبح قطاع الأعمال يعتمد و يستند إلى الوسائل الإلكترونية في مختلف نشاطاته، سواء في جانب المعاملات التجارية أو حتى التعاملات المالية كالشركات...، إلا أنه ظهر نمط جديد من الإجرام يهدد مجال الأعمال بصفة عامة، و هو ما يسمى بجرائم الأعمال الرقمية، بحيث تتميز هذه الجرائم بسرعة انتشارها و الطابع غير المادي، و التي جعلت من التشريعات تواجه تحديات كبيرة.

من هذا المنطلق، أسعى من خلال هذا الفصل التطرق إلى المفاهيم الأساسية لجرائم الأعمال الرقمية، من خلال عرض تعريفها و خصائصها و تمييزها عن جرائم الأعمال التقليدية، اضافة إلى ذلك إبراز التحديات التي تواجهها التشريعات سواء على الصعيد الإقليمي أو الدولي، و كذلك على المستوى الوطني، تحديدا التشريعات الجزائرية لرؤية مدى كفاية النصوص القانونية في مكافحة هذا النوع من الجرائم، بحيث تنقسم هذه الدراسة إلى مبحثين :

المبحث الأول : مفهوم جرائم الأعمال الرقمية

المبحث الثاني : الآليات الدولية و الوطنية لمكافحة جرائم الأعمال.

المبحث الأول: مفهوم جرائم الأعمال في البيئة الرقمية.

شهد مجال الأعمال نقلة نوعية من البيئة التقليدية إلى البيئة الالكترونية، ما أدى إلى ظهور وتشكل جرائم جديدة، تعرف بجرائم الأعمال الرقمية. والتي تتميز عن نظيرتها التقليدية. لذا سنتطرق إلى مفهومها، من خلال تعريفها أولا (المطلب الأول)، ثم إلى خصوصيتها سواء من حيث قواعد التجريم أو المسؤولية الناتجة عنها (المطلب الثاني)، لنستخلص أهم الخصائص التي تميزها (المطلب الثالث).

المطلب الأول: تعريف جرائم الأعمال الرقمية وخصائصها.

لم تلق جرائم الأعمال الرقمية اهتماما خاصا من طرف كل التشريعات، سواء الوطنية أو حتى الدولية. والتي رغم اختلافها عن الجرائم الأخرى إلا أنه يتم حصرها مع الجرائم الإلكترونية بصفة عامة. لكن هذا لا يعني التقليل من قيمتها، لأنها تعتبر من الجرائم الخطرة. لذا سأحاول التوصل إلى مفهوم جرائم الأعمال الرقمية، عن طريق تعريف المصطلحات المتعلقة بها أولا، ليتضح بعدها أهم الفروقات بينها وبين جرائم الأعمال التقليدية.

الفرع الأول: تعريف الجريمة الرقمية في مجال الأعمال.

قبل تعريف جرائم الأعمال الرقمية بصفة خاصة، لابد من فهم أولا الجرائم الواقعة في الفضاء الإلكتروني بصفة عامة.

أولا: تعريف الجريمة.

عرفها الفقيه الأستاذ محمود نجيب حسيني :"الجريمة هي فعل غير مشروع صادر عن إرادة جرمية يقرر له القانون عقوبة أو تدبيرا احترازيا"[1].

[1]- د.فريد روابح، مطبوعة محاضرات في القانون الجنائي العام، مقدمة لطلبة السنة ثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين –سطيف-، 2018-2019، ص28.

كما تعرف أيضا في مجال القانون الجنائي العام بصفة عامة، بأنها سلوك الفرد عملا كان أو امتناعا، يقابله عقوبة جزائية، وهو التعريف الذي ينطبق على عناصر الجريمة من حيث أثرها[1].

ثانيا: تعريف مصطلح "الأعمال": يمكن أن نستخلص أنه ذلك النشاط الإقتصادي الذي يشمل مجموعة من المجالات، منها التوزيع والخدمات، الصناعة، التجارة، الإستثمار، المؤسسات المالية...، والتي تلزم التشريع بوضع قواعد وأحكام قانونية تحكمها. بحيث لا يمكن حصر هذا المصطلح بمجال معين، كون أن النشاط الإقتضادي متنوع ومتجدد خاصة فيما يخص مجال التجارة، الذي يتميز بدوره بطابع السرعة.

ثالثا: الجريمة الإلكترونية: لم يتفق الفقه الجنائي على ضبط مصطلح معين لهذا النوع من الجرائم، فهناك من يسميها الجرائم المعلوماتية، الجرائم المستحدثة، الجرائم الرقمية، جرائم الكمبيوتر وغيرها.

أما بالنسبة للمشرع الجزائري، فإنه لم يرد منه أيضا تعريفا خاصا بالجريمة الإلكترونية، ولكنه تزامنا مع التعريفات الحديثة والتطور الذي تشهده التكنولوجيا، فقد اصطلح على مثل هذه الجرائم بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي قام بتعريفها في المادة 2 من قانون 09-04[2]:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

[1]- عاسية زروقي، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، ندوة وطنية، منشورة في كتاب : الجريمة المعلوماتية، جامعة الجزائر1، 12 نوفمبر 2019، ص7.

[2]- قانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق ل5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج ر ج ج الصادرة في 25 شعبان 1430 الموافق ل16غشت2009، العدد 47، ص5

بحيث أن المشرع اعتبر أن هذا المصطلح هو الأوسع بالنظر لموضوع الجريمة الالكترونية من خلال جمعه بين تقنية الحوسبة، التي تعتمد على الآليات التقنية لمعالجة البيانات، وتقنية الاتصالات الحديثة التي تستند إلى آليات تقنية أيضا لنقل المعلومات بكل أنواعها[1].

رابعا: تعريف جرائم الأعمال الرقمية.

من المعروف أن جرائم الأعمال ترتكب من طرف أشخاص ذو مكانة عالية، و هذا ما أضاف صفة الغموض على هذه الجرائم، و بالتالي صعوبة توجيه الإتهام إلى مرتكبيها. لذا لم ينص المشرع الجزائري على تعريف صريح و شامل لجرائم الأعمال كونها تختلف حسب اختلاف مجال نشاط الجاني.

أما بالنسبة للفقهاء، فلم يرد عنهم أيضا تعريف خاص، فهناك من عرفه على أساس معيار الموضوع، إذ يوجد من حصره في مجال الإقتصاد، و من ربطه بفكرة حدوث هذه الجريمة بمشروع اقتصادي، ما يفتح المجال أمام جرائم أخرى لا علاقة لها بالإقتصاد أو المعاملات التجارية. و هناك أيضا من عرفها على أساس الشخص الذي ارتكبها، أي أن جرائم الأعمال ترتكب من طرف من لهم صفات مميزة عكس الجرائم العادية، إذن لا يمكن دمج هذه التعاريف في قالب واحد،لإختلاف معاييرها[2]. لذا يمكن تعريف جرائم الأعمال بأنها :" تلك الأفعال غير المشروعة التي ترتكب عند مباشرة المعاملات التجارية و يؤدي إلى الإضرار أو التهديد بالضرر لسلامة المعاملات التجارية و الإقتصادية و المالية[3]".

---

[1]- مونة مقلاني، راضية مشري، الجريمة الإلكترونية –دلالة المفهوم وفعالية المعالجة القانونية-، مخبر الدراسات القانونية البيئية، مجلة أبحاث قانونية وسياسية، المجلد السادس، العدد الأول، جوان 2021، ص 496.

[2]- د.حسام بوحجر، القانون الجنائي للأعمال، محاضرات ألقيت على طلبة السنة الأولى ماستر قانون أعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 –قالمة-، 2020-2021، ص10/9.

[3]- حسين أحمد الجندي، القانون الجنائي للمعاملات التجارية –القانون الجنائي للشركات-، دار النهضة العربية، 1989، ص28.

و انطلاقا من هذا المفهوم الخاص الذي تتضمنه جرائم الأعمال على غرار الجرائم الأخرى العادية، و بالنظر إلى التطور الذي يشهده العالم، بما فيه الطابع التقني الذي يميز هذا النوع من الجرائم، فلا بد من امتداد جرائم الأعمال إلى الفضاء الإلكتروني، و يمكن القول أن جرائم الأعمال الرقمية، هي تلك الأفعال المجرمة التي تتم بواسطة وسائل رقمية سواء كان الحاسوب أو بالدخول غير المشروع للأنظمة المعلوماتية أو غيرها. و التي تستهدف المؤسسات المالية و الإقتصادية و التجارية بصفة عامة، بما فيها النشاط و المعاملات التجارية غير المشروعة، منها تبييض الأموال عن طريق الإحتيال الإلكتروني، اختراق المواقع التجارية، السطو على البطاقات الإئتمانية، سرقة البنوك...، بحيث لم يرد عن المشرع أي نص قانوني خاص بهذا النوع أيضا، كما هو الحال بالنسبة للجرائم التقليدية في مجال الأعمال.

الفرع الثاني: التمييز بين جرائم الأعمال الرقمية وجرائم الأعمال التقليدية.

تختلف جرائم الأعمال الرقمية عن نظيرتها التقليدية تحت جملة من النقاط، و نستخلص أهمها فيما يلي :

1_من حيث البيئة و الوسائل : تقوم الجريمة التقليدية على أرض الواقع و بوسائل مادية و ملموسة، بينما جرائم الأعمال الرقمية فهي تنشأ و تحدث في البيئة الرقمية، و ترتكب بوسائل تقنية حديثة و متطورة، و تكون غير مادية.

2_من حيث نطاق اقترافها : تخضع الجرائم العادية لإطار مكاني محدد بإقليم الدولة، بينما الجرائم المستحدثة فهي عابرة للحدود، مما يخلق تنازع في الإختصاصات المتعلقة بالضبط و المتابعة[1].

[1]- فتاش نورة، الجرائم امستحدثة، محاضرات مقدمة لطلبة السنة الثانية ماستر علم اجتماع الجريمة والإنحراف، قسم العلوم الإجتماعية، كلية العلوم الإنسانية والإجتماعية، جامعة 20 أوت 1995، سكيكدة، 2020-2021، ص12.

3_من حيث المجرم و أداء الأفعال الإجرامية : يختلف المجرم في الجريمة الرقمية عن المجرم العادي، أن الأول يمتلك خبرة فنية في مجال الإجرام المعلوماتي ، و كذا ثقافته السابقة بطبيعة الجريمة ما يجعله أكثر حرصا في ارتكابها.

بينما المجرم العادي فقد اعتاد على نوع محدد من الجرائم العادية، و التي يعتمد في ارتكابها على وسائل تقليدية يمكن أن يصل حتى إلى استخدام العنف. هذا ما يحدد نتيجة الجرائم.

فجرائم الأعمال الرقمية يكون هدفها الوصول إلى تحقيق الربح و السلطة و النفوذ، بينما التقليدية فيكون الدافع فيها الإنتقام و يصل حتى إلى الإضرار المادي بالغير.

المطلب الثاني: خصوصية جرائم الأعمال الرقمية من حيث قواعد التجريم و أحكام المسؤولية.

تتحقق صفة الجرم على فعل معين متى تحققت عناصرها، وهي الركن المادي وكذا المعنوي. والتي ينشأ عنها مسؤولية تقع على عاتق مرتكبها، بحيث أنها تقع أيضا على الشخص المعنوي، سواء كان لجنة معينة، أو شركة تجارية ما، وسواء كان مرتكب الجريمة ممثلها أم أشخاص أخرى قاموا بالفعل المجرم بطلب من هذا الشخص المعنوي. وتختلف جرائم الأعمال في هذا الخصوص عن غيرها من الجرائم، لذا سنتطرق إلى خصوصية هذا النوع من الجرائم من حيث قواعد التجريم، وكذا خصوصية أحكام المسؤولية.

الفرع الأول : خصوصية جرائم الأعمال من حيث قواعد التجريم.

من المعروف أنه لقيام أية جريمة لا بد من تحقق ثلاث أركان رئيسية، و المتمثلة في الركن الشرعي، الركن المادي و الركن المعنوي، و هذا ما نجده في الجرائم العادية، إلا أن الأمر يختلف

بالنسبة لجرائم الأعمال، و هذا ما سيتم توضيحه، من خلال دراسة خصوصية الركن المادي و الركن المعنوي.

أولا : خصوصية الركن المادي لجريمة الأعمال الرقمية.

تتميز جرائم الأعمال من حيث مكونات الركن المادي، بأنها جرائم خطر لا ضرر.

1_عناصر الركن المادي :

و يتكون من السلوك الإجرامي، النتيجة و العلاقة السببية.

أ_**السلوك الإجرامي:** هو كل سلوك غير مشروع مخالف للقانون، يمكن أن يكون ايجابيا بمعنى وقوع الفعل المجرم، أو سلبيا و يتمثل في الإمتناع عن القيام بفعل نص عليه القانون، إلا أن هذا لا يسري في جرائم الأعمال [1].

ب_**النتيجة:** الأثر الناتج عن السلوك الإجرامي، سواء كان اعتداء على حق يحميه القانون و يقرر له عقوبة. بمعنى أن للنتيجة مدلولان : يتمثل أوله في التغيير الذي يحدث في العالم الخارجي، و هذا كتأثير للسلوك الإجرامي، و آخر ثانوي يتجلى في الإعتداء على مصلحة يحميها القانون[2].

ج_**العلاقة السببية:** و هي تلك الرابطة بين السلوك الإجرامي و النتيجة، و التي تثبت حدوث الفعل المجرم، بحيث لولا ارتكابه لما حدثت النتيجة.

تعد جرائم الأعمال من جرائم الخطر لا الضرر، بحيث لا يشترط تحقق نتيجة معينة. فغالبية الجرائم في قطاع الأعمال هي جرائم ايجابية، يجرمها المشرع نظرا لخطورتها لا لمدى تحقق الضرر،

[1]- أوشن بولرياس ليلى، خصوصيات قواعد التجريم في مادة القانون الجزائي للأعمال، ملتقى وطني حضوري/إفتراضي، مداخلة منشورة في كتاب: جرائم الأعمال –الخصوصية والحوكمة-، جامعة بن يوسف بن خدة، الجزائر 1، 10 نوفمبر 2022، ص52.

[2]- محمد خميخم، الطبيعة الخاصة بالجريمة الإقتصادية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في القانون الجنائي والعلوم الإجرامية، جامعة الجزائر، كلية الحقوق، بن عكنون، 2011، ص36.

و الغرض هنا من المشرع اتباع سياسة وقائية أكثر من ردعية لأن غالبية جرائم الأعمال هي جرائم أموال يصعب اثباتها[1].

مثال ذلك عند الأمر بالبيع أو العرض للبيع، فيكفي هنا القيام بالعرض حتى و لو لم يتم البيع و لم تتحقق النتيجة، فهنا يعاقب الفاعل على القيام بعرضه للبيع سواء سلع أو خدمات.

ثانيا : خصوصية الركن المعنوي:

المبدأ أنه لا يحكم على أحد بعقوبة ما لم يكن قد أقدم على الفعل عن وعي و إرادة، غير أن في مجال الأعمال فإنه لا ينظر ما إذا كانت الجريمة عمدية أو غير عمدية، و لا ينظر إلى نية الجاني إذا كان فعله عن سوء أو حسن نية. لذا فإن جرائم الأعمال هي جرائم مادية بحتة ذات قاعدة استثنائية، بعيدة عن عنصري القصد و الخطأ[2].

الفرع الثاني : خصوصية أحكام المسؤولية في جرائم الأعمال الرقمية .

تعد المسؤولية الجنائية من أهم عناصر العلوم الجنائية، و التي تقع على الشخص بمجرد قيامه بجريمة معينة، و نظرا للمرونة و السرعة التي يتميز بها مجال الأعمال يجعلها تتفرع إلى جميع أحكام هذا المجال، بما في ذلك إسناد المسؤولية الجزائية للشخص المعنوي.

أولا_المسؤولية الجزائية عن فعل الغير.

إن الأصل في المسؤولية الجنائية أنها شخصية،بحيث لا يتم توقيع الجزاء على المرتكب الأصلي للجريمة أو المشارك فيها، و هذا يعتبر من أهم مبادئ المسؤولية الجنائية، إلا أن المشرع الجزائري قد أورد استثناء من هذه القاعدة بالمسؤولية عن فعل الغير، بمقتضى نصوص خاصة،

[1]- أوشن بولرياس ليلى، المرجع السابق، ص54.
[2]- المرجع نفسه، ص55.

و قد امتد هذا الإستثناء إلى جرائم الأعمال. إذ أنه لا شك أن يكون الخطأ الجزائي المقوم للجريمة شخصيا حتى يمكن مساءلة مرتكب جريمة الأعمال[1].

ثانيا_المسؤولية الجزائية للشخص المعنوي: إن المسؤولية للشخص المعنوي تعتبر من المسؤوليات الجزائية المستحدثة، رغم أن هذا الأمر كان مستبعدا، إلا أنه من مبررات توقيع الجزاء على الشخص المعنوي، ممارسة هذا الأخير لمختلف الأنشطة التجارية مايجعله أمام إمكانية ارتكاب جرائم مختلفة، وهذا أنه تم إقرار عقوبات تتمثل في غرامات مرتفعة لارتكابها أفعال غير مشروعة، ما يؤكد إلزامية إسناد المسؤولية للشخص المعنوي.

أما عن موقف المشرع الجزائري من هذه المسألة، فقد نص على أنه يخضع الشخص المعنوي للمسؤولية الجزائية عن الجرائم المرتكبة لصالحه من طرف أجهزته أو ممثليه القانونيين أو الحائزين على تفويض سلطات، عندما ينص القانون على ذلك[2].

المطلب الثالث: طبيعة جرائم الأعمال الرقمية وخصائصها.

تعتبر جرائم الأعمال الرقمية ذات طبيعة خاصة، نظرا للبيئة التي ترتكب فيها (الفرع الأول)، كما أنها تتميز بجملة من الخصائص التي تميزها عن غيرها من الجرائم خاصة التقليدية (الفرع الثاني).

الفرع الأول : طبيعة جرائم الأعمال الرقمية.

بحيث تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل المعلومات ومختلف البيانات مهما كان نوعها بسرعة وفي آن واحد، ما يؤدي إلى ارتكاب الفعل المجرم، هذا راجع لتوسع بنوك المعلومات بأنواعها، إضافة إلى ذلك رغبة الأفرا دفي ربط

[1]- د.مجدوب نوال، خصوصية سياسة التجريم والعقاب في قطاع الأعمال بالجزائر، مجلة القانون والعلوم السياسية، المجلد السابع، العدد الثاني، 2021، ص240.

[2]- قانون رقم 15-04، المتضمن قانون العقوبات، المعدل والمتمم بالأمر 24-06، المؤرخ في 19 شوال 1445 الموافق ل28 أبريل 2024،ج ر ج ج ، العدد 30.

حواسيبهم بشبكة الأنترنت على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الآلية للمعطيات، سواء كان ذلك عن طريق تجميعها أو تجهيزها أو تعديلها عن طريق إدخالها إلى في حواسيبهم المرتبطة بالأنترنت.[1]

وهذا لتسهيل عملية إرتكابهم لمختلف الجرائم خاصة في مجال الأعمال، مثل جرائم التزوير الإلكتروني، أو اختراق مواقع التجارة الإلكترونية وغيرها..

هذا الأمر ينتج عنه صعوبة التكييف القانوني لهذه الجرائم نظرا لميزتها وطبيعتها الخاصة. بحيث أن القواعد التقليدية لا يمكن تطبيقها على الظواهر الإجرامية المستحدثة. ما يثير مشاكلا حول مسألة الإثبات ومتابعة مرتكبيها من جهة أخرى[2].

الفرع الثاني: خصائص جريمة الأعمال الرقمية.

تتميز جرائم الأعمال الرقمية عن غيرها من الجرائم بجملة من الخصائص. نذكر اهمها فيما يلي:

1_جرائم تقنية: تتسم هذه الجرائم في كونها صورة من صور التنظيم بين الأطراف المرتكبين للعمل الإجرامي، بحيث غالبا ما يتميزون بأنهم من ذوي أصحاب النفوذ وذو مكانة عالية ، يرتكبون جرائمهم ببراعة، ويعتمدون على وسائل متطورة لضمان السرية المهنية. مثال ذلك جرائم تبييض لأموال، اختراق المواقع..[3]

[1]- رضوان علي، الإطار المفاهيمي للجريمة المعلوماتية "مفهومها وسمات مرتكبيها"، ملتقى وطني، مداخلة منشورة في كتاب الجريمة المعلوماتية، المرجع السابق، ص102.
[2]- المرجع نفسه، ص103.
[3]- حسام بوحجر، المرجع السابق، ص13.

2_ ذات طابع مالي و اقتصدي: يتوسع مجالها ليشمل كل الأعمال الاقتصادية وكذا المالية بمختلف أنواعها. وتخضع لحماية مصالح تجارية ومالية واقتصادية تامة. ويهدف المجرم من خلالها إلى عائدات مالية ومادية.[1]

3_ جريمة عابرة للحدود: أي أنها ذو طابع دولي، تتخطى الحدود الجغرافية الإقليمية. كون أنها ترتكب عبر الفضاء المعلوماتي، والتي يتفرع منها إشكالات سياسية، خاصة فيما يتعلق بإجراءات الملاحقة الجنائية في التحريات الخاصة بهذه الجريمة.[2]

4_ صعوبة اكتشافها و إثباتها: هي صعبة الإثبات، لكن ليست مستحيلة الإثبات، وأساس ذلك أنه غالبا ما يكون الجاني والمجني عليه مجهولين، نظرا لارتكاب الجريمة بوسائل فنية وتقنية. إضافة إلى ذلك أن السلوك الإجرامي المكون للركن المادي لهذه الجريمة يتم بسرعة وفي الخفاء، وأن الدليل الرقمي يمكن ان يتم محوه أو إتلافه في ظرف وجيز. هذا ما يجعل هذه الجريمة صعبة في الإثبات من جهة أخرى، كما توجد أسباب أخرى لصعوبةا لإثبات، من بينها وسيلة التنفيذ التقنية والتي تكون معقدة نوعا ما..[3]

5_سهلة الإرتكاب: تعد الجرائم الإلكترونية من الجرائم الهادئة، والتي لا تحتاج إلى العنف. بل تستند إلى شبكة الأنترنت، تتطلب خبرة فنية تقنية للتعامل مع جهاز الحاسوب في ارتكاب أفعال غير مشروعة، كالإختراق، التجسس الإلكتروني، التزوير الإلكتروني...[4]

[1]- حسام بوحجر، المرجع السابق، ص14.
[2]- د.بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، سبتمبر 2018، ص355.
[3]- د.عثماني رضوان، الجرائم الإلكترونية، محاضرات مقدمة لطلبة السنة ثانية ماستر قانون جنائي، معهد الحقوق، المركز الجامعي صالحي أحمد، النعامة، 2024-2025، ص9.
[4]- المرجع نفسه، ص10.

المبحث الثاني: الآليات الدولية والوطنية لمكافحة جرائم الأعمال الرقمية.

إن التطور التكنولوجي لم يقتصر فقط على مجال معين، بل امتد لكل المجالات، بما فيها الاقتصادي والمالي، مما أدى إلى تولد أنماط جديدة ومختلفة من الجرائم المختلفة، منها جرائم الأعمال الرقمية، وهذا ما جعل الدول تسعى لمكافحة هذا النوع من الجرائم، عن طريق تجريم هذه الأفعال وتقرير عقوبات خاصة بها، وتنقسم هذه الجهود إلى دولية ووطنية. لذا ستتناول في هذا المبحث الجهود المبذولة على كل من المستوى الدولي(المطلب الأول)، على المستوى الإقليمي (المطلب الثاني)، و المستوى الوطني (المطلب الثالث).

المطلب الأول: الجهود الدولية لمكافحة جرائم الأعمال الرقمية.

كأول خطوة لمكافحة الجرائم الإلكترونية، كان لابد من مبادرة الدول بإصدار مجموعة من الاتفاقيات، باعتبارها المصادر الأولى لكل التشريعات. لتليها التشريعات الأخرى الوطنية والداخلية، لتعزيز التعاون الدولي ومجابهة الجرائم المعلوماتية. وسنتطرق في هذا المطلب إلى نوعين من الجهود الدولية. أولها الاتفاقيات الدولية (الفرع الأول)، ثم بعد ذلك مظاهر التعاون الدولي (الفرع الثاني) ودورها في مكافحة الجرائم الإلكترونية.

الفرع الأول: الاتفاقيات والمؤتمرات الدولية لمكافحة جرائم الأعمال الرقمية.

تم انشاء مجموعة متعددة من الاتفاقيات حول مكافحة الجريمة الاكلترونية بصفة عامة، وتختلف حسب طبيعتها، فمنها كانت على شكل قوانين، أو قرارات لجمعية معينة..، لذا سنعرض أهم و أبرز الجهود المبذولة في هذا السياق.

أولا: جهود منظمة الأمم المتحدة:

قامت منظمة الأمم المتحدة ببذل جهود كبيرة من أجل التصدي لجرائم الانترنت، لما ينتج عنها من أضرار بالغة، ولمنع هذه الجرائم خاصة جرائم الإلكترونية فلابد من استجابة الدول

واتحادها وهذا ما تسعى إليه هذه المنظمة والتي تهدف إلى حفظ السلام والأمن الدوليين، وتحقيق التعاون الأمني لمواجهة الجرائم ذات البعد الدولي عن طريق إبرام العديد من الاتفاقيات الدولية الخاصة بموضوع الجرائم الإلكترونية[1].

