وزارة العليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي –تبسة–
كلية الحقوق والعلوم السياسية
قســـم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر
تخصص قانون جنائي وعلوم جنائية

أليات مكافحة الجرائم الالكترونية في التشريع الجزائري

اعداد الطـــالبة
شعبان كوثـــر

اشـــراف الاستـــاذ
جديدي طـــلال

لجنـــة المناقشـــة

الإسم واللقب	الرتبـــة العلمية	الصفـــــة
د. دنيا زاد ثابت	أستـــــاذ التعليم العالي	رئـــيســـا
د. جديدي طلال	أستـــــاذ محاضر "أ"	مشرفا ومقررا
د. جسين جفالي	أستـــــاذ محاضر "ب"	عضوا ممتحنا

السنـــــة الجامعيـــة
2025/2024~

الجمهورية الجزائرية الديمقراطية الشعبية
People's and Democratic Republic of Alegria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
جامعة الشهيد الشيخ العربي التبسي - تبسة
Echahid Cheikh Larbi Tebessi University- Tebessa
كلية الحقوق و العلوم السياسية
Faculty of Law and Political Sciences
جامعة الشهيد الشيخ العربي التبسي- تبسة
كلية الحقوق والعلوم السياسية
قسم العلوم السياسية

تبسة في: 29/06/2024

إذن بطبع مذكرة / تحرير على دعامة CD/DVD

أنا الموقع أدناه الأستاذ: ..بجيبي طاهر.....

تخصص: ..قانون جنائي وعلوم جنائية..

الرتبة العلمية: ..أستاذ محاضر أ.....

القسم: ..الحقوق.....

أرخص للطلبة:

1- ..شعباني كوثر.....

2- ...../.....

تحرير مذكرة ضمن متطلبات نيل شهادة الماستر.

تخصص : ..قانون جنائي وعلوم جنائية.... على دعامة CD/DVD

موسومة بعنوان :

..آليات مكافحة الجرائم الالكترونية في تشريع الجزائري.....".

لحساب السنة الجامعية 2024/2023

الدورة: الأولى [/] الدورة الثانية [X]

إمضاء المشرف

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
جامعة العربي التبسي - تبسة
Larbi Tebessi University - Tebessa

كلية الحقوق و العلوم السياسية
FACULTY OF LAW AND POLITICAL SCIENCES

جامعة العربي التبسي.تبسة
LARBI TEBESSI UNIVERSITY.TEBESSA

نيابة العمادة المكلفة بالدراسات والمسائل المرتبطة الطلبة

قسم القانون الخاص

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز بحث

(القرار رقم 1082 المؤرخ 27 ديسمبر 2020)

أنا الممضي أدناه، السيد (ة) : شيبان كوثر .....

الصفة: طالب ☑ أستاذ باحث ☐ باحث دائم ☐

الحامل (ة) لبطاقة التعريف الوطنية أو رخصة السياقة رقم: .....

الصادرة بتاريخ : ..... دائرة: ..... ولاية : .....

المسجل (ة) بكلية : الحقوق والعلوم السياسية قسم: الحقوق .....

والمكلف بانجاز أعمال بحث : مذكرة ماستير

تحت عنوان: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في انجاز البحث المذكور أعلاه

التاريخ: 2025/06/29

إمضاء المعني بالأمر

شيبان

وزارة العليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي –تبسة–
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص قانون جنائي وعلوم جنائية

أليات مكافحة الجرائم الالكترونية في التشريع الجزائري

اعداد الطالبة
شعبان كوثر

اشراف الاستاذ
جديدي طلال

لجنة المناقشة

الإسم واللقب	الرتبة العلمية	الصفة
د. دنا زاد ثابت	أستاذ التعليم العالي	رئيسا
د. جديدي طلال	أستاذ محاضر "أ"	مشرفا ومقررا
د. جسين جفالي	أستاذ محاضر "ب"	عضوا ممتحنا

السنة الجامعية

2025/2024~

شكر وعرفان

أحمد الله العلي القدير أن وفقني و أعانني على إتمام هذا العمل من غير حول مني و لا قوة فهو الذي له الفضل أولا وأخيرا فلله الحمد والمنة .

ألف ألف شكر لأستاذي الجليل الأستاذ : **جديدي طلال** المشرف على هذا العمل والذي لم يبخل علي طوال مدة إعداد هذه المذكرة بنصائحه القيمة وإرشاداته الصائبة وتشجيعاته المتواصلة، فله مني جزيل الشكر ووافر التقدير وعظيم الإمتنان، أطال الله في عمره وجزاه عني بخير ما جاز به عالما عن متعلم .

كما أتقدم بالشكر الجزيل لأعضاء اللجنة الموقرة

والشكر موصول أيضا لكل من أمدني بيد العون والمساعدة والنصح من أساتذي الأفاضل

وجزاهم الله عني خير الجزاء.

إهداء

إلى كل أفراد عائلتي بما رحبت .....فردا فردا

إلى كل من علمني حرفا أو أغدق علي علما أو أسدى لي نصحا

إلى كل أصدقائي و زملائي .

كوثر شعبان

~مقدمة~

مقدمـــــــــــــــــــــــة

إن الانتشار الواسع لتكنولوجيا المعلومات والإتصالات خلق عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول إلى درجة أنها تحولت إلى أداة لا يمكن الإستغناء عنها لسهولة وسرعة الإتصال والتواصل لذا فهي تعد من أهم إنجازات العصر الحديث، ولكن رافق هذه الإنجازات ظهور خبراء جدد يتمتعون بالخبرة والحرفية في تطويع هذه التقنية من أجل القيام بأعمال إجرامية وبأساليب مبتكرة حولت هذه الجريمة من صفتها التقليدية وأبعادها المحدودة إلى –أبعاد جديدة –تعتمد التقنية في تنفيذ الفعل المجرم الامر الذي ادى الى خلق انواع جدىدة من السلوك الإجرامي تمثلت في ظهور الجرىمة الالكترونية او الجريمة المعلوماتية او كما اصطلح على تسميتها بجرائم الفضاء الرقمي.

هذه التكنولوجيا توفر لعصابات الجريمة طرقا أكثر إبداعا وتعقيدا لارتكاب جرائمهم وفي الوقت نفسه توفر لسلطات إنفاذ القانون في إطار جهودها الرامية لمكافحة هذه الجريمة فرصا أكبر للتصدي لمرتكبي هذه الجرائم ولكن المشكلة هي أن القانون يتفاعل ببطء مع التغير التكنولوجي ولذا كانت النتيجة أن استخدام بعض التقنيات يكون واقعا خارج إطار ونطاق القانون، مما أدى بالمشرع الجزائري إلى تكثيف جهوده للتصدي لهذه الظاهرة المستحدثة من خلال رصد جملة من آليات المكافحة وإن تباينت في فعاليتها بتدرج مستويات ونطاق تطبيقها.

اولا / اهمية الموضـــوع

تظهر الأهمية العلمية لموضوع " أليات مكافحة الجرائم الالكترونية في التشريع الجزائري " في عدة أوجه نوجزها فيما يلي:

– نظرا للتوسع الكبير في استخدام التكنولوجيا في حياتنا اليومية اصبحت الجرائم الالكترونية تتخذ من الفضاء الرقمي مجالا لارتكابها، فلا تقتصر على امن الافراد وخصوصياتهم فحسب بل تمتد لتستهدف المؤسسات والدول في اقتصادها واستقرارها وتتنوع في اهدافها وصورها كالاستغلال غىر المشروع لبطاقات الائتمان، والاعتداء على الأشخاص والاموال عبر الإنترنت، ﻓﺈ فساد الأخلاق، والاستغلال الجنسي للأطفال، وﺗﺈ تلاف نظم المعلومات وغيرها ليس هذا فحسب، بل ساهمت التكنولوجيا في تطوىر طرق ارتكاب الجرائم التقلىدىة كالاتجار بالاشخاص والجرائم الارهابية مما القى على عاتق القائمىن بمكافحة هذه الجرائم في الدول عبئا شدىدا ومهاما صعبة تفوق القدرات العلمىة والفنىة والقانونىة المتاحة لهم وفق وسائل الإثبات الجنائي التقلىدىة المتبعة في جمع الأدلة، فكان حتما على

المشرع الجزائري أن يعمل جاهدا لاستحداث أليات وقواعد اجرائية تتلائم مع هذا النوع من الإجرام، فضلا عن إنشاء أجهزة متخصصة ىناط بها مهمة الوقاية والمكافحة لهذه الجرائم، وعليه أقدمت العديد من التشريعات على تعديل قواعدها الموضوعية والإجرائية بشكل تحاول من خلاله التصدي لهذه السلوكيات الإجرامية الجديدة بتعديل نصوصها أو سن نصوص خاصة جديدة من بينها المشرع الجزائري الذي ادخل تعديلا على قانون العقوبات واستحدث به قسما خاصا سماه جرائم المساس بانظمة المعالجة الآلية للمعطيات، ونظرا للنقائص التي شابت هذا التعديل ارتأى المشرع أن يصدر قانونا خاصا تبنى فيه مصطلحا آخر هو الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تضمنتها أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وتبرز الاهميـــــة العمليــة لهذه الدراسة من خلال :

-أنها توفر للباحثين في ميدان القانون الجنائي معرفة واسعة بأحدث التشريعات الجنائية في التشريع الجزائري بشأن الجرائم الالكترونية في النتائج التي يمكن التوصل إليها أو التي قد تسهم في تشخيص أوجه القصور في التشريع الجزائري من خلال معالجته للجرائم الالكترونية اوقتراح الحلول للتصدي لها.

ثانيــا / أسباب إختيار الموضوع

تم اختيار موضوع " أليات مكافحة الجرائم الالكترونية في التشريع الجزائري" بناءا على جملة من الأسباب الذاتية والموضوعية يمكن إيجازها فيما يلي:

1/ الأسبــاب الموضوعية

-إكتفى المشرع الجزائري بمعالجة بعض الجرائم الالكترونية دون أن يعرج على أي أحكام أو تدابير اجرائية لمكافحتها الا بصدور القانون 04/09 المتعلق بالقواعد الخاصة بالوقاية من جرائم تكنولوجيا الاعلام والاتصال وهو ما يعد من الدوافع الموضوعية لدراسة هذا الموضوع.

– بالرغم من تطور الجرائم الالكترونية الا ان الكثير من أليات المكافحة المعتمدة سواء كانت (قانونية /امنية او ادارية) لا تزال عاجزة عن مجارة هذا التطور خاصة مع استخدام المجرمين لتقنيات متقدمة مثل التشفير والشبكات الافتراضية لاخفاء هوياتهم مما يستدعي دراستها وتحليلها واقتراح سبل تعزيزها.

2/ الأسباب الذاتيـــة

– تتعلق بالرغبة الشخصية في التعمق في هذا الموضوع والتعرف على كل ما يتعلق به، وتزداد هذه الرغبة لكون الموضوع بعدين بعد قانوني وبعد تقني، مما سيجعل الدراسة على درجة كبيرة من الأهمية ومن شأنها أن تستقطب اهتمام أي باحث قانوني.

– إثراء هذا الموضوع والإسهام ولو بشكل متواضع في إضافة دراسة للمكتبة القانونية .

ثاثـــا/ أهداف إختيار الموضـــوع

– الإجابة على إشكالات البحث وتساؤلاته الفرعية.

– الكشف عن الأحكام المتعلقة بالجرائم الالكترونية التي تجمع بين صفتي الإمتداد خارج حدود الدولة الواحدة وارتكابها بأحدث الوسائل التكنولوجية التي تتمثل في الحاسب الآلي وشبكة الأنترنت، وذلك من خلال التعريف بهذه الجريمة والتعرف على خصائصها ووسائل ارتكابها واهم صورها في القوانين العامة و الخاصة.

–الوقوف على القواعد الاجرائية المتبعة في جمع الأدلة الإلكترونية التقليدية منها والحديثة لمكافحة الجرائم الالكترونية وتقييم مدى فعاليتها .

– التعرف على اهم المؤسسات او الهيئات المستحدثة في اطار مكافحة الجرائم الالكترونية .

رابعا / الدراســـات السابقة

رسالة دكتوراه موسومة ب: الإثبات الجنائي بالأدلة الرقمية، للباحثة وردة شرف الدين، مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر – بسكرة– للسنة الجامعية 2016 – 2017 حيث تناولت موضوع الدراسة من خلال تقسيمه إلى بابين، خصص الباب الأول لدراسة الأحكام العامة

للدليل الجنائي الإلكتروني، وخصص الباب الثاني لدراسة وسائل الإثبات المتبعة في جمع الدليل الجنائي الإلكتروني كما تناولت هذه الرسالة جانب من جوانب موضوع دراستنا من خلال دراسة القواعد الإجرائية لمكافحة الجرائم الالكترونية.

خامسا / اشكالية الموضـــوع

خلف عصر تكنولوجيا المعلومات والاتصالات وراءه اثارا سلبية نتجت عن استغلال الافراد والجهات للتقنيات المعلوماتية في غير الغرض الذي تستخدم من أجله، الأمر الذي القى مسؤولية كبيرة على عاتق المشرع الجنائي لمواجهة هذا النوع المستحدث من الاجرام، وطرح عديد المشكلات فيما يتعلق بالنصوص الموضوعية والاجرائية للقانون الجنائي بحثاعن إمكانية تطبيق هذه النصوص التقليدية على هذا النوع المستحدث من الإجرام مع الحفاظ على مبدأ شرعية التجريم والعقاب او استحدلث نصوص خاصة، وفي ظل دراك المشرع الجزائري لخطورة هذا الجرائم سعى إلى رصد جملة من الآليات لمكافحتها، وهو ما يدفعنا لطرح الإشكالية التالية :

ماهي الاليات الموضوعية والاجرائية التي رصدها المشرع الجزائري لمكافحة الجرائم الالكترونية؟ وما مدى فعاليتها ؟

سادسا / المنهج المتبـــع

بهدف الإجابة على إشكالية الموضوع وتساؤلاته الفرعية تم الإعتماد على المنهج الوصفي بإعتباره أكثر المناهج إستجابة وتماشيا مع هذا النوع من الدراسات، وذلك من خلال وصف وتعرىف الجرائم الالكترونية وتحديد خصائصها ووسائل إرتكابها وبيان صورها.

أما بالنسبة للمنهج التحليلي أو ما يعبر عنه بمنهج تحليل المضمون فقد إستعنا به عند تحلىلنا لمختلف النصوص القانونية – الموضوعىة والإجرائىة – في مجال مكافحـــة الجرائم الالكترونية.

سابعا / التصريـــح بالخطة

مقدمـــــــــــــــــــــــــة

سيتم تناول موضوع " أليات مكافحة الجرائم الالكترونية في التشريع الجزائري "وفق خطة ثنائية تتضمن فصلين كالآتي:

الفصل الاول: بعنوان " الأليات الموضوعية لمكافحة الجرائم الالكترونية في التشريع الجزائري" من خلال تقسيمه إلى مبحثين ، نتناول في المبحث الأول "مفهوم الجريمة الالكترونية ووسائل ارتكابها " بينما يخصص المبحث الثاني ل " مكافحة الجرائم الالكترونية في اطار قانون العقوبات والقوانين الخاصة"

الفصل الثاني : بعنوان " الأليات الإجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري" من خلال تقسيمه إلى مبحثين، يخصص المبحث الأول ل " القواعد الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري ويخصص المبحث الثاني لـــ" الاطار المؤسساتي لمكافحة الجرائم الالكترونية في التشريع الجزائري"

أنهي هذه الدراسة بخاتمة عرضنا فيها أهم النتائج التي توصلنا إليها، وأهم التوصيات التي وجهناها للمشرع الجزائري من أجل تطوير سياسته الجنائية في مجال مكافحة الجرائم الالكترونية وأليات مكافحتها.

الفصل الأول الآليات الموضوعية لمكافحة الجرائم الالكترونية في التشريع الجزائري

رافق التطور الهائل لتقنية نظم المعلومات وثورة الإتصالات ظهور أشكال جديدة من الإجرام في الفضاء الرقمي أطلق عليها تسميته " الجرائم الإلكترونية " هذه الجرائم تنوعت أشكالها وصورها غير أنها تتفق في مجملها على وجود نظام معلوماتي مشكل من الحاسب الآلي ومكوناته وشبكات الربط والإتصال وتعد من أخطر الجرائم واكثرها تعقيدا.

إن حداثة شبكة الأنترنت من جهة وخطورة الجرائم المترتبة عنها من جهة أخرى خلق فراغا تشريعيا واضحا لدى العديد من الدول فأصبحت مطالبة بالتفكير في إعادة النظر في سياستها التجريمية بصفة عامة بإيجاد عديد الخطط والأساليب التي تتجاوب مع هذا النمط الاجرامي المستحدث المرتكب بتقنية المعلومات، وبالفعل إتجهت الدول إلى العمل على تطوير آليات مكافحة هذه الجريمة بتعديل تشريعاتها إما عن طريق تطويع نصوص قوانين العقوبات التقليدية أو عن طريق إستحداث نصوص قانونية جديدة متفرقة سواء في قانون العقوبات أو في بعض القوانين الأخرى، وقد حاولنا من خلال هذا الفصل أن نعرض جوانب الإطار التشريعي الموضوعي للجرائم الالكترونية من خلال بعض النصوص القانونية التي تعكس إرادة المشرع الجزائري في تبني التكنولوجيا المستحدثة ومكافحة الجرائم الناتجة عنها، أو من خلال النصوص التي تتناول هذه الجريمة بالتنظيم ضمن القوانين العقابية.

وفي هذا الشأن سوف نعمد من خلال هذا الفصل إلى بيان " **الأليات الموضوعية لمكافحة الجرائم الالكترونية في التشريع الجزائري**" وذلك من خلال تقسيمه على مبحثين، الأول بعنوان " **مفهوم الجريمة الالكترونية ووسائل ارتكابها** " والثاني بعنوان " **مكافحة الجرائم الالكترونية في قانون العقوبات والقوانين الخاصة**".

الفصل الأول الآليات الموضوعية لمكافحة الجرائم الالكترونية في التشريع الجزائري

المبحث الاول : مفهوم الجريمة الالكترونية ووسائل ارتكابها

كانت الجرىمة الالكترونية تتدرج ضمن الجرائم التقلىدىة مثل السرقة والغش والتزوىر... ولم تصبح جرىمة قائمة بذاتها بمفهومها وأركانها الخاصة إلا بعد دخول الانترنت في مطلع التسعىنات، حىث ظهرت أنماط جدىدة من الجرائم لم ىعد القاضي الجنائي ىجد لها وصف ضمن قائمة الجرائم التقلىدىة، الأمر الذي أدى إلى الإفلات بالعدىد من المجرمىن من العدالة عملا بمبدأ الشرعىة.

لذا سنتطرق في هذا المطلب إلى التعرىف بـــــ **(الجرىمة الالكترونية وخصائصها)** في المطلب الأول ثم بىان أهم **(وسائل ارتكابها)** في المطلب الثاني .

المطلب الاول : مفهوم الجريمة الالكترونية وخصائصها

تعددت التعاريف التي قيلت بشأن الجريمة الالكترونية وتباينت فيما بينها ضيقا واتساعًا وقد أسفر ذلك على تعذر إيجاد فهم موحد لظاهرة الجريمة الالكترونية لارتباط مفهومها بتكنولوجيا المعلومات وتطوراتها المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل إلكتروني، وكذا شبكات الربط والاتصال، لذلك فإنه من الضروري أن يكون أي تعريف لهذا النمط من الجرائم متسم بالمرونة بما يسمح باستيعاب سائر التقنيات المبتكرة الحالية والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات، وما سيتبع ذلك من تسهيل للوصول إلى الحلول المناسبة .

ونظرا لاختلاف الفقهاء القانونىىن فىما بىنهم حول إعطاء معنى موحد لهذه الجرىمة سوف نعرض من خلال هذا المطلب لـــــــ **(مفهوم الجرىمة الالكترونية)** في الفرع الاول ونتناول **(أهم خصائصها)** في الفرع الثاني وهذه الخصائص التي تمتاز بها تجعل منها جرائم تختلف كل الاختلاف عن الجرائم التقلىدىة.

الفرع الاول : مفهوم الجريمة الالكترونية

سنتناول التعريف الفقهي ثم التعريف القانوني للجريمة الالكترونية .

اولا/ التعريف الفقهي للجريمة الالكترونية[1]

هناك العديد من التعريفات الفقهية التي نتناول اهمها فيما يلي: عرفها الفقيه MERWE بانها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات"[2].

وقد وجه لهذ التعريف عديد الانتقادات منها أن تعريف الجريمة الالكترونية يستدعي " الرجوع إلى العمل الأساسي المكون لها وليس فحسب إلى الوسائل المستخدمة لتحقيقه " ويعزز هذا النقد أنه " ليس لمجرد أن الحاسب قد استخدم في الجريمة أن نعتبرها من الجرائم الالكترونية "[3] .

---

[1]– هناك تعبيرات شاعت في بداية ظهور الجريمة الالكترونية واتسع استخدامها حتى عند الفقهاء والدارسين القانونيين كالغش المعلوماتي أو غش الحاسوب، والإحتيال المعلوماتي أو احتيال الحاسوب وغيرها، مما يجعل التركيز على أن الظاهرة الإجرامية المستحدثة تتمحور رغم اختلاف أنماط السلوك الإجرامي– حول فعل الغش أو النصب أو الإحتيال–وهناك مصطلح آخر فرنسي المنشأ يكثر استخدامه بين رجال الفقه القانوني اللاتيني وهو مصطلح الجرائم المعلوماتية وكلمة المعلوماتية الواردة في هذا المصطلح هي ترجمة عربية للمصطلح الفرنسي " Information" الذي أوجده الفرنسي "فيليب دريفس" نتيجة لتجميعه للمقطع الأول من كلمة المعلومات مع المقطع الأخير من كلمة "Automatique " أتوماتيك لوصف المعالجة الآلية للمعلومات، وهناك ايضا مصطلح الجرائم الالكترونية" Electronic crime "حيث ان –E تستخدم كبادئة قبل الكلمة لتحول مدلولها التقليدي إلى مدلول له ارتباط بالحاسوب مثل البريد الالكتروني، ويمكن الأخذ بمصطلح الجرائم المعلوماتية أو الجرائم الإلكترونية لكثرة استعمالهما وشيوعهما بين رجال الفقه والقانون والتقنيين المختصين بتكنولوجيات الاعلام الالي واللذان يقابلهما مصطلح شائع باللغة الفرنسية يتمثل في" La cybercriminalité " وبالانجليزية "Cybercrime " لمزيد من التفصيل حول ذلك انظر وردة شرف الدين، الإثبات الجنائـــــــــــي بالأدلة الالكترونية – دراسة مقارنة – أطروحة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة بسكرة 2016 / 2017 ص 89.

[2]– طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية 2009 ص 153.

[3] – يونس عرب، جرائم الكمبيوتر والإنترنت– المعنى والخصائص والصور واستراتيجية المواجهة القانونية– انظر الموقع الالكتروني http://www.abhatoo.net.ma ساعة الزيارة 13.20 تاريخ الزيارة 2025/01/03 .

كما يعرفها خبراء منظمة التعاون الاقتصادي والتنمية OECD بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"[1] .

ويعتمد هذا التعريف على معياريين، أولهما (وصف السلوك) وثانيهما (اتصال السلوك) بالمعالجة الآلية للبيانات أو نقلها، ويلاحظ من تعريف منظمة التعاون الاقتصادي والتنمية أنه لا يقتصر على جرائم الكمبيوتر والانترنت، ذلك أن المعالجة الآلية للبيانات تمتد لتشمل كل ما يمكن القيام به عن طريق الاتصالات السلكية واللاسلكية، بما في ذلك الهاتف الأرضي والمحمول، وكل التجهيزات التي تشمل المعالجة الالكترونية والمعلوماتية للبيانات[2].

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف الجريمة الإلكترونية بأنها " أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية"[3].

كماعرفها خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[4].

---

[1] – وردة شرف الدين، المرجع السابق ص 99.

[2]– عبد المحسن بدوي محمد أحمد، الجرائم المعلوماتية، مقال منشور ضمن مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية، عدد335، الرياض لسنة1431 ص 66.

[3]– زيوش عبد الرؤوف وزغيشي مصطفى، الجرائم الالكترونية الاقتصادية–المفهوم والدوافع–مقال منشور في مجلة الدراسات القانونية والاقتصادية، مجلد 07، عدد 01 لسنة 2024 ص 403.

[4]– سمير شعبان، الجريمة الالكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم مقال منشور في مجلة دراسات وابحاث، المجلة العربية للأبحاث فى العلوم الإنسانية والإجتماعية ، عدد 01 لسنة 2019 ص 118.

وبالرجوع لهذين التعريفين نجد انهما يشيران إلى إمكان حصول جريمة الكمبيوتر بالامتناع، وهذا اتجاه محمود إذ أغفلت معظم التعريفات الإشارة إلى ذلك، كما انها ادرجت جرائم لا تثير أية إشكالية في انطباق النصوص الجنائية التقليدية عليها ولا تمثل جرائم جديدة ".