1_دور الأمم المتحدة في مكافحة الجريمة الالكترونية: رسمت الأمم المتحدة سياسة ناجحة في ما يخص تحقيق العدالة الجنائية، عن طريق إقرار مجموعة من التوصيات وعقد مؤتمرات دورية كل خمس سنوات، وهذا لدعم وتعزيز التعاون الدولي في مجال مكافحة الجرائم[2].

_مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا 1990:

يعتبر القرار الصادر من هذا المؤتمر من أبرز الجهود التي بذلتها الأمم المتحدة، حيث انعقد في هافانا سنة 1990، حيث أوصى في قراره المتعلق بالجرائم ذات الصلة بالحاسوب الدول الأعضاء على مضاعفة جهودها لمواجهة ومكافحة إساءة استعمال هذا الجهاز، إضافة إلى تجريم هذه الأفعال جنائيا[3]. لأنه يدرك مدى ازدياد استعمال الحاسوب كإحدى طرائق الجريمة الاقتصادية، وصعوبة الكشف عنها[4].

بحيث ألزم الدول على اتخاذ بعض التدابير التالية متى اقتضى الأمر ذلك:

_تحديث القوانين والإجراءات الجنائية، مع ضمان تطبيق الجزاءات والقوانين على نحو ملائم، وكذا النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة[5].

---

[1] محمود محمد صفاء الدين على شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، كلية الحقوق، جامعة المنوفية، ص528. بحث على الموقع الإلكتروني: https://jslem.journals.ekb.eg

[2]-المرجع نفسه، ص528.

[3]-ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الإتجاهات الدولية في مكافحة الجريمة الإلكترونية،مجلة دراسات و أبحاث، المجلد الأول ، العدد الأول، المركز الجامعي سوق أهراس، الجزائر، ص244.

[4]- مؤتمر الأمم المتحدة الثامن ،الجرائم ذات الصلة بالحاسوب، المنعقد في هافانا،كوبا الفترة 27 آب/أغسطس-7أيلول/سبتمبر 1900 وثيقة رقم A/CONF-144/28.

[5]-مؤتمر هافنا 1990، السالف الذكر مادة 2/أ/2، ص212.

_التكفل بمصادرة أو رد الأصول المكتسبة بطرق غير مشروعة. مع تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب[1].

_حث الدول الأعضاء على مضاعفة الأنشطة على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسوب، عن طريق الدخول كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الجنائية. كما ألزم لجنة منع المجرمين على مجموعة من الأعمال، منها تعزيز الجهود الدولية في مجال تطوير المعايير التي تساعد الدول الأعضاء في معالجة الجرائم المرتبطة بالحاسوب[2]...

_و من المؤتمرات أيضا التي عقدتها منظمة الأمم المتحدة، المؤتمر الثاني عشر لمنع المجرمين والعدالة الجنائية في 12-19 أفريل 2010 بالبرازيل، بحيث تم فيها مناقشة مختلف التطورات المتعلقة باستعمال الانترنت من جانب المجرمين والسلطات المختصة في مكافحة الجريمة. حيث احتلت الجرائم الإلكترونية محلا بارزا في جدول أعمال المؤتمر لمدى خطورتها[3].

2_دور الجمعية العامة للأمم المتحدة في مكافحة الجريمة الإلكترونية:

أقرت الجمعية العامة مجموعة قرارات لمواجهة جرائم الانترنت، بحيث دعت إلى مكافحة إساءة استعمال تكنولوجيا المعلومات، وكان هذا من خلال القرار رقم 56-121[4].

إن الاعتماد على تكنولوجيا المعلومات، قد حقق زيادة كبرى في التعاون والتنسيق على المستوى العالمي، والذي أدى إلى حدوث أثر خطير على جميع الدول نتيجة إساءة استعمال تكنولوجيا المعلومات. بحيث أن الثغرات في مجال حصول الدول على تكنولوجيا المعلومات واستخدامها قد يضعف فعالية التعاون الدولي على مكافحة هذه الظاهرة، وبالتالي ضرورة تيسير

[1]-مؤتمر هافانا 1990، السالف الذكر، مادة 2/أ/3، ص212.

[2]-مؤتمر هافانا 1990، السالف الذكر،مادة 3 و5، 213.

[3]-محمود محمد صفاء الدين على شرشر، المرجع السابق، ص535.

[4]-قرار رقم 56-121، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الجمعية العامة،الدورة السادسة والخمسون،البند 110 من جدول الأعمال،الأمم المتحدة، 2002، ص1.

تمديد نطاق تكنولوجيا المعلومات خاصة في الدول النامية ، إذ أنها تشدد إلى تعزيز التنسيق والتعاون بين الدول في مكافحة استعمال تكنولوجيا المعلومات. كما تدعو الجمعية العامة الدول الأعضاء لوضع قوانين وسياسات وممارسات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وأن تأخذ بعين الاعتبار أعمال وانجازات لجنة منع الجريمة والعدالة الجنائية، والمنظمات الدولية والإقليمية الأخرى[1].

ثانيا: مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات-البرازيل 1994:

انعقد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات سنة 1994 بالبرازيل، والذي جرم بعض الأفعال واعتبرها من الجرائم المعلوماتية كالاحتيال والغش المتعلق بالكمبيوتر عن طريق إتلاف المعطيات، التزوير المعلوماتي وكذا الدخول غير المصرح به. أما من الجانب الإجرائي فقد تناول مجموعة من القواعد الإجرائية فيما يخص بيئة الجرائم المعلوماتية من خلال القيام بإجراء التفتيش والضبط في مجال تكنولوجيا المعلومات، وكذا تفتيش شبكات الحاسب الآلي. كما أوصى أيضا على التعاون بين الضحايا والشهود وكذا مستخدمي المعلومات لإتاحة استخدامها قضائيا كما أجاز اعتراض الاتصالات داخل نظام الحاسب الآلي وممارسة الرقابة عليه[2].

ثالثا: قانون الاونيسترال النموذجي:

1_قانون الاونستيرال النموذجي المتعلق بالتجارة الالكترونية لسنة 1996: يعتبر هذا القانون من أبرز الجهود الدولية في مجال مكافحة الجرائم المعلوماتية على الصعيد الدولي. وقد شكل خطوة أساسية ضمن المساعي التي قامت بها لجنة الأمم المتحدة للقانون التجاري الدولي

[1]- قرار 56-121، الجمعية العامة، السالف الذكر، ص1-2.

[2]-ليندة شرابشة، المرجع السابق، 245-246.

"الاونستيرال" لوضع نصوص نموذجية تهدف إلى تزويد المشرعين الوطنيين بقواعد مقبولة دوليا، من شأنها تذليل العقبات القانونية وتعزيز القدرة على التنبؤ بالتطورات القانونية في مجال التجارة الالكترونية، وذلك لمواجهة الجرائم المعلوماتية في هذا المجال. وقد حظي هذا القانون بقبول واسع من قبل المشرعين الوطنيين والمتعاملين، لاسيما بعد اعتماده من قبل لجنة الأمم المتحدة لسنة 1996[1].

2_ قانون الاونيسترال المتعلق بالتوقيع الالكتروني لسنة 2001: يمثل هذا القانون امتدادا لجهود لجنة الاونيسترال في مجال مكافحة الجرائم المعلوماتية المرتبطة بالتجارة الدولية، من خلال إرساء قواعد موحدة تهدف إلى حماية التوقيع الالكتروني، وهي قواعد تبنتها العديد من الدول ضمن تشريعاتها الوطنية[2].

رابعا: جهود الإتحاد الدولي للإتصالات: يضم الاتحاد الدولي للاتصالات 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية إذ يعتبر وكالة متخصصة داخل الأمم المتحدة والذي وفر بدوره منبر استراتيجي للتعاون بين أعضائه. حيث يسعى لوضع استراتيجيات لتطوير نموذج التشريعات السيبرانية قابل للتطبيق وطنيا وعالميا، بالإضافة إلى استراتيجيات أخرى لتهيئة الأرضية الوطنية والإقليمية الملائمة لوضع الهياكل التنظيمية والسياسات المتعلقة بالجرائم الإلكترونية وهذا من أجل تكثيف وتعزيز الأمن الإلكتروني العالمي[3].

[1]-د.يعيش تمام شوقي، الجريمة لمعلوماتية، دراسة تأصيلية مقارنة، مطبعة الرمال، الوادي، الجزائر، جانفي 2019،الطبعة الأولى، ص 45.

[2]-المرجع نفسه، ص45-46.

[3]-د.فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، الصادرة عن كلية الحقوق، جامعة حمة لخضر، الوادي، العدد الثاني، 2015،ص12.

خامسا: اتفاقية تريبس:

تم التوقيع عليها من قبل الدول الأعضاء عام 1994، بحيث تم دراسة حقوق الملكية الفكرية من قبل موقعي الاتفاقية العامة للتعريفات والتجارة عن طريق توقيع اتفاق الجهات المتصلة بالتجارة من حقوق الملكية الفكرية. وقد تضمنت اتفاقية تحرير التجارة العالمية مختلف جوانب النشاط التجاري على الصعيد الدولي، وبالنظر للقيمة التي تكتسيها الملكية الفكرية من حيث حمايتها في ظل نظام تجاري عالمي جديد، فقد جاءت اتفاقية تريبس كوسيلة مهمة لتحرير التجارة العالمية والتي شكلت نقاشا طويلا أثناء المفاوضات التي استمر لمدة من الزمن بين الدول النامية والدول الصناعية المتقدمة[1].

قامت اتفاقية تريبس الخاصة بأوجه التجارة المرتبطة بحقوق الملكية الفكرية من خلال موادها، على مكافحة الجريمة المعلوماتية وذلك بالنص في المادة 10 الفقرة1 على أن برامج الحاسب الآلي تتمتع بالحماية سواء كانت بلغة المصدر أو بلغة الآلة، كما نصت في الفقرة 2 من نفس المادة على حماية البيانات المجمعة[2].

الفرع الثاني: أشكال التعاون الدولي لمكافحة جرائم الأعمال الرقمية.

يعد التعاون القضائي من الآليات الإجرائية الدولية لمجابهة الجرائم المعلوماتية، ويتمثل في التعاون القضائي، الذي ينقسم إلى شقين، التعاون الأمني والمساعدات القضائية، ثم دراسة النوع الثاني المتمثل في إجراء تسليم الجرمين.

أولا: التعاون القضائي:

تتطلب إجراءات التحقيق والملاحقة القضائية في جرائم الانترنت تتبع النشاط الإجرامي منذ بدايته إلى غاية تنفيذه، مع تحديد الأضرار التي لحقت بها، ومواقع حدوثها، ونظرا لأن هذه

[1]-بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، تخصص قانون عام، كلية الحقوق، جامعة الجزائر01 يوسف بن خدة، الجزائر، 2017-2018. ص21-22.

[2]-بدري فيصل، المرجع السابق، ص22.

العناصر تمتد لبلدان مختلفة فإن ملاحقة مرتكبي هذه الجريمة يقتضي وجود تعاون فعال بين السلطات القضائية لهذه البلدان لتوسيع نطاق الولاية القضائية، وعليه سنتناول أبرز صورتين للتعاون القضائي، هما: التعاون الأمني كصورة أولى ثم المساعدة القضائية كصورة ثانية[1].

1_ **التعاون الأمني:** من البديهي أن تشكل الحدود الجغرافية مشكلة الاختصاص الإقليمي عائقا أمام تنفيذ الإجراءات الجنائية لملاحقة الجرائم، خاصة فيما يتعلق بجريمة الانترنت التي تعتبر جريمة عابرة للحدود. فقد يرتكب الجاني هجومه في دولة لكنه يمتلك جنسية دولة أخرى، بينما تقع آثار الجريمة في دولة ثالثة. ولهذا تبرز الحاجة الماسة إلى توحيد الجهود وتبادل المعطيات والمعلومات المتعلقة بالجريمة، والتي تسمح بكشف هوية المجرمين باعتبار أن الدولة لا يمكنها مواجهة هذه الجريمة بمفردها، فأجهزة الشرطة لا يمكنها تعقب مرتكبي الجرائم وملاحقتهم إلا ضمن حدودها، مما يجعل الجناة في مأمن من المتابعة بمجرد مغادرتهم حدود الدولة.[2]

أ_إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الانترنت ونشرها: تهدف هذه المكاتب إلى تعزيز التعاون وتكثيفه بين سلطات الدول القضائية في مجال مكافحة الجريمة وضبط المجرمين وملاحقتهم وهذا من خلال متابعة المعلومات الخاصة بهم، إضافة على ذلك تقديم الدعم وتبادل الخبرات عندما يقتضي الأمر ذلك[3].

ب_التعاون في إطار المنظمة الدولية للشرطة الجنائية "الأنتربول":

تسعى هذه المنظمة إلى تعزيز التعاون الفعال بين أجهزة الشرطة في الدول الأعضاء من أجل التصدي للجرائم، من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأطراف والتي تقوم بجمع البيانات والمعلومات الخاصة بكل من المجرم والجريمة،

[1]-قزران مصطفى، زرقين عبد القادر،الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، الصادرة عن مخبر نظام الحالة المدنية جامعة خميس مليانة، المجلد الثامن، العدد الثاني، جوان 2022، ص1225.

[2]المرجع نفسه، ص1225-1226.

[3]-المرجع نفسه، ص1226.

وتتبادلها فيما بينها. أما في ما يخص مجال الجرائم الالكترونية، فقد قامت منظمة الأنتربول في عام 2004 بإنشاء وحدة خاصة لمكافحة جرائم التكنولوجيا، والتي تعاونت مع مجموعة الدول الثمانية الكبرى (G8) من أجل وضع استراتيجيات للتصدي لهذا النوع من الجرائم، عن طريق إنشاء مركز اتصالات أمني عبر الشركة. ولقد حققت المنظمة الدولية للشرطة الجنائية مجموعة من الإنجازات المختلفة في ظل مكافحة الجرائم الإلكترونية، ولا تزال مواصلة لجهودها في هذا المجال[1].

وفي جانب آخر، أنشأ المجلس الأوروبي سنة 1991 في لكسمبورغ، شرطة أوروبية بمثابة رابط يصل بين أجهزة الشرطة الوطنية في الدول الأعضاء، لضبط مرتكبي الجريمة ومنها الجريمة الالكترونية. وبالنظر إلى الجانب العربي فقد قام مجلس وزراء الداخلية والعدل العرب سنة 2010 بإنشاء المكتب العربي للشرطة الجنائية، بهدف تعزيز وتنمية التعاون لتقديم الدعم بين الدول الأعضاء فيما يخص الجريمة والجاني[2].

ج_**شرطة الويب الدولية**: تم إنشاء هذه المنظمة الأمنية عام 1986 في الولايات المتحدة الأمريكية، بحيث تضم متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة من العالم، والتي تقوم بتلقي شكاوى مستخدمي الانترنت وملاحقة القراصنة والجناة الكترونيا وإيجاد الأدلة ضدهم وتمثيلهم أمام المحكمة. ونظرا لاتساع نطاق نشاط هذه المنظمة، فإنه يقوم بدوره بتسهيل عمل الفريق من حيث تتبع الأنشطة الإجرامية التي تتم على مستوى العالم من خلال الانترنت. لكن من الضروري احترام حقوق

[1]- فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، الصادرة عن كلية الحقوق و العلوم السياسية، تيارت، المجلد الثامن، العدد الأول،2022، ص438.

[2]-المرجع نفسه، ص439.

الإنسان من حيث سرية المعلومات وتبادلها وعدم المساس بالحريات العامة، وهذا من خلال وضع ضوابط وقواعد للحد من هذه الظاهرة وتفاديا للإساءة وتجاوز حدود المبادئ العامة[1].

د_القيام بعمليات أمنية مشتركة: وهذا من خلال مراقبة وتعقب الجريمة المعلوماتية والقيام بالتفتيش العابر للحدود للأنظمة المعلوماتية وشبكات الاتصال لأجل ضبط الأدلة الرقمية. وكل هذا يتطلب تعاون دولي فعال خاصة العمليات الأمنية[2].

2_المساعدات القضائية الدولية:

إن المساعدة القضائية الدولية هي كل إجراء قضائي تقوم به السلطات المختصة بناء على الدولة الطالبة، في الدولة المطلوب منها، بهدف تسهيل إجراءات المحاكمة[3]. وقد قام المشرع الجزائري بالاعتماد بعد المصادقة على اتفاقية العربية لمكافحة جرائم المعلوماتية على هذا النوع من التعاون القضائي، وهذا من خلال النص عليها في القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[4]. وكان ذلك في الفصل السادس منه والمعنون ب"التعاون والمساعدة القضائية الدولية" في المادة 16 الفقرة 1 منه كالتالي:".....،يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني"[5]. وفي الفقرة الثانية تناول طلبات المساعدة في حالة

[1]-فريد ناشف، المرجع السابق، ص439.

[2]-قزران مصطفى، زرقين عبد القادر، المرجع السابق، ص1226.

[3]- عصماني ليلى، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الالكتروني، مجلة القانون – المجتمع والسلطة، الصادرة عن مخبر البحث القانون، جامعة وهران2، المجلد التاسع ، العدد الثاني، 2020، ص16.

[4]-قانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق ل5 غشت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 14 شعبان 1430، 16 غشت 2009، ص5.

[5]- المادة 16، فقرة 1، قانون رقم 09-04، السالف الذكر، ص8.

الاستعجال إذا تم ذلك عبر وسائل الاتصال السريعة بحيث يمكن في حالة الاستعجال، مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية ..."[1].

أشكال المساعدة القضائية:

أ_**تبادل المعلومات**: تتمثل في تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بخصوص جريمة ما. و بخصوص الجرائم الإلكترونية، نصت صراحة الإتفاقية الأوروبية في المادة 23 منه على إلزامية توافر التعاون الدولي بين الدول الأعضاء لتسهيل تبادل المعلومات بينها فيما يخص الجريمة. كما أوصى أيضا مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين 1990، في قراره المتعلق بالجرائم ذات الصلة بالحاسوب، الدول الأطراف بتكثيف جهودها وأنشطتها المبذولة على الصعيد الدولي لمكافحة الجرائم الإلكترونية. كما حثهم أيضا على دخولهم كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في ظل الجرائم المعلوماتية[2].

أما بالنسبة للتشريع الجزائري، فقد نص المشرع الجزائري عليها في المادة 17 من القانون 09-04 على هذا النوع من الإجراء كالتالي:"تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات....".

ب_**نقل الإجراءات**: يقصد به أن تقوم الدولة التي ارتكبت في إقليمها الجريمة الإلكترونية بنقل إجراءات التحقيق والبحث الخاصين بهاته الجريمة إلى دولة أخرى قد امتدت آثار الجريمة إليها أيضا، وهذا بناء على شروط اتفاقية دولية، ومن بين التطبيقات العملية لتبادل المساعدة القضائية ما قامت به الجمعية العامة للأمم المتحدة حول إنشاء المعادة النموذجية حول نقل الإجراءات في المسائل والقضايا الجنائية[3].

---

[1]-المادة 16 الفقرة 2، القانون رقم09-04، سالف الذكر، ص8.

[2]-الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية و الاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، الصادرة عن مخبر النظام القانوني للعقود و التصرفات في القانون الخاص، جامعة خميس مليانة، المجلد الرابع، العدد الرابع، ديسمبر 2022، ص18.

[3]-وريدة جندلي، التعاون الدولي لمكافحة الجريمة المعلوماتية، الفاعلية والتحديات، مجلة القانون والعلوم السياسية، الصادرة عن معهد الحقوق بالمركز الجامعي النعامة، المجلد العاشر، العدد الثاني، 2024، ص327.

ج_**الإنابة القضائية**: بحيث تقوم دولة ما بطلب دولة أخرى من أجل مباشرة إجراء قضائي حول دعوى تحت النظر داخل حدودها الإقليمية نيابة عنها، تحت شروط قد قررتها الاتفاقية الدولية بينهما. بحيث تهدف الإنابة القضائية لإزالة العوائق التي تعرقل سير الإجراءات الجنائية بسبب التطور الذي تشهده الظواهر الإجرامية. وقد تم إبرام مجموعة من الاتفاقيات الجديدة من شأنها تسهيل الإجراءات من خلال الاتصال المباشر بين السلطات المختصة بالتحقيق. وهذا تزامنا مع سرعة الجريمة الإلكترونية، ومن بين هذه الاتفاقيات الاتفاقية الأمريكية الكندية، التي تنص على التبادل الشفوي للمعلومات في الحالات الاستعجالية[1].

ثانيا: تسليم المجرمين كآلية للتعاون القضائي:

وهو أن تقوم دولة ما بمطالبة دولة أخرى بتسليمها الشخص (الجاني) المتواجد بإقليمها (إقليم الدولة المطلوب منها التسليم) إما من أجل محاكمته لارتكابه الجريمة محل التسليم، أو بهدف حكم الإدانة الصادر ضده، وقد يكون من الدولة طالبة التسليم أو المحكمة الدولية. وقد نصت اتفاقية بودابست على هذا الإجراء ضمن المواد من 2 إلى11 [2]. وكذا في قانون الإجراءات الجزائي الجزائري، في الكتاب السابع الباب الأول منه، والمادة 694 كالتالي:" تحدد الأحكام الواردة في هذا الكتاب شروط تسليم المجرين وإجراءاته وآثاره وذلك ما لم تنص المعاهدات والاتفاقيات السياسية على خلاف ذلك"[3].

1_ شروط التسليم:

[1]-طاهر ياكر، المرجع السابق، ص19.

[2]-وريدة جندلي، المرجع نفسه، ص329.

[3]- القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل و يتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386 الموافق ل8 يونيو 1966، المتضمن لقانون الإجراءات الجزائية، ج.ر ج ج، عدد84، الصادرة في 4 ذو الحجة عام 1427 الموافق لـ 24 ديسمبر سنة 2006، سنة.،ص4.

تنقسم شروط التسليم إلى ثلاث عناصر، المتعلقة بالجريمة، الشخص المطلوب تسليمه، مايسمى بمبدأ التخصيص في التسليم.

أ_الشروط المتعلقة بالجريمة:

_ الجرائم القابلة للتسليم:

لا يمكن التسليم في الجرائم السياسية والعسكرية، بحيث لا يسري هذا المبدأ بشكل مطلق على الدول المتحالفة عسكريا. كما أن هناك مجموعة من الأسس التي تتبعها الدول من أجل تحديد هذه الجرائم، منها الأسلوب الحصري الذي يتم من خلاله إنشاء قائمة تضم جملة من الجرائم على سبيل الحصر، تلحق هذه القائمة بالمعاهدة. ويتمثل الأساس الثاني في معيار الجسامة، أن تنص الاتفاقية والتشريع الداخلي الخاص بها على الحد الأدنى للعقوبة المقررة للجريمة المعنية بالتسليم. أما الأساس الأخير فهو اللجوء إلى النظام المختلط، والذي يجمع ويشمل الأسلوبين السابقين، ويحدد الحد الأدنى للعقوبة للجرائم موضوع التسليم[1].

_**التجريم المزدوج**: وهو أن يكون سبب طلب التسليم مجرما في تشريع كلا الدولتين (طالبة التسليم والمطلوب منها)، فليس من المنطق أن يكون الفعل غير مجرم في إحدى الدولتين ويتم تقديم طلب تسليم الشخص مرتكب هذا الفعل. وهذا ما نص عليه المشرع الجزائري في المادة 697 فقرة 2 من قانون الإجراءات الجزائية كما يلي:" .... لايجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة". أما بالنسبة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة فقد نصت عليه في المادة 16 منها كالتالي:" شريطة أن

[1]- عبد الحميد عمارة، نظام تسليم المجرمين في ظل التعاون القضائي الدولي، مجلة الباحث للدراسات الأكاديمية، الصادرة عن كلية الحقوق و العلوم السياسية جامعة باتنة، العدد الحادي عشر، جوان 2017، ص736.

يكون الجرم الذي يلتمس بشأنه التسليم معاقبا عليه بمقتضى القانون الداخلي لكل من الدولة الطالبة والدولة متلقية الطلب"[1].

ب_الشروط المتعلقة بالشخص المطالب بالتسليم:

غالبا ما لا يشكل التسليم مشكلة في ما يخص الشخص المطلوب إذا كان لا يحمل جنسية الدولة المطلوب منها التسليم، وبالتالي يسهل هذا الأمر سير الإجراءات المتعلقة بعملية التسليم. عكس ما إذا كان هذا الشخص تابعا للدولة المطلوب منها هذا الإجراء. لأن المبدأ العام أن الدولة لا تسلم رعاياها، وهذا المبدأ تأخذ به معظم الدول من بينها الجزائر، عكس الدول الأنجلوكسية التي تتبع مبدأ تسليم رعاياها كالولايات المتحدة الأمريكية وبريطانيا[2].

إضافة إلى هذا، فإنه يمنع تسليم الأشخاص الذين يملكون حق اللجوء السياسي، لأنه من اللازم حمايتهم من التعرض للمضايقات في حالة عودتهم إلى بلدهم الأصلي. كما يجب توفير الحماية القانونية للشخص المطلوب تسليمه بصفة عامة، وكذا حماية وإعفاء الذين يمتلكون مشاكل في الصحة أو السن، والذي قد يؤثر بشكل سلبي على المعني بالأمر[3].

_مبدأ التخصيص في التسليم:

[1]-وريدة جندلي، المرجع السابق، ص329.

[2]- رياض بركات، د.مسيكة محمد الصغير، تسليم المجرمين كآلية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، الصادرة عن جامعة الدكتور مولاي الطاهر، سعيدة، المجلد الحادي عشر، العدد الأول، جوان 2024، ص138.

[3]-المرجع نفسه، ص139.

يعتبر هذا المبدأ بمثابة عرف دولي، تلتزم الدول الأطراف بتطبيقه، بحيث يقصد به عدم محاكمة الشخص المطالب بالتسليم عن جريمة سابقة، بل يتم محاكمته في إطار الجريمة موضوع التسليم فقط. وهو مبدأ أساسي في مجال تسليم المجرمين[1].

2_ إجراءات التسليم:

تتم إجراءات التسليم بثلاث مراحل، وكأول خطوة تقوم بها الدولة طالبة التسليم، هو تقديم طلب التسليم مرفقا بجميع الوثائق والبيانات اللازمة، ومنها الأدلة الخاصة بالجريمة التي تثبت فعل الجاني بالجريمة، كتبرير لتسليمه من أجل معاقبته. كما تجيز بعض الدول للشخص المطلوب تسليمه تقديم أدلة براءته أمام الدولة المطالب منها التسليم، لمقارنتها مع الأدلة الموجهة ضده من طرف الدولة طالبة التسليم. من أجل تقرير إمكانية تسليمه أم لا. و يخضع التسليم لشروط التشريع الداخلي للدولة المطلوب منها التسليم إضافة إلى معاهدة التسليم التي تسري بينهما. إذ يمكن للدولة الطالبة للتسليم أن ترفق طلبها بطلب آخر فيما يخص احتجاز الشخص المطلوب تسليمه المتواجد في إقليمها، من أجل ضمان حضوره لإجراءات التسليم. بعدها يبقى الأمر ضمن قرار الدولة المطلوب منها التسليم، إما بالرفض لأسباب مختلفة، منها محاكمة ومعاقبة الشخص على جريمة أخرى غير التي هي محل التسليم، أو بالقبول شرط أن تضمن الدولة طالبة التسليم حقوقه والإنصاف وفي معاملته طيلة فترة الإجراءات[2].

المطلب الثاني: الجهود الإقليمية لمكافحة جر ائم الأعمال الرقمية.

إضافة إلى الآليات الدولية لمجابهة الجرائم الإلكترونية، تم إرساء آليات أخرى على المستوى الإقليمي، وهذا دعما للجهود الدولية من جهة، ومن جهة أ×رى ترغب كل دولة تطبيق آليات تتناسب مع تشريعاتها. ومثال ذلك سندرس الجهود المختلفة على المستوى الأوروبي (الفرع

[1]- عبد الحميد عمارة، المرجع السابق، ص736-737.

[2]- المرجع نفسه، ص737-738.

الأول)، و كذا الإتحاد الإفريقي (الفرع الثاني)، إضافة إلى الجهود على المستوى العربي (الفرع الثالث).

الفرع الأول : على المستوى الأوروبي :

إن أبرز الإتفاقيات التي تساهم في مكافحة هذا النوع من الجرائم، نجد الإتفاقية اتفاقية بودابست لسنة 2001، إضافة إلى ذلك شرطة اليوربول التي تعتبر همزة وصل بين الدول الأعضاء لتبادل المعلومات فيما يخص الجرائم الإلكترونية بأنواعها.

أولا: الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية "اتفاقية بودابست 2001".

تعد اتفاقية بودابست لعام 2001 محطة رائدة في مجال التعاون الدولي ضد الجريمة المعلوماتية، باعتبار أنها الاتفاقية الإقليمية الوحيدة من حيث نطاقها وعدد الدول المنظمة إليها. تم الاعتماد عليها وإدخالها حيز التنفيذ سنة 2004. بحيث تسعى لتوحيد القوانين الوطنية، وتهدف لتطوير تقنيات التحقيق وتكثيف التعاون الدولي[1].

قامت اتفاقية بودابست بتحديد الإطار القانوني العام للجرائم الإلكترونية، مثل الدخول غير المشروع أو الاعتداء على سلامة البيانات أو التزوير المعلوماتي وغيرها من الجرائم المعلوماتية. كما أنها اشترطت لاعتبار هذه الأفعال جرائم كأن ترتكب هذه الجرائم على وجه حق أو بطرق عمدية وهذا لتحديد وإقرار المسؤولية الجنائية. وألزمت من جهة أخرى الدول الأعضاء عند سن القوانين الوطنية والداخلية أن تأخذ بعين الاعتبار الاتفاقية الدولية لحقوق الإنسان كالاتفاقية الأوروبية لحماية حقوق الإنسان والحريات العامة لعام 1950، والمعهد الدولي

[1].كوثر مازوني، الجريمة المعلوماتية، أعمال الندوة الوطنية، مجلة الندوة الوطنية، جامعة الجزائر 01، دار الخلدونية للنشر، الجزائر، الطبعة الأولى، 2019، ص177.

للحقوق المدنية والسياسية لعام 1966. بحيث يجب على الدول الأطراف الاعتماد على مبادئ الاتفاقية منها مبدأ الإقليمية، ومبدأ الاختصاص، النسبية ومبدأ الجنسية[1].

ثانيا: اليوربول كآلية للحد من الجر ائم الإلكترونية.

أنشأت اليوربول مايدعى ب"المركز الأوروبي" لمكافحة الجريمة الإلكترونية (EC3)، ولقد أشرف هذا المركز على تقديم الدعم التشغيلي والإستراتيجي والتحليلي والجنائي لإجراءات التحقيق التي تقوم بها الدول الأعضاء في مجال الحد الجرائم الإلكترونية، كما يركز أيضا على صور معينة من الجرائم الإلكترونية منها الاحتيال عن طريق الدفع،أو تلك التي تنتج من التكنولوجيا...[2]

الفرع الثاني: جهود الإتحاد الإفريقي

قام المؤتمر الاستثنائي لوزارة الإتحاد الإفريقي المسؤول عن تكنولوجيا المعلومات والاتصالات، بطلب من مفوضية الإتحاد الإفريقي للإشراف مع لجنة الأمم المتحدة الاقتصادية لإفريقيا، لإنشاء اتفاقية خاصة بالتشريع القضائي، من أجل الالتزام بالمتطلبات القانونية والتنظيمية للمعاملات والأمن الإلكترونيين. كما حث على إلزامية توفير الحماية القانونية للأنظمة المعلوماتية، وكذا البيانات الشخصية. إضافة إلى ذلك وجوب سن قوانين لمكافحة الجريمة الإلكترونية. وفي يونيو 2004، تم الموافقة على اتفاقية الإتحاد الإفريقي حول مجال الأمن السيبراني وحماية البيانات الشخصية[3].

[1]-الطاهر ياكر، المرجع السابق، ص23.

[2]-محمد نذير بن عرفة، يوسف حوري، اليوروبول كآلية لمكافحة الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، الصادرة عن جامعة عمار الثليجي الأغواط، الجزائر، المجلد الحادي عشر، العدد الأول، جانفي 2025، ص45.

[3]-د.فاروق خلف، المرجع السابق، ص14.

الفرع الثالث: على مستوى الدول العربية.

أولا: القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية لسنة 2004:

بعد انتشار الجريمة المعلوماتية وفرض سيطرتها على الصعيد العالمي، وجدت الدول العربية نفسها مجبرة على إبرام اتفاقية إقليمية كدرع لتصدي ومكافحة كل أشكال الجرائم المعلوماتية، لذا تم إصدار "القانون العربي الاسترشادي لمكافحة الجريمة الإلكترونية"، بمشاركة بين وزراء الداخلية العرب ومجلس الوزراء العرب في مجال الأمانة العامة لجامعة الدول العربية. و هذا بعد تقديم كلا المجلسين مشروع فيما يخص مكافحة الجريمة المعلوماتية. تم الاعتماد على هذا القانون من طرف مجلس وزراء العدل العرب في ذروته التاسعة عشر بموجب القرار رقم 495 المؤرخ في 2003/10/08، ومن طرف مجلس وزراء الداخلية العرب في دورته الحادية والعشرين[1].

ولقد اعتمدت جامعة الدول العربية ما يسمى بقانون الإمارات العربي الاسترشادي لمكافحة جرائم المعلومات التقنية وهذا نسبة لدولة الإمارات العربية المتحدة التي قدمت هذا المقترح. بحيث يمنع هذا القانون نسخ برامج الكمبيوتر بدون إذن، ويتم معاقبة من يخالف هذا الأمر ويقوم بقرصنة البرامج بغرامة مالية إضافة إلى مصادرة المنتجات والحبس لمدة تمتد إلى ثلاث سنوات[2].

ثانيا:الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

انعقدت هذه الاتفاقية بتاريخ 2010/12/21 بالقاهرة، من طرف مجموعة الدول العربية، التي تهدف إلى تعزيز التعاون فيما بينها لمكافحة الجرائم المعلوماتية والحفاظ على سلامة

[1]-بن دراج علي إبراهيم، محاضرات في الجرائم المعلوماتية، الملقاة على طلبة السنة الثانية ماستر، تخصص قانون الجنائي والعلوم الجنائية، قسم الحقوق، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، 2020-2021، ص39-40.

[2]-بدري فيصل، المرجع السابق، ص34.

مجتمعاتها. وهذا أخذا بالمبادئ الدينية والأخلاقية السامية، والتزاما بالمعاهدات والمواثيق العربية والدولية[1].

بحيث تنطبق هذه الاتفاقية على جرائم تقنية المعلومات بهدف مكافحتها وملاحقة مرتكبيها، وذلك في حالة ما إذا ارتكبت في أكثر من دولة، أو تم الإعداد لها أو الإشراف عليها في دولة أو دول أخرى، أو ارتكبت من طرف منظمة تمارس أنشطتها في أكثر من دولة، أو أيضا إذا ارتكبت في دولة وامتدت آثارها إلى دولة أخرى[2].

ألزمت هذه الاتفاقية الدول الأعضاء على احترام حدود إقليم كل دولة، والالتزام بصون السيادة ومبادئ هذه الاتفاقية وعدم الخروج عن موادها[3].

وقد تناولت هذه الاتفاقية بعض الجرائم في فصلها الثاني، نذكر منها: جريمة الدخول غير المشروع، جريمة الاعتراض غير المشروع، جريمة التزوير والاحتيال...

كما نصت أيضا على عنصر الشروع في ارتكاب الجريمة والمسؤولية الجنائية للأشخاص الطبيعيين والمعنويين، مبينة في فصلها الثالث الأحكام الإجرائية. أما في فصلها الرابع، فقد تناولت آليات التعاون القانوني والقضائي.

المطلب الثالث: الآليات الوطنية لمكافحة جرائم الأعمال الرقمية.

إن التطور المستمر للجانب الرقمي، ساهم في زيادة تعدد الجرائم الإلكترونية. لا من حيث نوعها، ايجابية كانت أو سلبية. أو موقعها القانوني، ولا حتى من جانب معيار قوتها الإجرامية، من حيث الحد الأدنى والحد الأقصى. وهذا ماجعل من المشرع الجزائري الوقوف من أجل مواجهة مثل هذه الجرائم والتصدي لها. وسنتطرق لمختلف التشريعات العامة، بداية من

[1]-الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المنعقدة في 15-1-1432 الموافق ل21-12-2010، القاهرة، جمهورية مصر العربية.

[2]-المادة الثالثة، الفصل الأول، نفس الإتفاقية.

[3]-المادة الرابعة، الفصل الأول، نفس الإتفاقية.

منطلق الهرم القانوني وهو الدستور الجزائري، والقواعد الإجرائية و الجزائية (الفرع الأول)، مرورا إلى التشريعات والهيئات الخاصة (الفرع الثاني).

الفرع الأول : التشريعات العامة لمكافحة جرائم الأعمال الإلكترونية.

تنقسم القواعد العامة لمكافحةالجرائم بمختلفها، إلى قسمين، قسم خاص بالأحكام الإجرائية، وآخر خاص بالأحكام الجزائية.

أولا: الآليات القانونية الإجرائية

1_الدستور الجزائري[1]: يعتبر الدستور الإطار القانوني الذي تستند إليه مختلف التشريعات الوطنية. و بالغوص فيه نجد أنه قد عالج جرائم الأعمال بطريقة غير مباشرة، بحيث تضمن دستور 2020 كأول مبدأ حول حماية الحقوق الأساسية والحريات العام للأفراد، وهذا من خلال المادة 35:"تضمن الدولة الحقوق الأساسية و الحريات. وبالإسقاط من المادة 37 التي تنص على "...المواطنين سواسية أمام القانون.."، فنرى أن جرائم الأعمال تعاقب عليها دون النظر إلى المركز الاجتماعي أو الاقتصادي للجاني. لنجد أيضا أنه نص على حماية المستهلكين وضمن لهم الأمن والسلامة وكذا حقوقهم الاقتصادية وهذا في المادة 62 منه. وبالنظر أيضا في المادة 79 الفقرة 2:"....يعاقب على الخيانة والتجسس..."، وهذا ما يدل على تجريم بعض الأفعال التي تعتبر ضمن جرائم الأعمال والتي تهدد الجانب الاقتصادي والمالي. وقد سعى أيضا لمكافحة الفساد من خلال إنشاء السلطة العليا للشفافية والوقاية من الفساد ومكافحته في المادة 204.

[1]- الدستور الجزائري ، الصادر في 15 جمادى الاولى 1442 الموافق ل30 ديسمبر 2020، المعدل والمتمم، ج ر ج ج،العدد 82، ص4.

2_ القانون المدني[1]: باعتباره الشريعة العامة، فقد كان للقانون المدني دور في مكافحة الجرائم المعلوماتية، من حيث تقدير الضرر والتعويض، ما إن كان أحد أطراف الدعوى مدنيا. وكذا من جانب الإثبات وهذا من خلال المواد من 323 إلى 333 منه ، من بينها الإثبات بالشهود.

3_ القانون التجاري[2]: مرورا بالتشريعات العامة لمكافحة الجرائم الإلكترونية، خاصة فيما يخص الأعمال ، نجد أن للقانون التجاري دور أيضا في هذه المكافحة، والذي بدوره يحكم المعاملات والممارسات التجارية ..،بما في ذلك تحديد مسؤولية الأشخاص الطبيعية والمعنوية، كما يعتبر مرجع عام لتحديد الأنشطة التجارية وتبيان موقعها القانوني. ومنه تستخلص الأفعال التي تعتبر جرائما.

3_ قانون الإجراءات الجز ائية[3]:

إن الجرائم الإلكترونية تخضع لإجراءات المتابعة، كما هو الحال بالنسبة للجرائم التقليدية. ومن بين هاته الإجراءات: التفتيش، الاستجواب، التسرب، الضبط...، إلا أن المشرع الجزائري قد وضع أحكام صارمة فيما يخص التفتيش الإلكتروني. كما أنه قام بتوسيع نطاق اختصاص وكيل الجمهورية ليشمل مجال الجريمة المعلوماتية. وبهذا يكون المشرع الجزائري قد أجاز للجهات المختصة بالتحقيق والتدقيق في مثل هذه الجرائم باللجوء إلى وسائل وتقنيات متطورة تتماشى مع تطور الجريمة، لتسهيل عملية كشف ملابسات الجريمة الإلكترونية وضبط

[1]-الأمر 75-58، المؤرخ في 20 رمضان 1395 الموافق ل26 سبتمبر 1975، يتضمن القانون المدني، ج ر ج ج ، عدد 78 الصادرة في 24 رمضان 1395 الموافق ل30 سبتمبر1975، المعدل والمتمم.

[2]-القانون رقم 05-02 الصادر في 06 فبراير 2005، يعدل و يتمم الأمر رقم 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، و المتضمن القانون التجاري، ج.ر ج ج ، عدد 11 المؤرخة في 09 فبراير 2005.

[3]- الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18صفر1386 الموافق ل8يونيو1966، التضمن قانون الإجراءات الجزائية، ج.ر ج جعدد 65، الصادرة في 17 محرم 1443 الموافق لـ 26 أوت سنة 2021،ص7.

الأدلة، مع تحديد موقعها وملاحقة مرتكبيها. ومن بين هذه الوسائل، اعتراض المراسلات وغيرها، وبهذا يكون قانون الإجراءات الجزائية متزامنا مع الجرائم الإلكترونية[1].

ثانيا: مكافحتها وفقا للقو انين الجز ائية:

1_**قانون العقوبات**[2]: إن التطورات المستجدة في مجال الجريمة الرقمية، جعل من المشرع الجزائري يتماشى مع هذه الثورة، بحيث قام بتجريم الأفعال التي تضر أنظمة الحاسب الآلي وتؤثر عليها بشكل سلبي، سواء بإتلافها أو تدميرها وغيرها. وقد جاء في قانون العقوبات رقم 04-15، الذي أشار إلى جملة من الجرائم وخصص لها قسم خاص ، المتمثل في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، في تسع مواد، من المادة 394 مكرر إلى 394 مكرر 8. بحيث طرأ على هذا القانون جملة من التعديلات، وكان آخر تعديل في 2024 وهو القانون رقم 24-06 ، والذي مس بعض المواد من هذا القسم، بل قام بتحديد العقوبات الأصلية والعقوبات التكميلية، بما فيها تشديد قيمة الغرامة المقررة كعقوبة أصلية أساسية، إضافة إلى مجموعة من تعديلات أخرى بعيدة على هذا المجال.

بحيث أدرج في هذا القسم مجموعة من الجرائم التي صنفها حسب طبيعتها مع تحديد العقوبة المقررة لها حسب درجتها . منها جرائم الولوج إلى المعطيات المعالجة، جريمة الحذف والتغيير لهذه المعطيات...

[1]-بن لعربي أسماء، الفحلة مديحة، مكافحة الجريمة الإلكترونية في الجزائر رؤية تشريعية واستراتيجيات عملية، المجلة الأكاديمية للبحوث القانونية والسياسية،الصادرة عن كلية الحقوق و العلوم السياسية، الأغواط المجلد التايع، العدد1، الأغواط، 2025، ص1246.

[2]-قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-156، يتضمن قانون العقوبات، الجريدة الرسمية الجمهورية الجزائرية، عدد71، الصادر ب10 نوفمبر 2004.

الفرع الثاني: التشريعات والهيئات الخاصة لمكافحة جرائم الأعمال الرقمية.

إضافة إلى القواعد العامة التي تحكم الجرائم بكلا نوعيها التقليدية والإلكترونية. توجد قواعد آليات خاصة تحكمها، لا يمكن القول أنها خاصة بجرائم الأعمال الرقمية، إلا أنه يتم الإستناد عليها في مكافحة هذه الجرائم، و إضافة إلى ذلك أيضا أنشأ المشرع هيئات خاصة لمجابهة هذا النوع من الجرائم الرقمية.

أولا: القوانين الخاصة لمكافحة جرائم الأعمال الرقمية.

1_**قانون البريد والاتصالات السلكية واللاسلكية**[1]: بعد هذا القانون نلاحظ مسايرة التشريعات للتطور التكنولوجي فيما يخص مجال الاتصالات، والتي ساهمت وسهلت إجراء العمليات والتحويلات المالية عن طريق الوسائل الإلكترونية. ونجد هذا في المادة 87 من هذا القانون كالتالي:" يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات... أو عن الطريق الإلكتروني". وبالرجوع إلى المادة 4 الفقرة 2 منه، فقد نصت على استعمال حوالات دفع الكترونية، كما أن هذا القانون جاء ليضمن حماية وسرية المراسلات والتي نصت عليها المادة 105 في الفقرة 4 كالتالي:" لايمكن بأي حال من الأحوال انتهاك سرية المراسلات". كما أقر عقوبة لكل موظف أو عون يخالف أحكام هذا القانون في إطار ممارسة مهامه، سواء بفتح أو تخريب أو انتهاك سرية المراسلات، أو حتى القيام بالمساعدة في ارتكاب هذه الأفعال[2].

[1]-القانون رقم 2000-03، المؤرخ في جمادى الأولى 1421 الموافق لـ5 أوت2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية الجمهورية الجزائرية، العدد 48، الصادرة في 6 جمادى الأولى عام 1421 الموافق لـ 6 أوت سنة 2000،ص3.

[2]د.بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، سبتمبر 2018، ص365.

2_ **القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**[1]:

جاء هذا القانون ليسد الثغرات فيما يخص مكافحة الجرائم الإلكترونية، بحيث يهدف إلى إرساء قواعد وأحكام خاصة للحد من هذه الجرائم. كم أنه وضح المشرع من خلال المادة 3 من هذا القانون نطاق تطبيقه، والذي يضمن حماية وسرية المراسلات والاتصالات، والنظام العام، كما أوجب وفقا لأحكام قانون الإجراءات الجزائية وهذا القانون، ودون الخروج عنها مراقبة الاتصالات الإلكترونية، مبينا الحالات المسموحة لاتخاذ هذا الإجراء من خلال الفصل الثاني من هذا القانون. كما وضع المشرع القواعد الإجرائية، منها تفتيش المنظومات المعلوماتية، إجراء حجز المعطيات المعلوماتية..، كما حدد التزامات مقدمي الخدمات ومهامهم. وبصدد هذا القانون تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته مع تحديد مهامها. كما نص أيضا على التعاون الدولي والمساعدة القضائية الدولية.

3_**قانون التجارة الإلكترونية**[2]: بحكم طابع السرعة الذي يتميز به مجال التجارة، فقد شهد تطورا سريعا بسبب الثورة المعلوماتية. لذا قام المشرع بسن هذا القانون رقم 18-05 المتعلق بالقواعد العامة للتجارة الإلكترونية للسلع والخدمات. وقد حدد المشرع من خلاله الممارسات التجارية بما فيها أيضا التزامات كل من المستهلك الإلكتروني وواجبات المورد الإلكتروني، كما وضح كيفيات الدفع عبر الطرق الإلكترونية. وقام المشرع بحماية هذا المجال من خلال تجريم بعض الأفعال التي تهدد التجارة عامة، والمستهلك الإلكتروني بصفة خاصة.

[1]-قانون رقم 09-04، المرخ في 14 شعبان 1430 الموافق ل5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، ج ر ج ج العدد 47الصادرة في 25 شعبان 1430 الموافق ل16غشت2009، ص5.

[2]-قانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق ل10 مايو 2018، يتعلق بالتجارة الإلكترونية، ج.ر العدد28، الصادرة في 30شعبان1439 الموافق ل16مايو2018، ص4.

4_**قانون 03-06 المتعلق بالعلامات**[1]: جاء هذا القانون إضافة إلى قانون الملكية الصناعية، لحماية العلامات ومنها التجارية وحقوقها، بحيث أن كل من يخالف الالتزامات المتعلقة بها، أو خرقها، وقام بتقليديها وانتهاك حقوق الغير أو صاحب العلامة، فإنه بتابع ويعاقب قانونا، بحيث جاء في الفقرة 2 من المادة 26 منه:" ...يعد التقليد جريمة يعاقب عليها ....".

5_ **القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**[2]: والذي عالج مجموعة المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي. كما تم النص على إنشاء سلطة وطنية تتمتع بالشخصية المعنوية والاستقلال المالي لحماية هذه المعطيات. وقد تطرق أيضا المشرع من خلال هذا القانون إلى حماية المعطيات المتعلقة بخدمات التصديق والتوقيع الإلكترونيين وحمايتها. كما نص أيضا على ضمان سرية المعطيات من التلف أو النشر أو الدخول غير المشروع، وكذا حمايتها من أشكال المعالجة غير المشروعة. مرفقا بإقرار عقوبات وأحكام إدارية وجزائرية دون الإخلال طبعا بالتشريع ساري المفعول (قانون العقوبات).

6_ **القانون المتعلق بالتوقيع والتصديق الإلكترونيين**[3]: يحدد هذا القانون رقم 15-04 القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين والذي يهدف إلى حمايتها سواء من التزوير أو استعمالهما بغير حق، عن طريق الرقابة وكذا إنشاء السلطة الحكومية والاقتصادية المسؤولة عن التصديق الإلكتروني. كما حدد واجبات كل من يقوم بإصدارها مع تحديد مسؤولية مؤدي هذه الخدمات، وتقرير العقوبة المالية والجزائية في حالة عدم إحترام أحكام القانون.

[1]-الأمر رقم 03-06 المؤرخ في 19جمادى الاولى1424 الموافق ل19يوليو2003، يتعلق بالعلامات، ج.ر العدد44، الصادرة ب23جمادى الاولى1424 الموافق ل23يوليو2003 ، ص22.

[2]-قانون رقم 18-07 المؤرخ في 25رمضان1439 الموافق ل10يونيو2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر العدد 34، الصادرة ب25رمضان1439 الموافق ل10يونيو2018، ص11.

[3]- قانون رقم 15-04 المؤرخ في 11ربيع الثاني1436 الموافق ل1فبراير2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر العدد 06، الصادرة ب30ربيع الثاني1436 الموافق لفبراير2015، ص6.

ثانيا: الهيئات الخاصة بمكافحة جرائم الأعمال الإلكترونية.

1_ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

تم إنشاء هذه الهيئة بموجب القانون رقم 09-04 المتعلق بالقواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتحديدا في المادة 13 منه، والتي جاء في الفقرة 2 من هذه المادة أنه :" تحدد تشكيلة الهيئة وتنظيمها و كيفيات سيرها عن طريق التنظيم".[1]

كما قام المشرع في هذا القانون، بوضع جملة من المهام، تلتزم بتطبيقها، في المادة 14 منه، والتي تتمثل في: تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحويلات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية. إضافة إلى ذلك تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكانهم[2].