وفي رأي آخر ذهب الفقيه ALTER SOLARZ إلى أن جريمة الكمبيوتر هي " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"[1].

نلاحظ ان هذا التعريف يشترط ان يكون الفعل مما يقع ضمن نطاق قانون العقوبات، ويكون هنا قد جزم بشمول قانون العقوبات لأنماط السلوك الإجرامي في جرائم الكمبيوتر رغم الجدل القائم حول مدى انطباق نصوص التجريم التقليدية على هذه الأفعال .

ثانيا/ التعريف القانوني للجريمة الالكترونية

تبنى المشرع الجزائري مفهوما ضيقا للجريمة المعلوماتية في الامر 15/04 المعدل لقانون العقوبات لينتقل بعد ذلك لمفهوم أوسع في قانون 04/09 المتضمن القواعد العامة للوقاية من جرائم تكنولوجيا الاعلام والاتصال.

1/ المفهوم الضيق للجرائم المعلوماتية

تبنى المشرع الجزائري في الامر رقم 15/04[2] التعريف الضيق للجريمة الالكترونية والقائم على معيار موضوع الجريمة وحصر مفهوم الجريمة في الاعتداءات الماسة بالأنظمة المعلوماتية، ولكنه لم يقدم تعريفا للمساس بأنظمة المعالجة الآلية للمعطيات، فإذا كان مفهوم المساس نعني به "الاعتداء" فان أنظمة المعالجة الآلية للمعطيات عبارة عن "آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات" وعليه نعني بنظام المعالجة الآلية للمعطيات " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج

[1] – يونس خالد عرب مصطفى، الموقع الالكتروني السابق ص54 .

[2]– القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر 156/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات.

والمعطيات وأجهزة الإدخال والإخراج، وأجهزة الربط التي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، على أن يكون هذا المركب خاضع لنظام الحماية الفنية " وبالتالي ينصرف وصف الجريمة الالكترونية في القانون 15/04 الى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات فقط، وحتى بمناسبة تعديل قانون العقوبات لسنة 2006[1] لم يمس بالنصوص التجريمية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات بل شدد في العقوبات المقررة لهذه الأفعال فقط، وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها لذلك آثر استخدامه لمصطلح "المساس بنظم المعالجة الآلية للمعطيات" مع الإشارة إلى انه عاد واستعمل مصطلح " تكنولوجيا الإعلام والاتصال" لكن هذا الاستعمال كان عرضيا فقط وذلك بمناسبة نصه على الجرائم الإرهابية، أما عن مصطلح المساس بأنظمة المعالجة الآلية للمعطيات ينصرف وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها[2].

2/ توسيع مفهوم الجرائم المعلوماتية في قانون 04/09

سدا للفراغ والقصور التشريعي للقانون 15/04 في احتوائه لمفهوم الجريمة الالكترونية سن المشرع قانونا أخر هو القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيات الإعلام والاتصال[3]، الملاحظ في هذا القانون انه وسع من مفهوم الجريمة الالكترونية حيث جاء في المادة 02 منه بتعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها " الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

---

[1]– قانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم قانون العقوبات، الجريدة الرسمية رقم 84 لسنة 2006

[2]– حابت امال،الجريمة المعلوماتية في التشريع الجزائري بين قانوني 15/04 و 04/09 مقال منشور في مجلة هيرودوت للعلوم الانسانية والاجتماعية مجلد 07، عدد 25، لسنة 2003 ص 55 .

[3]– القانون 04/09 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

وبهذا يكون المشرع الجزائري انتقل من المفهوم الضيق للجريمة الالكترونية الذي كان ينحصر في الجرائم التي تقع على الأنظمة المعالجة أليا إلى مفهوم أوسع لها، فهي بالإضافة للجرائم التي تقع على هذه الأنظمة المعلوماتية هي كل الجرائم التي ترتكب أو تساهم وتسهل في ارتكابها الأنظمة المعلوماتية وأنظمة الاتصالات بما فيها الهاتف النقال والثابت، بذلك تعد أي جريمة وقعت على نظام معلوماتي أو استعمل فيها نظام معلوماتي أو أوسيلة اتصال جريمة متصلة بتكنولوجيا الإعلام والاتصال، وعليه تتمثل أصناف الجرائم المعلوماتية حسب قانون 04/09 الى :

- الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات.

- جرائم الوسيلة المعلوماتية أي تلك التي يكون فيها النظام المعلوماتي وسيلة لتنفيذ الجريمة.

-جرائم الاتصال الالكتروني أي تلك التي تنفذ عن طريق الاتصالات الالكترونية.

وعليه يمكن القول ان المشرع الجزائري تبنى معيار موضوع الجريمة لتحديد معالم الجريمة الالكترونية والذي يجب ان يقع على نظام معلوماتي فسمى الجرائم الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر07، ثم ترك المجال واسعا لأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية في القانون رقم 04/09 .

الفرع الثاني : خصائص الجريمة الالكترونية

مثلما للجرائم العادية خصائص وصفات تتسم بها فإن الأمر ينطبق على الجرائم الالكترونية، وتعد الجرائم التي ترتكب من خلال الحاسوب وشبكة الإنترنت هي جرائم ذات خصائص متفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها، وعليه سنتناول اهم الخصائص التي تميزها عن غيرها.

أولا/ الجرىمة المعلوماتىة تتسم غالبا بالطابع الدولي

الطابع العالمي لشبكة الإنترنت وما ىرتبه من جعل معظم دول العالم في حالة اتصال دائم ىسهل من ارتكاب الجرىمة من دولة إلى دولة أخرى، فالجريمة الالكترونية لا تعترف بالحدود بىن الدول والقارات ولذلك فهي تعتبر شكلا جدىدا من أشكال الجرائم العابرة للحدود الإقلىمىة بىن دول العالم كافة[1].

إذ ىمكن من خلال النظام المعلوماتي ارتكاب العدىد من الجرائم مثل جرائم التعدي على قواعد البىانات وتزوىر واتلاف المستندات الإلكترونىة، والاحتىال المعلوماتي، وسرقة بطاقات الائتمان، والقرصنة، وغسىل الأموال،كما أن قدرة تقنىة المعلومات على اختصار المسافات وتعزىز الصلة بىن مختلف أصقاع الأرض انعكست أىضا على طبىعة الأعمال الإجرامىة التي ىعمد فىها المجرمون إلى استخدام هذه التقنىات في انتهاكاتهم للقانون، وهو ما ىعني أن مساحة مسرح الجرىمة الالكترونية لم تعد محلىة أي أنها أصبحت عالمىة، والجرىمة الالكترونية تعد من الجرائم التي ىتم ارتكابها عبر المسافات حىث لا ىتواجد الفاعل على مسرح الجرىمة بل ىرتكب جرىمته عن بعد، وهو ما ىعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجرىمة، ومن ثم تتباعد المسافات بىن الفعل الذي ىتم من خلال جهاز كمبىوتر الفاعل وبىن النتىجة أي المعطىات محل الاعتداء، وبالتالي لا تقف الجرىمة المعلوماتىة عند الحدود الإقلىمىة لدولة معىنة بل تمتد إلى الحدود الإقلىمىة لدولة أخرى مما ىزىد من صعوبة اكتشافها[2].

ثانيا / الجريمة الالكترونية صعبة الاكتشاف والاثبات

[1]– سوىر سفىان، جرائم المعلوماتىة، مذكرة لنىل شهادة الماجستىر في العلوم الجنائىة وعلم الإجرام، كلىة الحقوق والعلوم السىاسىة، جامعة أبو بكر بلقاىد، تلمسان 2011/2010 ص 19.

[2] – سوىر سفىان، المرجع السابق ص 20.

الجريمة الالكترونية جريمة هادئة لذلك يصعب إكتشاف زمن وقوعها أو الشخص الذي قام بها حيث تعود الأسباب التي تقف وراء الصعوبة في إكتشاف الجريمة الإلكترونية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى ولا لآثار الدماء، كما أن المجرم يمكنه إرتكاب هذه الجريمة في دول وقارات مختلفة إذ أن الجريمة الإلكترونية كما سبق وأشرنا جريمة عابرة للحدود، وكذلك فإنّ قدرة المجرم تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملاً إضافياً في صعوبة إكتشاف هذا النوع من الجرائم، ومن هنا فهذه الجريمة تحدث في سرية تامة لان مجرمي المعلومات يتمتعون بتقنيات عالية تمكنهم من عدم كشف الجريمة التي قاموا بها[1]، ان صعوبة إثبات الجريمة الالكترونية يرجع إلى انها لا تترك أيّ آثار مادية لها بعد إرتكابها، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا توجد مستندات ورقية بحيث يصعب الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر[2].

ثالثا / الجريمة الالكترونية جريمة مستحدثة

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم الالكترونية– سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها– من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته ومكاناته أجهزة الدولة الرقابية، بل انه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها وعلى الرغم من المزايا والمنافع الإيجابية المترتبة عن هذه العولمة وثورة المجتمع الإلكتروني، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم، ومن أبرزها جرائم غسيل الأموال، وتهريب المخدرات، واختراق قطاع الأعمال، والإفلاس

[1]– نعيمة داودي، الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها) مقال منشور في مجلة مهد اللغات مجلد 02، عدد01 لسنة 2020 ص 48 و49.

[2] – رصاص فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شهادة ماجستير في القانون العام جامعة أبي بكر بلقايد – كلية الحقوق والعلوم السياسية، تلمسان 2012/2011 ص45 .

بالتدليس والغش، والفساد ورشوة الموظفين العموميين وسرقة الملكيات الفكرية، والاتجار غير المشروع في الأسلحة وفي السلاح والأطفال، والاتجار غير المشروع في الأعضاء البشرية، وجرائم الحاسب الآلي أو الجرائم الإلكترونية[1].

المطلب الثاني : وسائل ارتكاب الجرائم الالكترونية

على الرغم من أن دراسة وسائل إرتكاب الجرائم الالكترونية من الناحية الفنية والتقنية بعيدا عن لغة القانون إلا أنه لزاما علينا التعرض لهذه الوسائل لإرتباط الجرائم الالكترونية إرتباطا وثيقا بها ولازالة الغموض وتوضيح بعض المصطلحات التقنية المرتبطة بتكنولوجيا المعلومات والتي قد تمر معنا في المباحث المتقدمة من الدراسة.

وعليه وفي هذا الشأن سوف نتناول من خلال هذا المطلب "**وسائل ارتكاب الجرائم الالكترونية** " وذلك من خلال فرعين اعتمدناهما تقسيما لهذا المطلب، الأول بعنوان "**الحاسب الالي والانترنت** " والثاني بعنوان " **الهاتف النقال والخدمات المرتبطة به**"

الفرع الاول : الحاسب الالي والانترنت

تختلف وسائل إرتكاب الجرائم الالكترونية عنها في الجريمة التقليدية نظرا لحداثة الأولى وارتباطها بتكنولوجيا المعلومات والإتصالات، لذا فالمعرفة المعمقة للوسائل المستخدمة من قبل المجرمين قد تساعدنا على فهم المدى الكامل لهذه الظاهرة ومكافحتها بشكل أكثر فعالية.

أولا / تعريف جهاز الحاســـــب الآلـــــــي

[1] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الاسكندرية 2008 ص 57.

الحاسوب في اللغة (إسم) من الفعل حَسَبَ و الجمع حَوَاسِيبٌ. حَسَبَ المَالَ: ونحوه حِسَابًا وحسبانا عَـــــــــــدَهُ وأَحْصَاهُ وقَـــــــــدَرَهُ، فهـــــــــو حَاسِبٌ، والمفعول مَحْسُوبٌ[1]، وهو إسم آلة من حَسَبَ.

والحاسوب الآلي أو الإلكتروني هو" جهاز مبرمج لأداء عمليات سريعة أو لتخزين المعلومات واسترجاعها في أي وقت"[2] .

ويعرف الحاسب الآلي بدلالة مكوناته بأنه " مجموعة من الأدوات الإلكترونية تقوم بمجموعة مترابطة ومتتالية من العمليات على مجموعة من البيانات الداخلية، تتناولها بالمعالجـــــــة وفقا لمجموعة من التعليمات والأوامر الصادرة إليه، المنسقة تنسيقا منطقيا حسب خطة موضوعة مسبقا لحل مسألة معينة معرفة، بغرض الحصول على نتائج ومعلومات تفيد في تحقيق أغراض معينة وتسمى التعليمات والأوامر جمـــــــلا، ومجموعة الجمل تسمـــــــــــــــى برنامجـــــــا، والشخص الذي يصمـــــــــــــــم البرنامج يسمـــــــــــــــــى مبرمجا"[3].

ويعد الحاسب الآلي وسيلة النفاذ إلى شبكة الأنترنت ومن ثمة لا يتصور ارتكاب جريمة أنترنت بدونه ويبرز دور الحاسوب بشكل واضح إذ ما تم توصيله بشبكة الأنترنت حيث يتحول إلى أداة وبيئة لارتكاب مختلف أنواع الجرائم التقليدية، لاسيما منها العابرة لحدود الدول .

---

[1]– المعجم الوسيط، مجمع اللغة العربية، مكتبة الشروق الدولية 2004 ص 171، نسخة إلكترونية متوفـــــــرة علـــــــــــــى موقع المكتبة الوقفية للكتب المصورة www.waqfeya.comتاريخ الزيارة 2025/01/06 ساعة الزيارة 13.41

[2]– معجم المعاني الجامع، متوفر على العنوان الإلكتروني www.almaany.comتاريخ الزيارة 2025/01/06 ساعة الزيارة 12.30 .

[3]– محمد الفيومي، مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، المكتب الجامعي الحديث،الإسكندرية، مصر 1998 ص 07. مشار له عند علي جعفر جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنـــــــــــــة منشورات زين الحقوقيـــــــــــــــــة، د ب ن 2013 ص 37 .

ثانيا/ شبكـــــــــــــة الأنترنـــــــــــــــت

سوف نتطرق بالدراسة لشبكة الأنترنت كوسيلة من وسائل ارتكاب الجرائم الالكترونية، حيث سنتناول تعريف شبكة الأنترنت ثم طريقة عمل الأنترنت، وفي الأخير سوف نتعرض لخدمات الأنترنت.

1/ تعريف شبكـــــــــة الأنترنـــــــــــــــت

الشبكة في اللغة (إسم) الجمـــــــــــــــع شَبَكَـــــــــــــاتٌ وشِبَـــــــــاكٌ وشَبَكٌ، والشبكة هي كل متداخل متشابك[1].

أما الأنترنت كلمة إنجليزية مركبة مختصرة مكونة من مقطعين (Inter) وهي اختصار للكلمة الإنجليزية (International) وتعني دولي و(Net) إختصار لكلمة (Network) وتعني شبكة حيث تم إشتقاق مصطلح أو تسمية الشبكة العالمية (Interconnection Network) وهي الشبكة التي تربط ألاف الشبكات من أجل التواصل وتبادل المعلومات عبر مئات الملايين من الحواسيب عبر العالم[2] .

شبكة الشبكات، الفضاء السيبراني، الشبكة العنكبوتية الإلكترونية، كثيرة هي التعابير التي تشير إلى ظاهرة الشبكة العالمية " الأنترنت " والتي تعني إصطلاحا " الوسيلة أو الأداة التواصلية بين الشبكات المعلوماتية دون إعتبار للحدود الدولية ".

ويمكن تعريفها أيضا بأنها " شبكة دولية تربط ألاف الشبكات وملايين أجهزة الحاسوب بعضها ببعض عبر العالم ويمكن الدخول إليها من خلال جهاز الحاسوب والأجهزة الذكية كالهواتف المحمولة واللوحات الإلكترونية[3]، ويستخدم الأنترنت العديد من الأشخاص والمؤسسات لتبادل الرسائل

---

[1]– معجم المعاني الجامـــــــــــــع، الموقع الالكترونـــــــــي السابق.

[2]– أسامة أحمد المناعسة وجلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة – وفقا لقانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 ، ط 2، دار الثقافة للنشر والتوزيع، عمان، ص 36 .

[3]– اللوحة الالكترونية tablette tactile عبارة عن حاسوب محمول رفيع الحجم على شكل شاشة تعمل باللمس دون لوحة مفاتيح، وتوفر تقريبا نفس الخدمات التي يوفرها الحاسوب الشخصي، فهي تمكن من التواصل مع الوسائط المتعددة كالتلفزيون والأنترنت وتصفح البريد الإلكتروني، كما تسمح بتثبيت تطبيقات إضافية يتم تحميلها أو شراؤها

والمعلومات[1] فالأنترنت نفسها لا تحتوي على معلومات ولكنها توفر السبل لتبادل المعلومات بين الحاسبات الآلية الرقمية[2].

وهذه الشبكة رغم عالميتها وخط سيرها عبر الدول والقارات إلا أنها لا تخضع لملكية فرد أو مؤسسة أو دولة، وتختلف الشبكات الممتدة أو العالمية عن الشبكات المحلية في أنها تربط بين أجهزة الحاسب الالي أكثر بكثير من الشبكات المحلية، وأنها نظرا لبعد المسافات تحتاج إلى أجهزة اتصال ودعائم تقنية لتوفير الإتصال الجيد لتيسير انسياب المعلومات.

2/ طريقـــة عمـــل الأنترنـــت

الأنترنت يربط أجهزة الحاسوب مختلفة الأحجام والأنواع معا، و ليكون الأنترنت قادرا على ربط أجهزة الحاسوب المختلفة ويوفر امكانية تبادل المعلومات فلا بد من توافق تلك الأجهزة مع مجموعة قوانين اتصال قياسية تدعى البروتوكول، ومن ثمة تستخدم كل أجهزة الحاسوب المرتبطة بالأنترنت ما يسمى بروتـــوكول الأنترنت-" Internet Protocole IP" وهو عبارة عن" قوانين تحكم تقسيم رسائل البيانات إلى وحدات (Packets) وتحكم توجيه البيانات من المرسل إلى المستقبل"[3]، ولكي يلج

عبر الأنترنت فهي جهاز وسط بين الكمبيوتر المحمول والهاتف الذكي . علالـــــــي أمينة، مكافحة الجرائم العابرة للحدود المرتكبة بتقنية المعلومات، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة عنابة 2019 هامـــــــــــــش رقم 05 ص 70 و 71 .

[1]- عبد الغني مصطفى و فاطمة بوجيري، مقدمة في الانترنت، مؤسسة لورد العالمية للشؤون الجامعية، البحرين 2006 ص 22.

[2]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، طبعة أولى، مطابع الشرطة، القاهـــــرة 2009 ص 58.

[3]- تحقيقا وضمانا لآليات التخاطب والتواصل بين مختلف الحاسبات الآلية عبر العالم معا، فقد وجدت بروتوكولات الأنترنت الموحدة والتي تعنى بجعل تبادل المعلومات والبيانات عملية قياسية ومتاحة بغض النظر عن نظام المستخدم في طرفي الإتصال وأهم بروتوكـــــــــــــولات الأنترنت هي :

-TCP/IPوهو بروتوكول التحكم بالإتصال عبر الأنترنت - HTTPيستخدم لأغراض عرض النصوص وقراءتها ويمكن للمتصفح الإنتقال بين العناوين بسهولة ويسر - SMTP و يستخدم لأغراض تبادل الرسائل الإلكترونية .

المستخدم إلى الأنترنت فهو بحاجة إلى صلاحية الدخول إليه، ويحقق مستخدمو الحاسوب المنزلي ذلك عادة عبر الإتصال الهاتفي الأرضي بمزود خدمـــــــة الأنترنت ويطلق عليه (ISP _ InternetServise Provider)عبر جهاز مودم[1]، وهناك طريقة أخرى للوصول إلى الأنترنت تتأتى بربط خط مؤجر Leased Line بشبكة محلية (LAN_Local Area Network) ويستخدم هذه الطريقة عادة مؤسسة أو شركة كبيرة تمتلك عقدة " Node " خاصة بها على الأنترنت أو تكون مرتبطة بمزود لخدمة الأنترنت[2].

أما بالنسبة لشبكة اتصال الأنترنت فإن الإتصال المباشر بين جهاز حاسوب وآخر يتم عن طريق شبكة داخلية (Internal Network) سلكية(Wire Network) أو لاسلكية (Wireless Network) تنقل الإشارات بواسطة الموجات الصغرية أو البلوتوث داخل المقار، وللإتصال بشبكة الأنترنت يربط كل من جهازي الحاسوب بجهاز مودم الذي يتصل بأسلاك الهاتف و مقسمه، ثم يتصل بشبكة الأنترنت عبر كوابل الشبكة البحرية العنكبوتية[3]

3/ خدمـــــــــــات الأنترنـــــت

عديد الخدمات التي تقدمها شبكة الأنتنرنت نوجزها فيما يلي:

أ/ البريـــــد الإلكترونـــــــــــــي

لمزيد من التفصيل أنظر عبد الحسن الحسيني : القاموس الموسوعي في المعلومات والإتصالات والمعلوماتية القانونية مكتبة صادر بيروت 2004 ص 792 . أسامة أحمد المناعسة وجلال محمد الزغبي، المرجع السابق ص 37.

[1]– المودم عبارة عن وحدة ربط تستخدم في إرسال وإستقبال البيانات عبر خطوط الهاتف وبما أن الحواسيب تعمل مع الإشارات الرقمية بينما صممت خطوط الهاتف لحمل الإشارات التناظرية وهي أصوات المستخدمين، فإن وظيفة المودم تحويل الإشارات العددية إلى إشارات تناظرية لنقلها عبر خطوط الهاتف .

[2]– عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية – شبكة الأنترنت، شبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات – دراسة قانونية مقارنة – طبعة أولى، دار الثقافة للنشر والتوزيع 2011 ص 54 .

[3]– هناك توجه أمريكي جديد بدأ تنفيذه لتطوير شبكة الأنترنت العنكبوتية لكي تتصل إشاراتها عبر الأقمار الصناعية بدلا من الكوابل الأرضية، وبعض الشركات الأردنية و رجال الأعمال بدؤا بالفعل في إستخدام هذه التكنولوجيا . لمزيد من التفصيل أنظر عادل عزام سقف الحيط، المرجع السابق ص57.

تنوعت تعريفات البريد الإلكتروني عند شراح القانون إلا أن المضمون واحد، يمكن تعريفه بأنه "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"[1].

وعرفه لآخرون بأنه " وسيلة إتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة تليفونات عامة أو خاصة، وغالبا يتم كتابة الرسالة على جهاز الكمبيوتر ثم يتم إرسالها إلكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه، حيث يتم ارسالها عبر خطوط التليفون إلى كمبيوتر المرسل إليه[2].

أما القانون الفرنسي فقد عرفه بأنه " كل رسالة أيا كان شكلها نصية أو صوتية أو مصحوبة بصور وأصوات يتم ارسالها عبر شبكة عامة للإتصالات ويتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعادتها"[3].

يوفر البريد الإلكتروني إمكانية الإتصال بملايين البشر حول العالم كبديل للبريد التقليدي ويعتبر من أقدم وأشهر الخدمات التي تقدمها شبكة الأنترنت، ويرجع تاريخها إلى بدايات السبعينات من القرن الماضي، ويمكن من خلالها كتابة الرسائل وتضمينها ملفات وصور أو مستندات وذلك بعد معرفة عنوان البريد الإلكتروني للمرسل له، وكذلك استقبال الرسائل من أي مستخدم لشبكة الأنترنت وذلك بصورة سريعة جدا لا تتعدى الثواني، وإلى جانب تأمين عملية المراسلة ذاتها فإنه يجري تشفير هذه الرسائل والوثائق والمستندات المرفقة بها .

يقوم المشتركون في نظام البريد الإلكتروني بكتابة الرسائل على هيئة خطاب عادي ثم يسقطون الخطابات داخل بنك ذاكرة جهاز حاسوب مركزي عن طريق جهاز مودم، ويقوم المتلقي بالتقاط

---

[1]–محمود محمد لطفي صالح، المعلوماتية وإنعكاساها على الملكية الفكرية للمصنفات الرقمية – دراسة مقارنة – دار الكتب القانونية، دار شات للنشر والبرمجيات، مصر، الإمارات 2014 ص 185.

[2]– يتكون البريد الإلكتروني من جزأين رئيسيين هما : رأس « Header » ونص Body » ويحتوي الرأس على معلومات حول المرسل والمستقبل والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب، ويحتوي النص على الرسالة التي تم إعدادها وعلى ملحقاتها إن وجدت. عادل عزام سقف الحيط، المرجع السابق ص 204.

[3]– المادة الأولى (01) من القانون الفرنسي الصادر في 22 جوان 2004 بشأن الثقة في الإقتصاد الرقمي .