2_الهيئات القضائية الجزائية المتخصصة:

إن تأثير الفضاء الإلكتروني السلبي، خاصة على أنظمة الكمبيوتر، من خلال الاختراقات المختلفة وتدمير هذه الأنظمة ، جعل من المشرع اللجوء إلى مظاهر ووسائل تقنية جديدة، بحيث تم إنشاء أقطاب جزائية متخصصة لمكافحة الجرائم المعلوماتية، ومحاولته للتقليل منها، وهذا دعما للقضاء العادي، الذي عجز عن التصدي لهذا النوع من الجرائم[3].

[1]-المادة 13، قانون رقم 09-04،السالف الذكر، ص8

[2]-المادة 14، قانون رقم 09-04، السالف الذكر، ص8.

[3]-بن لعربي أسماء، الفحلة مديحة، المرجع السابق، ص1250.

ثالثا: الأجهزة التابعة للأمن والدرك لمكافحة جر ائم الأعمال الرقمية.

لم يقتصر جهد الدولة الجزائرية حول مكافحة الجرائم الإلكترونية، فقط من حيث القوانين والهيئات، بل تطلب الأمر إلى تدخل أجهزة الدفاع الوطني بكلا شقيه، الأمن والدرك الوطنيين، وكان لهما دور في مساعدة العدالة، بما في ذلك الكشف عن مثل هذه الجرائم وكذا تسهيل عمليات إجراءات البحث والتحقيق، وضبط الجناة.

1_جهاز الأمن الوطني.

أ_ المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني:

تم إنشاء المصلحة المركزية للجريمة المعلوماتية بمقتضى قرار من المدير العام للأمن الوطني، وكانت بمثابة استجابة من مصالح الأمن الجزائية لمطلب الأمن المعلوماتي والعمل على الحد من التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، وكان هذا من ضمن المجهودات التي تبذلها المديرية العامة للأمن الوطني ومكافحة الإجرام السيبراني، والتي ساهمت هذه المصلحة المركزية في إعادة تنظيم التشكيل الأمني للشرطة القضائية، بحيث كانت هذه المصلحة بمثابة محور لإنشاء جهاز أمني خاص بمكافحة الجريمة المعلوماتية على مستوى المديرية العامة للأمن الوطني. وتم الاعتماد على هذه المصلحة وإدراجها ضمن الهيكل التنظيمي لمديرية الشرطة القضائية، في جانفي 2015. ومن بين المهام التي خولت لهذه المصلحة أن تساعد الشرطة في ما يخص التحقيق والتحريات سواء داخليا أو دوليا، بما في ذلك المساهمة في التكوين المتخصص لعناصر الشرطة المتواجدين على مستوى فرقة مكافحة الجريمة المعلوماتية على مستوى أمن الولايات[1].

[1]-سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد في الإجرام..واقعها وآليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد العاشر، العدد الأول، جوان 2023، ص548.

ولتكثيف وتشجيع مهام المديرية الوطنية العامة للأمن الوطني حول مكافحة الجرائم الإلكترونية، ونظرا للطابع الدولي لهذه الجرائم، فقد قامت هذه المديرية عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL، وبالتالي تسهيل الإجراءات القضائية الخاصة بتسليم المجرمين، وكذا تبادل المعلومات وملاحقة وضبط المجرمين حتلا ا لمتواجدين خارج إقليم الدولة[1].

ب_نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني:

قامت الشرطة العلمية العامة للأمن الوطني بتكفيل نيابة مديرية الشرطة العلمية والتقنية بمهمة محاربة الجريمة الإلكترونية، بحيث تختص بإجراءات البحث والتحري بما يخص الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. بحيث تشمل ثلاث وحدات تتمركز كل منها بولاية ما، وهي: المخبر المركزي للشرطة العلمية والمتواجد بالجزائر العاصمة، المخبر الجهوي للشرطة العلمية ومقره قسنطسنة، والمخبر الجهوي للشرطة العلمية بوهران. ويقوم كل مخبر بمهام البحث والتحقيق وكذا تحليل الأدلة الجنائية بمختلف أصنافها.

2_جهاز الدرك الوطني:

أ_المعهد الوطني للأدلة والإجرام للدرك الوطني:

يتشكل هذا المعهد من إحدى عشر دائرة متخصصة في مجالات متنوعة. بحيث تضمن توفير وإنجاز الخبرة، التكوين بالتعليم، وكذا تقديم المساعدات التقنية. كما أنها تساعد المحققين في المعاينات في المجال التقني، وتتكفل دائرة الإعلام الآلي الإلكتروني بتحليل الدلائل

[1]- عائشة فاضل، المسؤولية الجزائية في الجرائم الالكترونية (الجزائر نموذجا)، مجلة الحقوق والحريات، الصادرة عن مخبر الحقوق و الحريات في الأنظمة المقارنة عن جامعة بسكرة، المجلد الحادي عشر، العدد الأول، 2023، ص639/638.

الرقمية ومعالجتها. وبالتالي مساعدة العدالة من الجانب التقني وتقديم الأدلة التي تمت معالجتها كدليل إثبات[1].

ب_مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني:

تم إنشاء هذا المركز عام 2008، يعتبر كمركز توثيق، بحيث أن مقره متواجد ببئر مراد رايس، يقوم هذا المركز بتحليل بيانات الجرائم الإلكترونية وضبط مرتكبيها مهما كانت صفتهم، حفاظا على سلامة الأنظمة المعلوماتية، خاصة تلك المستعملة في المؤسسات المالية كالبنوك...، بحيث يقوم بمساعدة المحققين وتسهيل الإجراءات من خلال ضبط الأدلة، معاينة الجرائم وغيرها. ومن المهام الموكلة لهذا المركز أن تلتزم بضمان المراقبة الدائمة على شبكة الانترنت، المشاركة في قمع الجرائم المعلوماتية، التعاون مع مختلف مصالح الأمن، وكذا مساعدة الوحدات الإقليمية للدرك الوطني في البحث عن الأدلة...[2]

[1]-عائشة فاضل، المرجع السابق، ص638.

[2]-سميحة بلقاسم، حميد بوشوشة، المرجع السابق، ص552/551.

ملخص الفصل الأول :

يتضح من خلال هذا الفصل، أن فهم الإطار المفاهيمي لجرائم الأعمال الرقمية يعتبر قاعدة أساسية. إلا أن التشريعات بما فيها التشريع الجزائري لم تعط مفهوما دقيقا لهذا النوع من الجرائم، ما يجعلها لا تزال مبهمة، رغم طبيعتها المتميزة و الخاصة. اضافة إلى ذلك، نلاحظ تعدد الآليات المعتمدة لمجابهة هذه الجرائم سواء على المستوى الدولي الذي يشمل المؤتمرات و الإتفاقيات، و كذا الإقليمي. أما الوطني، فنجد أن المشرع رغم ارساله لمجموعة من القواعد العامة و الخاصة للتصدي لهذه الجرائم، إلا أنه مازال يواجه قصورا، خاصة فيما يتعلق بجرائم الأعمال بصفة خاصة.

الفصل الثاني : أهم صور جرائم الأعمال في البيئة الرقمية والآليات الإجرائية للكشف عنها

تمهيد:

بعد التطرق إلى المفاهيم الأساسية، و كذا آليات مكافحة هذه الجرائم، تبرز الحاجة إلى دراسة و تصنيف صور جرائم الأعمال الرقمية، و التي تتعدد و تتنوع نظرا لطابع السرعة الذي تتميز به هذه الجرائم. إلا أنه ركزت في هذا الفصل على أبرز صور جرائم الأعمال في البيئة الرقمية، و التي باتت تهدد النشاط التجاري و الإقتصادي للمؤسسات و الشركات، مرورا بعد ذلك إلى أهم الآليات الإجرائية المعتمدة للكشف عن هذه الجرائم بما في ذلك ضبط الدليل لإثباتها.

المبحث الأول : أهم صور جرائم الأعمال الرقمية

تتميز جرائم الأعمال كونها ذات طابع تقني وغير تقليدي، ما يجعلها أمام مواجهة أشكال وأنماط جديدة من الأفعال الإجرامية، خاصة أنها تتنوع وتتجدد باستمرار، لذا سنقوم بتصنيف أهم وأبرز الجرائم الواقعة على قطاع الأعمال عبر الفضاء الإلكتروني، منها الواقعة على التجارة الإلكترونية (المطلب الأول)، أو التي محلها التزوير الإلكتروني (المطلب الثاني)، أو تلك الماسة بالأموال خاصة جريمة تبييض الأموال باستعمال وسائل الدفع الحديثة (المطلب الثالث).

المطلب الأول : جرائم التجارة الإلكترونية

أصبحت التجارة الإلكترونية من أهم الوسائل التي ساهمت في خلق المنافسة بين مختلف المؤسسات والشركات، نظرا لطابع السرعة الذي تتميز به. إلا أن التطور التكنولوجي أثر سلبا على المعاملات التجارية من جهة أخرى. بحيث شهدت جرائم التجارة قفزة نوعية من الطابع التقليدي إلى الطابع الإلكتروني، مما جعل جرائم التجارة الإلكترونية تصنف ضمن الجرائم الخطرة والصعبة في مجال الأعمال بصفة خاصة. وسنذكر مثال ذلك الجرائم الواقعة على مواقع التجارة الإلكترونية (الفرع الأول والثاني)، والتي تهدد الثقة بين أطراف العمل التجاري، ونجد أيضا جرائم أخرى ماسة بعمليات البيع والإشهار ،منها جريمة مخالفة مقتضيات الإشهار والترويج الإلكتروني والإستبيان المباشر، والتي نص عليها قانون التجارة الإلكترونية 18-05 (الفرع الثالث).

الفرع الأول: جريمة اختراق مواقع التجارة الإلكتروني

تقع هذه الجريمة على المواقع التي تمارس من خلالها مختلف النشاطات التجارية، وهذا باختراقها أو قرصنتها، وتعتبر هذه الجريمة بمثابة اعتداء على خصوصية وسرية هذه المواقع، كنظيرتها التقليدية المتمثلة في تدمير محل تجاري يعرض فيه مختلف السلع والخدمات الموجهة للزبائن[1]. بحيث تتجلى صور جريمة الاختراق في الدخول غير المشروع للنظام المعلوماتي أو الموقع، أما الصورة الثانية فهي البقاء غير المشروع لهذا النظام.

[1]-حورية قويقح، جرائم التجارة الإلكترونية ومعوقاتها، مجلة دراسات اقتصادية، الصادرة عن جامعة الجلفة،المجلد 17، العدد 1، الجزائر، 2023، ص276-277.

أولا: أركان جريمة اختراق مو اقع التجارة الالكترونية.

قام المشرع الجزائري بتجريم كل تواجد غير مشروع بشكل عمدي داخل أنظمة المعالجة الآلية للمعطيات. ومن بينها الأنظمة التي تتضمن موضوع تجاري حتى وإن لم يؤدي هذا الفعل إلى نتيجة معينة وسواء كان ذلك بشكل كلي أو جزئي.

1_الركن المادي: والمتكون من فعلين ، إما الدخول أو البقاء غير المصرح بهما إلى البيانات الإلكترونية. ويتجلى ذلك فيما يلي:

أ_**الدخول غير المشروع**: لم يرد تعريف محدد لهذا الفعل، لكن يمكن أن يعرف بعملية الدخول إلى بيانات الحاسوب دون علم وإرادة صاحب المسؤولية على النظام[1].

ولم يحدد المشرع الجزائري الوسيلة المعتمدة في عملية الدخول إلى النظام. لكن هناك عدة طرق لتحقيق هذا الفعل داخل مواقع التجارة الإلكترونية، منها استخدام كلمة المرور بطريقة غير مشروعة ودون إذن صاحب الحق في استخدامها[2]، أو عن طريق الاعتماد على برمجيات وشفرات خاصة لارتكاب جريمة الدخول غير المرخص به[3].

أما فيما يخص شرط وقوع هذه الجريمة، فيرى المشرع الجزائري أن جريمة الدخول غير المشروع تقع فقط إذا كان النظام غير متاح للجميع.

ب_**البقاء غير المشروع**: يعرف فعل البقاء غير المرخص به على أنه التواجد داخل نظام المعالجة الآلية للمعطيات، دون إرادة ورضا صاحب السلطة على هذا النظام. ويمكن القول أيضا أنه هو عدم قطع الجاني للاتصال بالنظام بعد إدراكه أن دخوله فيه غير مشروع[4].

---

[1]-صالح شنين، الحماية الجنائية للتجارة الالكترونية-دراسة مقارنة-، مذكرة مقدمة لنيل شهادة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2012-2013، ص67.

[2]- ليلى تركي، الجرائم الواقعة على مواقع التجارة الإلكترونية في قانون العقوبات الجزائري، مجلة البحوث في العقود وقانون الأعمال، الصادرة عن جامعة الإخوة منتوري قسنطينة، المجلد التاسع، العدد الأول، جوان 2024، ص153.

[3]-خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للمعاملات الإلكترونية في النظام السعودي-دراسة تحليلية مقارنة-،مذكرة لنيل شهادة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، 2009، ص104.

[4]-حورية قويقح، المرجع السابق، ص111.

ولهذا الفعل المجرم صورتين، تتمثل الأولى في تجاوز الفاعل للمدة المرخصة والمحددة له داخل النظام المعلوماتي، أما الثانية فهي أن يدخل الفاعل عن طريق الخطأ والصدفة لهذا النظام، لكنه يستمر في البقاء دون الخروج منه حتى بعد علمه بالفعل المجرم الصادر منه[1].

أما فيما يخص صفة الجاني، فإن المشرع لم يشترط صفة معينة له وهذا بالرجوع للمادة 394 مكرر من قانون العقوبات04-15 المعدل والمتمم التي جاءت بعبارة: "..كل من يدخل أو يبقى..." والذي قد يكون شخصا عاديا أو غير ذلك، أو يعمل في البرنامج أو لا يعمل فيه.

وعليه فإن جريمة الدخول أو البقاء غير المشروع لا تتطلب تحقق نتيجة إجرامية، بل يكفي تحقق عنصر الولوج و الاستمرار فيه غير المرخص بهما داخل النظام أو الموقع الإلكتروني. فقد نص المشرع فقط على تشديد العقوبة في حال ما إذا ترتب على هذا السلوك تخريب أو حذف أو تغيير لمعطيات المنظومة. وهذا من خلال الفقرة 2 و 3 من المادة 394 مكرر من قانون العقوبات المعدل والمتمم.

2_**الركن المعنوي:** جاء في المادة 394 مكرر من قانون العقوبات عبارة:" كل من يدخل أو يبقى عن طريق الغش"، والتي يفهم منها أن جريمة الدخول أو البقاء غير المشروع هي من الجرائم العمدية . وبالتالي تحقق عنصري العلم والإرادة . وهنا يتجلى العنصر المعنوي في علم الجاني بأن هذا الفعل مجرم، وتتجه إرادته إلى القيام به، أي الدخول أو البقاء في النظام أو موقع التجارة الإلكترونية. وإلا فلن تتحقق الجريمة.

ثانيا: العقوبة المقررة للجريمة:

وتتمثل في صورتين كالتالي:

1_العقوبة في صورتها المبسطة: يعاقب بالحبس كل من من ستة (6) أشهر إلى سنتين، وكذا بغرامة حدها الأدنى 60.000دج و 200.000دج كحد أقصى.

2_العقوبة في صورتها المشددة: في حال ما إذا ترتب على هذه الجريمة حذف أو تغيير معطيات المنظومة، فيتم مضاعفة العقوبة المذكورة سابقا.

[1]-حورية قويقح، المرجع السابق، ص111.

أما إذا ترتب عليها تخريب نظام اشتغال المنظومة، فتكون العقوبة بالحبس من سنة (1) إلى ثلاث (3) سنوات، وبغرامة تكون بين 100.000دج كحد أدنى و 300.000 دج كحد أقصى.

الفرع الثاني: جريمة الاتجار بمعلومات تجارية غير مشروعة.

ويقصد بها :"الاتجار عمدا بمعلومات غير مشروعة ومخزنة في أنظمة الكترونية، قصد الربح غير المشروع منها وذلك باستخدامها لارتكاب جرائم ورائها"[1].

أولا: أركان جريمة الاتجار بمعلومات تجارية غير مشروعة.

سنتناول الركن المادي والمعنوي لهذه الجريمة.

1_الركن المادي: بمجرد توافر السلوك الإجرامي يقوم الركن المادي والذي ينقسم إلى صورتين، هما التعامل في معطيات صالحة لارتكاب الجريمة، والتعامل في معطيات متحصله من هذه الجريمة.

أ_التعامل في معطيات صالحة لارتكاب الجريمة: قام المشرع بتجريم مجموعة من الأفعال من خلال الفقرة الأولى للمادة 394 مكرر2 من قانون العقوبات، وتعد من الجرائم الخطرة خاصة وأنها تشمل كل التعاملات المرتبطة من بينها ما يتعلق بقطاع البنوك. وقبل وصول المعطيات إلى يد الجاني لاستغلالها في ارتكاب الجرائم، فإن هذه العملية الأخيرة تمر بمجموعة من المراحل الخاصة، وأولها القيام بتصميم المعطيات والبحث فيها ثم تجميعها إلى أن تصبح متاحة وتحت تصرف الغير وهذا بعد نشرها أو توفيرها أو الاتجار فيها. ولا يشترط أن تتوفر كل هذه الجريمة حتى تقع الجريمة، بل يكفي وقوع فعل واحد منهم فقط[2].

ب_التعامل في معطيات متحصلة من الجريمة: بحيث جاء في الفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات أنه تتحقق هذه الصورة من السلوك الإجرامي بتحقق إحدى الأفعال التالية: حيازة معطيات متحصلة من جريمة الدخول أو البقاء غير المرخص بهما، أو التلاعب بالمعطيات، أو إفشائها أو نشرها أو استعمالها.

---

[1]-صباح عبد الرحيم، وهيبة عبد الرحيم، جرائم التجارة الإلكترونية، المجلة الدولية للبحوث القانونية والسياسية، الصادرة عن مخبر السياسات العامة و تحسين الخدمة العمومية، جامعة الوادي، المجد الأول، العدد الأول، 2017، ص40.

[2]- أ.محمد خليفة، د.نصيرة مهيرة، الإجرام المعلوماتي وأثره في مجال الأعمال، ملتقى وطني حضوري/إفتراضي، جامعة يوسف بن خدة –الجزائر1- ، 10 نوفمبر 2022، مداخلة منشورة في كتاب جرائم الأعمال –الخصوصية والمكافحة-، ص 114.

أما فيما يخص النتيجة الإجرامية ، فإن المشرع قام بتجريم الأفعال سابقة الذكر وصنفها ضمن جرائم الخطر بحيث لا يطلب قيامها تحقق نتيجة معينة، إلا أنها يمكن أن تؤدي إلى إحداث ضرر فعلي[1].

2_**الركن المعنوي**: من خلال ما جاء في المادة 394 مكرر 2ق.ع :"..عمدا وعن طريق الغش.."، فإن هذه العبارة توحي بأن جريمة الاتجار بمعطيات غير مشروعة هي من الجرائم العمدية. والتي تطلب قصدا خاصا من الجاني والمتمثل في التحضير المسبق لاستعمال هذه المعطيات لارتكاب الجريمة (الصورة الأولى) وقصدا عاما فيما يخص التعامل في المعطيات المتحصلة من الجريمة (الصورة الثانية).

ثانيا: العقوبة المقررة لجريمة الإتجار بمعطيات تجارية غير مشروعة.

يعاقب كل من قام عمدا وعن طريق الغش بهذه الجريمة بالحبس من سنة (1) إلى (5) سنوات، وبغرامة من 1000000 دج كحد أدنى إلى 5000000دج كحد أقصى.

ثالثا: أحكام مشتركة

_إذا ارتكبت جريمتي الدخول أو البقاء غير المشروع لمواقع التجارة الإلكترونية، و الإتجار بمعطيات تجارية غير مشروعة من قبل شخص معنوي ، فإنه يتم معاقبته بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

_يعاقب أي شخص قام بالمشاركة والمساهمة سواء في مجموعة أو ضمن اتفاق،وسواء بفعل أو عدة أفعال مادية بغرض الإعداد والتحضير لهذه الجريمتين،بالعقوبات المقررة للجريمة ذاتها.

_يعاقب كذلك على فعل الشروع في ارتكاب إحدى الجنح سابقة الذكر بالعقوبة المقررة للجنحة ذاتها.

[1]- أ.محمد خليفة، د.نصيرة مهيرة، المرجع السابق، ص114.

الفرع الثالث: جريمة مخالفة مقتضيات الإشهاروالترويج الإلكتروني والاستبيان المباشر

نصت المادة 40 من قانون التجارة الإلكترونية على تجريم كل الأفعال المخالفة لأحكام المواد 30 و 31 و 32 وكذا 34 من نفس القانون. والتي سنعالجها من كلا جانبيها، سواء من حيث أركانها، أو من حيث الجزاء والعقوبة المقررة لها.

أولا: أركان جريمة مخالفة مقتضيات الإشهاروالترويج والاستبيان المباشر.

والمتمثلة فيما يلي:

1_الركن المادي: يتجلى السلوك الإجرامي هنا في قيام الجاني بالأفعال التالية:

_مخالفة مقتضيات الإشهار والترويج أو رسالة ذات هدف تجاري عن طريق الاتصالات الإلكترونية.

_الاستبيان المباشر عن طريق انتحال صفة شخص طبيعي دون موافقته.

_إخلال المورد الإلكتروني بالتزاماته فيما يخص شروط وضعه لمنظومة إلكترونية.

_الإشهار والترويج للمنتجات الممنوعة من التسويق.

أما بالنسبة للنتيجة، فلا يشترط هنا تحقق نتيجة معينة، بحيث أن الجريمة تقع بمجرد تحقق عنصر من عناصر السلوك الإجرامي.

2_الركن المعنوي: يتجلى ذلك في القصد الجنائي العام، بحيث يكون الجاني على دراية وعلم بالفعل المجرم الذي يقوم به. بينما يتمثل القصد الجنائي الخاص في اتجاه نيته إلى تحقيق أحد الأفعال المذكورة سابقا.

ثانيا: العقوبة المقررة لجريمة مخالفة مقتضيات الإشهاروالترويج الإلكتروني والاستبيان المباشر.

يعاقب على القيام بهذه الجريمة ، والمتمثلة في مخالفة أحكام المواد 30 و 31 و 32 و 34 من قانون التجارة الإلكترونية 18-05، بغرامة تقدر ب 50.000دج كحد أدنى و 500.000دج كحد أقصى. وهذا دون المساس بحقوق الضحايا في التعويض.

المطلب الثاني : جريمة التزوير الإلكتروني

تعتبر جرائم التزوير من المواضيع الأكثر حساسية في مجال النظام الجزائي، و الأكثر خطورة أيضا[1]. فهي من صور الغش المعلوماتي بحيث حلت الوسائل الرقمية في هذه الجريمة محل الوسائل التقليدية بالأوراق ، و يبرز هنا البعد بين الوسيلتين، لا من حيث سعة التخزين و سرعة استرجاع المعلومات، ولا حتى من حيث تنظيمها[2].

لذا سنتطرق أولا إلى تعريف التزوير الإلكتروني و عناصره، ثم إلى أركان هذه الجريمة و العقوبة المقررة لها.

الفرع الأول : تعريف التزوير الإلكتروني.

لقد عرفه أحد الفقهاء على أنه تغيير الحقيقة في المحررات المعالجة آليا بهدف استعمالها[3]. و عرف أيضا أنه :"تغيير الحقيقة في مستند أو محرر أو سجل إلكتروني بأية وسيلة كانت، و بنية استعماله ، تغييرا من شأنه الاضرار بمصلحة الدولة أو الأفراد[4]".

أما فيما يخص التعريف القانوني لهذه الجريمة ، فلا نجد أن المشرع الجزائري قد عرف مصطلح "التزوير" في المادة 3 من قانون رقم 24-02[5] كالتالي : كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم ... من شأنه إحداث ضرر ...".

و بالتالي فإنه لم يرد عن المشرع أي تعريف خاص للتزوير المعلوماتي. لذا فإنه من خلال ما سبق ، يتضح أن التزوير الإلكتروني هو : "تغيير الحقيقة بأي وسيلة كانت بغية تعديل المضمون سواء بالحذف أو الإضافة ، و الذي يؤدي إلى الإضرار[6]".

---

[1]-أحمد محمد محروس عبد العال، التزوير الإلكتروني بين التشريع التقليدي وتليات المواجهة الحديثة، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار السبعون، 2025، ص44.

[2]- د.عمارة فتيحة، جريمة التزوير الإلكتروني، مجلة القانون والمجتمع، الصادرة عن مخبر القانون و المجتمع بجامعة أدرار، المجلد السابع، العدد الأول، 2019، ص167.

[3]-حسين طاهري، الجرائم الالكترونية، دار الخلدونية للنشر والتوزيع، القبة، الجزائر، الطبعة الأولى، 1444-2022، ص85.

[4]-إلهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، أطروحة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق ، جامعة الحاج لخضر، باتنة، 2016، ص64.

[5]-قانون رقم 24-02، المؤرخ في 16 شعبان 1445 الموافق لـ26 فبراير 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية للجمهورية الديمقراطية الجزائرية الشعبية، العدد 15، الصادرة بـ15 شعبان 1445 الموافق لـ29 فبراير2024، ص5.

[6]-أحمد محمد محروس عبد العال، المرجع السابق، ص51.

الفرع الثاني: وسائل التزوير الإلكتروني.

يختلف محل جريمة التزوير الإلكتروني حسب اختلاف الوسيلة المعتمدة في ارتكاب هذه الجريمة، فيمكن أن يكون محررا إلكترونيا، أو بطاقات سواء بطاقة الائتمان أو البنكية، وقد تمس هذه الجريمة التوقيع الإلكتروني.

أولا_ المحرر الإلكتروني.

يعتبر المحرر الإلكتروني محلا لجريمة التزوير الإلكتروني، لذا سنتطرق أولا إلى تعريفه ، ثم تمييزه عن المحرر التقليدي.

1_ تعريف المحرر الإلكتروني:

وعرفه قانون الأونسترال النموذجي بشأن التجارة الإلكترونية 1996 في المادة 2 فقرة أ تحت اسم "رسالة بيانات" كالتالي : "المعلومات التي يتم إنشائها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية...". ليتبين أنه تم استعمال مصطلح رسالة بيانات دون المستند الإلكتروني، وهذا راجع لتعدد وتنوع الوسيلة المعتمدة في التعامل مع هذا المستند، والتي تمت الإشارة عليها على سبيل المثال لا الحصر.

بينما المشرع الجزائري لم يعرف المستند الإلكتروني، لكن من خلال القانون المدني رقم 75-58 المعدل والمتمم، في المادة 323 مكرر منه والتي جاءت ب: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تضمنتها وكذا طرق إرسالها"، نجد أن المشرع قد أشار عليه بشكل ضمني غير صريح، لقوله:"....مهما كانت الوسيلة التي تتضمنها..."، أي أنها سواء كانت هذه الوسيلة مادية أو غير ذلك أي إلكترونية[1].

[1]-ط.د.خليفي فتيحة، د.مهمداوي محمد صلاح، التزوير المعلوماتي في البيئة الرقمية، مجلة الدراسات القانونية الصادرة عن مخبر السيادة و العولمة كلية الحقوق و العلوم السياسية جامعة يحيى فارس المدية،المجلد الثامن، العدد الثاني، المدية –الجزائر-، 2022، ص262.

2_ **تمييز المستند الإلكتروني عن المستند التقليدي:**

لابد من وجود نقاط معينة تميز أحدها عن الآخر، لذا سنتعرض لأبرز هذه النقاط ،المتشابهة منها والمختلفة.

أ_**أوجه التشابه:** نرى أن كلاهما يتضمن حروف ورموز تمثل فكرة و موضوع معين. وكذا التمتع بحماية جزائية[1].

كما أن للمستندات الإلكترونية نفس الحجية المقررة للمستند التقليدي في مسألة الإثبات. هذا ما نصت عليه المادة 323 مكرر 1 من القانون المدني، بحيث اعتبر المشرع الجزائري أن الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، تحت شرط التأكد من هوية الشخص المصدر لها.

ب_**أوجه الاختلاف:** أما فيما يخص نقاط الاختلاف بينهما، فنرى أن النقطة الأولى والأساسية هي القالب الجوهري الذي تعكس فيه المعلومات، لتكون المستندات الإلكترونية مدرجة داخل نظام معلوماتي[2]، أما التقليدية فتكون وسيلة ورقية.

كما أنهما يختلفان أيضا من حيث اكتشاف عملية التزوير الواقعة على المستند. لذا فإن المحرر التقليدي يتميز بسهولة اكتشاف هذا الفعل المجرم، لوضوح اختلاف المستند الأصلي عن الذي تم نسخه وكذا إمكانية الإطلاع على مضمونه بمجرد النظر إليه، عكس المستند الإلكتروني الذي يتميز بسرية أكثر، وهذا راجع لإلزامية وضعه تحت وسيط إلكتروني قابل لقراءة مضمونه[3].

ثانيا: بطاقة الائتمان والبطاقة البنكية.

1_بطاقة الائتمان: تعرف بطاقة الائتمان على أنها :" بطاقة معدنية أو بلاستيكية ممغنطة عليها اسم حاملها وتاريخ إصدارها وتاريخ نهاية صلاحيتها، ورقم سري لا يعرفه إلا حاملها[4]". وتعرف

[1]-د.عادل مستاري، أ.رواحنة زوليخة،جريمة التزوير الإلكتروني، مجلة العلوم الإنسانية، الصادرة عن جامعة محمد خيضر،بسكرة، العدد 46، ص300.

[2]-أيمن عبد الله فكري، الجرائم المعلوماتية –دراسة مقارنة في التشريعات العربية والأجنبية-، الطبعة الأولى، مكتبة القانون والإقتصاد، المملكة العربية السعودية، 2014، ص385.

[3]- صالح شنين، الحماية الجنائية للتجارة الإلكترونية –دراسة مقارنة-، رسالة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013، ص 48.

[4]- مريم تومي، صدراتي وفاء، تزوير بطاقات الائتمان صورة خاصة من جريمة التزوير الإلكتروني، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الخامس، العدد الثاني، الأغواط –الجزائر-، 2021، ص1001.

أيضا بأنها " بطاقات تصدر بواسطة مؤسسة مالية باسم إحدى الأشخاص وتقوم تلك البطاقة بوظيفتي الوفاء والائتمان[1]".

فبطاقة الائتمان تقوم على فكرة أساسية وهي الائتمان، فهي جوهر البطاقة لافتراضها وجود فاصل زمني بين تقديم مانح الائتمان لوسائل الوفاء لعملية الشراء وبين استرداد كل الوسائل[2]".

أما بالنسبة للتعريف التشريعي، فلم يرد عن المشرع الجزائري تعريفا خاصا ببطاقة الائتمان، لكن تم الإشارة عليها بصفة عامة وبشكل ضمني، باعتبار أنها من وسائل الدفع، وكان ذلك من خلال القانون التجاري المعدل والمتمم بموجب القانون 05-02[3]، في الفصل الثالث من الباب الرابع منه، تحت عنوان "في بطاقات الدفع والسحب"، تحديدا في المادة 543 مكرر 23 – الفقرة الأولى-، على أنه :" تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها سحب أو تحويل الأموال".

2_**البطاقة البنكية**: لم يرد هي الأخرى تعريفا لها من قبل المشرع الجزائري، لكن بالنظر إلى المشرع الفرنسي، نجد أنه عرفها بأنها كل بطاقة تسمح لحاملها بسحب أو بنقل الأموال، بحيث لا تصدر إلا من طرف هيئة قرض أو مؤسسة مالية، أو مصلحة تملك الترخيص بإصدار أو وضع البطاقات كالمصارف، الخزينة العامة أو مصالح البريد[4].

3_**التمييز بين كل من البطاقة الائتمانية والبطاقة البنكية**: سنرى أهم الفروقات بينهما من خلال الجوانب االتالية:

_**من حيث الوظيفة والمصدر**: تصدرها البنوك أو شركات التمويل، تسمح بطاقة الائتمان لحاملها بالاقتراض من البنك أو المؤسسة المالية لشراء سلع أو خدمات ، مع إمكانية السداد لاحقا إما كاملا أو مع فوائد.

[1]-فايز رضوان، بطاقات الوفاء، الطبعة الأولى، المطبعة العربية، مصر، 1990، ص71.

[2]- علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية –دراسة مقارنة-، مجلة الحقوق، العدد الثالث، الكويت، 2013، ص 465.

[3] القانون 02/05 المؤرخ في 26 فيفري 2005، المعدل و المتمم للأمر 59/75 المتضمن القانون التجاري، ج.ر عدد11، سنة 2005.

[4]-توايمية ديانة ملاك، دور البطاقة البنكية في تعزيز التجارة الإلكترونية، مذكرة لنيل شهادة ماستر، قسم الحقوق –تخصص قانون أعمال-، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2021-2022، ص14.

أما البطاقة البنكية فتصدرها البنوك لزبائنها، كما تتيح سحب الأموال أو الدفع مباشرة من الحساب البنكي المرتبط بها.

_**من حيث الرصيد والسداد**: يعتمد رصيد بطاقة الائتمان على الحد الائتماني الممنوح من البنك. وبالنسبة للسداد فيجب سداد المستخدم للمبلغ إما خلال الفترة المسموحة (بدون فوائد) أو على أقساط لكن مع أخذ فوائد.

بينما البطاقة البنكية فتعتمد على الرصيد المتوفر في الحساب البنكي. بحيث عند السداد يخصم المبلغ فورا من الحساب ولا تسمح بالشراء بالدين.

_**من حيث الأمان**: تحتوي كل منهما على شريط مغناطيسي أو شريحة ورقم سري للمعاملات الإلكتروني.

ثالثا: التوقيع الإلكتروني.

إنه من الصعب تكييف التوقيع اليدوي مع النظم المعلوماتية ، للتطور الذي شهدته هذه الأخيرة ، لذلك تم الاعتماد و التوجه إلى ما يسمى بالتوقيع الإلكتروني ، ليتماشى مع طبيعة المحرر الإلكتروني . و قد أعطى له المشرع نفس القيمة القانونية للتوقيع التقليدي اليدوي.

1_تعريف التوقيع الإلكتروني :

عرف المشرع المصري التوقيع الإلكتروني على أنه حروف، أرقام، رموز، أو إشارات لها طابع منفرد، تسمح بتحديد شخص صاحب التوقيع و تمييزه عن غيره، و يتم اعتماده من الجهة المختصة[1].

و عرفه قانون الأونسترال الخاص بالتوقيع الإلكتروني 2001 في الفقرة (أ) من المادة 2 الجزء الأول على أنه : "بيانات في شكل إلكتروني مدرجة في رسالة بيانات ، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ، و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".

[1]- عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني، الطبعة الاولى، دار الكتب القانونية، مصر، 2007، ص15 وبعدها.

أما بالنسبة للتشريع الجزائري، فقد جاء في قانون 15-04[1] في المادة 2 منه ، بتعريف التوقيع الإلكتروني و قد عرفه "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا بيانات إلكترونية أخرى ، تستعمل كوسيلة توثيق".

2_صور التوقيع الإلكتروني :

إن التوقيع الإلكتروني لا ينحصر في شكل معين، بل يختلف و يتنوع حسب الوسيلة التي يعتمد عليه فيها، لذا سنتطرق إلى أنواع من صور التوقيع الإلكتروني و المتمثلة في : التوقيع الكودي، التوقيع البيومتري، و التوقيع الرقمي.

أ_التوقيع الكودي.

يتمثل التوقيع الكودي في مجموعة من الأرقام أو الحروف أو كلاهما، تكون من اختيار صاحب التوقيع لتأكيد و تحديد شخصيته، و تكون سرية و لا يعلمها إلا هو، أو من يبلغه بها بنفسه، و يعتبر هذا التوقيع بمثابة ضمان لتوثيق للمعاملات الإلكترونية، كما هو الحال للتوقيع اليدوي، بحيث يستعمل هذا التوقيع غالبا في عمليات الدفع الإلكتروني، و كذا العمليات المصرفية، عن طريق البطاقات الممغنطة، و مختلف البطاقات الحديثة التي تحتوي على ذاكرة إلكترونية[2].

ب_التوقيع البيومتري.

يشمل هذا البصمة، سواء بواسطة الإصبع أو شبكية العين ، أو البصمة الصوتية...، شرط أن تكون خاصية ذاتية للشخص صاحب التوقيع، كذا وجوب توفير حماية خاصة لهذه الخصائص، حتى لا يتم العبث بها و بالتالي تمتعها بالحجية القانونية. بحيث أن التوقيع البيومتري يتم عبر استعمال الحاسب الآلي و الكاميرا، بما في ذلك أيضا جهاز لقراءة البصمة[3].

[1]- قانون رقم 15-04، سالف الذكر.

[2]-د.عمرو أحمد عبد المنعم دبش، إثبات المستندات الإلكترونية"الإثبات الالكتروني"، مجلة العلوم القانونية والاجتماعية-، الصادرة عن جامعة زيان عاشور-، الجلفة، المجلد الرابع، العدد الأول، مارس 2019، ص41.

[3]- محمد الشريف بولعراس، أسامة طلحي، جريمة التزوير المعلوماتية، مذكرة مقدمة لنيل شهادة ماستر، كلية الحقوق –تخصص قانون إعلام آلي وانترنت-، جامعة محمد البشير الإبراهيمي-برج بوعريريج-، الجزائر، 2021-2022، ص245

ج_التوقيع الرقمي.

يعتمد هذا النوع من التوقيع على عملية التشفير ، و التي تثبت و تؤكد صحة و أصل البيانات[1]. كما يهدف التشفير إلى تحويل الرسائل إلى أشكال غير مفهومة، ليعيدها إلى هيئتها الأصلية. و تستخدم التوقيعات الرقمية ما يسمى بالترميز بالمفتاح العمومي، الذي يستعمل في إنشاء مفتاحين مختلفين، لكن بينهما رابطة رياضية. بحيث يتم استخدام إحداهما في إنشاء توقيع رقمي مبهم و غير مفهوم خارجيا، بينما يستخدم الآخر في إعادة الرسالة التي تحمل التوقيع إلى شكلها الأصلي بعدما تم التحقق من صحة هذا التوقيع[2].

الفرع الثالث: أركان جريمة التزوير الإلكتروني والعقوبة المقررة لها.

حتى تكتمل صفة الجريمة على التزوير الإلكتروني، لابد من توافر كل من الركن المادي والمعنوي،كما هو الحال بالنسبة للتزوير التقليدي والجرائم الأخرى.

أولا: أركان جريمة التزوير الإلكتروني.

1_**الركن المادي**: لقيام هذا الركن يلزم توافر السلوك الإجرامي والمتمثل في تغيير الحقيقة، والذي ينتج عنه ضرر.

أ_**تغيير الحقيقة**: يعتبر هذا السلوك الإجرامي العنصر الأول والأساسي لقيام جريمة التزوير، وإذا انتفى فلا تعد جريمة على الإطلاق. ويقصد بتغيير الحقيقة استبدالها بما يخالفها[3]. ويقصد به أيضا المساس بالحقيقة القانونية النسبية بتغييرها، وليس تغيير الحقيقة الواقعية المطلقة[4].

وقد يكون موضوع التزوير هنا إما ماديا أو ماديا.

_**التغيير المادي**: والمتمثل في الشكل المادي المعتمد في تغيير الحقيقة، والذي يدركه البصر. كما يمكن أن يكون غير ظاهرا والذي يتطلب الاستعانة بخبير[5].

---

[1]-سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص245.

[2]-راضية مشري، جريمة تزوير التوقيع الالكتروني في التشريع الجزائري، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، الصادرة عن جامعة قالمة، العدد 20، جوان 2017، 127-128.

[3]-بدر أحمد الجاسر الراجحي، جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الكويتي، مجلة الحقوق، الصادرة عن مجلس النشر العلمي، العدد الأول، الكويت، 2020، ص175.

[4]- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص138.

[5]-صالح شنين، المرجع السابق، ص59.

ويتم تزوير المحرر الإلكتروني من خلال تغيير مضمون المحرر بعد إنشاء المحرر الأصلي، سواء بتعديله بإضافة أو حذف بيانات معينة. وقد يتم إنشاء محرر مشابه لمحرر آخر باستخراج محرر طبق الأصل للمحرر الأول، ولا تتطلب هذه الطريقة إتقانا فنيا، بل يكفي أن يظهر بصورة محرر أصلي.

فبالنسبة لبطاقة الائتمان، التي تعتبر من بين أهم صور التزوير الإلكتروني، فيكون ذلك في تغيير إما كلي عن طريق استبدال معلومات حاملها الأصلي والشرعي بمعلومات و معطيات أخرى، أو جزئي وذلك بإضافة حرف أو رقم على البطاقة المزورة، أو بحذفهم بواسطة مادة كيميائية.

وكذا الحال بالنسبة للبطاقات البنكية باعتبارها أيضا محررا الكترونيا.

أما بالنسبة للتوقيع الإلكتروني، الذي هو أيضا من أبرز صور التزوير الإلكتروني، فيتمثل ذلك في قيام الجاني بإدراجها عن طريق جهاز الماسح الضوئي، بعدها يتم إضافة هذا التوقيع على الوثيقة التي تتضمن البيان المزور، وتشمل هذه الطريقة أيضا تزوير البصمة والصورة الشخصية، ووضعها على المحرر[1].

_**التزوير المعنوي**: تتمثل هذه الصورة في التغيير الذي يمس موضوع المحرر، أو ظروفه أو ملابسته، وليس في الشكل الظاهري عكس التغيير المادي، بحيث لايترك أثرا ماديا او مرئيا، وهذا ما يجعل منه محررا صعبا في الإثبات[2].

ويقع التزوير المعنوي أثناء إنشاء المحرر وليس بعده، وغالبا ما يصدر من قبل الشخص المكلف بكتابة وتحرير هذا المحرر[3].

ب_**الضرر**: هو كل إخلال بمصلحة يحميها القانون، والمتمثلة في الثقة العامة، وقد يكون يكون فعل الإخلال فعليا أو محتملا، كثيرا أو بسيطا، خاصا أو عاما.[4]

[1]-د.عادل مستاري، أ.رواحنة زوليخة، المرجع السابق، ص301.
[2]-عمارة فتيحة، المرجع السابق، ص176.
[3]-راضية مشري، المرجع السابق، ص131.
[4]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، الطبعة الأولى، مكتبة شادي، القاهرة ، 2009، ص297-299.

2_**الركن المعنوي**: إن جريمة التزوير هي من الجرائم العمدية، التي تستلزم توافر القصد الجنائي العام وكذا الخاص.

أ_**القصد الجنائي العام**: يتجلى في إدراك وعلم الجاني أنه يقوم بتغيير حقيقية ضمن المحرر، وكذا بالضرر الناتج عن هذا الفعل، وقد يكون ضررا فعليا أو محتملا[1]. بمعنى لقيام الجريمة، يجب توافر عنصر العلم بالفعل المجرم وهو التزوير الإلكتروني، والإرادة في القيام به وإحداثه.

ب_**القصد الجنائي الخاص**: يتجلى ذلك في اتجاه نية الجاني أثناء ارتكاب الفعل إلى استعمال المستند المزور في الغرض الذي زور من أجله[2]، وكذا نيته في إحداث الضرر. وغياب هذه الأخيرة ينفي القصد الجنائي وبالتالي الجريمة بحد ذاتها.

ثانيا: العقوبة المقررة لجريمة التزوير الإلكتروني.

يعاقب مرتكب هذه الجريمة بالحبس من سنة (1) إلى ثلاث (3) سنوات ، وبغرامة حدها الأدنى 500.000دج و حدها الأقصى 2.000.000دج.

وإذا ارتكبت من طرف شخص معنوي فإنه يعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

كما يعاقب على فعل الشروع لارتكابها بنفس العقوبة المقررة للجريمة ذاتها. أما بالنسبة لفعل المشاركة أو الاتفاق على التحضير لهذ الجريمة فيعاقب عليه أيضا بنفس العقوبة المقررة للجريمة نفسها.

مطلب ثالث: جريمة تبييض الأموال باستخدام وسائل الدفع الإلكترونية.

إن موضوع تبييض الأموال كان و لا زال ظاهرة عالمية تهدد المجال الاقتصادي بصفة عامة، و هو من الجرائم الأكثر خطورة، و تأثيرا بشكل سلبي على النمو الاقتصادي.

جريمة اتخذت من آليات تقنية و حديثة أداة للظهور بشكل قانوني لا غبار عليه، جاهدة للتخفي عن أنظار العدالة. لنرى أن الجزائر لم تسلم أيضا من هذه الجريمة العملية غير

[1]-عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات، دار النهضة العربية، مصر، 2010، ص838.

[2]-محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1988، ص219.

المشروعة[1]. لذا سنتعرف في هذا المطلب على مفهوم جريمة تبييض الأموال في الفضاء الرقمي، و الوسائل المعتمدة في تطبيقها (الفرع الأول)، و كذا إلى أركان هذه الجريمة، و ما هو موقف المشرع الجزائري منها (الفرع الثاني).

الفرع الأول : تعريف جريمة تبييض الأموال بواسطة وسائل الدفع الإلكترونية.

سنتناول في هذا الفرع تعريف تبييض الأموال، والذي يعد مصطلحا شائعا في مجال الأعمال، ومرورا بعد ذلك وسائل الدفع الحديثة التي تعتبر وسيطا إلكترونيا يعتمد عليها مبيضو الأموال لتسهيل ارتكابهم لهذه الجريمة.

أولا : تعريف جريمة تبييض الأموال.

عرف جانب من الفقه تبييض الأموال بأنه تحويل الأموال المتحصل عليها بطرق غير قانونية أو المتهربة من الالتزامات القانونية إلى أشكال أخرى للاحتفاظ بها بغية التغطية على مصادرها المتحصل عليها منها[2].

كما عرفت أيضا أنها مجموعة العمليات المالية التي تتم داخل إقليم الدولة أو خارجها، لإخفاء حقيقة الأموال ومصدرها غير المشروع وإضفاء صفة الشرعية عليها وكأنها من مصدر مشروع[3].

وبالنسبة للتعريف التشريعي، فلم يرد عنه تعريف خاص لتبييض الأموال عبر الفضاء الرقمي، إلا أنه حدد مجموعة الأفعال التي تعتبر تبييضا للأموال بمجرد قيامها، والتي تعتبر أيضا من جهة عناصر مادية لهذه الجريمة الكترونيا. وهذا في المادة 389 مكرر من قانون العقوبات رقم 15-04 [4] كالتالي:

---

[1]- نادية عبد الرحيم، د.أمين بن سعيد، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية، مجلة الدراسات الاقتصادية والمالية، الصادرة عن جامعة الشهيد حمة لخضر، الوادي –الجزائر-، العدد العاشر – الجزء الثاني-، 2017، ص28.

[2]-عبد الخالق سيد أحمد، الآثار الاقتصادية والاجتماعية لغسيل الأموال، دار النهضة العربية، القاهرة، مصر، 1997، ص03.

[3]- الدليمي –مفيد نايف-، الجدثي، غسيل الأموال في القانون الجنائي –دراسة مقارنة-، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص33.

[4]-القانون رقم 04-15، سالف الذكر.

1_ 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 ارتكاب الجريمة الأصلية التي أتت منها هذه الممتلكات، على الإفلات من الآثار القانونية لفعلته.

2_ إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

3_ اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، أنها تشكل عائدات إجرامية.

4_المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله واسداد المشورة بشأنه.

ثانيا: تعريف وسائل الدفع الحديثة:

إن وسيلة الدفع هي تلك الأدوات التي بها يقوم الشخص بتحويل أمواله بغض النظر عن الأسلوب التقني المستعمل.

أما فيما يخص وسائل الدفع الحديثة، فهي مجموعة من الأدوات الإلكترونية الصادرة من طرف المؤسسات المالية كالمصارف...، كأداة للدفع، تستخدم فيها تكنولوجيا متطورة و متقدمة، و هي البطاقات البنكية، النقود الإلكترونية و الشيك الإلكتروني.

و جاء في نص المادة 5/6 من القانون 05/18[1] بأنها "كل وسيلة مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية" .

وتتمثل أطرافها في: المتعامل، المصرف الذي يتحصل على مبلغ، المصدر بوسيلة الدفع.

الفرع الثاني : أساليب جريمة تبييض الأموال.

سنتطرق أولا إلى الأساليب التقليدية، التي تعتبر الانطلاقة الأولى لظهور جريمة غسيل الأموال، ثم بعد ذلك الأساليب الحديثة و المتطورة التي ولدتها التكنولوجيا.

[1]-القانون رقم 18-05، سالف الذكر.

أولا : الأساليب التقليدية المتبعة في عملية تبييض الأموال.

تنقسم الأساليب التقليدية في قطاع الأعمال إلى أساليب مصرفية و أخرى تجارية.

1_الأساليب المصرفية.

أ_**الحصول على تسهيلات وضمانات للاقتراض من البنوك**: لضمان استرجاع البنوك ما تم اقتراضه منها، لابد من توافر مصدر لتسديد هذا القرض والقابلة للبيع والتي يستوفي البنك منها مبلغ القرض وكذا فوائده. لكن في حالة ما إذا تم الاقتراض بدون ضمانات أو أخرى غير كافية لتسديد مبلغ القرض، فإنه يصبح هنا دينا والذي يكفي لتغطية أموال البنك. أما فيما يخص استخدام هذه القروض كمصدر للحصول على أموال غير مشروعة، فيتم ذلك بتآمر واتفاق موظفي البنك أو الإدارة العامة مع عملائهم، بحيث يمنح القرض تسهيلات لشخص ما من خلال تقدير تلك الضمانات المقدمة بثمن أكبر من الثمن الحقيقي، لتباع بعدها بسعر السوق، والذي يكون أقل من الذي قدر عند المنح، وبالتالي يكون العميل قد حصل على مال غير مشروع بهذه الطريقة[1].