الرسالة عن طريق مهاتفة الحاسوب وإدخال كلمة مرور خاصة في النظام، ونظرا لسرعته الفائقة في توزيع الرسائل يعد البريد الإلكتروني أرخص بكثير من مكالمات الهاتف أو رسائل الفاكس[1]. وبالرغم من الفوائد الهائلة التي تقدمها هذه الخدمة إلا أنها من الممكن أن يساء استخدامها من قبل مجرمي المعلوماتية وتستخدم كوسيلة للتواصل بينهم وبين العصابات والضحايا المحتملين.

رسائل البريد الإلكتروني تمر عبر بلدان مختلفة ومناطق زمنية مختلفة مما يعرقل تحديد مصادر الإتصالات ومستلميها لأن الرسائل يمكن إرسالها ببساطة من خلال معيد إرسال" re- mailers" يقوم بإزالة المعلومات التعريفية واستبدالها بمعلومات كاذبة قبل إرسالها مرة أخرى، هذا النظام معروف بالإستفادة من تصدع في المنظومة لإنفاذ القانون بحيث يقوم معيدو الإرسال بإرسال الرسائل على الأقل عبر بلد معروف بعدم تعاونه مع المجتمع الدولي وإنفاذ القانون[2].

ب/مجموعات الأخبار

عبارة عن أماكن وساحات إفتراضية للقاء والتحادث بين مستخدمي شبكة الأنترنت من ذوي الإهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والصور والأفكار حول موضوع معين ويمكن أن يساء استخدامها للعثور على النساء والأطفال لغرض الإستغلال ولتحميل وتنزيل المواد الإباحية غير القانونية.

ت/ مواقع الويب

عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب والتي تتيح لأي شخص أو لأي جهة الإطلاع على المعلومات تخص أشخاص آخرين أو جهات أخرى قاموا بوضعها على هذه الخدمة ولكل مستخدم لشبكة الأنترنت أن ينشئ له موقع على شبكة الويب العالمية تتضمن معلومات يمكن

[1]– عادل عزام سقف الحيط، المرجع السابق ص 204 .

[2]– محمد الصالح حامدي، علاقة تكنولوجيا المعلومات بظاهرة الإتجار بالبشر في عصر العولمة وتأثيرها على دولة قطر المجلة العربية الدولية للمعلوماتية، المجلد الأول، العدد الثاني 2012 ص 03 .

إعادة تخزينها، والتي يمكن لأي مستخدم آخر في جميع أنحاء العالم استقبال هذه المعلومات من خلال نظم الإستقبال[1]، وهذه المواقع قد تكون مفيدة بما يخدم الغرض من إنشائها، كما يمكن أن يساء استخدامها .

ث/غرف الدردشـــــــــــة

هي مساحات معروفة في الفضاء الإلكتروني بـــــــــــــ (Cyber Space)تتيح لروادها التخاطب معا بشكل مباشر وتتمثل آلية عمل غرف المحادثة في صورتين، غرف المحادثة العامة وغرف المحادثة الخاصة الأولى تكون مجموعة المحادثة متاحة يلجها من يشاء من متصفحي المواقع، أما في الأخرى فمجموعة المحادثة تكون محصورة بين عضوين أو بين مجموعة حصرية يكونها الأعضاء أنفسهم ويستخدمون مخدم المحادثة الجماعية – ماسنجر – لتبادل حديث خاص وقد يتم التخاطب عن طريق الكتابات النصية[2].

يتم في غرف الدردشة الإتصال في الوقت الحقيقي تتميز بعدم أرشفة الرسائل كما لا يتم الإحتفاظ بملفات السجل (log files).

ج/ بروتوكـــــــــــــول نقـــــــــل الملفـــــــــات

تمكن هذه الخدمة المستخدم من نسخ الملفات من جهاز حاسوب إلى جهاز أخر وهي طريقة فعالة لتبادل الملفات عبر الأنترنت، يسمح من خلالها للمستخدمين بالوصول مباشرة إلى القرص الصلب لجهاز كمبيوتر آخر لتحميل وتنزيل الملفات .

ح/ شبكـــــــات النـــــــــــد للنـــــــــــد

هي شبكة كمبيوتر محلية مكونة من مجموعة من الأجهزة لها حقوق متساوية ولا تحتوي على مزود مخصص بل كل جهاز في الشبكة يمكن أن يكون مزودا وزبونا، بمعنى أن الكمبيوترات في

[1]– محمد أمين الشوابكة، جرائم الحاسوب و الأنترنت – الجريمة المعلوماتية – طبعة أولى، دار الثقافة للنشر والتوزيع 2007 ص 37 ، 38 .

[2]– عادل عزام سقف الحيط، المرجع السابق ص 203 .

الشبكة يستطيع كل منها تأدية وظائف الزبون والمزود في نفس الوقت، وبالتالي فإن كل جهاز على الشبكة يستطيع تزويد غيره بالمعلومات وفي نفس الوقت يطلب المعلومات من غيره من الأجهزة المتصلة بالشبكة وهذا النوع من الشبكات يطلق عليه أيضا اسم مجموعة عمل أو (workgroup)[1]. ويمكن فهم مجموعة العمل هذه بأنها مجموعة من الأجهزة التي تتعاون فيما بينها لإنجاز عمل معين وهي عادة تتكون من عدد قليل من الأجهزة لا يتجاوز العشرة يستطيع أعضاء مجموعة العمل رؤية البيانات والموارد المخزنة على أي من الأجهزة المتصلة بالشبكة والإستفادة منها[2]، تستخدم لإيجاد وتنزيل الملفات الموجودة على شبكة الأنترنت وتتم إساءة إستخدامها دون ترك مراسلات يمكن تسجيلها أو تعقبها[3].

د/ التشفيـــــــــــــــــــــــــــر

يعد التشفير طريقة لإرسال المعلومات بحيث يستطيع الأشخاص الذين لهم مفتاح الشفير فقط الإطلاع عليها وفهمها، بينما لا يستطيع أي شخص آخر لا يملك المفتاح معرفتها ويطلق عليه علم التعمية أو علم الكتابة السرية، وقد تكون هذه المعلومات رسائل مكتوبة أو محادثات هاتفية أو صور أو بيانات تنقل عبر وسائل الإتصال الحديثة[4].

والتشفير هو أهم طرق حماية المعلومات وأكثرها كفاءة خصوصا إذا كانت المعلومات ستنقل عبر شبكات اتصال سلكية أو لاسلكية يسهل التنصت عليها أو كانت المعلومات يتم تبادلها في شبكات الحواسيب الحديثة الواسعة الإنتشار التي يمكن إختراقها،كما يمكن إستخدامه لإخفاء محتوى الملفات الغير مشروعة على شبكة الأنترنت واخفاء الإتصالات .

---

[1]– شبكات الند للند، مقال منشور على الموقع الإلكتروني:www.bossla.comتاريخ الزيارة 2017/06/01 ساعة الزيارة 21.36 .

[2]- chawki wahab and mouhamed wahab ، echnology Is a Double-Edged Sword: Illegal Human Trafficking in the Information Age p19.web sit:www.DROIT-TIC.fr

[3]- chawki wahab and mouhamed wahab. op.cit. p 20.

[4]– عامر محمود الكسواني، التجارة عبر الحاسوب، دار الثقافة للنشر والتوزيع، الأردن 2008 ص2 .

إن مجرمي المعلوماتية قادرين على ارسال اتصالاتهم من خلال سلسلة من الناقلين يستخدم كل واحد منهم تكنولوجيات إتصال مختلفة، هذه التكنولوجيا قد مكنت المجرمين من أن ينأوا بأنفسهم بشكل أسهل عن الجرائم التي يرتكبونها ووفرت لهم درجة من عدم الكشف عن الهوية أو التمويه مما يسمح لهم بارتكاب جرائمهم مع حد أدنى من المخاطر[1].

الفرع الثاني : الهاتف النقال والخدمات المرتبطة به

سنتناول من خلال هذا الفرع التعريف بالهاتف النقال ثم التعرف على الخدمات التي يقدمها .

اولا / الهاتف النقال

أجهزة الهاتف النقال هي أحد الأجهزة الإلكترونية التي باتت تشكل جزءا هاما من الجرائم الإلكترونية كأداة تستخدم لارتكاب هذه الجرائم، والهاتف الخلوي أو الهاتف المحمول أو الهاتف الجوال أو الهاتف السيار Mobile Phone وهو أحد أشكال أدوات الإتصال والذي يعتمد على الإتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة ضمن مساحة معينة[2] .

ومع التطور التكنولوجي أصبحت أجهزة الهاتف النقال أكثر من مجرد وسيلة إتصال صوتي بحيث أصبح تستخدم كأجهزة كمبيوتر ويمكنها التصوير بنفس نقاء ووضوح الكاميرات الرقمية وكذلك يمكن من إرسال الرسائل القصيرة لأي مكان في العالم[3]، ويعد جهاز الهاتف النقال هو أحد الأجهزة الذكية التي تدار بواسطة أحد البرامج المعلوماتية، وبدون هذا البرنامج (الكيان المنطقي للنظام المعلوماتي) تصير المكونات المادية لهذا الجهاز والعدم سواء[4]، وبسبب الخدمات التي تقدمها

---

[1]- لمزيد من التفصيل أنظر محمد الصالح حامدي، المرجع السابق ص 6، 7، 8 .

[2]- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية – دراسة مقارنة – طبعة أولى، منشورات الحلبي الحقوقية 2014 ص 74 .

[3]- طارق عفيفي صادق أحمد، طارق عفيفي صادق أحمد، الجرائم الإلكترونية – جرائم الهاتف المحمول – دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، المركز القومي للإصدارات القانونية، القاهرة 201 ص 15 .

[4]- طارق عفيفي صادق أحمد، المرجع نفسه ص 17.

الهواتف النقالة لحامليها باتت بديلا لأجهزة الحاسب الألي حيث تحمل خصائصه ومكوناته، ولكن على نحو مصغر بل تحوي أيضا على مزايا تفوق أجهزة الحاسب الألي من حيث البرامج و التطبيقات الخاصة بالهواتف النقالة.

تأتي الأهمية العلمية للهاتف النقال من خلال القدرات التقنية التي يتمتع بها هذا الجهاز والتي ساعدت على إنتشاره بشكل ملحوظ في الأونة الأخيرة، إكتسبها نتيجة التطور المستمر في صناعته والتي إستفادت من الدراسات الحديثة في مجال المعلومات والإتصال نتج معها ظهور بعض الأجهزة التي يصعب عدها في إطار الهواتف الذكية، وتأتي على رأس الخدمات المضافة للهاتف الخليوي : خدمات الإتصال الصوتي وأحيانا خدمات الإتصال المرئي والمتوفرة في الهواتف الأكثر حداثة والتواصل عبر الرسائل النصية أو رسائل الوسائط المتعددة والإتصال بشبكة الأنترنت[1].

ثانيا / الخدمات المرتبطة بالهاتف النقال

سنتناول الخدمات التي يكون لها دور في ارتكاب الجريمة الالكترونية بإعتبارها أداة أو وسيلة لارتكابها، كتقنية البلوتوث، تقنية الكاميرا وخدمات الأنترنت المضافة بالهواتف الذكية .

1/ تقنية البلوتـــــــوث[2]

يمكن تعريفه بأنه "وسيلة ذات مواصفات عالمية تستخدم لربط كافة الأجهزة المحمولة مع بعضها البعض مثل الكمبيوتر والهاتف المحمول والكمبيوتر الجيني والأجهزة السمعية والرقمية ليتمكن مستخدموا هذه الأجهزة من تبادل المعلومات ونقلها فيما بينهم عبر أجهزتهم"[3].

---

[1]– سعد جاد الله حيدر، النظام القانوني لعقد الإتصالات الحديثة " الهاتف النقال " دار الكتب القانونية، 2012 ص19.

[2]– كلمة بلوتوث بالعربية تعني " السن الأزرق " أخذت من إسم ملك دنماركي (HARALD BLATAND) عاش في القرن العاشر للميلاد إشهر بمقدرته الفريدة على الإتصال والتواصل مع الأخرين. ينظر هالة محمد عنبة، دليل تطبيقات الحاسب والأنترنت والهاتف الجوال في الإدارة والتسويق، المنظمة العربية للتنمية الإدارية 2009 ص 50.

[3]– طارق عفيفي صادق أحمد، المرجع السابق ص 21 .

وعرفه البعض بأنه "منظومة لمجموعة من الأجهزة للإتصال فيما بينها بروابط لاسلكية قصيرة المدى وتستخدم في مختلف أجهزة الكمبيوتر المرتبطة بالشبكات المحلية وفي الهواتف المحمولة وغيرها من التقنيات اللاسلكية"[1].

والبلوتوث تقنية تعتمد على نظم اتصال الراديو ذو الموجات القصيرة لنقل البيانات لمسافات قصيرة وغالبا ما يكون في إطار ما يتراوح بين المتر والعشر أمتار وأحيانا يصل إلى المئة متر دون الحاجة إلى إستهلاك كبير من الطاقة الكهربائية، وسواء بين أجهزة الهواتف الذكية أو بين أحد هذه الهواتف وأحد الحواسيب الآلية، فهـــــــذه التقنية تمكن مستخدمي هذه الأجهزة من تبادل البيانات والمعلومات عبر الموجات اللاسلكية دون الحاجة لأن تكون هذه الأجهزة في ترتيب معين إذ تكون هذه التقنية فعالة حتى لو كانت هذه الأجهزة في أماكن مختلفة طالما كانت هذه الأماكن داخلة في نطاق البث[2] .

2/ تقنيـــــة الكاميـــــــرا المدمجـــــة

أصبحت الهواتف الذكية تحتوي على العديد من التقنيات المدمجة ومن ذلك الكاميرا الرقمية[3] والتي تحظى بإهتمام غالبية مستخدمي هذه الهواتف من أجل التصوير الفوتوغرافـــــي

---

[1]– طارق عفيفي صادق أحمد، المرجع السابق ص 22 .

[2]– يرجع التطور التاريخي لتقنية البلوتوث لعام 1980 عندما بدأت تجارب ربط الأجهزة الإلكترونية بواسطة الإتصال اللاسلكي للتغلب على عقبات الإتصال السلكي (الإستهلاك الإضافي للكهرباء، ورداءة الإتصال بين الأجهزة المربوطة سلكيا ببعض) أنظر هالة محمد عنبة، المرجع السابق ص 50 .

[3]– هذه الكاميرات لا تختلف عن آلات التصوير من حيث المهام إلا أنها تتميز بعدم حاجتها إلى عملية معالجة خارجية للصور الملتقطة بواسطتها كما في التصوير العادي، إذ يتم تنزيل الصور على وسيط إلكتروني قد يكون ذاكرة الهاتف أو ذاكرة إضافية، وبالتالي يلزم لقراءة أو إخراج الصور إتصال الكاميرا بقارئ إلكتروني كشاشة مصغرة متصلة بالكاميـــــرا ذاتها أو بجهاز الحاسوب أو الهاتف النقال . مقال بعنوان : ماهي الكاميرا الرقمية وماهي أنواعها ؟ منشور على الموقع الالكتروني التالي http://Lightfragrance.wordpress.com تاريخ الزيارة 2025/02/18 ساعة الزيارة 18.20 .

والفيديـــــــــــــــــــــــــــوي ويمكنها التصوير بنفس نقاء الكاميرا الرقمية ووضوحها[1]، وأيضا تسجيل مقاطع الفيديو وإرسالها إلى أي هاتف نقال أخر بواسطة نظام الوسائط بعد تفعيل الخدمة وإنزالها في جهاز الحاسب الآلي أو أي جهاز هاتف نقال أخر[2] .

3/ خدمـــــات الأنترنت للهاتـــــف النقـــــال

من الخدمات المميزة التي ساهمت في إنتشار إستخدام الهواتف الذكية تزويد هذه الاجهزة بالقدرة على الإتصال بشبكة الأنترنت وبالتالي صار بمقدور المستخدم الإستفادة من مختلف الخدمات الرقمية وفي أي مكان؛ وأصبح بإمكانه تسيير أعماله المالية أو التجارية أو الإدارية عن بعد وكذلك التواصل مع الأخرين عبر المواقع المختلفة وخاصة شبكات التواصل الإجتماعي، والغالب أن تفرض شركات الهاتف أو مزود خدمة الأنترنت رسما على مستخدم الهاتف عند رغبته الدخول إلى شبكـــــة الأنترنت أو عند رغبته في الحصول على بعض خدماتها أو عند تنزيل بعض الملفات.

ويوفر الهاتف النقال لمستخدميه إمكانية إرسال أو استقبال البيانات على شكل رسالة قصيرة للإبلاغ عن خبر موجز أو إيصال ملاحظة وباستخدام حروف وأرقام حتى 160 رقماوحرفا[3] عن طريقخدمات الرسائل الهاتفية القصيرة الإضافية(SMS)، وخدمات الوسائط المتعددة الإضافية(MMS)[4] وخدمة (EMS)[5]ويحصل المستخدم على الخدمتين الأخيرتين مقابل رسم إضافي.

---

[1]– صابرين يوسف عبد الله، دور الأدلة المرئية في الإثبات الجنائي، مقال منشور في مجلة كلية الحقوق، جامعة النهرين المجلد 19، العدد 02، لسنة 2017 ص 263 .

[2]– حنان ريحان مبارك المضحكي، المرجع السابق ص 79 .

[3]– أروى تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة إستخدامه في الإتصال بالأنترنت، دراسة مقارنـــــــة، مجلة الحقوق، مجلد 11، عدد 06، دمشق ص 17 .

[4]– تتضمن هذه الخدمة إرسال الرسائل النصية والمصورة والملفات الصوتية والمرئية كالفيديو بمحتوى أكبر مقارنة بالرسائل العادية يصل حجمه إلى 100 كيلو بايت في الرسالة الواحدة، بينما لا يتعدى حجم الرسالة القصيرة العادية 140 بايت.أنظر طارق عفيفي صادق أحمد، المرجع السابق، هامش 2 ص 19.

[5]– تسمى بخدمة الرسائل المتطورة وهي خدمة تتيح إمكانية إرسال الرسوم البيانية والنغمات إلى الهواتف الجوالة الأخرى المزودة بخدمة الرسائل المطورة، إضافة إلى الرسائل النصية، مقال بعنوان شرح لبعض مصطلحات الجوال منشور على

ومن خدمات الانترنت للهاتف النقال ايضا بروتوكول التطبيق اللاسلكي أو الواب هو نظام كمبيوتري يحول صفحات الأنترنت المصممة للكمبيوتر ليجعلها صغيرة بشكل يناسب الهواتف المحمولة أو الأجهزة الإلكترونية المحمولة الأخرى وتتيح خدمة بروتوكول التطبيق اللاسلكي إرسال الرسائل من أي بريد الكتروني والإتصال بأي موقع على الشبكة للإستفسار عن أي معلومات يريدها المستخدم، وهذا يعني أن الإشكالات التي تثيرها المواد التي يمكن الوصول إليها عبر أجهزة الحاسب يمكن أن تثار أيضا عند الدخول الى الأنترنت بواسطة الهاتف النقال كالإستخدام الإجرامي للشبكات.

الموقع الإلكتروني https://artist-dz.yoo7.com تاريخ الزيارة 2018/12/10 ساعة الزيارة 17.20 .

المبحث الثاني : مكافحة الجرائم الالكترونية في اطار قانون العقوبات والقوانين الخاصة

التجأت معظم الدول في إطار تشريعها الداخلية إلى العمل على مكافحة الجرائم الالكترونية واختلفت في كيفيتها التشريعية المتبعة في سبيل تلك المواجهة، فمنها من عمد إلى إصدار تشريع مستقل يعالج هذه الجرائم، ومنها من ذهب إلى التوسع في النصوص الجزائية القديمة لتشمل هذا النوع من الإجرام، ومن الدول من عالجها عن طريق سن نصوص خاصة تندرج ضمن قوانين خاصة أو عن طريق التعديل في قانون العقوبات الخاص بها على غرار المشرع الجزائري .

وفي هذا الشأن خصصنا هذا المبحث للخوض في (**مكافحة الجرائم الالكترونية في اطار قانون العقوبات والقوانين الخاصة)** الذي ارتأينا تقسيمه إلى مطلبين، عنوننا الأول ب (**مكافحة الجرائم الالكترونية في اطار قانون العقوبات)** في حين حملنا المطلب الثاني(**مكافحة الجرائم الالكترونية في اطار القوانين الخاصة)**

المطلب الاول : مكافحة الجرائم الالكترونية في اطار قانون العقوبات

خطى المشرع الجزائري خطوات كبيرة في مجال مكافحة الجريمة الالكترونية، ويعتبر القانون الجزائري من بين التشريعات السباقة في مجال مواكبة التشريعات الغربية التي سعت إلى مكافحة هذا

النوع من الجرائم، وذلك بعد أن أقر بتجريم صور الاعتداء على شبكة الانترنت و ايضا المساس بالبيانات المعالجة آليا في إطار أحكام التعديل الذي شمل قانون العقوبات[1].

وتشمل الجرائم الواردة في قانون العقوبات الجرائم المتعلقة (**بالمساس بأنظمة المعالجة الآلية للمعطيات)** وهو ما ستتم دراسته في الفرع الاول، و نعرض في الفرع الثاني لـــــ **(الجرائم المرتكبة بواسطة منظومة معلوماتية)** .

الفرع الاول : الجرائم الماسة بأنظمة المعالجة الألية للمعطيات

وتشمل هذه الجرائم كل من **(جريمة الدخول والبقاء الغير مشروع داخل نظام المعالجة الألية للمعطيات)** اولا و**(الاعتداءات العمدية على المعطيات داخل النظام)** نعرض لها ثانيا، ونعرج على **(المساس العمدي بالمعطيات خارج النظام)** ثالثا، واخيرا **(جريمة الاتفاق الجنائي في الجرائم السابقة)** رابعا.

اولا / جريمة الدخول والبقاء الغير مشروع داخل نظام المعالجة الالية للمعطيات

نصت المادة 394 مكرر في فقرتها الاولى من قانون العقوبات على ما يلي " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من (50.000 دج) إلى (100.000دج) كل من يدخل أو يبقـــى عـــن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك".

من خلال نص المادة 394 مكررف/01 يتمثل السلوك الاجرامي في جريمة الدخول والبقاء الغير مشروع داخل نظام المعالجة الالية للمعطيات في صورته البسيطة في مايلي :

---

[1]–جاء في القانون رقم 15/04 المتمم والمعدل للأمر 66–156 المتضمن قانون العقوبات قسم سابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، وفي عام 2006 ادخل تعديلا أخر لقانون العقوبات بموجب القانون رقم23/06 لكن هذا الأخير لم يمس بالنصوص التجريمية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات بل شدد في العقوبات المقررة لهذه الأفعال فقط، وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، لذلك آثر استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات

1/ فعل الدخول: كلمة الدخول ينصرف معناها إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي أو السيطرة على المعطيات والمعلومات التي يتكون منها، لكن فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، وإنما يتخذ هذا الوصف إنطلاقا من كونه قد تم دون علم ورضا صاحبه[1]، ولا يتطلب لقيام ركنها المادي توافر نتيجة معينة لاننا بصدد الجريمة في صورتها البسيطة[2]، وهي كذلك من الجرائم المستمرة لأن سلوك الجاني يمتد فيها طالما ظل يستغل النظام بطريقة غير مشروعة.

بمعنى اخر يستفاد من نص هذه المادة أنه يقصد بجريمة الدخول غير المصرح به الدخول غير المشروع – وهو ما عبر عنه المشرع – بالغش – إلى منظومة المعالجة الآلية هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع علمه بذلك .

ومن الحالات التي يكون الدخول غير مصرح به في النظام المعلوماتي، دخول الفاعل إلى النظام دون تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح ويدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول إليها وهذا الفرض في الغالب يتم من طرف العاملين في المؤسسات التي يوجد بها النظام المعلوماتي، ويتحقق الدخول غير المصرح به بأي وسيلة من الوسائل، فقد يتم باستعمال كلمة المرور الحقيقية متى كان الجاني مخول في استعمالها، أو عن طريق استخدام برامج خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر او من خلال شخص مسموح له بالدخول سواء ثم عن طريق شبكة الاتصال الهاتفية أو عبر الانترنت[3].

2/ فعل البقاء: تتحقق هاته الصورة في حالة البقاء الغير مشروع داخل النظام ضد ارادة من له حق السيطرة على النظام . كما تقوم هذه الجريمة عند الدخول بتصريح عندما تتحقق الافعال التالية:

- عند تجاوز المدة المحددة .

---

[1]– اجعود سعاد، الحماية الجزائية لتكنولوجيا الاعلام والاتصال في التشريع الجزائري – دراسة على ضوء النصوص المستحدثة " مقال منشور في مجلة الرسالة للبحوث الانسانية، مجلد 07، العدد 04 لسنة 2022 ص 219 .

[2]– حابت امال، المرجع السابق ص 57 .