ب_**الخدمات المصرفية الخاصة**: و هي مصارف خاصة تقدم خدمات مصرفية خاصة لصالح العملات الأغنياء، كانت نشأتها الأولى في سويسرا، بحيث جمعت هذه البنوك الكثير من الأموال بأقل عدد من الزبائن الذين تقدم لهم مجموعة من الخدمات البنكية. كما يتطلب من الزبون لفتح حساب لدى هذه البنوك، إيداع مبلغ مالي يقدر أو يفوق مليون دولار. و يتم تعيين مسؤول الخدمات الخاصة ليشرف على العمليات التي يجريها الزبون مع البنك، سواء داخل البنك أو أي مكان في العالم،و بالتالي قيام علاقة شخصية بين المسؤول و الزبون حول الخدمة الخاصة، ليصبح هذا المسؤول أمام المصالح المتعارضة بين خدمة الزبون و خدمة المصرف بهدف تحقيق مختلف الخدمات و الإيرادات لصالح البنك، إلى أن يصل المسؤول لمركز المستشار للزبون، و

[1]- قسمية محمد، مصادر وأساليب عمليات تبييض الأموال، مجلة الدراسات والبحوث القانونية، الصادرة عن مخبر الدراسات و البحوث في القانون و الأسرة و التنمية الإدارية، بكلية الحقوق جامعة محمد بوضياف ، المسيلة، الجزائر،المجلد التاسع، العدد الأول، 2024، ص172-173.

بالتالي تؤدي هذه العلاقة إلى إمكانية تجاوز كل من الزبون و المسؤول عن الخدمات، الضوابط الرقابية، من بينها عمليات غسيل الأموال [1].

ج_**إعادة الإقراض** : تتم هذه العملية من خلال إيداع الأموال غير المشروعة في أي بلد خارجي لا يوجد فيها لا ضرائب، و لا رقابة على البنوك، و كذا سهولة تأسيس الشركات، و تتمتع أيضا بالاستقرار السياسي و النقدي و كذا توافر وسائل الاتصال المتطورة، هنا يقوم أحد الأشخاص بطلب قرض من أحد البنوك الموجودة في بلد آخر بضمان تلك الأموال التي تم إيداعها في بنك البلد الأجنبي. و يمكن إستخدام هذه الأموال القذرة، التي تحمل صفة الشرعية، في عقد صفقات تجارية مثلا، أو شراء ممتلكات [2].

2_**الأساليب التجارية** : و تتمثل في :

أ_**عمليات السوق السوداء** : تتم هذه العملية عن طريق استبدال الدولارات غير الشرعية بعملات أجنبية أخرى، بحيث يمكن أن يقوم مبيضو الأموال بإعادة استبدالها مرة أخرى. وهناك أيضا وسطاء تابعين للعصابات الإجرامية الذين يقومون بالتعامل مع بنوك خاصة باستيراد بضائع من الولايات المتحدة الأمريكية، و يعرضون على المصدرين الأمريكيين الشراء بالدولار، ليقومون بعدها المستوردون بالوفاء للوسطاء بالعملية المحلية الكولومبية [3].

ب_**الفواتير المزورة** : هناك طريقة أخرى أيضا يعتمد عليها مبيضو الأموال في تحقيق هذه الجريمة، و ذلك عن طريق بيع و شراء السلع بين شركتين، بحيث يقوم الجاني بشراء سلع من الشركة المراد تحويل الأموال إليها في الدول التي لا يوجد فيها ملاحقات قضائية و بالتالي توافر الاستقرار النفسي، و يتم التحويل إما برفع قيمة السلع و الخدمات الموجودة في فواتير هذه الأخيرة، و يكمن الفرق بين القيمة الأولى للسلع و الثانية هو مقدار المال المغسول، أو اللجوء إلى إرسال مجموعة فواتير وهمية و مزورة كليا لا تمثل عمليات تبادل حقيقية، و ليكون هنا المال المغسول هو ذلك المبلغ الإجمالي المحرر بالفاتورة و المدفوع فعليا [4].

[1]- بن نقي سليمان، جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية، مجلة الأبحاث القانونية والسياسية، الصادرة عن مخبر تطبيقات التكنولوجيا الحديثة على القانون، جامعة محمد لمين دباغين، سطيف2، الجزائر، المجلد الثالث، العدد الثاني، 2021، ص155.
[2]-بن نقي سفيان، المرجع السابق، ص 155.
[3]- المرجع نفسه، 156.
[4]- د.علي زايد عبد الله ، غسيل الأموال عبر الوسائل الإلكترونية، القاهرة ، ص16.

ج_**الاستثمار في البورصة** : و هذا عن طريق شراء أسهم و سندات في البورصة و إعادة بيعها، و التي ينتج عن هذه العملية إما ربح أو خسارة ليتحصل غاسلو الأموال على شبكات من الغير بثمن هذه السندات، ثم إيداعها في البنك، و هذا لغرض تفادي إيداع الأموال في البنك لأول مرة[1].

ثانيا : الأساليب الحديثة المتبعة في عملية تبييض الأموال .

يعتمد مبيضو الأموال في ارتكاب جريمتهم عبر الفضاء الرقمي، على وسائل تقنية متطورة، وهي كالتالي:

1_البنوك الإلكترونية : أو بنوك الانترنت، لا تعتبر هذه البنوك بنوكا بالمعنى الحقيقي الذي يشمل القيام بالعمليات المصرفية بالطريقة المتعارف عليها، و هي ذهاب العميل شخصيا إلى البنك و الحصول على خدمات مصرفية عادية. بل هي عبارة عن بنوك افتراضية في الفضاء الإلكتروني، لها مواقع إلكترونية على مستوى شبكة الأنترنت هدفها تسهيل و تيسير إجراء العمليات المصرفية على العملاء، و يتم هذا الإجراء بمجرد إدخال العميل رقمه السري الخاص بحسابه على موقع البنك الإلكتروني و من ثم الوصول إلى الخدمات التي يريدها.[2]

و يتم الاعتماد على هذه البنوك في عملية تبييض الأموال عن طريق القيام بعمليتي الإيداع و التحويل من حساب آخر و بلد آخر، بغرض إضفاء طابع الشرعية على هذه الأموال القذرة. و غياب الرقابة المحكمة على مواقع البنوك الرقمية هو ما ساهم في الاعتماد على هذه الآلية من طرف مجرمي عمليات تبييض الأموال[3].

2_النقود الإلكترونية : عبارة عن قيمة نقدية مخزنة على أداة إلكترونية مدفوعة مسبقا، مستقلة على الحساب البنكي، بحيث تنقسم إلى صورتين، إما أن تكون في شكل نقود المخزون الإلكترونية، و التي تستلزم تخصيص مبالغ في حافظة النقود الإلكترونية و يكون هذا التخزين داخل بطاقة لها ذاكرة غير قابلة للاستخدام بمجرد انتهاء المبالغ المخزنة فيها، أما الصورة الثانية

[1]- بن نقي سفيان، المرجع السابق، ص156.

[2]- د.علي زايد عبد الله، المرجع السابق، ص18.

[3]- ط/د.منزول يمينة، جريمة تبييض الأموال باستخدام وسائل الدفع الإلكترونية، ملتقى وطني – حضوري/إفتراضي-، جامعة بن يوسف بن خدة-الجزائر 1-، 10 نوفمبر 2022، مداخلة منشورة في كتاب – جرائم الأعمال (الخصوصية والمكافحة)-، ص270.

فتتمثل في النقود الائتمانية الإلكترونية، و يتم الوفاء بطريقتين، إما بمقابل نقدي بشكل مباشر بين البائع و المشتري.[1]

3_التحويل الإلكتروني للأموال : يعرف على أنه :" عقد بين الأمر بالتحويل المصرفي و البنك مصدر الحوالة، يلتزم بموجبه البنك بأن يدفع بنفسه أو بواسطة غيره مبلغا من النقود يعادل قيمة الحوالة إلى المستفيد من الحوالة مقابل عمولة متفق عليها".[2]

بحيث بعد عملية إيداع النقود بالطرق المشروعة و القانونية على مستوى أحد البنوك، هنا يقوم مبيض الأموال بتحويلها مرة أخرى إلى حساب إحدى شركات المراجعة المالية في دولة أخرى خارجية يسري فيها نظام السرية المصرفية بحيث تمنع الغير من الإطلاع على دفاتر المصارف الحسابات داخل البنوك، و كذا يضمن سرية حقيقة عملاء البنك. و يتم بعد عملية الإيداع، قيام شركات المراجعة بالاقتراض من البنك الذي سبق إيداع الأموال فيها، بهدف إرجاع الأموال إلى المهربين لكن بعد تبييضها[3].

4_البطاقات الذكية : "بطاقات بلاستيكية أو ورقية مصنوعة من مادة يصعب العبث بها، تصدرها جهة البنك أو شركة استثمار، يذكر فيها اسم العميل الصادرة لصالحه و رقم حسابه، حيث يملك الحامل تقديم تلك البطاقات للتاجر لتسديد ثمن مشترياته، يقوم هذا الأخير بتحصيل تلك القيمة من الجهة المصدرة التي تقوم بدورها بإستيفاء تلك المبالغ من الحامل" [4].

5_أجهزة الصراف الآلي : يقوم مبيضو الأموال بصرف الأموال عن طريق ماكينات الصراف الآلي الخاصة بكل مصرف من أي بلد أجنبي، ثم يقوم فرع المصرف الذي سحب المال من جهازه بطلب تحويل للمبلغ من فرعه مصدر البطاقة، و يحول هذا الأخير تلقائيا بالتحويل، و تخصم القيمة على حساب عميله الذي يكون قد تهرب من كافة القيود المفروضة على التحويلات [5].

[1]-ط/د.منزول يمينة، المرجع السابق، ص271.
[2]-أنظر: عيسى لعلاوي، عبد العزيز خنفوسي، وسائل الدفع الإلكترونية المستحدثة في إطار تسهيل خدمات المعاملات المالية الرقمية، مجلة منازعات الأعمال، العدد التاسع عشر، 2016، ص135.
[3]-ط/د.منزول يمينة، المرجع السابق، ص271.
[4]- جلال عايد الشورة، وسائل الدفع الإلكتروني، جامعة عمان العربية الدراسات العليا، رسالة ماجستير، 2005، ص5.
[5]- نادية عبد الرحيم، أمين بن سعيد، المرجع السابق، ص31.

6_الشيك الإلكتروني : يعرف بأنه سند مكتوب تحت شروط شكلية، استقر عليها العرف التجاري، و يتضمن ثلاث أطراف، أمر صادر من صاحب الشيك (الساحب) إلى البنك أو المصرف (المسحوب عليه) بدفع مبلغ معين من المال إلى شخص آخر(المستفيد). بحيث يعتبر بديل الشيك الورقي وهو معالج إلكترونيا سواء بشكل كلي أو جزئي.

الفرع الثالث : أركان جريمة تبييض الأموال الرقمي والعقوبة المقررة لها.

إن جريمة تبييض الأموال على مستوى البيئة الرقمية لها أركان كما هو الحال لجريمة تبييض الأموال التقليدية،لذا بعد التطرق إلى أركان هذه الجريمة، سنرى ما العقوبة المقررة لها.

أولا : الركن المادي.

يتجسد الركن المادي لهذه الجريمة في ثلاث عناصر :

وجود جريمة أولية سابقة و المتمثلة في مصدر الأموال القذرة، و قيام الجاني بارتكاب نشاط إجرامي يتحقق به تبييض هذه الأموال غير المشروعة، و يكون هذا النشاط إما من خلال العمليات المالية و التجارية، سواء بسيطة كانت أم مركبة، بهدف إضفاء صفة المشروعية على هذا المال[1].

ثانيا: الركن المعنوي.

أما بالنسبة للركن المعنوي، فإنه يتجلى في عنصرين، أولهما، علم الجاني بالسلوك الإجرامي و الثاني هو إرادته في التوصل إلى النتيجة الإجرامية و تحقيقها من خلال إضفاء صفة الشرعية على الأموال غير المشروعة للأساليب.

ثالثا: العقوبة المقررة لهذه الجريمة.

1_يعاقب كل من قام بتبييض الأموال بالحبس من خمس (5) سنوات إلى عشر (10) سنوات، وبغرامة حدها الأدنى 1.000.000دج وحدها الأقصى 3.000.000دج.

2_ كما يعاقب على فعل الشروع والمحاولة في ارتكاب هذه الجريمة بالعقوبة المقررة للجريمة التامة.

[1]- بن نقي سفيان، المرجع السابق، ص158.

3_ أما إذا ارتكبت الجريمة من طرف الشخص المعنوي، فإنه يعاقب بما يلي:

_غرامة لا تقل عن أربع (4) مرات الحد الأقصى للغرامة المنصوص عليها لهذه الجريمة.

_مصادرة كل من الممتلكات والعائدات التي تم تبييضها، وكذا الوسائل المعدات التي استعملت في ارتكاب الجريمة.

_ في حالة تعذر تقديم أو حجز الممتلكات محل المصادرة، تحكم الجهة القضائية المختصة بعقوبة مالية تساوي قيمة هذه الممتلكات.

_كما يمكن للجهة القضائية أن تقضي عقوبة إضافة إلى ذلك، وتتمثل العقوبة إما بالمنع من مزاولة نشاط مهني أو اجتماعي لمدة لا تتجاوز خمس (5) سنوات. أو حل الشخص المعنوي.

المبحث الثاني: الآليات الإجرائية للكشف عن جرائم الأعمال الرقمية وكيفية إثباتها.

بعد التحول الرقمي الذي شهدته الجرائم الرقمية في مجال الأعمال و تنوعها، كان لابد من وضع قواعد خاصة للكشف عن الجرائم الإلكترونية و التي لا تنطبق عليها الإجراءات التقليدية، الأمر الذي جعل محل إثبات هذه الجرائم يختلف هو الآخر عن المحل التقليدي. وعليه سنتطرق إلى الآليات الإجرائية للكشف عن جريمة الأعمال الرقمية (المطلب الأول)، و الدليل الرقمي كمحل لإثبات هذه الجرائم (المطلب الثاني)، و مدى حجيته (المطلب الثالث).

المطلب الأول : الآليات الإجرائية للكشف عن جرائم الأعمال الرقمية.

كأول خطوة لتطبيق القواعد القانونية على جرائم الأعمال الرقمية، لابد من تطبيق مجموعة من الإجراءات المستحدثة للكشف عنها أولا، و التي كان لزاما على تطور هذه الإجراءات، لعدم تطابق و كفاية الإجراءات التقليدية للوصول إلى الدليل و كشف ملابسات الجريمة الإلكترونية، و سنعالج من خلال هذا المطلب أهم الإجراءات المتبعة للكشف عن هذا النوع من الجرائم، والمتمثلة في التفتيش الإلكتروني (الفرع الأول)، والإجراءات المستحدثة (الفرع الثاني).

الفرع الأول : التفتيش كإجراء أولي لضبط الدليل الرقمي.

يعتبر التفتيش من إجراءات التحقيق و ضبط الدليل المعتمد في إرتكابها و الذي يهدف إلى كشف ملابسات الجريمة، و الذي تقوم به جهة مختصة خولها القانون للقيام به. بحيث لا تقوم إجراءات التفتيش إلا تحت مجموعة من الشروط الموضوعية و الشكلية، و هذا لضمان إتمامه وفق حدود القانون.

أولا: تعريف التفتيش الإلكتروني وضوابطه.

سنتطرق أولا إلى تعريف التفتيش الإلكتروني، ثم إلى شروطه الموضوعية والشكلية.

1_تعريف التفتيش الإلكتروني.

لا يختلف التفتيش في مدلوله القانوني على ما هو سائد في فقه الإجراءات الجزائية، رغم الاختلاف الوارد على محل التفتيش. و يعرف بأنه إجراء من إجراءات التحقيق، تقوم به سلطة مختصة للدخول إلى نظم المعالجة الآلية للبيانات، بما ذلك المدخلات و التخزين و المخرجات

لأجل البحث فيها عن أفعال غير مشروعة مرتكبة، و التي تشكل سواء جنحة أو جناية، و كذا من أجل الحصول على أدلة لإثبات الجريمة.[1]

كما يناط به أيضا، أنه البحث عن الوسيلة المستخدمة في إثبات الجريمة. و بما أن المعلوماتية تتضمن كيانات مادية و أخرى معنوية، فهذا يعني أن هناك نوعين من التفتيش، يتمثل الأول في تفتيش الكيانات المادية، و الذي يشمل كل كيان ذو طابع ملموس مرتبط بالجريمة، يشترط أن يتم أولا تحديد المكان المتواجد فيه هذا الكيان، مع تبيان ما إذا كان المكان عام أو خاص[2].

أما النوع الآخر فهو تفتيش الكيانات المعنوية، هنا اختلف الفقه القانوني حول جواز خضوع المعدات المعنوية للتفتيش، لذا يبقى هذا الأمر راجع للمشرع حول نصه صراحة على إمكانية تفتيش المعدات المعنوية للحاسوب.[3]

2_ضوابط التفتيش الإلكتروني.

يخضع التفتيش كغيره من الإجراءات إلى شروط و ضوابط معينة، و إلا فإنه يعتبر أمر مخالف للقانون. و هي نوعان، ضوابط موضوعية و أخرى شكلية.

أ_الضوابط الموضوعية لإجراء التفتيش: و التي تتمثل في سبب التفتيش و محله، و الجهة المختصة بهذا الإجراء.

_**سبب التفتيش** : يعتبر السبب الشرط الأول و الأساسي للقيام بإجراء التفتيش و ضمان مشروعيته، و الذي يقوم بمجرد تحقق المبررات التالية :

_وقوع جريمة إلكترونية تصنف إما جناية أو جنحة، بحيث لا تدخل المخالفات ضمن دائرة التفتيش لعدم خطورتها.[4]

[1]-محمودي سميرة، خصوصية طرق الإثبات الجزائي في الجريمة الإلكترونية،

[2]-د.مجدوب نوال، آليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، الصادرة عن معهد الحقوق و العلوم السياسية بالمركز الجامعي آفلو،المجلد السادس، العدد 01، 2023، 195.

[3]- بن طالب ليندا، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية و السياسية، الصادرة عن كلية الحقوق و العلوم السياسية جامعة الوادي، الجزائر، العدد 16، جوان 2017، ص490.

[4]- د.مجدوب نوال، المرجع السابق، ص196.

_إتهام شخص أو أشخاص معينين، سواء بوصفهم فاعلين أصليين أو شركاء في الجريمة، أو حيازتهم لأشياء يمكن اعتبارها قرائن للتبرير بإحدى الأفعال المجرمة إما الإرتكاب أو المشاركة، و التي تسمح بتفتيشهم سواء لمتلكاتهم أو أجهزتهم[1].

_توافر قرائن و دلائل قوية و التي تؤكد على وجود أشياء في محل الجريمة تفيد في التحقيق و الكشف عن الحقيقة[2].

_محل التفتيش :

و المقصود به في الفضاء الإلكتروني، الوسيلة المعتمدة في ارتكاب الجريمة، و يتمثل في نظام الحاسب الآلي سواء بمكوناته المادية أو المعنوية، أو شبكات الاتصال التي تشمل مزود الإعلام الآلي و مكونات الحاسوب، أو المستندات الإلكترونية [3].

_السلطة الخاصة و المكلفة بالتفتيش :

باعتبار أن إجراء التفتيش سواء في الجريمة بصورتها العادية أو الإلكترونية، مخول إلى الجهات الخاصة بالتحقيق، غير أنه حرصا على تسهيل و سرعة اتخاذ أعمال التحقيق، فإن المشرع أجاز لسلطة التحقيق تكليف أعوان الضبطية القضائية للقيام بإجراء التحقيق.

و عليه فإنه يمكن لسلطة التحقيق القيام بالتحقيق بنفسها، أو عن طريق الإنابة، أو الاستعانة بخبير في المجال المعلوماتي على أن يحرص على اتخاذ التدابير اللازمة لحماية المعطيات المعلوماتية.[4]

[1]- مخلوف علمي، بو محراث ليندة، ضوابط التفتيش في الجرائم الإلكترونية، مجلة المعيار، الصادرة عن كلية أصول الدين، جامعة قسنطينة، الجزائر،المجلد الثامن وعشرون، العدد الأول، 2024، ص394.

[2]- مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية –جامعة محمد خيضر بسكرة-، العدد الثاني وعشرون، ص237.

[3]- د.مجدوب نوال، المرجع السابق، ص196.

[4]- بن خليفة إلهام، التفتيش كإجراء تقليدي لجمع الأدلة المتصلة بتكنولوجيا المعلومات، المجلة الدولية للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، 2020، ص33.

ب_الضوابط الشكلية للتفتيش :

إضافة إلى الشروط الموضوعية، أوجب المشرع شروط شكلية و إجراءات يلزم احترامها في القيام بإجراء التفتيش، و هذا ضمانا للوصول إلى نتائج دقيقة، و كذا ضمان حماية المتهم.

_احترام الميعاد الزمني للتفتيش :

جاء في قانون الإجراءات الجزائية في المادة 47 أنه: "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساءا.."، هنا يتضح الوقت المسموح للقيام بإجراء التفتيش، إلا أنه يوجد حالات استثنائية يجوز فيها الخروج عن هذه القاعدة.

و هذا ما وضحته نفس المادة، و مثال ذلك جرائم الأموال، الجرائم الماسة بأنظمة المعالجة الآلية خاصة و أن هذه الجرائم سهلة الإتلاف، ففي حالة ما إذا تسربت معلومات حول إجراء التفتيش إلى المتهم، فإنه بالتأكيد سيسعى إلى محو كلي أو جزئي لتلك المعطيات، و التي تعتبر دليلا بالتأكيد، لهذا أجاز المشرع القيام بإجراء التفتيش في كل ساعات الليل و النهار.

_وجود إذن التفتيش :

يلزم وجود إذن سابق لمباشرة التفتيش فيما يخص الجرائم الإلكترونية، باعتبار أنه يمس خصوصية الأشخاص من جهة، و احتمال استمرارية الجريمة و إمكانية ارتكابها في أي وقت من جهة أخرى[1].

بحيث نص المشرع الجزائري في قانون الإجراءات الجزائية(06_22) في المادة 44 ، على أنه لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص المراد تفتيشها إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق، على أن يتم استظهاره قبل الدخول إلى المنزل و الشروع في التفتيش، على أن يتضمن هذا الإذن بيان وصف الجرم موضوع البحث عن الدليل، و كافة البيانات الخاصة بالمكان محل التفتيش، و إلا يبطل إجراء التفتيش.

[1]- د.مجدوب نوال، المرجع السابق، ص 197.

أما فيما يخص وجوب حضور المتهم، فرغم أن القاعدة العامة تستلزم حضور المتهم أثناء التفتيش تحت طائلة البطلان، إلا أنه عندما يتعلق الأمر بالجرائم الإلكترونية، فإن المشرع قد خرج عن هذه القاعدة، حيث أقر و أجاز لأعوان الضبطية القضائية بمباشرة إجراء التفتيش دون قيد حضور المتهم، أو من ينوب عليه، لكنه اشترط بالتقييد و الحفاظ على السر المهني.

_تحرير محضر التفتيش :

لم يحدد المشرع الجزائري شروط محضر التفتيش في البيئة الإلكترونية، و تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي، و التي تعتبر كوسيلة إثبات على وقوع الجريمة و على مرتكبها أيضا. و تعرف المحاضر على أنها وثائق مكتوبة يحددها ضباط الشرطة القضائية أثناء ممارسته لمهامه،بحيث تضم ما تم معاينته من طرفه، و كذا ما قام به من عمليات و تلقى من صلاحيات[1].

ثانيا : ضبط الأدلة في جرائم الأعمال الإلكترونية .

يعتبر الضبط من إجراءات جمع الأدلة، فهو ذلك الأثر الذي يكتمل به إجراء التفتيش، و تعرف هذه العملية بأنها وضع اليد على الأشياء و الوسائل المعتمدة في ارتكاب الجريمة، و التي تساهم في الكشف عن الحقيقة، ووضعها في إحراز مختومة تقدم أمام القضاء كدليل للإثبات . و قد تكون هذه الوسائل المضبوطة إما مادية مثل بطاقة الائتمان، جهاز الحاسب الآلي و ملحقاته...، أو معنوية مثل البرامج المعالجة آليا، المراسلات الإلكترونية، البريد الإلكتروني المتواجد فيه الدليل[2]....

و عليه فإنه إذا تم ضبط دليل رقمي، فكأول إجراء يتم القيام به من طرف السلطة المباشرة للتفتيش هو الحجز، ففي حالة ما إذا كان ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون

[1]- عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلومات، مجلة دائرة البحوث والدراسات القانونية والسياسية ، الصادرة عن مخبر المؤسسات والنظم السياسية، العدد الرابع، جانفي 2018، ص59.

[2]- د.مجدوب نوال، المرجع السابق، ص198.

قابلة للحجز و الوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وهذا ما جاءت به المادة 6 في فقرتها الأولى من قانون 09-04[1].

و في كل الحالات، على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية ، كما أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستعمال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

في حالة استحال قيام السلطة المكلفة بالتفتيش إجراء الحجز وفق ما تم ذكره سابقا، لأسباب تقنية فإنه يتوجب عليها استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تتضمنها المنظومة المعلوماتية أو نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

أما بالنسبة للمعطيات المحجوزة ذات المحتوى المجرم، فإنه يمكن للسلطة التي تباشر التفتيش الأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على هذه المعطيات.

و عليه فإنه تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، فإنه لا يجوز استعمال المعطيات المتحصل عليها من الإجراءات السابقة لأي غرض، ما عدا إذا تعلق الأمر بالتحريات و التحقيقات القضائية.

الفرع الثاني : الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية.