[3]– بطيحي نسمة، جريمة الدخول او البقاء غير المشروع ، مقال منشور في مجلة الفقه القانوني والسياسي، جامعة ابن خلدون تيارت، المجلد 01 ، العدد 01 ص 78

- الدخول في النظام عن طريق الخطأ و لم يتم الانسحاب.
- طباعة نسخة من المعلومات .
- كما يمكن لفعل البقاء أن يجتمع مع فعل الدخول الغير مشروع الى نظام المعالجة الالية للمعطيات و ذلك في الحالة التي لا يكون للجاني فيها حق ا دخول و يدخل عن طريق الغش ويبقى رغم ذلك.[1]

كما تنص المادة 394 مكرر في فقرتها الثانية على أنه " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة

واذا ترتب عن الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة ...."

اورد المشرع الجزائري ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية بالنسبة لكل الأنظمة وظرف خاص مشدد إذا كان النظام متعلق بأنظمة معلوماتية تابعة لقطاع الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[2]، ولكي تتوفر هذه الظروف المشددة المذكورة في المادة 394 مكرر (فقرة 1 و 2) لا بد من إثبات وجود علاقة سببية بين فعل الدخول أو البقاء غير المرخص به والنتيجة الإجرامية التي حددتها المادة في محو او تعديل بيانات النظام أو تخريب تشغيل النظام ذاته، وعادة ما يأخذ التخريب صورة التعطيل[3] أو الإفساد[4]، وإلا كنا بصدد جريمة في صورتها البسيطة المذكورة في نص المادة 394 مكررف/01 من قانون العقوبات. تجدر الإشارة إلى أن هذه النتيجة ذاتها هي التي اعتبرها المشرع الجزائري ظرفا مشددا في الجريمة، أي أنه يكفي أن يترتب عن جريمة الدخول أو البقاء محوا أو تعديلا في بيانات النظام أو تخريب تشغيل هذا

---

[1] – اجعود سعاد، المرجع السابق ص 219 .

[2]– أما بالنسبة للدخول والبقاء في الانظمة التابعة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام هي بحد ذاتها ظرف مشدد حتى وان لم يتم تعديل أو تغيير أو محو أو إتلاف اشتغال المنظومة، فالظرف المشدد هنا هو محل الجريمة والمتمثل في الأنظمة المعلوماتية التابعة للدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.

[3] – المقصود بالتعطيل او الاعاقة كل فعل يتسبب في تباطؤ او ارتباك عمل نظام المعالجة و من ثم ينتج تغيير في حالة عمل النظام .

[4] – أما الإفساد والتعييب فالمقصود به كل فعل وان كان لا يؤدي الى التعطيل الا انه يؤدي الى جعل نظام المعالجة الالية غير قادر على الاستعمال السليم، وبالتالي الوصول الى نتائج غير تلك المرغوب فيها و التي كان من المفروض الحصول عليها.

النظام كي يتحقق الظرف المشدد ولا يهم أن يكون تحقيقها مقصودا من طرف الجاني أو غير مقصودة[1].

ثانيا/ الاعتداءات العمدية على المعطيات داخل النظام (التزوير المعلوماتي)

تنص المادة 394 مكرر 1 من قانون العقوبات على مايلي" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من (500.000 دج) إلى (2.000.000 دج) كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو بطريق الغش المعطيات التي يتضمنها" .

تتجسد هذه الاعتداءات العمدية الواردة في نص المادة 394 مكرر 1 في الصور التالية:

1/ فعل الإدخال : المقصود به إضافة معطيات جديدة على الدعامة الخاصة سواء كانت خالية أو كان يوجد عليها معطيات من قبل، كما يتحقق فعل الادخال في كل حالة يتم فيها إدخال برنامج غريب.

2/ فعل الازالة : المقصود به ازالة جزء من المعطيات المسجلة داخل النظام أو كلها، وان ذهبنا إلى المعنى اللغوي فان معنى " **الحذف** " هو "**الاسقاط** " بينما يعني مصطلح " **الازالة**" " **الابعاد** " من المكان، ومنه فان المشرع قد يكون فرق في الاثار بين الفعلين، فحذف بيانات الكترونية معينة يكون بإسقاطها من موقعها في النظام المستهدف ولو كان بصفة مؤقتة، مما يعني ظرفيتها وبذلك تكون قابلة للاسترجاع عن طريق برامج خاصة " Logiciel de récupération de données électroniques" بالرغم من صعوبتها، ولكن إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل كامل، لذلك يكون المشرع قد فرق بين الفعلين الاجراميين واعتبر فعل الازالة أشد وطأة لذا فرق بين عقوبة كل فعل مجرم منهما[2].

[1] – حابت امال، المرجع السابق ص 57 .

[2] – بن دراح علي ابراهيم، محاضرات في الجرائم المعلوماتية مقدمة لطلبة السنة الثانية ماستر– تخصص قانون جنائي وعلوم جنائية– المركز الجامعي بأفلو 2021/2020 منشورة على الموقع الالكتروني :

3/ التعديل: ان المقصود به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويكفي أن تتحقق إحدى هذه الصور ولا تشترط اجتماعها[1] .

يرجع سبب تجريم المشرع الجزائري للأفعال المذكورة أعلاه بنص مستقل عن جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة واللتان تمثلان الطريق العادي للوصول إلى المعطيات الموجودة داخل النظام وارتكاب جريمة محو أو إدخال أو تعديل ضدها، إلى وجود طرق أخرى لاقتراف هذه الأفعال عن بعد أي دون الدخول او البقاء في النظام، كاستخدام مثلا القنابل المعلوماتية الخاصة بالمعطيات أو برامج الفيروسات[2].

ولا يشترط اجتماع هذه الصور جميعا لكي تقوم الجريمة بل يكفي ارتكاب فعل واحد (الادخال، المحو التعديل) لكي تقوم الجريمة لكن القاسم المشترك بين هذه الافعال هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة أو محو أو تعديل أخرى قائمة .

ثالثا/ المساس العمدي بالمعطيات خارج النظام (الاحتيال المعلوماتي)

نصت المادة 394 مكرر 2 على ما يلي " يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من (1.000.000 دج) إلى (5.000.000 دج) كل من يقوم عمدا وعن طريق الغش بما يأتي:

1 – تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2 – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

---

https://www.cu-aflou.dz › DocPdf › publications تاريخ الزيارة 2025/02/15 الساعة 11.23 .

[1] – اجعود سعاد، المرجع السابق ص 220 .

[2] – بطيحي نسمة، المرجع السابق ص 80 .

من خلال الفقرة الاولى من نص المادة اعلاه نرى انه يقصد بالمعطيات الخارجية للنظام تلك المخزنة او تلك المفرغة في دعامة مادية خارج النظام كالأقراص أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب، ويقصد بالمعطيات المعالجة إما تلك التي أصبحت جزءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، وإما تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل إرسال المعلومات بين أجهزة المنظومة المعلوماتية، فالأولى تعتبر معطيات داخلية للنظام والثانية هي معطيات النظام الخارجية[1] وعليه فأي تلاعب بالمعطيات المذكورة أعلاه، و استعمالها عمدا أو عن طريق الغش بإحدى الطرق المحددة في نص المادة اعلاه أي تصميمها أو بحثها أو تجميعها أو توفيرها أو نشرها أو الاتجار بها أو حيازتها أو إفشاءها أو نشرها يعد جريمة اعتداء على المعطيات الخارجية لنظام المعالجة، فالغاية من تجريم هذه الافعال وقائية لأن هذه الجرائم هي جرائم خطر يهدف المشرع من خلالها الى تفادي وقوع الضرر .

كما جرم التعامل في المعطيات المحصلة من إحدى الجرائم المنصوص عليها في القسم السابع مكرر بحيازتها أو نشرها او استعمالها لأي غرض كان وهي المحصلة أو نتيجة لارتكاب الاعتداءات الماسة بأنظمة المعالجة الألية للمعطيات..

رابعا/ جريمة الاتفاق الجنائي لارتكاب جريمة معلوماتية

تنص المادة 394 مكرر5 من قانون العقوبات على مايلي " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"

من خلال نص المادة يشترط للعقاب على الاتفاق الجنائي مايلي:

- اشتراط المشاركة في مجموعة او اتفاق.

- يجب أن يكون الغرض من الجماعة هو الإعداد لارتكاب جريمة من جرائم المساس بنظام المعالجة الآلية للمعطيات

- تجسيد التحضير بفعل مادي كتبادل المعلومات حول كيفية ارتكاب الجريمة.

[1] – حابت امال ، المرجع السابق ص 58 .

– القصد الجنائي وهو توفر العلم لدى كل فرد من الجماعة انه عضو فيها وان تتجه إرادته للقيام بإعمال تحضيرية ولا يشترط أن يعلم الفرد بنشاط غيره .

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد، كما انه المشرع عاقب على الاتفاق الجنائي بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار[1]، فرغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي.

اما بالنسبة للركن المعنوي فان جرائم المساس بأنظمة المعالجة الالية للمعطيات هي جرائم عمدية إذ تعد جرائم الدخول و البقاء الغير مشروع بصورتيها البسيطة أو المشددة و جرائم الاعتداءات العمدية على المعطيات و الاعتداء العمدي على سير عمل النظام عن طريق التعامل في المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم من قبيل الجرائم العمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم و الارادة[2] ، وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة فإذا أثبت الجاني انتفاء السببية بين السلوك الاجرامي والنتيجة الجرمية كأن يثبت أن التعديل أو المحو أو عدم صلاحية النظام للقيام بمهامه يرجع الى قوة قاهرة أو حادث فجائي ينتفي القصد الجنائي وإذا كان الجاني يعتقد أن دخوله أو بقاؤه داخل النظام مسموح به أي مشروع او كان الجاني يجهل بوجود حظر الدخول او البقاء ينتفي القصد الجنائي.

أما بالنسبة لنية الغش التي أقرنها المشرع بالركن المعنوي فهي لا تدل على اشتراط توافر قصد جنائي خاص أي قصد الإضرار بالغير فهي قرينة على سوء النية تتحقق بمجرد ارتكاب الواقعة

[1] – المادة 176 من قانون العقوبات على انه " كل جمعية او اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تألف بغرض الإعداد لجناية أو أكثر، او لجنحة أو أكثر معاقب عليها بخمس (05) سنوات حبس على الأقل ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

[2] – اجعود سعاد، المرجع السابق ص 222.

المادية فالجريمة مثلا تقوم بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الارادة اليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الاجرامي إلا أنه ليس عنصرا في الجريمة[1].

الفرع الثاني : الجرائم الواقعة بواسطة منظومة معلوماتية

بموجب تعديلات قانون العقوبات تم ادراج مواد خاصة بالجرائم الالكترونية بهدف مواكبة التطورات التكنولوجية وحماية المجتمع من مخاطر الاستعمال غير المشروع لتكنولوجيا الاعلام والاتصال، وهذه الجرائم هي في الاصل جرائم تقليدية ترتكب في الواقع المادي لكن مع تطور وسائل الاتصالات انتقلت هذه الجرائم الى الفضاء الرقمي مما استدعى تدخل المشرع لتكييفها قانونيا وتوفير نصوص جديدة تأخذ بعين الاعتبار وسيلة ارتكاب الجريمة دون ان تغير من طبيعتها الاصلية، وبالتالي فالمشرع قام بتكييف الجرائم التقليدية مع الوسائط الحديثة لضمان شمولية الردع والحماية مع تشديد العقوبات احيانا نظرا لخطورة هذه الافعال وصعوبة تعقب مرتكبيها في العالم الرقمي، ونظرا لصعوبة الالمام بكل هذه الجرائم سوف نكتفي بتناول نماذج منها توضيحا لطبيعتها، ومن بينها سوف نعرض اولا لـــــــ **(جرائم الارهاب الالكتروني)** ونتناول ثانيا **(جرائم الاعتداء على حرمة الحياة الخاصة)**

اولا / الارهاب الالكتروني

اتجه المشرع الجزائري قبل تعديل قانون العقوبات لسنة 2016 إلى تجريم أفعال توصف في ظاهرها بالإرهاب، مستعملا دائما عبارات أكثر شمولية في وقتها وفاتحة المجال لاستيعاب وسائل جديدة قد تستعمل في ارتكاب مثل هذه الجرائم مستقبلا، اذ كان يستعمل دائما عبارات مثل " بأية طريقة " أو " بأي وسيلة كانت"[2]، إلا أنه وتكريسا لمبدأ الشرعية وتجاوزا لمسألة اصطدام القضاء في

---

[1]– عباس كريمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مقال منشور في مجلة البيبان للدراسات القانونية والسياسة، عدد04 ديسمبر 2017 ص 125 و 126 .

[2]– بالعودة إلى نصوص قانون العقوبات قبل تعديله سنة 2016 بموجب القانون 02/16 المؤرخ في 10 يونيو 2016 يظهر أن المشرع أراد من خلال نص المادة 87 مكرر ق.ع حين استعمل عبارة " عن طريق اي عمل" توسيع نطاق تجريم أفعال الإرهاب ليستوعب حسب الوضع الظاهر باية طريقة أو وسيلة تستحدث مستقبلا قد تستعمل في ارتكاب هذه الأفعال بما يفتح المجال إلى إدخال ما يسمى أفعال الإرهاب الالكتروني في نطاق التجريم والعقاب، ونقصد هنا

العديد من المرات بقاعدة عدم جواز القياس في المادة الجزائية من جهة، ومن جهة أخرى لخلق توافق مع نص المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تجرم الأفعال المرتبطة بالإرهاب والمرتكبة بواسطة التقنية[1]، لجأ المشرع الجزائري إلى تعديل قانون العقوبات لسنة 2016 بإضافة المادتين 87 مكرر 11 و 87 مكرر 12 ليضم بعض الافعال المرتبطة بالإرهاب المرتكبة بواسطة تكنولوجيا الإعلام والاتصال ونعالجها في الصور الاتية :

1/ استخدام تكنولوجيات الإعلام والاتصال في السفر لأنشطة إرهابية

عددت المادة 87 مكرر 11 من قانون العقوبات صور للأنشطة الإرهابية ومن بينها ما جاءت به الفقرة الأولى من تجريم للسفر ونصت بأنه ".. كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها" وفي الفقرة الأخيرة: " يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة " وبالتالي تستخدم تكنولوجيات الإعلام والاتصال في تسهيل السفر الذي يكون غرضه أنشطة إرهابية.

وحددت المادة نفسها في الفقرة الأولى نطاق تجريم السفر لغرض الإرهاب، بحيث يطبق نص المادة على الجزائري والأجنبي الذي يأتي جريمة السفر لأغراض إرهابية أو يستخدم تكنولوجيات الإعلام والاتصال في ارتكابها، ويكون القصد الخاص من السفر هو ارتكاب الأعمال الإرهابية أو من

الأفعال التي تستعمل فيها التقنية المعلوماتية كأداة للاعتداء وليس كهدف، ليدعم المشرع هذا النص بموجب تعديل قانون العقوبات رقم 02/16.

[1]– حصرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة في 21 ديسمبر 2010 ظاهرة "الإرهاب الإلكتروني في" استخدام تقنية المعلومات للأعمال الإرهابية " وعددتها المادة 15 منها بأن: " الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلوماتهي " نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية، نشر النعرات والفتن والاعتداء على الأديان والمعتقدات".

خلال التدبير أو الإعداد أو المشاركة أو التدريب أو تلقي تدريب على الأعمال الإرهابية[1]، وتعد أعمال التدبير أو الإعداد أو المشاركة بمثابة أعمال مساعدة أو معاونة في قانون العقوبات الجزائري، ومنصوص عليها في القواعد العامة التي تحكم الاشتراك في الجريمة في المواد من 42 إلى 44 قانون العقوبات .

2/ استخدام تكنولوجيات الإعلام والاتصال في الأعمال المسهلة للسفر لأنشطة إرهابية

اعتبر المشرع الجزائري تكنولوجيا الاعلام والاتصال وسيلة تسهيل للسفر سواء من خلال توفير وجمع الأموال أو التمويل، وكذا تنظيم السفر، وسنتناول هذه الصور كالاتي:

أ/ تكنولوجيا الإعلام والاتصال وسيلة توفير وجمع للأموال أو تمويل للسفر

ورد في نص المادة 87 مكرر 11ف2و3 من قانون العقوبات تجريم لأفعال "التوفير والجمع والتمويل" ويعد التوفير بمثابة إيجاد للمصادر التي يتم جمع الأموال منها، أما جمع الأموال يعني تحصيلها من مصادر مختلفة، ويعد القائم بجمع الأموال ليس هو من يعمل على توفيرها، بالتالي تظهر ضرورة تجريم كل فعل على حدى، ومن جانب آخر يعد التوفير والجمع للأموال بمثابة أعمال تندرج تحت المفهوم العام لـــــ "التمويل"[2] ويكون التوفير بمثابة وسيلة مباشرة بينما الجمع وسيلة غير مباشرة للتمويل[3].

---

[1] –جاء في البروتوكول الإضافي لاتفاقية مجلس أوروبا لمنع الإرهاب في المادة 38 منه في البند الأول على أنه لاغراض هذا البروتوكول يعني (تلقي تدريب للإرهاب) " تلقي تعليمات بما في ذلك الحصول على المعرفة أو المهارات العملية من شخص آخر في صنع أو استخدام المتفجرات أو الأسلحة النارية أو غيرها من الأسلحة أو المواد الضارة أو الخطرة، أو في الوسائل أو الطرق بغرض تنفيذ جريمة إرهابية أو المساهمة في ارتكابها".

[2] – وهذا ما أكدته المادة 05 الفقرة الاولى من البروتوكول الإضافي لاتفاقية مجلس أوروبا لمنع الإرهاب والتي عرفت "تمويل السفر إلى الخارج لغرض الإرهاب" بأنه " توفير أو جمع للأموال كليا أو جزئيا بأي وسيلة كانت سواء بشكل مباشر أو غير مباشر، وذلك لتمكين أي شخص من السفر إلى الخارج لغرض الإرهاب" .

[3] – بعجي عبد النور، الإرهاب الالكتروني، بين عولمة الجريمة وضرورة المكافحة، مقال منشور في مجلة الدراسات والبحوث القانونية ، المجلد 07، العدد 02 سنة 2022 ص 79.

وبالرجوع إلى قانون العقوبات لا نجد تعريف ل "التمويل" في المادة 87 مكرر 4 ويبقى الامر محال للقوانين الخاصة المكلمة لقانون العقوبات[1] .

ب/ تكنولوجيا الإعلام والاتصال وسيلة تنظيم أو تسهيل للسفر

جرمت المادة 87 مكرر 11 في الفقرة الثالثة تنظيم وتسهيل السفر لارتكاب أنشطة إرهابية، لكن لم تحدد معنى أو نطاق اعمال التنظيم والتسهيل، وبالتالي يرجع في ذلك للأحكام العامة التي تتعلق بالمساهمة في الجريمة في صورة المساعدة أو المعاونة.

ثانيا/ جرائم الاعتداء على حرمة الحياة الخاصة

تزداد الجرائم تعقيدا وخطورة اذا كانت مرتكبة عن طريق تكنولوجيا الاعلام والاتصال لاعتدائها على الحياة الخاصة للأفراد في ظل التخفي خلف ستار حرية التعبير، فيقوم الجاني باستغلال بيانات ومعلومات وصور الافراد أسوء استغلال، إذ تقوم بتداول هذه المعلومات والمراسلات والصور على شبكات التواصل والاعتداء عليها بالتنصت والتسجيل والتقاط أو تسجيل أو نقل المكالمات أو الاحاديث الخاصة أو السرية.

1/ جريمة الاعتداء على الحق في الصوت والصورة[2]

---

[1] – وفي هذا الصدد تناول القانون 01/05 المؤرخ في 06 فبراير 2005 المتضمن قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما في المادة 03 منه تعريف لجريمة تمويل الإرهاب بنصه على أنه" كل فعل يقوم به كل شخص بأي وسيلة كانت مباشرة او غير مباشرة وبشكل غير مشروع وبإرادة الفاعل من خلال تقديم أو جمع الأموال بنية إستخدامها كليا أو جزئيا من أجل ارتكاب الجرائم الموصوفة بأفعال ارهابية أو تخريبية المنصوص والمعاقب عليها بالمواد من 87 مكرر الى 87 مكرر 10 من قانون العقوبات ".

[2] – لم يكن المشرع الجزائري ينص صراحة على إضفاء صفة التجريم إزاء أي مساس بحرمة الحياة الخاصة، الا بعد أن قام بإرساء نصوص تجرم كل فعل من شأنه أن يمس بخصوصية الافراد (المواد 303 مكرر2 و 303 مكرر3 من قانون العقوبات الجزائري) فقد كانت مظاهر الحياة الخاصة محصورة فقط في انتهاك حرمة المسكن، وفض المراسلات البريدية وكشف اسرارها إلى أن أورد المشرع لفظ " الحياة الخاصة " لاول مرة في القانون رقم 23/06 المعدل والمتمم لقانون العقوبات الجزائري، وقد جاء هذا القانون بصور جديدة وحصرية تمثل انتهاك لحرمة الحياة

بين المشرع الجزائري أشكال الاعتداء على الحق في الصوت والصورة من خلال المادة 303 مكرر الفقرة الاولى من قانون العقوبات الجزائري "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطنين، وذلك بأن ارتكب أحد الافعال الاتية في غير الاحوال المصرحة بها قانونا أو بغير رضا المجني عليه :

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أورضاه.
- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه"

ويتبين من خلال الفقرة الاولى أن المشرع الجزائري قد اتخذ معيار خصوصية المحادثات ضابطا لا تتحقق دونه جريمة الاعتداء على الحق في الخصوصية، فالعبرة ليست بحماية المكان وانما بطبيعة الواقعة أو المحادثة، لان حماية القانون تمتد لتشمل المكالمات وكل حديث خاص أو سري ولو كان قد أجري في مكان عام، وقد أضفى المشرع الجزائري الصفة الجرمية على كل ما من شأنه أن يمس بسرية الاحاديث الخاصة استنادا لنص المادة 303 مكرر من قانون العقوبات الجزائري سالفة الذكر وذلك سعيا منه على تأمين حق كل فرد في أن تضمن لحياته قدرا من الخصوصية.

كما جرم المشرع افعال الالتقاط والنقل لصور الاشخاص بغير رضاهم ويتحقق النقل بتمكين شخص آخر من الاطلاع على الصورة مثل إرسال صورة من احد حسابات شبكات التواصل الإجتماعي لشخص إلى حساب شخص آخر بغرض الاضرار به أو التشهير او الابتزاز .

2/ جرائم القذف والسب عبر الانترنت

اصبحت شبكات التواصل الاجتماعي تمثل بيئة خصبة للاعتداء على الاشخاص اذ يساء استخدام هذه الشبكات في اغلب الاحيان للنيل من شرف الانسان، وقد جرم المشرع الجزائري القذف بموجب نص المادة 296 من قانون العقوبات[1] والذي يقصد به الادعاء بواقعة شائنة او اسنادها للغير والاسناد

الخاصة من ضمنها انتهاك سرية المحادثات الشخصية حيث اعتبر المشرع الجزائري أي فعل من شأنه المساس بحرمة الحياة الخاصة للافراد جريمة تعرض صاحبها للمساءلة القانونية.

[1]- عرفت المادة 296 من قانون العقوبات جريمة القذف بأنها" يعد قذف كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به، أو اسنادها اليهم أو الى تلك الهيئة، ويعاقب على نشر هذا الادعاء أو ذلك الاسناد مباشرة أو بطريق اعادة النشر، حتى و لو تم ذلك على وجه التشكيك أو اذا قصد به شخص أو هيئة دون

يفيد نسبة الامر الى شخص معين باي وسيلة وسائل التعبير ويكون من شأن الواقعة ان تسبب لضحية احتقارا عند اهل وطنه[1]، وعليه تتحقق الصورة بالعلنية ففي نص المادة المذكورة اعلاه ذكر المشرع النشر واعادة النشر وجاء الشطر الاخير من نص المادة ليستدرك الفراغ بطريقة غير مباشرة ويضيف الحديث والصياح والتهديد والكتابة و المنشورات و اللافتات والاعلانات كوسائل لنشر الادعاء واعادة نشره .

أما فيما يخص العقوبة المقررة لجريمة القذف فنص عليها المشرع في المادة 298 من قانون العقوبات حيث " يعاقب على القذف الموجه الى الافراد بالحبس من شهرين(02) الى (06) ستة أشهر وبغرامة من (25000 دج) الى (50.000 دج) أو باحدى هاتين العقوبتين ويضع صفح الضحية حدا للمتابعة الجزائية، ويعاقب على القذف الموجه الى شخص أو أكثر بسبب انتمائهم الى مجموعة عرقية أو مذهبية أو الى دين معين بالحبس من شهر (01) الى سنة (01) و بغرامة من (10.000 دج) الـــــــــــــــــــــــى (100.000 دج) أو باحدى هاتين العقوبتين فقط ، اذا كان الغرض هو التحريض على الكراهية بين المواطنيين أو السكان ".

كما عاقب المشرع الجزائري على جريمة السب بموجب نص المادة 297 من قانون العقوبات[2] دفاعا عن الافراد الذين تم المساس بشرفهم واعتبارهم، ولقد اقر المشرع الجزائري صورتين لجريمة السب الصورة الاولى هي – التعبير المشين و البذيء– وقد يكون السب بالكلمات او عن طريق الحركات او قد يكون بوسائل تعبيرية قد تكون بالقول الشفوي او الكتابة وقد تكون مطبوعة او مخطوطة كما يدخل في نطاقها الرموز والصور.

ذكر الاسم ، ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة.

[1]– زروقي عاسية، جرائم الإعتداء على الحياة الخاصة عبر شبكات التواصل الإجتماعي واليات الحماية، مقال منشور في مجلة القانون والعلوم السياسية، المجلد 08، العدد 02 لسنة 2022 ص 14 .

[2] – عرفت المادة 297 من قانون العقوبات جريمة السب بأنها " يعد سبا كل تعبير مشين أو عبارة تتضمن تحقير أو قدحا لا ينطوي على إسناد أية واقعة" .

اما الصورة الثانية فهي– العلنية– وتتحقق بالقول او الكتابة او الصور او الرسائل السمعية او البصرية او باي وسيلة الكترونية، وهذا الإعتداء على الحياة الخاصة يتم عبر الشبكات اذن فالنصوص التقليدية تتلائم الى حد ما مع الجرائم المستحدثة التي تمس بالحياة الخاصة للافراد عبر الانترنت .

كما عاقب المشرع الجزائري على جميع افعال الاعتداء بالاساءة الى شخص رئيس الجمهورية والتي قد تمس بشرفه واعتباره باي صورة من صور الاساءة التي ذكرت ضمن احكام المادة 144 مكرر من قانون العقوبات على انه " يعاقب بالحبس من (03) أشهر إلى (12) شهرا وبغرامة من (50.000 دج) الى (250.000 دج) او بإحدى هاتين العقوبتين كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى..."

ومن خلال المادة اعلاه نلاحظ ان المشرع قد احسن عندما وسع التجريم ليشمل كل وسيلة الكترونية او معلوماتية او اعلامية اخرى ترتكب عن طريقها جرائم الاساءة لرئيس الجمهورية و بالتالي يكون قد شمل كل ما قد يكشف في المستقبل من تقنيات الاعلام والاتصال .

المطلب الثاني : مكافحة الجرائم الالكترونية في اطار القوانين الخاصة

على اعتبار الجريمة الإلكترونية ظاهرة اجرامية مستحدثة تستهدف الاعتداء على المعلومات المخزنة او المعالجة في نظام الحاسب الآلي أو المتبادلة عبر الشبكات فإن طبيعتها المنفردة أدت إلى صعوبة إدراجها ضمن الأوصاف التقليدية في القوانين الجنائية الوطنية، إذ يتعين مواجهة هذه الجريمة الإلكترونية بنصوص تجريمية جديدة.

وعليه سوف نعرض للجرائم الالكترونية في القوانين الخاصة قبل صدور القانون 04/09 و بعد صدوره الذي احدث قفزة نوعية في مجال مكافحة الجرائم الالكترونية.

الفرع الاول : قبل صدور القانون 04/09

الفصل الأول الآليات الموضوعية لمكافحة الجرائم الالكترونية في التشريع الجزائري

قبل صدور القانون 04/09 كانت القوانين التي تتناول الجرائم الالكترونية محدودة مما جعل من الصعب ملاحقة مرتكبيها، وكانت المنظومة القانونية تفتقر الى نصوص واضحة ومحددة تتناول الجرائم الالكترونية بشكل صريح ومباشر ولعل ابرزها قبل صدور القانون 04/09 هي الجرائم الالكترونية الواردة في القانون المتعلق بالتأمينات الاجتماعية، وما تعلق بالجرائم الواقعة على حقوق المؤلف والحقوق المجاورة .

اولا / الجرائم الالكترونية في اطار القانون 01/08 المتعلق بالتامينات الاجتماعية[1]

لا تخلوا البطاقة الإلكترونية او بطاقة الشفاء[2] التي أعدتها الدولة لخدمة مختلف المستفيدين منها من المزورين وممن يسيئون استعمالها، لهذا وجب على المشرع التدخل بقوانين توفر الحماية للهويات الرقمية التي تكون محمولة في كل بطاقة وكذا مستفيديها، ومن اجل حماية بطاقة الشفاء حث المشرع في مواد القانون 08_01 المعدل و المتم للقانون 83_11 المتعلق بالتأمينات الاجتماعية على حماية جزائية لها متمثلة في الجرائم التي يتوقع ارتكابها ضد هذه البطاقة الالكترونية[3] لهذا حاولنا و بعد استقراء مواد هذا القانون نجد انه تم تقسيم الجرائم الواردة فيه الى جرائم تمس بمعطيات و بيانات البطاقة وأخرى تتمثل في الاستخدام غير المشروع نعرض لها في ما يلي.

1/ الجرائم الماسة ببيانات ومعطيات البطاقة

[1] – تمم هذا 01/08 المؤرخ في 23 يناير 2008 احكام القانون 83-11 المؤرخ في 2 يوليو سنة 1983 بباب خامس مكرر عنوانه "احكام جزائية" يتضمن المواد 93 مكرر 2 و 93 مكرر 3 و 93 مكرر 4 و 93 مكرر 5 و 93 مكرر 6.

[2] – تعد بطاقة الشفاء وسيلة تمكن حامليها المنتسبين الى هيئة الضمان الاجتماعي من الحصول على العلاج والخدمات المرتبطة به القابلة للتعويض من قبل الهيئة بتقديمها لهياكل العلاج او مقدمي الخدمات المرتبطة بالعلاج بدل الوفاء المباشر وفي الحالات التي حددها القانون. انظر عباوي نجاة، الحماية الجزائية لبطاقة الشفاء الالكترونية مقال منشور في مجلة الحقيقة للعلوم الانسانية والاجتماعية، صادرة عن جامعة احمد دراية- ادرار- العدد 41 لسنة 2017 ص 294 .

[3] – ولمزيد من التفصيل حول بطاقة الشفاء الالكترونية انظر المادة 6 و المادة 6 مكرر1 و المادة 6 مكرر 2 من القانون 01/08 والمرسوم التنفيذي رقم 116/10 المؤرخ في 18 افريل 2010 الذي يحدد البطاقة الالكترونية للمؤمن له اجتماعيا والمفاتيح الالكترونية لهياكل العلاج ولمهنيي الصحة وشروط تسليمها واستعمالها وتجديدها .

نص المشرع عن العقوبات المترتبة عن الجرائم التي تقع على البطاقة الإلكترونية وكذا المفتاحين الإلكترونيين الذين يكملان العمل بها في نصوص المواد 93 مكرر 03 حتى 93 مكرر 06 من القانون 01/08 .

أ / جريمة طمس أو إتلاف المعطيات

تقوم هذه الجريمة في حق كل من قام بالتلاعب بالمعطيات عن طريق الغش بالتعديل، أو الحذف الكلي أو الجزئي لها سواء التقنية أو الإدارية التي تأتي في البطاقة الإلكترونية الممنوحة للمؤمن له اجتماعيا، والأمر سيان على من يثبت عليه أحد صور الركن المادي للجنح التي ذكرناها أنفا على المفتاح الالكتروني الذي يمنح لهيكل العلاج، أو على المفتاح الالكتروني المقدم المهني الصحة، فإنه تقع عليهم عقوبة الحبس من (02) سنتين إلى (05) خمس سنوات وتوقع عليهم غرامة مالية تقدر من (500.000 دج) إلى (1.000.000 دج)[1].

ب/ جريمة التلاعب بالمعطيات

وسع المشرع الجزائري من الجرائم المحتمل ارتكابها على البطاقة الالكترونية، و يخص بالذكر أنه كل من يعد يعدل أو ينسخ بطريقة غير قانونية للمعطيات الواردة سواء في البطاقة الالكترونية، المفتاح الإلكتروني لهيكل العلاج أو المقدم المهني للصحة له نفس العقوبة المقررة لجريمة طمس او اتلاف المعطيات، وحتى يضفي المشرع حماية أكبر ويكون النص أكثر صرامة حرص أن يعاقب بنفس العقوبة كل من يشرع في أحد الجنح سابقة الذكر وهو ما استشف من مصطلح "المحاولة" الذي استعمله المشرع[2].

2/ الجرائم الماسة بالاستخدام غير المشروع للبطاقة

[1] – المادة 93 مكرر 3 في فقرتها الاولى من القانون 01/08 المتعلق بالتأمينات الإجتماعية .

[2] – المادة 93 مكرر 3 في فقرتها 2 و 3 من القانون 01/08 المتعلق بالتأمينات الاجتماعية.

فضلا عن الجرائم التي تمس بالمعطيات المدرجة في البطاقة، نص المشرع على الجرائم الناجمة عن الاستعمال غير المشروع للبطاقة أو أحد المفاتيح الإلكترونية، حيث يمكن تقسيمها إلى جريمة تسليم أو الاستلام بطريقة غير مشروعة، وجريمة أخرى تتعلق بنسخ، صنع، حيازة، أو توزيع سواء المفتاح أو البطاقة الالكترونيين بطريقة غير قانونية.

أ/ جريمة التسليم أو الاستلام غير المشروعين للبطاقة والمفتاح الالكترونيين

لم يفرق المشرع الجزائري بين من يسلم أو يستلم بطاقة الشفاء او المفتاح الالكتروني للمؤمن له اجتماعيا بهدف يتنافى مع القانون، وإنما قد أوقع عليهما نفس العقوبة التي حددت بسنتين (02) حبس إلى (05) خمس سنوات وبغرامة مالية تقدر بـ (100.000 دج) إلى (200.000 دج)[1]، وعليه كل شخص استلم أحد هاتين الوسيلتين بطريقة غير مشروعة يشوبها التباس أو تكون بطريقة تخالف القانون يتعرض لهذه العقوبة ويستوي الأمر لمن يسلمها لأغراض غير قانونية .

ب/ جريمة سوء الحيازة والتوزيع للبطاقة والمفتاح الإلكترونيين

عاقب المشرع الجزائري بعقوبة تبدأ من (02) سنتين وبغرامة مالية تقدر بـ(500.000) دج إلى (5.000.000 دج) كل شخص يقوم بـ: نسخ أو صنع او حيازة او توزيع البطاقة أو المفتاح بطريقة غير قانونية[2] كون أن مهمة صنع و طبع أو نسخ هذه البطاقات والمفاتيح مخول لهياكل الدولة فقط.

وقد عاقب المشرع الجزائري الشخص المعنوي الذي يرتكب أحد الجنح سواء الماسة بالمعطيات أو القيام بسوء استعمال البطاقة أو المفتاح الإلكترونين تكون بما يقابل خمسة أضعاف الحد الأقصى

[1] – المادة 93 مكرر 02 من نفس القانون .

[2] – المادة 93 مكرر 04 من القانون 01/08 المتعلق بالتأمينات الاجتماعية.

للغرامة المالية المقررة في أحد الجنح المنصوص عليها في المادتين 93 مكرر 03 و 93 مكرر 04[1] حيث ترى أن النص صارم أكثر مع الشخص المعنوي عن الشخص الطبيعي من حيث الغرامة المالية.

و تجب الإشارة إلى أنه لفت انتباهنا تكرار المشرع في المواد سابقة الذكر الجملة يفتتح بها المواد تتمثل في " دون الإخلال بالعقوبات المنصوص عليها في التشريح المعمول به" وهو ما يؤكد بأنه إذا تعلق الأمر بالحماية الجزائية لحقوق المؤمنين اجتماعيا فيما يخص بطاقة الشفاء الخاصة بهم أو المفتاح الالكتروني ، فإن القاضي لن يلجأ أو يستند فقط على الجنح المذكورة في القانون 01/08 وإنما يجيز له المشرع بالعبارة السابقة أن يلجا لأي نص يجرم أفعالا غير مشروعة يكون موضوعها المفتاح أو البطاقة الالكترونيين كجريمة التزوير أو انتحال صفة .. إلخ[2].

ثانيا/ الامر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة[3]

- ارتكاب جنحة التقليد عن طريق:
- الكشف غير المشروع للمصنف او المساس بسلامة مصنف او اداء الفنان مؤدي او عازف .
- استنساخ مصنف او اداء باي اسلوب من الاساليب في شكل نسخ مقلدة
- استيراد او تصدير نسخ مقلدة من مصنف او اداء...
- بيع نسخ مقلدة لمنصف او اداء .
- تاجير او وضع رهن التداول لنسخ او لمصنف او اداء[4].

-ارتكاب جنحة التقليد عن طريق انتهاك الحقوق المحمية فيبلغ المصنف او الاداء عن طريق التمثيل او الاداء العلني او البث الاذاعي السمعي او السمعي البصري او .....او أي منظومة معالجة معلوماتية[1]

---

[1] – المادة 93 مكرر 5 من نفس القانون.

[2] – بن خدير سعاد وقويدر ميمونة، الحماية القانونية للهوية الرقمية للمؤمن له اجتماعيا في اطار رقمنة خدمات الضمان الاجتماعي – بطاقة الشفاء نموذجا– مقال منشور في مجلة البحوث في الحقوق والعلوم السياسية المجلد 10، العدد 03 لسنة 2025 ص 309 .

[3] – امر رقم 03–05 مؤرخ في 19 يوليو سنة 2003يتعلق بحقوق المؤلف والحقوق المجاورة .

[4] – المادة 151 من الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة.

-الاشتراك بالعمل او بالوسائل الحائزة عليها للمساس بحقوق المؤلف او أي مالك للحقوق المجاورة[2].

الفرع الثاني : بعد صدور القانون 04/09

يعتير القانون 04/09 اول قانون اجرائي تضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام الاتصال وقد مهد الطريق أمام القضاة ووكلاء الجمهورية والشرطة القضائية للتصرف في مثل هذه الجرائم وهو ما يعد نقلة نوعية في التشريع الجزائري وأساسا مهما لاستقبال قوانين لاحقة أثر تخصصا وهو ما تجسد فعلا من خلال قوانين مكافحة الجرائم الالكترونية الصادرة بعده والتي سنتناولها في هذا الفرع .

أولا / الجرائم الالكترونية في اطار القانون المتعلق بالتوقيع والتصديق الإلكترونيين[3]

عرف المشرع الجزائري التوقيع الإلكتروني بأنه" البيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا بيانات الكترونية اخرى تستعمل كوسيلة توثيق" [4].

---

[1] – المادة 152 من نفس الأمر .

[2] – المادة 154 من نفس الأمر .

[3] – القانون رقم 15/ 04 المؤرخ في 10 فيفري2015 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين.

[4] – المادة 2 ف/01 من نفس القانون .

كما عرف شهادة التصديق الإلكتروني بأنها " وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والمواقع"[1]

اذن يرتبط التوقيع والتصديق الإلكترونيين بمجموعة من البيانات والمعلومات ذات الطابع الشخصي الذي يشكل الاعتداء عليها جريمة يعاقب مرتكبها بأحكام جزائية وردت في هذا القانون وسنتناول صور هذا الإعتداء فيما يلي :

1/ إفشاء البيانات الشخصية أو إساءة استعمالها

وفقا لهذا القانون يعاقب بالحبس من(03) ثلاث أشهر إلى (03) ثلاث سنوات وبغرامة من (1.000.000دج) إلى(5.000.000 دج) أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة او افشاء او استعمال بيانات انشاء توقيع الكتروني موصوف خاصة بالغير[2].

2/ الاخلال بسرية البيانات

لقد اراد المشرع ان يضفي حمايته على المعلومات الشخصية التي تؤخذ من الافراد واسبغ عليها صفة السرية لما لها من خصوصية معينة وحسنا فعل عندما جرم الاخلال بسرية هذه البيانات[3] فتخزين المعلومات لا يعني ان هذه المعلومات قد انتقلت من الخصوصية الى العلانية كما ان الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات الى جميع الناس .

3/ جمع البيانات الشخصية للمعني دون موافقته

نص القانون رقم 04/15 في المادة 43 منه على أنه " لا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع البيانات الشخصية للمعني إلا بموافقته الصريحة، ومتى أخل بهذا الواجب يعاقب بالحبس من

---

[1] – المادة 2 ف/07 من نفس القانون

[2] – المادة 68 من نفس القانون.

[3] – تنص المادة 42 من نفس القانون على انه " يجب على مؤدي خدمات التصديق الالكتروني ان يحافظوا على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكترونية الممنوحة فاذا اخلوا بهذا الواجب يعاقب بالحبس من 3 اشهر الى (02) سنتين وغرامة من 200000 دج الى (1.000.000 دج) او بإحدى هاتين العقوبتين وفقا لما جاء به نص المادة 70 من نفس القانون .

ستة أشهر إلى ثلاث سنوات وبغرامة من 200000 ج إلى مليون (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط[1].

ثانيا / الجرائم الالكترونية في اطار القانون المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية[2]

اكد هذا القانون على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد وفي حالة مخالفة ذلك يتعرض المخالف للأحكام الجزائية التي تضمنها هذا القانون والمتمثلة فيما يلي :

1 / انتهاك سرية المراسلات الإلكترونية

جرم المشرع الجزائري بموجب هذا القانون كل انتهاك لسرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو افشاء مضمونها أو نشره أو استعماله بدون ترخيص من المرسل أو المرسل إليه أو تغيير وجودها[3] وتتحقق هذه الجريمة باطلاع الشخص على الرسائل الإلكترونية أو سماع المحادثات الإلكترونية بصورة غير مشروعة بصرف النظر عن مضمونها أو محتواها فيما إذا كان يتضمن أسرار ام لا إضافة إلى افشاء مضمونها أو نشره أو استعماله بدون ترخيص.

2 / تحويل المراسلات الصادرة عن طريق البريد الإلكتروني

عاقب المشرع من خلال المادة 165 من القانون رقم 04/18 بالحبس من سنة(01) إلى(03) ثلاث سنوات وبغرامة من (1.000.000) مليون إلى (5.000.000) خمس ملاين دينار أو بإحدى هاتين العقوبتين كل متعامل للاتصالات الالكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية.

---

[1] – نصت على هذه العقوبة المادة 71 من نفس القانون .

[2] – اصدر المشرع الجزائري القانون رقم 04/18 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية والذي ألغى بموجبه القانون رقم 3/2000 المحددة للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية .

[3] – المادة 164 من نفس القانون .

ثالثا/ الجرائم الالكترونية في اطار قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

في محاولة من المشرع الجزائري لمواكبة التطورات والجرائم التي تهـدد خصوصـية الافـراد أصدر حديثا القانون رقم 18-07 المؤرخ في 10 يونيو 2018 والذي هدف من خلاله إلـى تحديـد قواعد حماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات الطابع الشخصي وذلك فـي إطـار احترام الحياة الخاصة للأفراد، هذا ويقصد بالمعطيات ذات الطابع الشخصي – وفقا لأحكام هذا القانون " كل معلومة بغض النظر من دعامتها متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غيـر مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عـدة عناصـر خاصـة بهويتـه البدنيـة أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الثقافية أو الاجتماعية"[1] .

أما معالجة هذه المعطيات فيقصد بها " كل عملية منجزة بطرق أو وسـائل آليـة أو بـدونها علـى معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو الحفظ أو الملاءة أو التغييـر أو الاسـتخراج أو الاطلاع أو الاستعمال أو الإتصال عن طريق الإرسال أو النشر وكذا الإغلاق أو التشفير أو المسح أو الإتلاف"[2] وعليه سوف نعرض لاهم صور الجرائم الواردة في هذا القانون .

1/خرق الحياة الخاصة عند معالجة المعطيات

[1]– المادة 03 ف/01 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 03 ف/03 من نفس القانون

أوجب المشرع أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أوشكلها في إطار حماية الحياة الخاصة للافراد وكل خرق لهذا الواجب يعاقب المخالف بالحبس من (02) سنتين إلى (05) سنوات وبغرامة من (200.000 دج) الى (500.000 دج)[1] .

2/ معالجة المعطيات الشخصية رقم اعتراض الشخص المعني

اشترط المشرع في المادة السابعة من القانون 07/18 معالجة المعطيات ذات الطابع الشخصي بالموافقة الصريحة للشخص المعني، فإذا تمت معالجة هذه المعطيات رغم اعتراضه يعاقب المخالف بالحبس من (01) سنة إلى (03) ثلاث سنوات وبغرامة من (100.000دج) الى (300.000 دج)[2]

3/ معالجة المعطيات الشخصية دون التصريح

يحب إخضاع كل عملية معالجة معطيات شخصية لتصريح مسبق من السلطة المختصة طبقا للمادة 12 من هذا القانون، وفي حالة القيام بالمعالجة دون الحصول على هذا التصريح يعاقب المسؤول بالحبس من (02) سنتين إلى (05) خمس سنوات وبغرامة (200.000 دج) الى (500.000 دج)[3]

4/ الاستعمال غير الشرعي للمعطيات الشخصية

المعلومات والبيانات الاسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد وواضح ومعين مسبقا، ولابد من التزام الجهة القائمة على النظام المعلوماتي بالهدف أو الغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها الكترونيا.

وعليه فلا يجوز وصول هذه المعلومات إلى شخص آخر أو جهة أخرى تجمع معلومات لغاية معينة لان هذا من شأنه الحاق الضرر بالشخص لذا تدخل المشرع الجزائري وعاقب بالحبس من (06) ستة

---

[1] – المادة 54 من القانون 07/18 المتعلق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المادة 55 من نفس القانون .

[3] – المادة 56 من نفس القانون .

أشهر إلى (01) سنة وبغرامة من (60.000 دج) الى 100.000 دج) أو بإحدى هـــاتين العقـــوبيتين فقط كل من قام بإنجاز أو باستعمال معالجة معطيات غير تلك المصرح بها أو المرخص لها[1].

5/ جمع المعطيات الشخصية بطريقة غير شرعية

تنطبق هذه الصورة على كل من قام بجمع معطيات ذات طابع شخصي بطريقة غير نزيهة أو غير مشروعة فهذا الفعل فيه انتهاك الحياة الخاصة للأفراد يتمثل في جمع معلومات صحيحة منهم لكن على نحو غير مشروع وغير قانوني، ويستند هذا الجمع صفة غير المشروعة إذا من الأساليب غير المشروعة المستخدمة الحصول على هذه البيانات أو المعلومات كمراقبة الرسائل المتبادلة واعتراضها عن طريق البريد الالكتروني أو بتوصيل أسلاك خفية إلى الحاسوب الذي تختزن فيه البيانات أو من حيث طبيعة مضمونها فتتمثل صفة عدم المشروعية في أن البيانات غير صالحة للجمع بسبب مضمونها، كان تتعلق بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرق للافراد فلا بد أن تكون بعيدة عن عمليات التجميع في الحواسيب لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للافراد[2].

وعليه يعاقب كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية او غير نزيهة او غير مشروعة بالحبس من (1) سنة الى (03) سنوات وبغرامة من(100.000 دج) الى (300.000 دج)[3]

6/ عرقلة عمل السلطة الوطنية عند اجراء تحقيق حول المعطيات الشخصية

تتمثل صور هذه الجريمة فيما يلي:

* الاعتراض على إجراء عملية التحقق في عين المكان.

*عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصـــرفها بالمعلومـــات والوثـــائق الضرورية لتنفيذ المهمة الموكلة لهم أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

---

[1] – المادة 58 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] –

[3] – المادة 59 من نفس القانون.

* عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر واضح. وعليه يعاقب كل من عرقل عمل السلطة الوطنية بـــ الحبس من (06) اشهر الى (02) سنتين وبغرامة من (60.000 دج) الى (200.000 دج)[1].

8/ نقل المعطيات الشخصية إلى دولة أجنبية

تعاقب المادة 64 من القانون 07/18 بالحبس من (01) سنة الى (03) سنوات وغرامة من (500.000 دج) الى (1.000.000 دج) كل من ينقل معلومات ذات طابع شخصي نحو دولة اجنبية وذلك خرقا لاحكام المادة 44 من نفس القانون[2].

من خلال دراستنا يتبين أنه بالرغم من النواحي الإيجابية للأنظمة المعلوماتية إلا أنه ترتب عنها جوانب سلبية نجمت عن استغلال بعض الأفراد والجهات التقنيات المعلوماتية لتسهيل ارتكاب العديد من الجرائم كما أصبح النظام المعلوماتي ذاته محلاً للاعتداء عليه واساءة استخدامه.

رابعا / الجرائم الالكترونية في اطار القانون المتعلق بالاعلام[3]

يهدف هذا القانون العضوي إلى تحديد المبادئ والقواعد التي تنظم نشاط الإعلام وممارسته بحرية وقد تضمن الفصل السابع منه الجنح المرتكبة في اطار مماسة نشاط الاعلام، وسنعرض لاهم الجرائم الالكترونية الواردة فيه .

---

[1]– المادة 61 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – تنص المادة 44 من القانون 07/18 على انه" لا يجوز للمسؤول عن معالجة نقل المعطيات ذات الطابع الشخصي الى دولة أجنبية الا بترخيص السلطة الوطنية وفقا لأحكام هذا القانون، واذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص ازاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها...."