قام المشرع باستحداث قواعد إجرائية إضافة إلى الإجراءات السابقة مساعدة و تسهيلا للجهات المكلفة بالتحقيق حول الجريمة الإلكترونية بصفة عامة، و التمكن من ضبط الدليل الرقمي.

أولا : التسرب الإلكتروني.

تطرق المشرع الجزائري لهذا الإجراء، في قانون الإجراءات الجزائية رقم 06_22[2]، تحديدا في نص المادة 65 مكرر 12، بحيث عرفه بأنه :"قيام ضابط أو عون الشرطة القضائية، تحت

[1]- قانون رقم 09-04، سالف الذكر.

[2]- قانون رقم 22-06 سالف الذكر.

مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك". مثال ذلك،كأن يقوم بانتحال صفة شخص ما عن طريق استخدام أسماء و معلومات وهمية تظهر و كأنها حقيقية، سعيا إلى الكشف عن الجريمة.

و قد أجاز المشرع من خلال المادة 65 مكرر 14 ق.إ.ج للضابط أو العون المتسرب، حيازة أموال أو وثائق متحصل عليها أو المستعملة في ارتكاب الجرائم، و كذا وضع تحت تصرف مرتكبي هذه الجرائم كل الوسائل المادية ذات الطابع المالي أو وسائل النقل أو الاتصال، من أجل تنفيذ و إنجاح العملية. لكن دون أن يكون المتسرب مسؤولا جزائيا عن القيام بهذه الأفعال.

يقتضي اللجوء إلى هذا الإجراء الإلتزام و التقيد بالشروط التالية :

1_صدور إذن قضائي بالتسرب : لا يجوز لضابط أو عون الشرطة القضائية اللجوء إلى عملية التسرب إلا بإذن صادر عن وكيل الجمهورية أو قاضي التحقيق، حسب الحالة، و هذا ما جاءت به المادة 65 مكرر 11 ق.إ.ج ،شرط أن يكون الإذن مكتوبا و ليس شفهيا و إلا اعتبر باطلا .

2_احترام المدة المقررة للتسرب : حدد المشرع من خلال الفقرة 3 من المادة 65 مكرر 15 ق.إ.ج ، أنه لا يمكن أن تتجاوز مدة التسرب أربعة (4) أشهر، و هي قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية و الزمنية، كما يجوز للقاضي الذي رخص بإجراء عملية التسرب، الأمر بوقفها في أي وقت قبل انقضاء المدة القانونية المحددة.

3_تسبيب عملية التسرب : يعد التسبيب شرط جوهري لمشروعية عملية التسرب، لذلك اشترط القانون على السلطات المختصة عند إصدار الإذن بالتسرب، ذكر السبب الحقيقي الذي يبرر اللجوء إلى هذه العملية، و هذا تحت طائلة البطلان[1].

4_محل التسرب : بمعنى وجود جريمة معينة، ينصب عليها إجراء التسرب، و المنصوص عليها في المادة 65 مكرر5 ق.إ.ج، إلا أنه عندما يتعلق الأمر بالجرائم الإلكترونية الواقعة على قطاع

[1]- ديب كمال، مكافحة الجريمة المعلوماتية في التشريع الجزائري، ندوة وطنية، جامعة الجزائر 1، 12 نوفمبر2019، مداخلة منشورة في كتاب الجريمة المعلوماتية، ص415.

الأعمال، فإنه هنا نحصر فقط جرائم تبييض الأموال، و تلك الماسة بأنظمة المعالجة الآلية للمعطيات، و المذكورة في هذه المادة.

ثانيا : اعتراض المراسلات و المراقبة الإلكترونية و المراقبة الإلكترونية.

يقصد باعتراض المراسلات، تسجيل أو نسخ المراسلات التي تكون في صورة بيانات قابلة للإنتاج و التوزيع، التخزين، الاستقبال و العرض، و التي تتم عبر وسائل الاتصال السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و ضبط الأدلة الخاصة بها.[1]

و من خلال المادة 65 مكرر 5 من قانون 06_22[2] ، نرى أن المشرع الجزائري قد أجاز لسلطات التحقيق و الاستدلال باللجوء إلى إجراء اعتراض المراسلات السلكية و اللاسلكية و كذا تسجيل المحادثات و الأصوات، مع الاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل ضبط ملابسات الجريمة، و إثباتها دون التقيد بإجراء التفتيش المألوف[3].

و يمكن أن تتم عملية المراقبة الإلكترونية بإنشاء صندوق بريدي إلكتروني مستنسخ لمراقبة المشتبه به،و يتم تحويل الرسائل الصادرة عنه تلقائيا إلى الصندوق، و من خلال الاعتراض يمكن تحديد المعلومات التي اطلع عليها و كذا المواقع التي دخل إليها، كما يتم أيضا رصد نشاطات المجرمين الخطيرين أو شبكات إجرامية منظمة من خلال المراقبة المباشرة من قبل جهاز متخصص كالمراكز المتصلة بمراكز الاعتراض عبر الاتصالات، و كما يمكن أيضا استغلال الكاميرات الخاصة بحاسوب المجرم لنقل كل ما يقوم به صوتا و صورة[4]. كما نرى أن المشرع الجزائري لم يعتبر إجراء مراقبة الاتصالات كإجراء تحقيق، بل أجاز و أعطى تصريح للجهات القضائية باللجوء للاعتراض للوقاية من الجرائم الإلكترونية [5]و الذي أنشأ هيئة بموجب قانون 09-04 مكلفة بعمليات الوقاية من الجرائم المتصلة بالإعلام و الإتصال[6].

---

[1]- ديب كمال، المرجع السابق، ص411.

[2]- القانون رقم 06-22 سالف الذكر.

[3]- ديب كمال، المرجع السابق، ص412.

[4]- حسين طاهري، الجرائم الإلكترونية، دار الخلدونية للنشر والطباعة، القبة القديمة –الجزائر-، الطبعة الأولى، 2022، ص435.

[5]- د.مجدوب نوال، المرجع السابق، ص203.

[6]- أنظر المادة 13 و14 من قانون 09-04، سالف الذكر.

إلا أنه من جهة أخرى، نجد أن المشرع الجزائري قد أحاط هذا الإجراء بجملة من الشروط و الضوابط، كغيرها من الإجراءات، و المتمثلة في مايلي :

1_ **وجود إذن مكتوب: وهو** صادر عن وكيل الجمهورية أو قاضي التحقيق، يحدد فيه الجريمة محل الإجراء، طبيعة المراسلة، أو الاتصال محل المراقبة، و يتم هذا الإجراء تحت الإشراف المباشر للسلطة المصدرة للإذن[1].

2_**ضرورة الاعتراض لإظهار الحقيقة**: و الذي يعتبر سندا قانونيا يبرر إجراء الاعتراض، نظرا لاعتداء هذا الإجراء على سرية الاتصالات[2].

3_ أن يتم الإجراء على الجرائم التي يجوز فيها إجراء الاعتراض، و التي حصرها المشرع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[3]

4_ الالتزام بالسر المهني، و كذا المدة المحددة للاعتراض، و هي (4) أشهر قابلة للتجديد.

5_ **تحرير محضر حول عملية الاعتراض**: و الذي يحمل كل تفاصيل عملية الاعتراض ومعلوماتها من بدايتها إلى نهايتها.[4]

ثالثا: الحفظ أو الإفشاء العاجلان للمعطيات الإلكترونية :

يعتبر الحفظ و الإفشاء من الإجراءات المستحدثة التي تساهم في الوصول إلى الدليل الرقمي، بحيث نصت عليها المادة 10من قانون 09_04[5] المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال وكافحتها، و يقوم بهذا الإجراء مقدمو خدمات الأنترنت، بحيث يقومون بالحفظ عن طريق الحيازة بالأرشيف لضمان حماية المعطيات التي يمكن تجريدها من صفتها لأنها كانت على شكل مخزن سابقا، و هذا وفقا للنماذج المناسبة لوضع عملية الحفظ و موقع التنفيذ[6].

سنرى المعطيات محل التحفظ، و الشروط اللازم مراعاتها خلال عملية حفظ المعطيات.

---

[1]- ديب كمال، المرجع السابق، ص413.

[2]- المرجع نفسه، ص413.

[3]- المادة 65 مكرر 5، قانون 06-22، سالف الذكر.

[4]- ديب كمال، المرجع السابق، ص413.

[5] القانون 09-04 السالف الذكر.

[6]- د.مجدوب نوال ، المرجع السابق، ص 204.

1_المعطيات محل التحفظ :

حدد المشرع من خلال المادة 11 من قانون 09_04[1] ،المعطيات التي يتعين على مقدم الخدمات التحفظ عليها، و التي تتمثل فيما يلي :

_المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

_المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

_الخصائص التقنية و كذا تاريخ و وقت و مدة كل اتصال.

_المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

_المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال و كذا عناوين المواقع المطلع عليها.

2_ الضوابط الواجب مراعاتها خلال عملية حفظ المعطيات :

يلزم على مقدم خدمة الأنترنت احترام الضوابط المحددة قانونا و المتمثلة فيما يلي :

_احترام المدة الزمنية المقررة لعملية الحفظ، و المحددة بسنة واحدة،ابتداءا من تاريخ التسجيل، و بعد انتهائها يقوم مقدم الخدمة بسحب هذه المعطيات فوريا حتى يمنع الإطلاع عليها.[2]

_الالتزام بكتمان سرية العمليات المنجزة بطلب المحققين، و كذا المعلومات المتصلة بها، و هذا لضمان حماية المعطيات، و تجنب تغيير البيانات الخاصة بها من طرف أشخاص[3].

_الإفشاء العاجل لمعطيات السير وفقا لما هو منصوص عليه بموجب المادة 10 من قانون 09-04[4].

[1] القانون 09-04 السالف الذكر.
[2]- المادة 11، قانون 09-04، سالف الذكر.
[3]- يراجع المادة 10 فقرة 2من القانون09-04 السالف الذكر.
[4] يراجع المادة 10 من القانون 09-04 السالف الذكر.

المطلب الثاني: الدليل الرقمي كمحل للإثبات.

نظرا للخاصية التي تتميز بها الجرائم الإلكترونية بصفة عامة عن نظيرتها التقليدية، سواء من حيث الوسائل، المحل أو الإجراءات، كان لابد من ظهور نوع جديد من الأدلة ليتماشى مع طبيعة الجرائم الإلكتروني، وفي مجال الأعمال بصفة خاصة. والذي تختلف إجراءات الحصول عليه كما تم التطرق إليه سابقا. لذا سنتعرف على الدليل الرقمي وخصائه (الفرع الأول)، إضافة إلى ذلك صوره وشروط قبوله أمام القضاء كمحل للإثبات (الفرع الثاني).

الفرع الأول: تعريف الدليل الرقمي ومميز اته.

يتمتع الدليل الرقمي بمجموعة من الخصائص التي تميزه عن الدليل التقليدي المتعارف عليع.

أولا_ تعريف الدليل الرقمي:

لم يرد لا عن المشرع الجزائري ولا التشريعات المقارنة أي تعريف خاص بالدليل الرقمي.

إلا أنه وردت تعريفات أخرى مختلفة، بحيث يعرف على أنه:" الدليل المأخوذ من أجهزة الكمبيوتر، والذي يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور ... من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون[1]".

كما يعرف أنه:" الدليل الذي يجد له أساسا في العالم الإفتراضي إلى الجريمة[2]".

والدليل الرقمي هو مكون رقمي لتقديم معلومات على أشكال مختلفة كالرموز، الصور..، يعكس ويعبر عن فكر وقول يسمى بالكتابة الرقمية، والتي تشمل التي تتم عبر وسائل الإتصال الحديثة بغض النظر عن الوسيلة المستخدمة في تثبيتها[3].

[1]- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والظانترنت، دار الكتب القانونية، مصر، 2006، ص88.

[2]- عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، 2004، ص969.

[3]- د.بن الطيبي مبارك، د.رحموني محمد، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، المجلد الخامس، العدد الثاني، 2019، ص23.

ويتشابه الدليل الرقمي مع البرنامج المعلوماتي من حيث الشكل الرقمي، وطبيعتهما..، إلا أنهما يختلفان من حيث الوظيفة، فالبنسبة للبرنامج فإن دوره يختص في تشغيل الحاسوب، كما يوجد نوع من البرامج الذي يساهم في الحصول على الدليل الرقمي كبرنامج النسخ. أما الدليل الرقمي فدوره يتجلى في إثبات الجريمة المعلوماتية ونسبتها إلى من ارتكبها[1].

ثانيا: خصائص الدليل الرقمي:

يختلف الدليل الرقمي عن الدليل الجنائي التقليدي من عدة جوانب، نظرا للبيآة الإلكترونية التي يتمبز بها، لذا سنتطرف إلى الخصائص والمميزات التي يختص بها الدليل الرقمي:

1_الدليل الرقمي غير ملموس: أي أنه ليس للدليل الرقمي حيز مادي عكس الدليل التقليدي، إلا أنه يمكن ترجمته وإخراجه على شكل مادي ملموس، لكن هذا لايعني أن هذا الشكل المادي هو الدليل، بل هي مجرد عملية نقل لتلك المجالات من صورتها الرقمية إلى هيئة يمكن الإستدلال بها على معلومة معينة[2].

2_دليل علمي وتقني: يتكون الدليل الرقمي في أصله من بيانات ذات طابع إلكتروني غير مادي وغير ملموس، محلها أجهزة ومعدات الحاسب الآلي، وتدرك بواسطة هذه الأجهزة أو بالإستعانة بنظم برامجية حاسبية. هذا مايجعل منه دليلا علميا وذو طابع تقني حديث[3].

3_دليل متطور: يمتاز الدليل الرقمي بتطور تلقائي نظرا لتطور البيئة الرقمية التي تقوم على التجدد و الإستمرارية، كما أنه يتميز بطبيعة ديناميكية فائقة السرعة متعدية لحدود الزمان و المكان[4]. بحيث يساهم في تمكين المحققين من استغلال الأدلة على مستوى عالمي حسب موقع مسرح الجريمة في إطار تبادل المعلومات بين الدول بسرعة عالية[5].

4_ دليل قابل للإسترجاع : بحيث يمكن استرجاعه اذا تم حذفه، لأن الملفات المحذوفة تبقى لمدة من الزمن يمكن استردادها، ولأن الأثر الرقمي لا يمكن اخفاؤه بالكامل. كما أن للدليل المسترجع

---

[1]- عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، الكيفان، تلمسان، الجزائر، 2021، ص105.

[2]- المرجع نفسه، ص106.

[3]- عيدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائب والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، المجلد الحادي عشر، العدد الأول، 2019، ص138.

[4]- المرجع نفسه، ص138.

[5]- حسين طاهري، المرجع السابق، ص268.

نفس القيمة العلمية و القانونية و الثبوتية مما يشكل ضمانة قوية لحمايته من الإتلاف أو الفقدان[1].

الفرع الثاني : تقسيمات الدليل الرقمي و صوره.

أولا : تقسيمات الدليل الرقمي :

يشمل الدليل الرقمي كل المعلومات الرقمية بمختلف اشكالها و صورها، مما يجعل من وجود اختلاف حول تحديده و تقسيمه، بحيث تم الإعتماد على ثلاث معايير، موضحة كالتالي :

1_تقسيم الدليل الرقمي على أساس مصدره : يعتبر النظام المعلوماتي من مصادر الدليل الرقمي، و هذا يستخلص من التعريف الوارد في وثيقة المبادئ التوجيهية للجنة وزراء أوروبا و المصادق عليها بتاريخ 30_01_2019 ، و الذي عرفته أنه أي دليل ناشئ عن البيانات المنتجة من جهاز يعتمد تشغيله على البرامج أو البيانات المخزنة أو المنقولة على شبكة معلوماتية، و من أهم الوسائل التي يستخلص من الدليل الرقمي و الخاصة بالنظام المعلوماتي هي الأقراص الصلبة، الكاميرات أو الماسحات الضوئية المرتبطة بالحاسوب، و كذا كل أوعية التخزين الخارجية للبيانات كبطاقات الذاكرة. بما في ذلك أيضا الملفات المخزنة بالنظام المعلوماتي و البريد الإلكتروني، و من خلال فحص بروتوكولات الأنترنت أيضا[2].

2_تقسيم الدليل الرقمي على أساس طبيعة مخرجاته : تعرف مخرجات الحاسوب على أنه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات، و المتضمن لمعلومات معينة مسجلة عليه، و يكون إما معدا للإستخدام بواسطة نظام المعالجة الآلية للمعطيات أو مشتقا من هذا النوع[3].

و يقسم إلى ثلاث أنواع و هي :

أ_**مخرجات ذات طبيعة ورقية:** تسجل فيها المعلومات على الورق بواسطة الطابعات، و كذا طباعة الرسومات بدرجات مختلفة واضحة على الورق.

[1]- عميمر عبد القادر، المرجع السابق، ص108.
[2]- عميمر عبد القادر، ص110.
[3]-المرجع نفسه ، ص113.

ب_مخرجات ذات طبيعة رقمية: و التي تستخدم في تخزين المعلومات على الأشرطة و الأوراق المغناطيسية بدلا من الوثائق الرقمية.

ج_مخرجات مرئية : يتمثل هذا النوع في عرض المعطيات المعالجة آليا بواسطة الحاسب الآلي على شاشة صغيرة[1].

3_تقسيم الدليل الرقمي كدليل اثبات من عدمه : وهو نوعان[2]:

أ_أدلة رقمية أعدت لتكون وسيلة اثبات: قد تكون سجلات تم انشائها تلقائيا بواسطة الآلة كسجلات الهاتف، أو السجلات التي تم حفظ جزء منها بالإدخال و جزء آخر بواسطة الآلة.

ب_أدلة رقمية لم تعد لتكون وسيلة اثبات : هذا النوع من الأدلة ينشأ دون إرادة الشخص، بمعنى أن الجاني قد يترك أثرا لم يكن في الأساس راغبا لتركه.

يعد النوع الأول من هذه الأدلة أكثر أهمية كونه أعد أصلا ليكون أداة للإثبات، عكس النوع الثاني الذي لم يعد ليكون أثرا لمن صدر ضده.[3]

4_ تقسيم الأدلة على أساس وسائل تحصيله: يمكن الإعتماد أيضا إضافة إلى ماتم ذكره سابقا على مصادر أخرى لاستخلاص الدليل الرقمي، والذي يمكن أن ينتج من تسجيل الأصوات وتثبيتها كما ذكر سابقا، أو التقاط الصور من أماكن خاصة، أو ذلك الناتج عن مراقبة الإتصالات الالكترونية.[4]

ثانيا : صور الدليل الرقمي.

بعد التطرق إلى التقسيمات المعتمدة في تحديد مصادر الدليل الرقمي، يمكن تصنيفه إلى ثلاث صور رئيسية:

النصوص المكتوبة : و هي تلك التي تتم كتابتها بواسطة أداة رقمية، مثال ذلك رسائل البريد الإلكتروني، الملفات الإلكترونية، البيانات المسجلة داخل أجهزة الحاسوب.

[1]- حسين طاهري، المرجع السابق، ص266.
[2]- المرجع نفسه، حسين طاهري 267.
[3]- عميمر عبد القادر، المرجع السابق، ص115.
[4]- المرجع نفسه، ص116.

التسجيلات : كل تسجيل يتم ضبطه من خلال آلة رقمية، تتمثل في التسجيلات الصوتية على الهاتف أو الأنترنت.

الصور الرقمية : و هي عبارة عن تجسيد للحقائق المرئية، بحيث تعتبر بديل للصورة التقليدية الفوتوغرافية.[1]

و منه نرى أن المشرع الجزائري قد حافظ على البيئة التي يتواجد فيها الدليل الرقمي، و حمايته لها، من خلال اجازته لسلطات البحث و التحري بنسخ المعطيات محل البحث، على أن يضمنوا سلامتها في المنظومة المعلوماتية.[2]

و بذلك قد وسع من صور الدليل الرقمي، حيث نص على امكانية استعمال الوسائل التقنية لتشكيل المعطيات أو اعادة تشكيلها، من أجل جعلها قابلة للإستغلال في عملية التحقيق دون المساس بمحتواها.[3]

المطلب الثالث : أحكام الدليل الرقمي كدليل إثبات في جرائم الأعمال الرقمية.

يتطلب قبول الدليل الرقمي جملة من الشروط المعينة لذا سنعالج أهم هذه الشروط و الضوابط.

الفرع الأول : شروط قبول الدليل الرقمي كدليل إثبات في جرائم الأعمال الرقمية.

لا يمكن اعتبار الدليل الرقمي دليلا للإثبات إلا إذا استوفى الشروط التالية :

أولا : مشروعية الدليل الرقمي :

يقتضي قبول الدليل الرقمي أن يتم الحصول عليه وفق الإجراءات المشرعة و المنصوص عليها وفق القانون، فلا يجوز الإستناد إلا في إدانة المتهم على دليل غير مشروع تم التوصيل اليه بمخالفة الأحكام القانونية حتى و لو كان الدليل صادق فإنه يعد باطلا، فهنا يكمن دور القاضي في التأكد من هذه المسألة قبل إكمال سلطته في تقدير هذا الدليل، و هو ما يعرف بمبدأ الشرعية الإجرائية، كما يعد مشروعية الدليل الجزائي من أهم المبادئ التي تحكم الإثبات في

[1]- عميمر عبد القادر، المرجع السابق، ص 116.
[2]- المادة 6، قانون 09-04، سالف الذكر.
[3]- بحرية هارون، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري، ملتقى وطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الأنظمة المقارنة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر –بسكرة-، 16-17 نوفمبر 2015، ص06.

المواد الجزائية، و التي تدعم قاعدة شرعية التجريم و العقاب "لا جريمة و لا عقوبة و لا تدابير أمن إلا بقانون" ، فإضافة إلى تحقق شرط الحصول على الدليل الرقمي و كذا عملية تقديمه للقضاء وفق اجراءات صحيحة و سليمة قانونا، فيجب أن تكون الوسيلة المستخدمة في الإجراءات مشروعة و لا تتنافى مع ما سبق ذكره[1].

ثانيا: أن يكون للدليل الرقمي أصل في أوراق الدعوى مع عرضه في الجلسة:

على القاضي أن يبني حكمه على أسس صحيحة من أوراق الدعوى و عناصرها، و أن يكون الدليل الذي اعتمد عليه قائما في تلك الأوراق، و أن يتم عرضه في الدعوى.[2]

فلا يمكن أن يستند القاضي في حكمه على دليل لم يساهم في تكوين قناعته، أو لم يكن له أصل في أوراق الدعوى أو كان موجودا لكن لم يطلع عليه الأطراف، لأن هذا يعد اخلالا و مساسا بحقوق الدفاع المخول للأطراف[3].

ثالثا: أن يكون الدليل يقينيا :

يشترط أن يكون الدليل غير قابل للشك، و أن يكون قريبا للحقيقة قدر المستطاع، بعيدا عن الظن و هذا حتى يتمكن الحكم بالإدانة، و أن لا يكون مجال لإفتراض عكس هذا الدليل إلا عندما يصل اقتناع القاضي إلى حد الجزم و اليقين[4].

قابلية الدليل للنقاش :

أن تكون الأدلة المتحصل و المتوصل إليها، سواء من جرائم الحاسوب و الأنترنت، أو بيانات معروضة على شاشة الحاسوب أو مدرجة في حاملات البيانات، أم كانت أشرطة و أقراص ضوئية أو ممغنطة، محلا للمناقشة في الجلسة، فلا يمكن أن يؤسس القاضي قناعته إلا على العناصر التي تم طرحها و مناقشتها أمام أطراف الدعوى، ليكون المتهم على علم بالأدلة المقدمة ضده.[5]

[1]- عميمر عبد القادر، المرجع السابق، ص158.
[2]- المادة 212، قانون 22-06، سالف الذكر.
[3]- عميمر عبد القادر، المرجع السابق، ص154.
[4]- د.بن الطلبي مبارك، د.رحموني محمد، المرجع السابق، ص27.
[5]- المادة 212- الفقرة الأخيرة-، قانون 22-06، سالف الذكر.

الفرع الثاني : حجية الدليل الرقمي في اثبات جرائم الأعمال الرقمية.

تعد مرحلة الحكم بمثابة المرحلة الحاسمة في الدعوى الجنائية، لذا فإن الحكم يمثل أهم اجراءات الدعوى، و عملية تقدير الأدلة يشكل جوهر هذا الحكم، بحيث أن الدليل الإلكتروني يخضع كغيرها من الأدلة لتقدير القاضي، فالمشرع الجزائري لم يفرد نصوص خاصة تقيد القاضي مقدما بقبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، و هذا راجع لمبدأ حرية الإثبات كقاعدة عامة في المواد الجزائية، و هذا ما جاء في المادة 212 و 307 من قانون إجراءات جزائية.[1]

و بإعتبار أن الدليل الرقمي من الأدلة العلمية و التي تتطلب دراية خاصة لا يمتلكها القاضي، فإنه لا يمكن التنازع حول قيمته الإثباتية، و هذا راجع لخصوصيته من حيث القوة الإستدلالية من الناحية العلمية، حتى و إن وقع الشك حول إمكانية العبث به أو لوجود خطأ فيه، فالأمر هنا يعود للخبير، لأنه يعتبر مسأل فنية، فإذا سلم الدليل من أي عيب أو عبث فعلى القاضي هنا قبول الدليل حتى و إن لم يكن مقنعا.[2]

و عليه يمكن القول أنه لا يوجد في القانون الجزائري ما يتضمن قواعد خاصة بالدليل الرقمي، لذا فالدليل الرقمي بإعتباره من الوسائل العلمية الحديثة في الإثبات الجنائي، ولا يطرح أي إشكال من حيث اعتباره حجة، خاصة اذا تم استخلاصه وفق اجراءات و ضمانات قانونية صحيحة و فنية تضمن سلامته و صحته، حيث يخضع للإقتناع الشخصي للقاضي كباقي الأدلة المقدمة في الدعوى.[3]

[1]- د.بن الطلبي مبارك، د. رحموني محمد، المرجع السابق، ص28.
[2]- د.بن الطلبي مبارك، د. رحموني محمد، المرجع السابق، ص28.
[3]- المرجع نفسه، ص29.