[3] – قانون عضوي رقم 14/23 المؤرخ في 27 غشت 2023 يتعلق بالاعلام .

1/ نشر معلومات تمس بسرية التحقيق

جرم المشرع الجزائري كل نشر أو بث عبر وسيلة إعلام، كل معلومة أو وثيقة تمس بسرية التحقيق الابتدائي والقضائي و/أو فحوى مناقشات الجهات القضائية التي تصدر الحكم إذا كانت جلساتها سرية و/أو تقارير عن المرافعات المتعلقة بالحياة الخاصة وبشرف الأشخاص[1].

2/ نشر كل ما يتعلق بإعادة تمثيل الجنح والجنايات الواردة في قانون العقوبات[2]

جرم المشرع الجزائري كل نشر او بث عبر وسيلة إعلام، صورا أو رسوما أو أية بيانات توضيحية أخرى تعيد تمثيل كل ظروف الجنايات أو الجنح أو جزء منها المنصوص عليها في المواد 255 و256 و257 و258 و259 و260 و261 و262 و263 مكرر و333 و334 و335 و336 و337 و338 و339 و341 من قانون العقوبات.

3/ اهانة رؤساء الدول واعضاء البعثات

جرم المشرع الجزائري كل فعل يتضمن اهانة صادرة من وسيلة إعلام، تجاه قادة الدول الأجنبية وأعضاء البعثات الدبلوماسية والقنصلية المعتمدين لدى الجمهورية الجزائرية الديمقراطية الشعبية[3].

وقد عاقب المشرع الجزائري بنفس العقوبة كل من يرتكب احدى صور الجرائم المنصوص عنها اعلاه بعقوبة الغرامة التي تتراوح ما بين (100.000 دج) الى (500.000 دج).

[1] – المادة 46 من القانون المتعلق بالإعلام .

[2] – المادة 47 من نفس القانون .

[3] – المادة 48 من نفس القانون .

الفصل الثاني الاليات الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري

تشكل الاليات الاجرائية المحور الثاني المكمل لأي سياسة وطنية ترمي لمكافحة الجريمة إذ توفر القواعد الاجرائية وسائل كشفها وإثباتها ومتابعتها، وتعتبر الجريمة الالكترونية من الجرائم المستحدثة التي شغلت أجهزة العدالة ، وبالرجوع إلى وسائل الإثبات التقليدية ومن ضمنها المعاينة والشهادة والخبرة القضائية نجد أنها غير قادرة على إثبات الجرائم الالكترونية، ذلك أنها وضعت بالأصل لإثبات جرائم تقليدية تخلف ورائها أدلة مادية وذلك على عكس هذا النوع من الجرائم التي تعتبر من الجرائم الناعمة التي لا تخلف ورائها أي أثر مادي ملموس ومن هنا جاءت صعوبة إثباتها بوسائل الإثبات التقليدية.

وعليه فان خصوصية الجرائم الإلكترونية والمشاكل الاجرائية التي تثيرها أمام القائمين على التحري والتحقيق والذي أثر على مستوى مكافحة هذا النوع من الاجرام إستدعى من المشرع الجزائري التطوير في سياسته الجنائية بتطوير وسائل الإثبات الجنائي واجراءات التحقيق والتحري بصورة تتلائم مع هذه الخصوصية وتمكن رجال الشرطة القضائية والمحققين من كشف الجريمة والتوصل إلى مرتكبيها والتحقيق معهم وجمع الأدلة بالسرعة والدقة اللازمين، وتقديمهم للمحكمة **ليس ذلك فحسب** بل قد تبنى المشرع الجزائري ايضا اطارا مؤسساتيا فعالا يضم مختلف الفاعلين من جهات امنية وادارية وقضائية تهدف الى تعزيز القدرات في الوقاية والكشف والتحقيق ومعاقبة مرتكبي هذه الجرائم بما يضمن حماية الفضاء الرقمي و تحقيق الامن السيبراني .

وتبعا لما سبق سوف نتناول من خلال هذا الفصل " **الأحكام الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري** " والذي قسمناه بدوره إلى مبحثين، الأول بعنوان" **القواعد الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري** " والمبحث الثاني جاء بعنوان "**الاطار المؤسساتي لمكافحة الجرائم الالكترونية في التشريع الجزائري** "

المبحث الاول : القواعد الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري

ان دراسة الاحكام الاجرائية تعد ضرورية لفهم مدى فاعلية النظام القانوني الجزائري في التصدي للجريمة الالكترونية ومدى احترامه للضمانات القانونية والحقوق الدستورية في ظل التطور التشريعي وعليه سعى المشرع الجزائري الى وضع منظومة قانونية متكاملة لا تقتصر فقط على تجريم الافعال الالكترونية بل تمتد الى تحديد احكام اجرائية خاصة تضمن فعالية المتابعة القضائية لهذه الجرائم بالنظر الى طبيعتها التقنية المقعدة وصعوبة الاثبات فيها من خلال: تعدیل قانون الإجراءات الجزائیة بالقانون رقم 22/06 المؤرخ في 20 دیسمبر 2006 وایضا إصدار القانون رقم 04/09 المؤرخ في 5 غشت سنة 2009 یتضمن القواعد الخاصة للوقایة من الجرائم المتصلة بتكنولوجیات الإعلام والاتصال ومكافحتها والذي ضم مجموعة من القواعد الإجرائیة الخاصة والحدیثة للتحري والتحقیق في الجرائم الالكترونية الامر الذي منح الجهات القضائية صلاحيات استثنائية تتلائم مع متطلبات البحث في البيئة الرقمية كاجراءات التفتيش والحجز وغيرها.

وفي هذا الشأن خصصنا هذا المبحث للخوض في " **القواعد الاجرائية لمكافحة الجرائم الالكترونية في التشريع الجزائري** " والذي ارتأينا تقسيمه إلى مطلبين، عنوننا الأول ب " **القواعد الاجرائية وفقا لقانون الاجراءات الجزائية** " في حين حملنا المطلب الثاني عنوان " **القواعد الاجرائية وفقا للقانون 04/09** "

المطلب الاول : القواعد الاجرائية وفقا لقانون الاجراءات الجزائية

عمل المشرع الجزائري على تطویر أسالیب التحقیق وإجراءاته فیما یخص مكافحة الجرائم الماسة بأنظمة المعالجة الآلیة للمعطیات لتتلائم مع خصوصیة هذه الجرائم بموجب تعدیل قانون الإجراءات الجزائیة بموجب القانون رقم 22/06 وذلك بإضافة قواعد استثنائیة من القواعد العامة المنظمـــة (**للتفتیش والضبط وهو ما سنتناوله في الفرع الاول**) كما استحدث مایسمى بأساليب االتحري الخاصة المتمثلة في (**إجراء اعتراض المراسلات و تسجیل الأصوات و التقاط الصور والذي خصصنا له الفرع الثاني**) (**واجراء التسرب الذي سنتاوله بالدراسة في الفرع الثالث**) وقيد من خلالها المشرع السلطات القضائية المختصة الإذن بها في حال إذا اقتضت ضرورات التحري

والتحقيق في جرائم محددة على سبيل الحصر ومنها جرائم المساس بانظمة المعالجة الالية للمعطيات.

الفرع الاول : قواعد التفتيش والضبط المتبعة في الجرائم الإكترونية وفقا لقانون الإجراءات الجزائية

للوقوف على الأحكام المقررة للتفتيش في الجرائم المعلوماتية لابد من التفرقة بين قواعد التفتيش والضبط في حالة الجناية أو الجنحة المتلبس بها، وقواعد التفتيش والضبط في حال التحقيق الابتدائي، ثم قواعد التفتيش والضبط في حال التحقيق بمعرفة قاضي التحقيق وفقا لما يلي:

اولا/ تفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالات التلبس بالجريمة[1]: ويكون ذلك وفقا للقواعد التالية :

1/ الحصول على إذن مسبق من قبل السلطة القضائية المختصة

نصت المادة 44 من قانون الاجراءات الجزائية انه " لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش . ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون" .

[1]– تنص المادة 41 ق إ ج على أنه " توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها، كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى افتراض مساهمته في الجناية أو الجنح، وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية لإثباتها".

وعليه يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها واجراء الحجز فيها، وذلك تحت طائلة البطلان. وتنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون، واذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا بطلان الإجراءات العارضة.

2/ حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

يخضع التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 47ف/3 ق إج لقواعد خاصة تختلف عن القواعد العامة المقررة في البندين 1 و 2 من المادة 45 ق إج وتختلف هذه القواعد حسب حالتين :

* **الحالة الأولى:** إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45 إج لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات بالشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش بمسكنه وكذلك الأمر إذا حصل التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالجريمة.

***الحالة الثانية:** أصبح ضابط الشرطة القضائية إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبس بها أو تحقيق متعلق بالجرائم الماسة بانظمة المعالجة الالية للمعطيات أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر وأن الحال يقتضي عدم

نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو لاحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله[1].

ولضابط الشرطة القضائية وحده مع الأشخاص الحاضرين عملية التفتيش الحق في الاطلاع على الأوراق أو المستندات قبل حجزها، غير أنه عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر، وتغلق الأشياء أو المستندات المحجوزة ويختم عليها إذا أمكن ذلك، فإذا تعذرت الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق ويختم عليه بختمه ويحرر جرد الأشياء والمستندات المحجوزة[2].

3/ ميقات التفتيش والضبط في الجرائم الماسة بانظمة المعالجة الالية للمعطيات

إذا كان قانون الإجراءات الجزائية قد وضع قاعدة عامة تحدد بدقة الميقات الذي يجوز فيه دخول المساكن وتفتيشها وإجراء الحجز بها، وهو بين الساعة الخامسة صباحا والساعة الثامنة مساء، فإنه وضع استثناء لتلك القاعدة، وهو جواز دخول المساكن وتفتيشها في أي وقت من اليوم ليلا ونهارا، دون التقيد بذلك الميقات القانوني[3] اذا تعلق الامر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب و كذا الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، أو أن يقوم قاضي التحقيق بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك[4]، لان الغرض من الإسراع في الإجراء والقيام به خارج الميقات المحافظة على الدليل نظرا للطبيعة الخاصة لهذا النوع من الجرائم التي يستفيد فيها

---

[1] – المادة 47 مكرر ق إ ج المعدلة بموجب القانون 22/06 .

[2] – المادة 45 ف/ 02 ق إج المعدلة بموجب القانون 22/06 .

[3] – هذه الاستثناءات وردت في المواد 47/ف/ 1 و2 و3 من ق إ ج .

[4] – المادة 47 ف /4 ق إ ج .

المشتبه فيه من التطور التكنولوجي ولا تمس هذه الأحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من المادة 45 من ق إج .

ثانيا /التفتيش والضبط في الجريمة الالكترونية في مرحلة التحقيق الابتدائي

نصت المادة 64 إ ج أنه " لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات. ويجب أن يكون هذا الرضا مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر في ذلك في المحضر مع الإشارة إلى رضاه وضرورة التقيد بالأحكام المنصوص عليها في المواد 44 إلى47 ق إ ج. غير أنه عندما يتعلق الأمر بتحقيق في إحدى/ الجرائم المنصوص عليها في المادة 47 ق إ ج فإنه تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر .

ثالثا/ التفتيش والضبط في الجرائم الالكترونية في مرحلة التحقيق القضائي

يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات. على أن يباشر التفتيش وفقا للمادة 81 ق إ ج في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة "[1]

إذا اقتضى الأمر أثناء القيام بتحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها، وعلى قاضي التحقيق أن يتخذ مقدما جميع الإجراءات اللازمة لضمان احترام كتمان سر المهنة، ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا، ويستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق ويجوز لمن يعنيهم الأمر الحصول على نفقتهم،

[1] – المادة 79 من قانون الاجراءات الجزائية .

وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق مضبوطة إذا لم تخل دون ذلك مقتضيات التحقيق[1].

الفرع الثاني : إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور[2]

عمل المجتمع الدولي على حماية الحياة الخاصة للأفراد فمنعت المواثيق الدولية وكذا القوانين الوطنية التصنت على المكالمات الهاتفية وانتهاك سرية المراسلات، وكل ما يمس حرمة الحياة الخاصة إلا أن هذا المنع لم يعد مطلقا، فقد أجازت إستثناءا الإعتداء على الحياة الخاصة للأفراد لضرورة الحد من الجرائم، وهي الطرق المستخدمة في مجال التحريات الخاصة باستعمال الوسائل التقنية الحديثة بغية التحقيق في الجرائم الخطيرة وكشف مرتكبيها، وأغلب التشريعات نصت صراحة على جواز استعمالها وفق شروط محددة.

الاعتراض والتسجيل والالتقاط هي عدة تسميات يمكن اختزالها في مصطلح واحد هو "المراقبة" التي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مسموعة أو مرئية نتيجة الإشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي يكتنفها[3].

---

[1] – المادة 84 من نفس القانون .

[2]– كانت القاعدة العامة في قانون الاجراءات الجزائية الجزائري قبل تعديله أن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من الإجراءات القضائية التي لا يجوز اتخاذها إلا على مستوى التحقيق القضائي بموجب أمر من قاضي التحقيق، ولا يمكن اللجوء إليها خلال مرحلة التحريات الأولية حتى ولو تعلق الأمر بحالة تلبس ثم استحدث المشرع اللجوء إلى هذه الأساليب بموجب القانون 06 / 22 المؤرخ في20 / 12 / 2006 المواد من 65 مكرر 5 إلى 65 مكرر 10.

[3]– فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مقال منشور في مجلة العلوم الانسانية، عدد 33، جوان 2010 ص 236 .

اولا / المقصود بـــ إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور

يقصد بإعتراض المراسلات " عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في إرتكاب الجريمة" [1].

والمقصود بالمراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية هي" كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أي أجهزة أخرى كهربائية مغناطيسية" [2].

والملاحظ على المشرع الجزائري أنه حدد وسيلة الإتصال عموما في أي وسيلة إلكترونية أو لاسلكية كهربائية أو مغناطيسية وبالتالي يمكن القول أن اعتراض الإتصالات السلكية أو اللاسلكية يكون محصورا في التنصت التلفوني أو في مراقبة المكالمات الهاتفية فقط ، ويتم الإعتراض باستخدام وسائل فنية تتعلق بالتنصت والتحكم أو مراقبـــة محتـــوى الإتصالات، كذلك يمكن أن تشمل وسائل الإعتراض على تسجيل البيانات[3].

اما المقصود بتسجيل الأصوات فهو " وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية " ويتم ذلك عن طريق حفظ الحديث عن طريق جهاز معد لذلك للإستماع إليه مرة أخرى عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها أو بواسطة أدوات تقنية مخصصة لهذا الغرض عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريـــق التقاط إشارات لاسلكيـــة أو إذاعيـــة[4]، وتبعا

---

[1]– شول بن شهرة و بن بادة عبد الحليم، الآليات القانونية والمؤسساتية للوقاية من الفساد ومكافحته، مقال منشور في مجلة جيل للأبحاث القانونية المعمقة، العدد 8، نوفمبر 2016 ص 18 .

[2]–أنظر المادة 08 ف/21 من القانون رقم 3/2000 المؤرخ في 05 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

[3]– وردة شرف الدين، مشروعية أساليب التحري الخاصة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مقال منشور في مجلة المفكر، العدد 15، جوان 2017 ص 543 .

[4]– زوزو زليخة، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد الثامـــــــــن الجزء الثاني، جوان 2017 ص 763 .

لذلك أصبح يمكن أخذ اعتراف الشخص ضد نفسه بصورة خفية ودون رضاه وموافقته بتسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية[1].

كما نعني بإجراء التقاط الصور " وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص" ولم يشترط المشرع تقنية معينة لالتقاط الصور فقد تكون بواسطة آلات التصوير العادية التي تثبت الصورة أو بواسطة آلات الفيديو التي تقوم بالتقاط الصورة والصوت معا وقد حصر المشرع إجراء التقاط الصور في الأماكن الخاصة دون العامـــة.

ثانيا / الضمانات القانونية للقيام بهذه الاجراءات

لا يجوز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور دون موافقة وعلم المعنيين بهـــا غير أن مصلحة التحقيق قد تستلزم القيام بهذه العمليات عندما تكون المصلحة العامة أولى بالرعاية من الحفاظ على أسرار الحياة الخاصة، الأمر الذي دفع بالتشريعات الداخلية إلى إحاطتها بجملة من الضمانات القانونية التي تعمل على منع تعسف السلطات العامة وتصون الحرية الفردية للأشخاص.

1/ الجرائم المعنية بهذه الإجراءات

يتم القيام بإجراء إعتراض المراسلات وتسجيل الأصوات والتقاط الصور في جرائم محددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات .

2/ الإذن بمباشرة الإجراءات

إن السلطة القضائية هي المختصة عموما بإصدار هذا الإذن ويعد ذلك ضمانة لازمة لمشروعية هذه العمليات، وبالرجوع إلى نص المادة (65) مكرر من قانون الإجراءات الجزائية فإنه لا يمكن اللجوء إلى هذا الإجراء إلا بعد الحصول على إذن مكتوب ومسبب من طرف وكيل الجمهورية في حالة التحري أو قاضي الحقيق في حالة فتح حقيق قضائي، ويتعين على السلطة القضائية قبل منح الإذن تقدير فائدة الإجراء وجديته وملائمته لسير الدعوى، كما يجب أن يتضمن الإذن الممنوح من طرف وكيل الجمهورية أو قاض التحقيق ذكر جميع العناصر التي تسمح بالتعرف

[1]– فوزي عمارة، المرجع السابق ص 237 .

على الإتصالات المطلوب التقاطها والأماكن المقصودة سواء سكنية أو غيرها[1]، والجريمة التي تبرر اللجوء إلى هذا الاجراء ومدتها، ويسلم الإذن مكتوبا لمدة أقصاها أربع أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية[2].

3/ كيف تتم العمليـــة

يسمح الإذن بوضع الترتيبات التقنية دون موافقة المعنيين ودون علمهم، إذ يجوز لضابط الشرطة القضائية ولأي عون مؤهل مسخر من طرفه دخول المساكن لوضع أجهزة الإعتراض والتصنت والتصوير والتسجيل، دون التقيد بالزمن المحدد في المادة (41) من قانون الإجراءات الجزائية ودون علم ورضا صاحب المسكن، ويجوز لضابط الشرطة القضائية إصدار تسخيرة لكل عون مؤهل لدى مصلحة أو هيئة أو وحدة عمومية عامة أو خاصة مكلفة بتقنيات الإتصال والعمليات التقنية والتسجيلات السمعية والبصرية، وكل إجراء علمي من شأنه كشف الممارسات الإجرامية والتي تستعمل فيها تقنيات حديثة وبآليات متطورة[3]، وبالنظر لسرية هذه الإجراءات وخطورتها وتفاديا للتعسف في استعمالها من طرف ضباط الشرطة القضائية، فإن المشرع أخضعهم للرقابة المستمرة والمباشرة لوكيل الجمهورية أو قاضي التحقيق الذي أذن لهم بالقيام بهذا الإجراء .

4/ محضر العمليات

يجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص القيام بتحرير محضر عن كل عملية إعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الإلتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والإنتهاء منها[4]، وتتم هذه العملية دون المساس بالسر المهني المنصوص عليه في المادة(45) نفس القانون .

---

[1]– تستعمل هذه الوسائل في المحلات السكنية والأماكن الخاصة والعامة، ويقصد بالمحلات السكنية الأماكن المسكونة وكل توابعها كما ورد في قانون العقوبات، بينما تعتبر الأماكن العامة أي مكان معد لإستقبال الكافة أو فئة معينة من الأشخاص لأي غرض من الأغراض، وعن المكان الخاص فهو مكان غير معد للسكن، وإنما يستخدم لمزاولة نشاط كالمحلات التجارية أو مقاهي الأنترنت.

[2]– المادة (65 مكرر 7)من قانون الإجراءات الجزائية .

[3]– المادة (65 مكرر8) من قانون الاجراءات الجزائية.

[4]– المادة (65 مكرر9)من نفس القانون .

الفرع الثالث : إجراء التسرب

يعد التسرب أهم وأخطر طرق التحري وجمع المعلومات التي يقوم به إلا الضباط الأكفاء ذوو الخبرة ويستخدم فيها مختلف أساليب التنكر وانتحال الشخصية لكسب ثقة المشتبه فيهم بقصد تحديد طبيعة ومدى النشاط الإجرامي، حيث يزرع الضابط في موقع النشاط ليكون وجها لوجه مع الهدف يتعامل ويتجاوب معهم كأحد أفراد العصابة[1] وسنتناول تعريف التسرب والضوابط أو الضمانات القانونية لهذا الإجراء في التشريع الجزائري.

اولا/ تعريف اجراء التسرب

يعرف التسرب على أنه " تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط الشرطة القضائية أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو شريك"[2] .

فيما يخص التعريف القانوني للتسرب فقد تناوله المشرع الجزائري في المادة (65 مكرر12) من القانون رقم 06-22 بقوله:"يقصد بالتسرب قيام ضباط أو عــون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف."

على الرغم من أن القواعد العامة في الاثبات الجنائي تستوجب النزاهة و الشرعية في الحصول على الدليل وترفض أي دليل ناتج عن تحريض الضبطية القضائية للمتهم على ارتكاب الجريمة، فإن التسرب يخرج عن هذه القاعدة إذ يسمح لضباط الشرطة بالقيام بأفعال إيجابية تشكل جريمة في

---

[1]-رابح وهيبـــــــــــة، التسرب في التشريع الإجرائي الجزائري، مقال منشور ضمن مجلة جامعة القدس المفتوحة للأبحاث والدراسات العلىا، جامعة القدس المفتوحة، العدد السادس والثلاثون، الجزء الأول، فلسطين 2015 ص 301.

[2]- عبد الرحمان خلفي، الاجراءات الجزائية في التشريع الجزائري والمقارن، الطبعة الثانية، دار بلقيس، الجزائـــــــــــــــــــــــــــــــر 2016 ص 75 .

الظروف العادية وهي إستعمال هوية غير حقيقية[1]، وأن يرتكب من الأفعال المحددة والواردة في القانون على سبيل الحصر، وتعد الهوية المستعارة هي أحد أهم عناصر ضمان نجاح عملية التسرب وهي التي تعبر عن المتسرب ذاته، ولكن بإسم ولقب ومكان إقامة وغير ذلك من معطيات مغايرة للحقيقة [2].

ويمكن تصور عملية التسرب في نطاق الجرائم الالكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وإشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والإتصال المباشر مستخدما في ذلك أسماء وصفات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي، كما لو كان فاعل مثلهم سعيا منه للإستفادة منهم حول كيفية ارتكاب الجريمة .

ثانيا/ الضوابط القانونية لعملية التسرب في التشريع الجزائري

نظرا لخطورة هذا الإجراء فقد أحاطه المشرع بمجموعة من الضوابط والشروط يمكن تلخيصها كما يلي:

1/ إقتضاء ضرورات التحري والتحقيق إجراء التسرب

ضرورات التحري والتحقيق من الشروط الأساسية للجوء إلى هذا الإجراء من أجل الكشف عن الجريمة وبالإضافة إلى أن التسرب يجب أن ينصب على جناية أو جنحة منصوص عنها قانونا[3] فمن الضروري أن يكون هذا الإجراء هو الوحيد الذي بواسطته يمكن إظهار الحقيقة بعد أن أثبتت الإجراءات الأخرى عدم نجاعتها، وبمفهوم المخالفة فإن وجود أدلة كافية تعزز الإشتباه أو تدعم الإتهام فإنه لا داعي للمخاطرة بإجراء عمليات التسرب، فإن هذه الأخيرة تجرى عند الضرورة فقط والمتمثلة في قلة أو صعوبة الحصول على أدلة أو براهين[4].

2/ الأفعال المأذون بها للمتسرب

---

[1]– نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي، دار هومه، الجزائر 2013 ص 451 و 452 .

[2]– وردة شرف الدين، الاثبات بالادلة الالكترونية، المرجع السابق ص 331 و 332 .

[3]– وهي الجرائم المنصوص عنها بموجب المادة (65 مكرر 5) من قانون الإجراءات الجزائية .

[4]– وداعي عز الدين، التسرب كأسلوب من أساليب البحث و التحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، مقال منشور في المجلة الأكاديمية للبحث القانوني، مجلد 16 عدد 02، 2017 ص 211.

من الأفعال التي يجوز للمتسرب القيام بها بوصفه فاعلا أو شريكا للمجموعة الاجرامية دون أن يكون مسؤولا جزائيا ما يلي :

- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين الايواء أو الحفظ أو الإتصال[1] .