خلاصة الفصل الثاني :

نستخلص من هذا الفصل، أنه تعدد و تنوع صور جرائم الأعمال لا يزال في استمرار، و هذا لحساسية هذا القطاع من حيث تعرضه للجرائم، و الذي فرضته البيئة الرقمية، مما أدى فرض تحديات على المنظومة القانونية، سواء من حيث تصنيف هذه الجرائم، أو من الوسائل و الآليات الإجرائية لمكافحتها، خاصة أنها تتخذ شكلا أكثر تعقيدا مثل جرائم تبييض الأموال، التزوير الإلكتروني، و خاصة تلك الماسة بأنظمة المعالجة الآلية التي من شأنها تهدد مواقع التجارة الإلكترونية و غيرها من الجرائم الماسة بهذا القطاع، و التي يمكن أن تتطور لشكل جرائم أخرى.

أما من حيث وسائل الإثبات، فيعتبر الدليل الرقمي محلا لإثبات الجرائم الإلكترونية بصفة عامة، و الذي له الحجية بإعتباره من الوسائل التقنية، غير أنه يلزم أن يستوفى شروطه و أن يكون صحيحا سالما من أي عبث.

الخاتمة :

بعد دراستي لموضوع جرائم الأعمال الرقمية، سواء من الجانب النظري، الذي عالجت فيه أهم ما يتعلق بهذا النوع من الجرائم، سواء من مفهومها أو طبيعتها، أو حتى خصوصيتها من حيث قواعد التجريم و المسؤولية، اضافة إلى ذلك الجهود المبذولة لمكافحتها سواء وطنيا أو حتى دوليا. و فيما يخص الجانب التطبيقي الذي تطرقت فيه إلى صور هذه الجرائم و اجراءات الكشف عنها و ضبط الدليل الرقمي، و مدى حجيته في الإثبات، توصلت إلى مجموعة من النتائج و التي سأوضحها في نقاط رئيسية مرفقة بتوصيات ، آمل أن تساهم بشكل متواضع في اثراء النقاش القانوني حول هذا الموضوع.

1_النتائج :

تبقى هذه النتائج نسبية، و التي قد تعرف تعديلات مستقبلية، نظرا للتطور الذي نشهده حاليا و كذا مع مرور الوقت، و نستخلصها فيما يلي :

_عدم اهتمام التشريعات الوطنية و حتى الدولية بما فرضته البيئة الرقمية على قطاع الأعمال.

_غياب تعريف خاص، صريح و دقيق لجرائم الأعمال في البيئة الرقمية.

_عدم وجود نصوص قانونية خاصة لتنظيم هذا النوع من الجرائم بصفة خاصة رغم حساسيتها و سرعة انتشارها في البيئة الرقمية سواء على المستوى الوطني أو حتى الدولي.

_اعتماد المشرع على القواعد العامة للجرائم التقليدية، و التي لا تتلائم مع جرائم الأعمال الرقمية.

_نقص الآليات التقنية و الإجرائية للكشف عن هذا النوع من الجرائم، بما في ذلك التحقيق و الإثبات.

_ضعف التنسيق التقني بين الجهات القضائية و كذا الأمنية في معالجة قضايا جرائم الأعمال الرقمية.

_نقص الوعي القانوني و كذا المؤسساتي بمدى خطورة هذا النوع من الجرائم، خاصة و أنه يتمتع بالإستمرارية و التجدد بسبب طبيعة البيئة الرقمية و تطورها.

2_التوصيات :

أرجو أن تساهم هذه التوصيات و لو بالقليل في تسليط الضوء على الجوانب و الثغرات الواقعة على جرائم الأعمال الرقمية، و التي استخلصتها فيما يلي :

_ضرورة مراعاة خصوصيات هذا النوع من الجرائم، و وضع تعريف مستقل لها حتى تحظى بإستقلالية عن الجرائم الأخرى كنظيرتها التقليدية.

_ضرورة تعديل بعض التشريعات، مع نص قوانين خاصة لتنظيم جرائم الأعمال الرقمية.

_تشديد الوصف الجنائي و العقوبات المقررة لجرائم الأعمال الرقمية، لتحقيق الردع و المساهمة في القضاء و الحد من هذه الجرائم.

_ضرورة مراعاة الطبيعة التي تميز هذا النوع من الجرائم و هذا تماشيا معها لسد الثغرات التي يمكن أن تعرقل الجهود المبذولة لمكافحتها.

_ضرورة ابرام إتفاقيات دولية و ملتقيات وطنية في قطاع الأعمال لتحديد إطار الإختصاص القضائي و التعاون الدولي في ما يخص هذا النوع من الجرائم.

_تشجيع الجامعات على تنظيم ندوات تعالج جرائم الأعمال الرقمية بصفة خاصة و كيفية مكافحتها.

_ضرورة نشر الوعي الرقمي لإدراك مدى خطورة جرائم الأعمال في هذه البيئة بصفة خاصة.

_تنسيق دورات تكوينية للقضاة و سلطات المصالح الأمنية بأنواعها، حول خصوصية قطاع الأعمال في البيئة الرقمية، و كيفية معالجتها، بما في ذلك التعامل مع الأدلة الرقمية و تحليلها.

قائمة المصادر المراجع :

المصادر:

1_الدستور الجزائري ، المؤرخ في 15 جمادى الاولى 1442 الموافق ل30 ديسمبر 2020، المعدل والمتمم، الجمهورية الرسمية للجمهورية الجزائرية،العدد 82.

_المعاهدات والإتفاقيات الدولية:

1_ مؤتمر الأمم المتحدة الثامن ،الجرائم ذات الصلة بالحاسوب، المنعقد في هافانا،كوبا الفترة 27 آب/أغسطس-7أيلول/سبتمبر 1900 وثيقة رقم A/CONF-144/28.

2_قرار رقم 56-121، مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الجمعية العامة،الدورة السادسة والخمسون،البند 110 من جدول الأعمال،الأمم المتحدة، 2002.

3_الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المنعقدة في 15-1-1432 الموافق ل21-12-2010، القاهرة، جمهورية مصر العربية.

القوانين:

1_القانون رقم 2000-03، المؤرخ في جمادى الأولى 1421 الموافق ل5 أوت2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية الجمهورية الجزائرية، العدد 48، الصادرة في 6 جمادى الأولى عام 1421 الموافق لـ6 أوت سنة 2000.

2_قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-156، يتضمن قانون العقوبات، الجريدة الرسمية الجمهورية الجزائرية، عدد71، الصادر بـ10 نوفمبر 2004.

3_القانون رقم 05-02 الصادر في 06 فبراير 2005، يعدل و يتمم الأمر رقم 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، و المتضمن القانون التجاري، ج.ر عدد 11 المؤرخة في 09 فبراير 2005.

4_القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل و يتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386 الموافق ل8 يونيو 1966،

المتضمن لقانون الإجراءات الجزائية، ج.ر عدد84، الصادرة في 4 ذو الحجة عام 1427 الموافق لـ 24 ديسمبر سنة 2006.

5_قانون رقم 09-04، المرخ في 14 شعبان 1430 الموافق ل5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، الجريدة الرسمية الجمهورية الجزائرية العدد 47الصادرة في 25 شعبان 1430 الموافق ل16غشت2009.

6_قانون رقم 15-04 المؤرخ في 11ربيع الثاني1436 الموافق ل1فبراير2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر العدد 06، الصادرة ب30ربيع الثاني1436 الموافق لفبراير2015.

7_قانون رقم 18-05 المؤرخ في 24 شعبان 1439 الموافق ل10 مايو 2018، يتعلق بالتجارة الإلكترونية، ج.ر العدد28، الصادرة في 30شعبان1439 الموافق ل16مايو2018.

8_قانون رقم 18-07 المؤرخ في 25رمضان1439 الموافق ل10يونيو2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر العدد 34، الصادرة ب25رمضان1439 الموافق ل10يونيو2018.

الأوامر:

1_الأمر 75-58، المؤرخ في 20 رمضان 1395 الموافق ل26 سبتمبر 1975، يتضمن القانون المدني، الجريدة الرسمية الجمهورية الجزائرية، عدد 78 الصادرة في 24 رمضان 1395 الموافق ل30 سبتمبر1975، المعدل والمتمم.

2_الأمر رقم 03-06 الؤرخ في 19جمادى الاولى1424 الموافق ل19يوليو2003، يتعلق بالعلامات، ج.ر العدد44، الصادرة ب23جمادى الاولى1424 الموافق ل23يوليو.2003

3_ الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18صفر1386 الموافق ل8يونيو1966، التضمن قانون الإجراءات الجزائية، ج.ر عدد 65، الصادرة في 17 محرم 1443 الموافق لـ 26 أوت سنة 2021.

المراجع :

المراجع العامة :

1_محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1988.

المراجع المتخصصة :

1_حسين طاهري، الجرائم الالكترونية، دار الخلدونية للنشر والتوزيع، القبة، الجزائر، الطبعة الاولى، 1444-.2022

2_أيمن عبد الله فكري، الجرائم المعلوماتية –دراسة مقارنة في التشريعات العربية والأجنبية-، الطبعة الأولى، مكتبة القانون والإقتصاد، المملكة العربية السعودية، .2014

3_فايز رضوان، بطاقات الوفاء، الطبعة الأولى، المطبعة العربية، مصر، 1990.

4_عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني، الطبعة الاولى، دار الكتب القانونية، مصر، المحلى الكبرى، .2007

5_سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الاولى، دار النهضة العربية، القاهرة، 1999.

6_محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، دون طبعة، الإسكندرية، 2004.

7_أنظر: عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، الطبعة الأولى، مكتبة شادي، القاهرة ، .2009

8_عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات، دار النهضة العربية، مصر، .2010

9_عبد الخالق سيد أحمد، الآثار الإقتصادية والإجتماعية لغسيل الأموال، دار النهضة العربية، القاهرة، مصر، 1997.

10_الدليمي –مفيد نايف-، الجدثي، غسيل الأموال في القانون الجنائي –دراسة مقارنة-، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

11_حسين طاهري، الجرائم الإلكترونية، دار الخلدونية للنشر والطباعة، القبة القديمة – الجزائر-، الطبعة الأولى، 1444-2022.

12_ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، .2006

13_عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، 2004.

14_عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، الكيفان، تلمسان، الجزائر، 2021.

15_حسين أحمد الجندي، القانون الجنائي للمعاملات التجارية –القانون الجنائي للشركات-، دار النهضة العربية، 1989.

16_حسين طاهري، الجرائم الإلكترونية، دار الخلدونية للنشر والتوزيع، القبة القديمة – الجزائر-، الطبعة الأولى.

17_د.يعيش تمام شوقي، الجريمة لمعلوماتية، دراسة تأصيلية مقارنة، مطبعة الرمال، الوادي، الجزائر، جانفي ،الطبعة الأولى، 2019.

المقالات :

1_حورية قويقح، جرائم التجارة الإلكترونية ومعوقاتها، دراسات اقتصادية، المجلد السابع عشر، العدد 1، الجزائر، .2023

2_ليلى تركي، الجرائم الواقعة على مواقع التجارة الإلكترونية في قانون العقوبات الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد التاسع، العدد الأول، جوان .2024

3_صباح عبد الرحيم، وهيبة عبد الرحيم، جرائم التجارة الإلكترونية، المجلة الدولية للبحوث القانونية والسياسية، المجد الأول، العدد الأول، .2017

4_أحمد محمد محروس عبد العال، التزوير الإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار السبعون، 2025.

5_عمارة فتيحة، جريمة التزوير الإلكتروني، مجلة القانون والمجتمع، المجلد السابع، العدد الأول، 2019.

6_خليفي فتيحة، د.مهمداوي محمد صلاح، التزوير المعلوماتي في البيئة الرقمية، مجلة الدراسات القانونية (صنف ج)، المجلد الثامن، العدد الثاني، المدية –الجزائر-، 2022.

7_د.عادل مستاري، أ.رواحنة زوليخة،جريمة التزوير الإلكتروني، مجلة العلوم الإنسانية، العدد 46، بسكرة..

8_مريم تومي، صدراتي وفاء، تزوير بطاقات الإئتمان صورة خاصة من جريمة التزوير الإلكتروني، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الخامس، العدد الثاني، الأغواط – الجزائر-، 2021.

9_علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الإئتمان الإلكترونية – دراسة مقارنة-، مجلة الحقوق، العدد الثالث، الكويت، 2013.

10_د.عمرو أحمد عبد المنعم دبش، إثبات المستندات الإلكترونية"الإثبات الالكتروني"، مجلة العلوم القانونية والاجتماعية-جامعة زيان عاشور-، الجلفة، المجلد الرابع، العدد الأول، مارس 2019.

11_راضية مشري، جريمة تزوير التوقيع الالكتروني في التشريع الجزائري، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، قالمة، العدد 20، جوان 2017، 127-

12_بدر أحمد الجاسر الراجحي، جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الكويتي، مجلة الحقوق، العدد الأول، الكويت، 2020.

13_راضية مشري، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، حوليات جامعة قالمة للعلوم الإجتماعية والإنسانية، العدد عشرون، جوان 2017.

13_د.نادية عبد الرحيم، د.أمين بن سعيد، جريمة تبييض الأموال في ظل رقمنة الخدمات المصرفية، مجلة الدراسات الإقتصادية والمالية، جامعة الشهيد حمة لخضر، الوادي –الجزائر- ، العدد العاشر –الجزء الثاني-، 2017.

14_قسمية محمد، مصادر وأساليب عمليات تبييض الأموال، مجلة الدراسات والبحوث القانونية، المجلد التاسع، العدد الأول، المسيلة-الجزائر-، 2024.

15_بن نقي سليمان، جريمة غسيل الأموال بين الوسائط الإلكترونية والنصوص التجريمية، مجلة الأبحاث القانونية والسياسية، المجلد الثالث، العدد الثاني، 2021،

16_د.علي زايد عبد الله ، غسيل الأموال عبر الوسائل الإلكترونية، القاهرة ، ص16.
Ass.Univ.Bull.Environ.Res.Vol.26NO.1March.2023.

17_ عيسى لعلاوي، عبد العزيز خنفوسي، وسائل الدفع الإلكترونية المستحدثة في إطار تسهيل خدمات المعاملات المالية الرقمية، مجلة منازعات الأعمال، العدد التاسع عشر، 2016.

18_د.مجدوب نوال، تاآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والإقتصادية، المجلد السادس، العدد الثالث، 2023.

19_بن طالب ليندا، التفتيش في الجريمة المعلوماتية، العدد واحد وعشرون، جوان 2017.

20_مخلوف علمي، بو محراث ليندة، ضوابط التفتيش في الجرائم الإلكترونية، المجلد الثامن وعشرون، العدد الأول، 2024.

21_مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية – جامعة محمد خيضر بسكرة-، العدد الثاني وعشرون، جوان 2011.

22_بن خليفة إلهام، التفتيش كإجراء تقليدي لجمع الأدلة المتصلة بتكنولوجيا المعلومات، المجلة الدولية للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، 2020.

23_د.عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلومات، مجلة دائرة البحوث والدراسات القانونية والسياسية ، مخبر المؤسسات والنظم السياسية، العدد الرابع، جانفي 2018.

24_د.بن الطيبي مبارك، د.رحموني محمد، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، المجلد الخامس، العدد الثاني، 2019.

25_عيدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، المجلد الحادي عشر، العدد الأول، 2019.

26_مونة مقلاني، راضية مشري، الجريمة الإلكترونية –دلالة المفهوم وفعالية المعالجة القانونية-، مخبر الدراسات القانونية البيئية، مجلة أبحاث قانونية وسياسية، المجلد السادس، العدد الأول، جوان 2021.

27_د.مجدوب نوال، خصوصية سياسة التجريم والعقاب في قطاع الأعمال بالجزائر، مجلة القانون والعلوم السياسية، المجلد السابع، العدد الثاني، .2021

28_ د.بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، سبتمبر 2018.

29_ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الإتجاهات الدولية في مكافحة الجريمة اإلكترونية،مجلة دراسات و أبحاث، المجلد الأول ، العدد الأول، المركز الجامعي سوق أهراس، الجزائر.

30_د.فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، الصادرة عن كلية الحقوق، جامعة حمة لخضر، الوادي، العدد الثاني، 2015.

31_قزران مصطفى، زرقين عبد القادر،الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، الصادرة عن مخبر نظام الحالة المدنية جامعة خميس مليانة، المجلد الثامن، العدد الثاني، جوان 2022.

32_فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، الصادرة عن كلية الحقوق و العلوم السياسية، تيارت، المجلد الثامن، العدد الأول،.2020

33_عصماني ليلى، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الالكتروني، مجلة القانون –المجتمع والسلطة، الصادرة عن مخبر البحث القانون، جامعة وهران2، المجلد التاسع ، العدد الثاني، 2020.

34_الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية و الاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، مخبر النظام القانوني للعقود و التصرفات في القانون الخاص، جامعة خميس مليانة، المجلد الرابع، العدد الرابع، ديسمبر 2020..

35_وريدة جندلي، التعاون الدولي لمكافحة الجريمة المعلوماتية، الفاعلية والتحديات، مجلة القانون والعلوم السياسية،المجلد العاشر، العدد الثاني، 2024..

36_عبد الحميد عمارة، نظام تسليم المجرمين في ظل التعاون القضائي الدولي، مجلة الباحث للدراسات الأكاديمية، الصادرة عن كلية الحقوق و العلوم السياسية جامعة باتنة، العدد الحادي عشر، جوان 2017.

37_رياض بركات، د.مسيكة محمد الصغير، تسليم المجرمين كآلية لتفعيل التعاون الدولي لمكافحة الجرائم المعلوماتية، مجلة الدراسات الحقوقية، الصادرة عن جامعة الدكتور مولاي الطاهر، سعيدة، المجلد الحادي عشر، العدد الأول، جوان 2024..

38_-محمد نذير بن عرفة، يوسف حوري، اليوروبول كآلية لمكافحة الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، الصادرة عن جامعة عمار الثليجي الأغواط، الجزائر، المجلد الحادي عشر، العدد الأول، جانفي 2025.

39_بن لعربي أسماء، الفحلة مديحة، مكافحة الجريمة الإلكترونية في الجزائر رؤية تشريعية واستراتيجيات عملية، المجلة الأكاديمية للبحوث القانونية والسياسية،الصادرة عن كلية الحقوق و العلوم السياسية، الأغواط المجلد التايع، العدد1، الأغواط، 2025،.

40_د.بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، سبتمبر 2018.

41_سميحة بلقاسم، حميد بوشوشة، الجريمة الإلكترونية بعد جديد في الإجرام..واقعها وآليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد العاشر، العدد الأول، جوان 2023.

42_عائشة فاضل، المسؤولية الجزائية في الجرائم الالكترونية (الجزائر نموذجا)، مجلة الحقوق والحريات، الصادرة عن مخبر الحقوق و الحريات في الأنظمة المقارنة عن جامعة بسكرة، المجلد الحادي عشر، العدد الأول، 2023.

الرسائل و الأطروحات :

1_صالح شنين، الحماية الجنائية للتجارة الإكترونية-دراسة مقارنة-، مذكرة مقدمة لنيل شهادة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2012-2013.

2_خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للمعاملات الإلكترونية في النظام السعودي-دراسة تحليلية مقارنة-،مذكرة لنيل شهادة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، 2009.

3_إلهام بن خليفة، الحماية الجنائية للمحررات الالكترونية من التزوير، أطروحة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق ، جامعة الحاج لخضر، باتنة، 2016.

4_صالح شنين، الحماية الجنائية للتجارة الإلكترونية –دراسة مقارنة-، رسالة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013.

5_جلال عايد الشورة، وسائل الدفع الإلكتروني، جامعة عمان العربية الدراسات العليا، رسالة ماجستير، .2005

6_بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، تخصص قانون عام، كلية الحقوق، جامعة الجزائر01 يوسف بن خدة، الجزائر، 2017-2018

7_توايمية ديانة ملاك، دور البطاقة البنكية في تعزيز التجارة الإلكترونية، مذكرة لنيل شهادة ماستر، قسم الحقوق –تخصص قانون أعمال-، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، الجزائر، 2021-2022.

8_محمد الشريف بولعراس، اسامة طلحي، جريمة التزوير المعلوماتية، مذكرة مقدمة لنيل شهادة ماستر، كلية الحقوق –تخصص قانون إعلام آلي وانترنت-، جامعة محمد البشير الابراهيمي-برج بوعريريج-، الجزائر، 2021-2022.

9_محمد خميخم، الطبيعة الخاصة بالجريمة الإقتصادية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في القانون الجنائي والعلوم الإجرامية، جامعة الجزائر، كلية الحقوق، بن عكنون، 2011.

مداخلات لملتقيات علمية :

1_أ.محمد خليفة، د.نصيرة مهيرة، الإجرام المعلوماتي وأثره في مجال الأعمال، ملتقى وطني حضوري/إفتراضي، جامعة بن يوسف بن خدة –الجزائر1- ، 10 نوفمبر 2022، مداخلة منشورة في كتاب جرائم الأعمال –الخصوصية والمكافحة-.

2_ط/د.منزول يمينة، جريمة تبييض الأموال باستخدام وسائل الدفع الإلكترونية، ملتقى وطني –حضوري/إفتراضي-، جامعة بن يوسف بن خدة-الجزائر 1-، 10 نوفمبر 2022، مداخلة منشورة في كتاب –جرائم الأعمال (الخصوصية والمكافحة)-.

3_ديب كمال، مكافحة الجريمة المعلوماتية في التشريع الجزائري، ندوة وطنية، جامعة الجزائر 1، 12 نوفمبر2019، مداخلة منشورة في كتاب الجريمة المعلوماتية.

4_محمودي سميرة، خصوصية طرق الإثبات الجزائي في الجريمة الإلكترونية،ندوة وطنية، مداخلة منشورة في كتاب الجريمة المعلوماتية،كلية الحقوق- جامعة الجزائر1- ، 12 نوفمبر 2019.

5_عاسية زروقي، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، ندوة وطنية، منشورة في كتاب : الجريمة المعلوماتية، جامعة الجزائر1، 12 نوفمبر .2019

6_أوشن بولرياس ليلى، خصوصيات قواعد التجريم في مادة القانون الجزائي للأعمال، ملتقى وطني حضوري/إفتراضي، مداخلة منشورة في كتاب: جرائم الأعمال –الخصوصية والحوكمة-، الجزائر 1، 10 نوفمبر 2022.

10_رضوان علي، الإطار المفاهيمي للجريمة المعلوماتية "مفهومها وسمات مرتكبيها"، ملتقى وطني، مداخلة منشورة في كتاب الجريمة المعلوماتية، جامعة الجزائر1، 12 نوفمبر2019.

مطبوعات و محاضرات رسمية :

محاضرات :

1_د.فريد روابح، مطبوعة محاضرات في القانون الجنائي العام، مقدمة لطلبة السنة ثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين –سطيف-، 2018-2019.د.حسام بوحجر، القانون الجنائي للأعمال، محاضرات ألقيت على طلبة السنة الأولى ماستر قانون أعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 – قالمة-، 2020-2021.

2_د.عثماني رضوان، الجرائم الإلكترونية، محاضرات مقدمة لطلبة السنة ثانية ماستر قانون جنائي، معهد الحقوق، المركز الجامعي صالحي أحمد، النعامة، 2024-2025.

3__بن دراج علي إبراهيم، محاضرات في الجرائم المعلوماتية، الملقاة على طلبة السنة الثانية ماستر، تخصص قانون الجنائي والعلوم الجنائية، قسم الحقوق، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، الأغواط، 2020-2021، ص39-40.

مو اقع الأنترنت :

1_محمود محمد صفاء الدين على شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، كلية الحقوق، جامعة المنوفية،. بحث على الموقع الإلكتروني: https://jslem.journals.ekb.eg

الفهرس

ملخص الدراسة:

تندرج جرائم الأعمال ضمن الجرائم المستحدثة، والتي تتميز بطابع خاص كونها جرائم خطر لا جرائم ضرر. والتي تستوجب نصوص قانوية خاصة تحكمها وتنظمها، وبالتالي التصدي لها. وهذا حماية لقطاع الأعمال بصفة عامة، وللشركات والمعاملات التجارية والمالية، وضمان الثقة المتبادلة بين أطراف هذه المعاملات بصفة خاصة.

Summary :

Digital business crimes are classified as emerging offenses that fall within the scope of crimes of result. Owing to their particular legal nature, they require the adoption of specific legislative provisions to regulate and criminalize such conduct. Addessing these offenses is essential to ensure the legal protection of the business sector at large, Including corporate entities and commercial and financial transactions, while also safeguarding the mutual trust between the parties engaged in such activities.