وبالتالي يمكن للعون المتسرب إستعمال الاموال المتحصل عليها من ارتكاب الجرائم المذكورة بنص المادة (65 مكرر 5) حيث يمكن للمتسرب تسخير الوسائل المادية لفائدة الخلية الإجرامية من نقل وإيواء. اما بخصوص الوثائق القانونية فالمقصود بها توفير الوثائق الرسمية حسب الضرورة كإستخراج بطاقة تعريف أو رخصة سياقة، وبالتالي يحتاج إلى جهاز لتزوير الوثائق الرسمية. ويقوم المتسرب بهذه الأفعال من أجل أن يوهم المشتبه فيهم بأنه فاعل معهم أو شريك لهم أو خاف لمتحصلات الجريمة، لكن بالمقابل لا يجوز له أن يقوم بأي فعل يشكل تحريضا على ارتكاب أية جريمة، وبالتالي يكون المشرع قد ضحى بمبدأ مشروعية الحصول على الدليل من أجل حماية المجتمع عندما تعجز الأساليب التقليدية للتحري والتحقيق عن مواجهة هذا النمط من الجريمة[2].

3/ الإذن بإجراء عملية التسرب

نظرا لخطورة هذا الإجراء فقد أخضعه المشرع لضوابط وجعله ينفذ من طرف السلطة القضائية وتحت رقابتها المباشرة والسلطة المختصة بمنح الإذن للقيام بعملية التسرب حصرها المشرع في وكيل الجمهورية وذلك قبل فتح تحقيق قضائي، أما بعد فتح تحقيق قضائي يأمر به قاضي التحقيق المكلف بالقضية بعد إخطار وكيل الجمهورية، والإذن بالتسرب أمر جوازي متروك لوكيل الجمهورية أو قاضي التحقيق، ويعتمد اتخاذ هذا القرار على العناصر والمعطيات المتوفرة حول القضية التي تبرر اللجوء لهذا الإجراء ومدى ضرورته ولضمان فعالية التحقيق .

[1]– المادة (65 مكرر 5) من قانون الإجراءات الجزائية .

[1]– نجيمي جمال، المرجع السابق ص 451 و 452 .

4/ الأشخاص القائمون بعملية التسرب

أما عن الجهات المخولة بإجراء عمليات التسرب فهم ضباط الشرطة القضائية المذكورون في المادة 15 من قانون الإجراءات الجزائية ، ويستثنى من هؤلاء لاعتبارات ميدانية الولاة ورؤساء المجالس الشعبية البلدية بالإضافة إلى مساعدي ضباط الشرطة القضائية، فالأعوان يمارسون مهامهم تحت مسؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية وتصدر باسمهم، كما أضافت المادة (65 مكرر13) مصطلح المسخرين ويقصد بهم كل الأشخاص من الجنسين ممن يراه ضابط الشرطة القضائية القائم بتنسيق عملية التسرب مفيدا لإنجاز مهمته وهذا دائما تحت رقابة القضاء[1] .

5/ مضمون تقرير ضابط الشرطة القائم بالعملية

إن المشرع الجزائري وبتقنينه لعملية التسرب وفي المادة (65 مكرر13) نص صراحة على أن ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب دون سواه ملزم بتحرير تقرير عن عملية التسرب هذا التقرير يكون كتابيا يتضمن العناصر الضرورية للعملية والتي يمكن أن نفهم منها مراحل العملية الأفعال المجرمة، هوية العناصر المشتبه فيهم، وكذا ألقابهم أو أسمائهم المستعارة، دور كل واحد فيهم في الأفعال الإجرامية، طرق تعاملهم مع الإجرام، الوسائل المادية والأدلة المحجوزة وكذا ذكر الأماكن والعناوين وكل ما هو متصل بالأفعال المعاقب عليها المرتبطة بالجريمة الأصلية، وهنا يستحسن أن يخضع التقرير إلى التسلسل الزمني، والأفعال الرئيسية والأدلة والبراهين المتحصل إليها[2].

6/ الحماية القانونية للعون المتسرب

نظرا لخطورة عملية التسرب فقد أضفى قانون الإجراءات الجزائية حماية على العون المتسرب تمتد هذه الحماية إلى أفراد أسرت ومن أهم مظاهر هذه الحماية :

---

[1] – زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلة دفاتر السياسة و القانون، جامعة قاصدي مرباح ورقلة، عدد 11، جوان 2014 ص 120 و 121 .

[2] – زوزو هدى، المرجع نفسه ص 121 .

- **الإعفاء من المسؤولية الجنائية:** حيث لا يسأل العون المتسرب عن أي جريمة يرتكبها سواء بصفته فاعلا أو شريكا أو خاف، ولهذا فإن التسرب يعتبر سبب إباحة وليس مانعا من موانع المسؤولية بإعتباره يندرج ضمن ما أذن به القانون .
- **حظر كشف هويّة العون المتسرب:** حيث لا يجوز طبقا للمادة (65 مكرر16) إظهار الهوية الحقيقية لضباط وأعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، وتفعيلا لهذه الحماية نص قانون الإجراءات الجزائية على معاقبة كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من (2) سنتين إلى (5)خمس سنوات وبغرامة من (50.000 د ج) إلى (200.000 دج) .

فإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب و جرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة من (5)خمس سنوات إلى (10) سنوات والغرامة من (200.000 دج) إلى (500.000 دج)

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من (10) عشر سنوات الى (20) عشرين سنة، والغرامة من (500.000 دج) إلى (1.000.000 دج).

كما رتب المشرع حماية أخرى تتمثل في عدم تقديم العون المتسرب للإدلاء بشهادته شخصيا حفاظا على حياته بل يقتصر الأمر على إدلاء ضابط الشرطة القضائية المكلف بتنسيق العملية وحده دون سواه بشهادته تحت مسؤوليته[1].

المطلب الثاني : القواعد الاجرائية في القانون 04/09

إن خصوصية الجرائم المعلوماتية والمشكلات الاجرائية التي تثيرها أمام جهات التحري والتحقيق إستدعى الدول إلى التطوير في سياستها الجنائية بتطوير إجراءات التحقيق والتحري واستحداث إجراءات تعمل على مجابهة الجريمة الالكترونية بوجه عام تتماشى وطبيعتها الخاصة وتمكن رجال القضاء من كشف الجريمة والتوصل إلى مرتكبيها والتحقيق معهم، وجمع الأدلة بالسرعة والدقة اللازمين وتقديمهم للمحاكمة، حيث تم إدراج هذه الإجراءات في القانون رقم 04/09 وتتمثل هذه الإجراءات في **(مراقبة الاتصالات الإلكترونية)** وهو ما سنتناوله في الفرع الاول

[1]– المادة (65 مكرر18) من قانون الإجراءات الجزائية .

و(**وإجراءالتحفظ العاجل على البيانات المعلوماتية المخزنة**) نخصص له الفرع الثاني، ونتناول (**تفتيش وحجز المنظومات المعلوماتية في فرع ثالث**).

الفرع الأول: مراقبة الاتصالات الإلكترونية

أجاز القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها اللجوء إلى استعمال تقنية مراقبة الإتصالات بشأن الكشف عن الحقيقة في الجرائم الماسة بتكنولوجيات الإعلام والإتصال عن طريق إجراءات وقواعد خاصة نظمها هذا القانون بالرغم من مساسها بحقوق وحريات الأفراد.

اولا / تعريف مراقبة الإتصالات الالكترونية

نص المشرع على إجراء مراقبة الإتصالات الإلكترونية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وعلى غرار التشريعات المقارنة لم يتطرق المشرع إلى تحديد المقصود بمراقبة الإتصالات الإلكترونية وإنما إكتفى بتحديد مفهوم الإتصالات الإلكترونية بأنها "كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية "[1] بينما يقصد بالمراقبة " تجميع و تسجيل محتوى الإتصالات الإلكترونية ومن ثمة الإطلاع عليها والكشف عنها"[2].

ثانيا/ ضمانات مراقبة الإتصالات الإلكترونية

يعد هذا الاجراء من أخطر الإجراءات التي تمس الإنسان في حقه في الخصوصية الأمر الذي أدى بالمشرع الجزائري إلى وضع ضوابط وضمانات موضوعية وشكلية لمراقبة الإتصالات الإلكترونية، والتي يجب على السلطة المختصة احترامها عند مباشرتها لإجراء تجميع وتسجيل محتوى الإتصالات نوجزها فيما يلي :

1/ الضمانات الموضوعية : يمكن إيجاز الضوابط الموضوعية لمراقبة الاتصالات الإلكترونية في ما يلي :

---

[1]– المادة(02 بند/و) من القانون 04/09 .

[2]– ثابت دنيا زاد، مراقبة الإتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مقال منشور في مجلة العلوم الإنسانية والإجتماعية، جامعة العربي التبسي، تبسة ، العدد 6 ص207 .

أ/ الغرض من اللجوء إلى هذا الإجراء

أقر المشرع اللجوء إلى إجراء مراقبة الإتصالات الإلكترونية في حالات إستثنائية لما لها من إعتداء على حق الإنسان في حرمة حياته الخاصة واتصالاته الشخصية، وذلك بغرض الوصول إلى حقيقة الجريمة والكشف عن مرتكبيها خلال مرحلتي جمع الإستدلالات والتحقيق الإبتدائي ولم يتم التوصل إلى ذلك عن طريق الإجراءات التقليدية .

ب/ حالات اللجوء إلى هذا الإجراء

نص المشرع الجزائري على الحالات التي تسمح باللجوء إلى هذا الإجراء في المادة (04)من القانون 09-04 كالأتي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام
- أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني
- من أجل مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

عندما يتعلق الأمر بالحالة الأولى، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته المنصوص عليها في المادة 13 من نفس القانون، إذنا لمدة ستة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الحالة الأولى موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

2/ الضمانات الشكلية لمراقبة الإتصالات الالكترونية[1]: من الضوابط الشكلية التي جاء بها قانون الإجراءات الجزائية ما يلي :

أ/ ضرورة صدور أمر يكون مسببا من السلطة القضائية المختصة

من أهم الضمانات التي أقرها المشرع الجزائري ضرورة الحصول على إذن من السلطة القضائية المختصة لمباشرة إجراء مراقبة الإتصالات الإلكترونية ويتعلق الأمر بقاضي التحقيق أو وكيل الجمهورية بحسب الحالة – كما سبق بيانه – ومن الشروط التي يجب توافرها في الإذن أن يكون مكتوبا طبقا لما نصت عليه صراحة المادة(4ف/2) من القانون 09-04إضافة إلى شرط الكتابة يجب أن يذكر في الإذن صراحة أن الاذن يتعلق بمراقبة الإتصالات الإلكترونية .

كما يجب على السلطة المختصة ذكر الأسباب التي دفعت إلى إصدار الإذن بمراقبة الإتصالات الإلكترونية ومن ثمة يجب أن يؤسس الإذن على الحالات المنصوص عنها في المادة (4) من القانون 09-04 .

ب/ بيانات الإذن بمراقبة الاتصالات الالكترونية

ينصب الإذن بمراقبة الاتصالات الالكترونية على محل معين يتمثل في إتصالات الشخص الإلكترونية، وعليه يجب أن يحدد الإذن كل العناصر التي تسمح بالتعرف على الإتصالات الإلكترونية المطلوب تجميعها وتسجيلها، والذي يجب أن يحدد بدقة طبيعة هذه الإتصالات إذا كانت مراسلات إلكترونية تتعلق برسائل تصل بريده الالكتروني أو أحاديث خاصة تتم عبر شبكة الانترنت [2].

ويجب أن تبقى الإجراءات المتعلقة بمراقبة الإتصالات الإلكترونية في إطار المعلومات المبحوث عنها وهو الشرط الذي نص عليه المشرع الجزائري والذي اوجب ألا تستخدم المعلومات والمعطيات التي تسلمها أو تجمعها الهيئة لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم

[1]–بالرجوع الى القانون 09-04 نلاحظ أن المشرع الجزائري لم يوضح بدقة الاجراءات الشكلية الواجبة الاتباع وأخضعها للقواعد العامة المنصوص عليها في قانون الاجراءات الجزائية .

[2] – ثابت دنيا زاد، المرجع السابق ص 218 .

المتصلة بتكنولوجيا الإعلام والاتصال، وعدم الإلتزام بذلك يترتب عليه توقيع العقوبات المنصوص عنها قانونا[1].

كما يجب أن يتضمن الإذن تحديد الشخص المراد مراقبة إتصالاته الإلكترونية، ببيان إسمه ولقبه ومحل إقامته وكل ما يفيد في تعيينه ونفي الجهالة عنه ويجب أن يتخذ هذا الإجراء ضد هذا الشخص دون غيره، فإذا إمتدت المراقبة إلى غير المذكورين في الإذن عد باطلا [2] .

ت/ مدة الإذن بمراقبة الإتصالات الإلكترونية

المشرع الجزائري لم يحدد مدة معينة للقيام بإجراء المراقبة الالكترونية في القانون 09-04 وبالتالي يتم الرجوع الى القواعد العامة في الإجراءات الجزائية ومن ثمة فهذا الاجراء يتخذ لمدة 4 أشهر يمكن تجديدها اذا تطلبت مقتضيات البحث و التحري والتحقيق.

الفرع الثاني :التحفظ العاجل على البيانات المعلوماتية المخزنة

يعتبر التحفظ العاجل على البيانات المعلوماتية المخزنة إجراء حديث للتحري والتحقيق في الجرائم الالكترونية باعتباره إجراء كفيل لحماية سلامة البيانات المعلوماتية بطريقة أسرع من اتخاذ إجراءات التفتيش والضبط[3] .

---

[1] – المادة 26 من المرسوم الرئاسي رقم 183/20 المؤرخ في 13 يوليو 2020 يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية مؤرخة في 18 يوليـــــــــــــــــــــــو 2020 العدد 40 ص 05.

[3]– ثابت دنيا زاد، المرجع نفسه ص 218 .

[3]– نظرا لما يحققه اجراء التحفظ العاجل للبيانات المعلوماتية المخزنة في أنه اجراء أقل تدخلا وتطفلا من إجراءات التحري والتحقيق الأخرى كالتفتيش وغيرها، كما انه يضمن عدم ضياع الأدلة الرقمية الجوهرية والتي يمكن أن تكون الأدلة الوحيدة التي تثبت تورط أحد المجرمين المعلوماتيين، ويتم هذا الاجراء عن طريق إصدار أمر من السلطات القضائية المختصة إلى أشخاص أو مقدمي خدمة الأنترنت لحفظ المعطيات التي يملكونها والتي بحوزتهم قبل ضياعها أو محوها، لذا حرصت البعض من الدول على التنصيص على هذا الإجراء الحديث كوسيلة من الوسائل الفعالة لمكافحة الجرائم الالكترونية.

اولا / المقصود بالتحفظ العاجل على البيانات المعلوماتية المخزنة

يقصد بالتحفظ العاجل على البيانات المخزنة " توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى"[1].

وقد نظم المشرع الجزائري اجراء التحفظ العاجل للبيانات المعلوماتية المخزنة ضمن القانون 04/09 كإلزام من التزامات مقدمي خدمة الإنترنت في الفصل الرابع منه في المادتين(10 و 11) على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات بحفظ المعطيات، وتبعا لذلك سنتناول حفظ المعطيات المتعلقة بحركة السير واعتراض محتوى البيانات.

1/ حفظ المعطيات المتعلقة بحركة السير

إستحدث المشرع الجزائري إجراء حفظ المعطيات المتعلقة بحركة السير بموجب نص المادة (11) من القانون 04/09 ولكنه لم يعرفه، ويقصد بحفظ المعطيات المتعلقة بحركة السير أو ما يسمى بمعطيات المرور" تجميع أو تسجيل البيانات المتعلقة بخط سير البيانات في الوقت الفعلي عن طريق إلزام مقدم الخدمة بذلك في حدود قدرته الفنية بهدف تسهيل مهمة الجهات القائمة بجمع الأدلة في التعرف على مرتكب الجريمة والمساهمين فيها[2].

حيث نصت المادة (10 ف/ 1) من نفس القانون على أنه " في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) تحت تصرف السلطات المذكورة "

[1]– أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية 2015ص 180.

[2]– نادية سلامي، اليات مكافحة التجسس الالكتروني، اطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الجنائي جامعة العربي التبسي – تبسة 2019/2018 ص 258 .

وقد حدد المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمات[1] وهي المعطيات المتعلقة بحركة السير، حيث تعرف المادة (2ف/ه) المعطيات المتعلقة بحركة السير بأنهـــا " أي معطيات متعلقة بحركة الإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة اتصالات توضح مصدر الإتصال والوجهة المرسل اليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة " ونجد أن المشرع الجزائري قد حدد مجموعة معطيات تتعلق بحركة السير حيث نص على أنه " مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمات بحفظ :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال .
- الخصائص التقنية وكذا تاريخ ووقت ومدة الإتصال .
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أوالمستعملة ومقدميها .
- المعطيات التي تسمح بالتعرف على المرسل إليه أوالمرسل إليه ومكان الاتصال وكذا عناوين المواقع المطلع عليها[2].

وفي هذا الإطار لم يكتفي المشرع الجزائري بإلزام مقدمي خدمات الأنترنت بحفظ هذه المعطيات وإنما ألزم بذلك متعاملي الهاتف رغم أن إلتزامه أكثر تحديدا وحصرا بحيث يلتزمون فقط بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة وتلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

وتحدد مدة حفظ المعطيات المذكورة بسنة واحدة إبتداء من تاريخ التسجيل دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في المادة(11ف/4) من

---

[1] – وتعرف المادة (2ف/د) من نفس القانون مقدمي الخدمات :

- أي كيان عام أو خاص يقدم لمستعملي خدماتهالقدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات .
- أي كيان آخر يقوم بمعالجة أو خزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

[2]–المادة (11) من القانون 09-04 .

نفس القانون[1] ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

2/ إعتراض المعطيات المتعلقة بالمحتوى

يقصد بإعتراض البيانات المتعلقة بالمحتوى " تجميع البيانات التي تشير إلى المحتوى الإخباري للإتصال، بمعنى مضمون الإتصال أو الرسالة أو المعلومات المنقولة عن طريق الإتصال[2]، وعليه يكمن الفرق بين المعطيات المتعلقة بالمرور والمعطيات المتعلقة بالمحتوى في أن الأولى تغطي فقط المعطيات المنتجة خلال نقل المعطيات ولكن لا تغطي المعطيات المنقولة، كما أن الدخول إلى المعطيات المتعلقة بالمحتوى تمكن السلطات من تفحص طبيعة الرسائل والملفات المتبادلة، أما معطيات المرور فتمكن من كشف هوية مرتكب الجريمة دون معرفة محتوى الإتصال، كما أن الصعوبات التي تواجه إجراء حفظ المعطيات المتعلقة بالمرور تتمثل في إمكانية استخدام الجناة لخدمات الأنترنت التي تسمح بإجراء اتصالات مجهولة وسرية أو استخدام نهايات طرفية عمومية (كالإتصال من مقهى أنترنت مثلا) فهذا الإجراء لن يمكن من كشف المرسل، والصعوبات التي تواجه إجراء اعتراض المعطيات المتعلقة بالمحتوى فهو لجوء الجناة إلى تكنولوجيا التشفير مما يسمح لهم بحماية المحتويات المتبادلة بصورة يستحيل معها على سلطات التحقيق الدخول إليها[3]، وقد نص المشرع الجزائري على هذا الاجراء بطريقة غير مباشرة في المادة (10) من القانون 04/09 على أنه "في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها...."

---

[1]– تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من(50.000 دج) الى(500.000 د ج) ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات .

[2]– هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية – معلقا عليها – طبعة أولى دار النهضة العربية القاهرة، 2011 ص 266 . .

[3]– نادية سلامي، المرجع السابق ص 260 .

ورغم خصوصية هذا الإجراء فالمادة (10) التي تنص عليه جاءت عامة ولم تتضمن شروطه أو ضوابطه، وكل ما نصت عنه هو إلزام مقدمي الخدمات بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق

الفرع الثالث : تفتيش المنظومات المعلوماتية وحجز المعطيات

عمل المشرع الجزائري على تطوير أساليب التحقيق وإجراءاته لتتلائم مع خصوصية الجرائم الالكترونية وذلك من خلال سن أحكام جديدة وإضافية للتفتيش بموجب القانون 04/09 والذي إستحدث أحكاما خاصة بتفتيش المنظومات المعلوماتية وحجزها، ويرتبط إجرائي تفتيش المنظومات المعلوماتية وحجز أو ضبط المعطيات المعلوماتية من حيث كون الثاني هدف الأول كما يعدان من الإجراءات الخاصة والمختلفة عن التفتيش والحجز التقليدي.

أولا/ تفتيش المنظومات المعلوماتية

يمكن تعريف تفتيش المنظومة المعلوماتية انه " البحث عن طريق التفتيش والضبط عن البيانات المخزنة في النظام المعلوماتي للحاسب الآلي أو أي دعامة تخزين للمعلومات سواء كانت هذه البيانات مخزنة في جهاز واحد أو منظومة إتصالات"[1].

وقد نص المشرع الجزائري على إجراء تفتيش المنظومات المعلوماتية في المادة الخامسة (05) من القانون 04/09 وضمنه ضوابط التفتيش وشروط القيام به محيلا على الأحكام العامة الواردة في قانون الإجراءات الجزائية[2] ويمكن إجمال هذه الضمانات فيما يلي:

[1]– نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مقال منشور في مجلة الأندلس للعلوم الإنسانية والاجتماعية، المجلد 15، العدد 15، أفريل 2018 ص 321 .

[2]– نظم المشرع الجزائري إجراءات التفتيش بموجب نصوص المواد من(81 إلى 83) من قانون الإجراءات الجزائية كما أحالت أيضا إلى الأحكام المقررة في المواد من(45 إلى 47) حيث يخضع إجراء تفتيش المكونات المادية للحاسب الآلي وفقا لقواعد قانون الإجراءات الجزائية طبقا لطبيعة المكان الموجودة فيه سواء من الأماكن الخاصة أو العامة مع التقيد بالضمانات التي وضعها القانون .

1 / محل التفتيش

محل التفتيش هو المنظومة المعلوماتية وبما أن المنظومة تتكون من عناصر مادية وعناصر معنوية فلا توجد صعوبة بالنسبة للتفتيش الذي ينصب على المكونات المادية للنظام فهو يخضع للقواعد العامة في قانون الإجراءات الجزائية، وعلى إعتبار التفتيش هنا يتعلق بجريمة مرتكبة بتقنية المعلومات فهو يتجاوز الضمانات المقررة لتفتيش المساكن التي يمكن أن توجد بها مثل هذه المكونات المادية للنظام بحيث لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه ودون حاجة إلى رضائه عند القيـــام بهذا الإجراء[1]، كما أنه يجوز القيام بإجراء التفتيش بكل ساعة من ساعات النهار والليل[2]، واستغناء المشرع الجزائري عن هذا الشرط الأخير بخصوص التفتيش في الجرائم الالكترونية راجع إلى إدراكه للطبيعة المميزة لهذه الجرائم من حيث إمكانية ارتكابها في أي وقت وأدلة الإثبات فيها غير مرئية وسهلة المحو والإتلاف، وبالتالي فتأخير التفتيش إلى الموعد القانوني وفق المبدأ العام قد يكون سببا في ضياع الأدلة ومن ثم عرقلة سير التحقيق[3]، ومن جهة أخر يعود أيضا إلى تراجع أهمية هذا الشرط أو الضمانة مع ظهور تقنية " التفتيش عن بعد" والذي يمكن إجراؤه في أي وقت ومن أي مكان في العالم[4]، وبالرجوع إلى المادة الخامسة (05) من القانون 04/09 نجد أن المشرع الجزائري قد ركز على تفتيش المكونات المعنوية للمنظومة المعلوماتية وهذا ما يستفاد من صياغة نص المادة بقولها " يجوز الدخول بغرض التفتيش ولوعن بعد إلى:

" أ/ منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها

ب –منظومة تخزين معلوماتي ".

وقد استخدم المشرع هنا مصطلحي الدخول والتفتيش ويتضمن هذا الأخير قراءة وتمحيص وبحث وفحص البيانات وعلى العكس فإن كلمة الدخول (وإن كانت ذات معنى محايد – بمعنى اشتمالها

---

[1]– المادة (64) من قانون الاجراءات الجزائية.

[2]– المادة (47 ف /3–4) من نفس القانون .

[3] –Padova. Yann N04,Dalloz, op.cit P 770.

[4]– علالي أمينة، مكافحة الجرائم العابرة للحدود المرتكبة بتقنية المعلومات، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون العام، كلية الحقوق، جامعة عنابة ص 236 .

للتفيش وغيره من المصطلحات) يعبر عنها أحيانا **بالولوج** فهو مصطلح خاص بتكنولوجيا الإعلام والإتصال يحقق الوصول إلى البيانات المخزنة، فالدخول أو الولوج إجراء تفتيش، والتفتيش وسيلة لجمع الأدلة ويتم استخدام المصطلحين عموما من أجل تنسيق المفاهيم التقليدية والمصطلحات الحديثة[1]، وعلى اعتبار أن الدخول مصطلح معلوماتي فهو يستخدم في البيئة الإلكترونية وليس المادية، ويكون المشرع الجزائري قد حسم الخلاف الفقهي حول صلاحية المكونات المعلوماتية للتفتيش بإفرادها بنص خاص[2].

أ/ الحالة التي تكون فيها المنظومة المعلوماتية في الإقليم الوطني

إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أوجزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك[3].

والملاحظ هنا أن تمديد التفتيش إلى منظومة معلوماتية أخرى يكتسي طابعا خاصا، فهو يتم عن بعد وبشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومات، وواضح أيضا أن الولوج إلى منظومة المعلومات يتم هنا بمجرد الشك أو الاعتقاد بتواجد المعلومات محل البحث داخل هذه المنظومة أو تلك، وقد أوجب المشرع الجزائري على عكس التشريعات الداخلية لكي يكتسي هذا الإجراء طابعه الرسمي ويقع تحت طائلة القانون أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا ومتماشيا مع مقتضيات حماية الحياة الخاصة للأفراد، وهما الأمرين اللذان علق المشرع تحقيقهما على شرط إبلاغ الجهات القضائية المختصة مسبقا بذلك، ولاشك أن الجهات المختصة المقصودة في الفقرة الثانية من المادة الخامسة(5) من القانون 04/09 هي وكيل الجمهورية وقاضي التحقيق باعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش .

ب/ الحالة التي تكون فيها المنظومة المعلوماتية موزعة بين الإقليم الوطني وخارجه

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة

---

[1]– نادية سلامي، المرجع السابق ص 256 .

[2]– نادية سلامي، المرجع نفسه ص 256 .

[3]– المادة(05 ف/02) من القانون 04/09 .

السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل"[1] ولسلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني.

لم تتضمن المادة الخامسة من القانون 04/09 والمنظمة لإجراء التفتيش النص على السلطات القائمة به ولا على ضرورة وجود إذن بتفتيش المنظومة المعلوماتية، واكتفت بالإحالة على قانون الاجراءات الجزائية فتكون السلطة المختصة بالتفتيش هي قاضي التحقيق ووكيل الجمهورية، واللذان يأذنان لضباط الشرطة القضائية بالقيام به على أن يكون الإذن مكتوبا مع وجوب استظهاره قبل الدخول إلى المنزل أو الشروع في التفتيش، وأن يكون هذا الإذن متضمنا تحت طائلة البطلان وصف الجرم وموضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها[2] .

إلا أن القيام بتفتيش المنظومة المعلوماتية يطرح عديد الصعوبات والإشكالات التي لا يمكن الإستناد على حلها لقانون الاجراءات الجزائية[3]، ويتضح من هذا أن قواعد التفتيش المنصوص عنها في قانون الإجراءات الجزائية قررت أساسا لتفتيش المساكن وليس لتفتيش المنظومة المعلوماتية، مما يستلزم معه أن يحدد المشرع قواعد خاصة لها تنفصل عن القواعد التقليدية، وتكتسي هذه الإجراءات طابع الرسمية ولا تتم إلا بعد إعلام الجهات القضائية المختصة تطبيقا لنصوص قواعد الاجراءات الجزائية[4]، كما أجاز القانون 04/09 للسلطات المكلفة بالتفتيش تسخير كل شخص مختص في مجال عمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهامها[5].

ثانيا: حجز المعطيات المعلوماتية وفقا للقانون 09-04

إن الغرض من التفتيش هو ضبط الأدلة التي تفيد في ظهور الحقيقة، وعلى ذلك فإن الأشياء المتعلقة بالجريمة هي الأثر المباشر للتفتيش، وقد نص المشرع الجزائري على هذا الإجراء في المادة

---

[1] – المادة 05ف/3 من القانون 04/09 .

[2]– المادة (44) من قانون الإجراءات الجزائية الجزائري .

[3] – ان الاذن بالتفتيش مثلا يستوجب تحت طائلة البطلان أن يحدد بدقة الأماكن التي سيتم تفتيشها، لكن البيئة الرقمية من الإتساع بحيث تخزن ملايين البيانات والملفات المرتبطة ببعضها مما يستحيل معه التحديد، كما أن التفتيش قد يمتد لمنظومة معلوماتية موجودة في مسكن آخر مما يستلزم نص الإذن على ذلك أواستصدار إذن جديد.

[4]– المادتان (37 و 40) من قانون الإجراءات الجزائية .

[5]– المادة (05 ف/4) من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والإتصال.

السادسة(6) من القانون 04/09 مستخدما مصطلح (**الحجز**) حاسما بذلك الجدل القائم حول مدى قابلية المعطيات غير المادية للحجز مقررا صلاحيتها لذلك على اعتبار أن المكونات المادية لا يثير ضبطها أو حجزها أي إشكالية فهي تخضع للقواعد العامة في قانون الإجراءات الجزائية، أما المعطيات المعلوماتية فلا يمكن حجزها بالطرق التقليدية لذا فقد نص المشرع على أساليب حجزها في المادة السادسة (06) ذاتها كالأتي :

1/نسخ المعطيات المعلوماتية

عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة،ويتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز[1]

2/ الحجز عن طريق منع الوصول إلى المعطيات:

يسمى هذا الأسلوب أيضا (**بالتجميد**) بحيث إذا استحال إجراء الحجز وفقا لطريقة النسخ لأسباب تقنية يستوجب على السلطة القائمة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحويها المنظومة أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم استعمال هذه المنظومـــة[2]،كما أجاز المشرع للسلطات القائمة بالتفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[3].

[1]- المادة (06 ف/1). من القانون 09-04

[2]- المادة (07) من نفس القانون.

[3]- المادة (08) من نفس القانون .

المبحث الثاني : الاطار المؤسساتي لمكافحة الجرائم الالكترونية في التشريع الجزائري

في اطار السياسة الجنائية الرامية لمواجهة الجرائم الالكترونية او ما اصطلح المشرع الجزائري على تسميتها ابتداءا بالجرائم الماسة بانظمة المعالجة الالية للمعطيات بموجب تعديل قانون العقوبات سنة 2004 من خلال نصوص المواد من 394 مكرر وما يليها منه ثم الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ووعيا منه بعدم امكانية مواجهة هذا النمط الاجرامي المعقد والتقني العابر للحدود في كثير من الاحيان بنصوص موضوعية واجرائية فحسب او بمجرد التعاون والمساعدة القضائية او بتوسيع الاختصاص المحلي لبعض الجهات القضائية، استحدث المشرع بعض الهيئات الادارية مهمتها مكافحة هذه الجرائم المستحدثة، من اجل ذلك سوف نخصص المطلب الاول لـــ(**الهيئات الادارية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري**) ونعرض في المطلب الثاني لـــ (**الاجهزة الأمنية والقضائية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري)** .

المطلب الاول: الهيئات الادارية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري

قام المشرع الجزائري في مجال مكافحة الجريمة بشكل عام بإنشاء هيئات ذات طابع إداري مهمتها الأساسية مكافحة جرائم تكنولوجيا الاعلام والاتصال، وعليه سنخصص الفرع الأول لدراسة (**الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها)** ونعرض في الفرع الثاني ل(**السلطة الوطنية لحماية المعطيات الشخصية**) كما نعرج في الفرع الثالث على (**المعهد الوطني للبحث في علم التحقيق الجنائي**) ونخصص الفرع الرابع ل(**المعهد الوطني للأدلة الجنائية وعلم الاجرام**).

الفرع الاول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

أنشأ المشرع الجزائري هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها واعتبرها بموجب المرسوم الرئاسي 183/20 سلطة ادارية مستقلة توضع تحت سلطة رئيس الجمهورية[1].

اولا / تشكيلة الهيئة الوطنية لمكافحة جرائم تكنولوجيا الاعلام والاتصال وهي مكونة من جهازين : مجلس التوجيه ومديرية عامة، طبقا لنص المادة 05 من المرسوم.

* **مجلس التوجيه:** حددت المادة 06 من المرسوم الرئاسي المحدد لتشكيلة الهيئة تشكيلة مجلس التوجيه من الفئات الاتية : الوزير المكلف العدل ، الوزير المكلف الداخلية، الوزير المكلف بالمواصلات والاتصالات السلكية واللاسلكية، المدير العام للامن الداخلي، قائد الدرك الوطني، المدير العام للامن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، ويعين هذين الاخيرين رئيس الجمهورية.

* **المديرية العامة :** اكتفى المرسوم الرئاسي بوضعها تحت إدارة مدير عام[2]، وتضم مديرية العامة مديرية للمراقبة الوقائية واليقظة الالكترونية، مديرية للادارة والوسائل، ومجموعة من المصالح من دون تحديد تشكيلتها بدقة، والملاحظ ان المرسوم الرئاسي الجديد قد لجأ الى التقليص من الهياكل

[1]- المادة (02) من المرسوم الرئاسي 183/20 المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، وقد أعطى لها المرسوم الرئاسي رقم 19-261 المؤرخ في 06 يونيو2019 الملغى صفة المؤسسة العمومية التي تراجع عنها بصدور المرسوم الجديد كما حول تبعيتها من وزير الدفاع الى رئيس الجمهورية.

[2] - المادة (09) من المرسوم الرئاسي 183/20 .

الرئيسية المكونة للهيئة على خلاف سابقه، وعوضها بهياكل جديدة فرعية تعمل تحت سلطة المديرية العامة[1].

ثانيا/ اختصاصات الهيئة الوطنية لمكافحة جرائم تكنولوجيا الاعلام والاتصال: بالنسبة لمهام الهيئة ككل فقد تم توزيعها على مجلس التوجيه و المديرية العامة[2].

1/ مراقبة الاتصالات الالكترونية – دور وقائي وحصري–

تنص المادة 15 من المرسوم الرئاسي رقم 20–183 على انه تكلف مديرية المراقبة الوقائية و اليقظة الالكترونية والتي تتبع المديرية العامة بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، ويستنتج من هذه المادة الطابع الوقائي والحصري لمراقبة الاتصالات الالكترونية إذا كان الأمر متعلقا بالوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. معنى أن هذا الإجراء يتخذ من دون حدوث أي جريمة، بل تفاديا لحدوثها ونظرا لمساسه بحرمة وسرية المراسلات والاتصالات حصره المشرع في حالة الوقاية من الجرائم الإرهابية والتخريبية والماسة بأمن الدولة، إلا انه يشترط لتنفيذ المراقبة الوقائية للاتصالات الالكترونية بخصوص الجرائم الإرهابية والتخريبية والماسة بأمن الدولة شروط معينة هي: صدور إذن مكتوب من النائب العام لدى مجلس قضاء الجزائر للضباط المختصين بهذا الإجراء وهم المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة

[1] – خرشي امال، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، مقال منشور في مجلة الابحاث القانونية والسياسية، المجلد 04، عدد 01 لسنة 2022 ص 61.

[2] – بالعودة إلى دور هذه الهيئة كانت المادة 04 من المرسوم الرئاسي رقم 15–261 المتضمن انشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام والاتصال تحدد هذه المهام فهي تتنوع بين كونها هيئة استشارية، وهيئة تحري ومرصد الجمع وتسجيل وحفظ المعطيات الرقمية وهي مساعدة للقضاء بالإضافة إلى أنها هيئة تكوين للمحققين، لكن بعد إلغاء المرسوم 15–261 وتعويضه بالمرسوم 19–172 لم يحصر هذا الأخير مهام الهيئة ككل بل وزع المهام على تشكيلتها والمتمثلة في مجلس توجيه ومديرية عامة وهو نفس الامر الذي ابقى عليه المرسوم 183/20 الجديد.

بتكنولوجيات الإعلام والاتصال ومكافحتها. ويسلم الإذن لهم مدته 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[1].

ويكلف مجلس التوجيه بالقيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، نستنتج أن مجلس التوجيه للهيئة هو من يقرر حالات التهديد ولم يقصر هذا المرسوم حالة التهديد والخطر على تلك المتعلقة بالإرهاب والتخريب والمساس بأمن الدولة بل تعداها إلى كل الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[2].

2/ مساعدة السلطات القضائية الداخلية: جاء في نص المادة 14 من قانون رقم 09-04 انه من مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وعليه تتدخل الهيئة بطلب من الجهات القضائية المختصة لتقوم في إطار الخبرات القضائية بالإجراءات المنصوص عليها في القانون رقم 09-04 لاسيما المراقبة الالكترونية للاتصالات، وايضا الجرائم التي تتطلب اللجوء الى اساليب التحري الخاصة للهيئة[3].

3/ مساعدة السلطات القضائية الدولية : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدات الدولية لجمع الأداة الخاصة بالجريمة في الشكل الالكتروني، يمكن في حالة الاستعجالات، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة المذكورة أعلاه، و إذا وردت عن طريق الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها [4].

---

[1] – المادة 04 من القانون 04/09 .

[2] – المادة 07 ف/ 5 من المرسوم الرئاسي 183/20 .

[3] – المادة 15 ف/02 من نفس المرسوم الرئاسي.

[4] – المادة 16 من القانون 04/09 .

تنص المادة 10ف/06 من المرسوم الرئاسي رقم 20-183 انه من مهام المديرية العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام والاتصال تبادل المعلومات مع مثيلاتها في الخارج بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم .

كما يمكن لها طلب اجراءات تحفظية ويقصد بها طلب إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الإجراء في الفصل في مسألة معروضة على القضاء، وهو ما أبرزته المادتين 16 و 17 من القانون 09/04 فالدولة الطالبة يتعذر عليها القيام به بنفسها ولا يكون ذلك إلا بالإنابة القضائية.

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

لعل من أهم الآليات القانونية التي جاء بها القانون 07/18 إنشاء سلطة وطنية لحماية المعطيات ذات الطابع الشخصي تعمل على تجسيد الحماية القانونية للمعطيات. فالسلطة الوطنية هي مؤسسة إدارية تتمتع بالشخصية المعنوية والذمة المالية تنشأ لدى رئاسة الجمهورية يحدد مقرها بالجزائر العاصمة[1]

اولا / تشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي : تتشكل السلطة من ثلاثة أعضاء يختارهم رئيس الجمهورية وثلاثة قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.

كما تتكون السلطة من عضو عن كل غرفة من البرلمان، وممثل للمجلس الوطني لحقوق الإنسان وآخرين يمثل كل واحد منهم وزير الدفاع الوطني، وزير الشؤون الخارجية، الوزير المكلف بالداخلية، وزير العدل والوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيا والرقمنة، وزير الصحة، ووزير العمل والتشغيل والضمان الاجتماعي. يعين رئيس السلطة الوطنية وأعضائها بموجب مرسوم رئاسي لعهدة مدتها خمس سنوات قابلة للتجديد[2].

[1] – المادة 22 من القانون 07/18

[2] – المادة 23 من نفس القانون .

ثانيا/ اختصاصات السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي : تكلف السلطة الوطنية بتلقي تصريحات معالجة المعطيات الشخصية ومنح التراخيص في حالة قدرت وجوب ذلك كما تقوم بإعلام الشخص المعني والمسؤول عن المعالجة بحقوقه وواجباته، تقدم كذلك استشارات لكل من يلجأ لمعالجة المعطيات من أشخاص أو كيانات، كما تتلقى السلطة الوطنية كل الاحتجاجات والطعون والشكاوى حين تنفيذ معالجة المعطيات الشخصية، وهي منوطة بمنح الترخيص لنقل المعطيات للدول الأجنبية وفقا للقانون[1].

كما يمكن للسلطة الوطنية أن تأمر أيضا بالتغيرات اللازمة لحماية المعطيات أو إغلاقها أو سحبها أو إتلافها، وأن تقوم بنشر التراخيص الممنوحة في سجل وطني، كما تسهر على تطوير العلاقات مع الدول الأجنبية في هذا المجال وتقديم الاقتراحات اللازمة لتبسيط وتحسين الإطار التشريعي والتنظيمي في هذا المجال.

كما أنه من مهام السلطة الوطنية إصدار العقوبات الإدارية اللازمة في حالة خرق للقانون عند معالجة

المعطيات الشخصية وإعلام النائب العالم في حالة إدراكها وجود وصف جزائي .

ووفقا للمادة 26 من القانون 07/18 تلتزم السلطة الوطنية ممثلة في رئيسها وأعضائها بالحفاظ على الطابع السري للمعطيات، كما تمسك السلطة سجلا وطنيا تقيد فيه الملفات المعالجة سواء من طرف السلطات العمومية أو من طرف الخواص بصفتهم مسؤولين عن المعالجة، وتقيد فيه كافة التصريحات والتراخيص الممنوحة وكل المعطيات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم القانونية[2]

[1] – المادة 25 من القانون 07/18 .

[2] – المادة 28 من نفس القانون .

الفرع الثالث/ الوطني للبحث في علم التحقيق الجنائي[1]

هو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي[2] يوضع تحت وصاية الوزير المكلف بالداخلية ويتبع المديرية العامة للأمن الوطني[3].

تم تنظيم مصالح ومخابر وأقسام المعهد بموجب قرار وزاري مشترك ي مشترك تضمن (05) مخابر جهوية بوهران، قسنطينة، ورقلة، بشار وتمنراست وهي تشكل إمتداد لنشاطات المعهد في مجال الخبرة والتكوين والبحث العلمي ، وتتمثل مهام هذه المخابر في ما يلي:

- اجراء التحاليل والخبرة العلمية الضرورية لسير التحقيقات القضائية بطلب من المحققين والقضاة والسلطات المؤهلة.
- توفير الدعم التقني الضروري في تسيير مواقع حدوث الجريمة ووضع تقنيين ومختصين مجهزين بالوسائل الملائمة تحت تصرفهم .
- المساعدة في التكوين في مجالات علم التحقيق الجنائي الموجهة لكافة تقني السلسة القضائية وكذا البحث العلمي المطبق في علم التحقيق الجنائي[4] .

كما يضم هذا المخبر مصلحة الخبرات الخاصة بالدلائل التكنولوجية وتكلف بما يلي :

- معاينة المخالفات والتحريات في ميادين الدلائل المعلوماتية وجرائم الكومبيوتر والبصمات الصوتية ومعالجة الصورة والإشارة واستغلال الهواتف المحمولة وإعداد تقارير الخبرة .
- المساهمة في التعليم ونشاطات البحث التطبيقي في علم التحقيق الجنائي .

---

[1]– المرسوم الرئاسي رقم 432/04 المؤرخ في 29 ديسمبر 2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 84 مؤرخة في 29 / 12 / 2004 ص 25

[2] – المادة 02 من نفس المرسوم الرئاسي .

[3] – المادة 03 من نفس المرسوم الرئاسي .

[4]– المادة 09 من القرار الوزاري المشترك المؤرخ في 14 أفريل 2007 يتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية ل لمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 36 مؤرخة في 03 يونيو 2007 ص 17.

- ضمان تسيير البنوك معطيات علم التحقيق الجنائي فيما يخص المحفوظات الآلية للبصمات الصوتية والمخالفات المرتبطة بتكنولوجيا الإعلام والإتصال .

ويضم المخبر ايضا ثلاث مخابر متخصصة مخبر التحليل الجنائي للصوت ومخبر الأدلة المعلوماتية وجرائم الكمبيوتر إضافة إلى مخبر إستغلال الهواتف المحمولة[1]

الفرع الرابع : المعهد الوطني للأدلة الجنائية وعلم الاجرام[2]

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي[3].

ويقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي الجزائر العاصمة بمختلف دوائره بإجراء الخبرات في إطار التحريات الأولية والتحقيقات القضائية بما في ذلك دائرة الإعلام الآلي والإلكترونيك التي أسندت لها مهمة تحليل الأدلة الخاصة بالجرائم المعلوماتية، وذلك بتحليل الدعامات الإلكترونية وإصلاح الدعامات التالفة، إنجاز المقاربات الهاتفية وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها

ومن بين الاختصاصات المسندة للمعهد الوطني للادلة الجنائية وعلم الاجرام[4]:

- اجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.

---

[1] – الملدة 10 من نفس القرار الوزاري .

[2]– المرسوم الرئاسي رقم 04 / 183 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام، الجريدة الرسمية رقم 41 المؤرخة في 27 جوان 2004 ص 18

[3] – المادة 02 من نفس المرسوم الرئاسي .

[4] – المادة 06 من المرسوم الرئاسي 183/04 .

- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الاجرام .
- المبادرة و إجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام .
- تصميم وانجاز بنوك المعطيات .

المطلب الثاني : الاجهزة الأمنية والقضائية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري

عملت الجزائر على إنشاء جهات امنية وقضائية متخصصة لمكافحة الجريمة المعلوماتية، نظرا لما تتميز به هذه الجرائم من ميزات تختلف عن الجرائم التقليدية، وعليه سنخصص الفرع الاول لـــ (**الاجهزة الأمنية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري**) ونعرج في الفرع الثاني على (**الاجهزة القضائية**) ونخصص ذلك للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

الفرع الاول: الاجهزة الأمنية المختصة بمكافحة الجرائم الالكترونية في التشريع الجزائري

سنتناول في هذا الفرع كل من مصالح الشرطة القضائية على مستوى المديرية العامة للأمن الوطني والمديرية العامة للدرك الوطني.

اولا / مصالح الشرطة القضائية على مستوى المديرية العامة للأمن الوطني

قامت المديرية العامة للأمن الوطني في إطار سياسة التخصص في مجال الشرطة القضائية بإدخال تعديلات على الهياكل التنظيمية الخاصة بمصالح الشرطة القضائية، وذلك من أجل جعل المصالح المكلفة بمكافحة الجريمة أكثر ملائمة مع الواقع وأكثر استعدادا لما تشير إليه التنبؤات المستقبلية، ففي مجال الجريمة المعلوماتية بات من الضروري وضع آليات عملياتية[1].

[1] – مصطفاوي عبد القادر، الشرطة الوطنية ومكافحة الجريمة المعلوماتية، بحث مقدم الى فعاليات الملتقى الدولي حول محاربة الجريمة المعلوماتية ، مركز البحوث القانونية والقضائية، الجزائر من 5 الى 6 ماي 2010 ص 121

وعليه فإن مصالح الشرطة القضائية، كفيلة بالتصدي ومعالجة هذا النوع من الإجرام الذي لم يسبق التعامل معه من قبل، فتم إنشاء مصالح متخصصة في مكافحة هذا الإجرام. تتمثل في:

1/ على مستوى مخابر الشرطة العلمية

إثر تفاقم ظاهرة استخدام التكنولوجيا في مختلف أشكال الإجرام، تم سنة 2007 ، تدعيم المخابر الثلاث للشرطة العلمية والتقنية و المتواجدة بكل من العاصمة، وهران وقسنطينة، بأقسام مختصة في الأدلة الإلكترونية، تتمثل مهامها في استغلال الأجهزة الإلكترونية التي يشتبه استخدامها في ارتكاب الجرائم وذلك لاستخراج المعطيات المخزنة بداخلها والتي قد تساعد المحققين في التحقيق وتلك التي تشكل في حد ذاتها أدلة إقناع، ومن أهم الأجهزة التي تتكفل باستغلالها هذه الأقسام: أجهزة الكمبيوتر ولواحقها، أدوات التخزين، أقراص وماضية، أقراص صلبة، اجهزة الهواتف النقالة واجهزة التصوير الرقمية[1].

2/ المصالح الولائية للشرطة القضائية

في شهر جانفي سنة 2010 ، تم تنصيب 23 خلية عملية على مستوى المصالح الولاية للشرطة القضائية التابعة لأمن الولايات موزعة كما يلي: 08 خلايا على مستوى ولايات الوسط،08 خلايا على مستوى ولايات الشرق، 06 خلايا على مستوى ولايات الغرب،01 خلية على مستوى ولايات الجنوب. وقد تم اختيار المحققين التابعين لهذه الخلايا على أساس الشهادات الجامعية التي يحملونها، والخبرة التي يمتلكونها في مجال الشرطة القضائية، ثم تكوين تأهيلي أولي ليلتحقوا بعدها بمناصبهم الجديدة.

وتعتبر المديرية العامة للأمن الوطني عضوا في المنظمة الدولية للشرطة الجنائية، من خلال وجود مكتب مركزي وطني تابع لمديرية الشرطة القضائية/المديرية العامة للأمن الوطني وهي من أهم صور التعاون الشرطي الدولي لما تتيحه هذه الأخيرة من التبادل المعلوماتي وتسهيل تنفيذ الإجراءات القضائية الخاصة بتسليم المجرمين، مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا، وقد بادرت المديرية العامة للأمن الوطني في اقتناء أحدث الوسائل والمعدات التي تستخدم في التحقيقات الجنائية، لتحقيق أكبر فعالية في البحث عن الأدلة وتنوير

[1] – مصطفاوي عبد القادر، المرجع السابق ص 122 .

الجهات القضائية[1]، كما انتهجت المديرية العامة للأمن الوطني سياسة التفتح على المجتمع لجلب المواطن واشراكه في مكافحة الجريمة بكل أنواعها، كإنشاء موقع خاص بالشرطة القضائية الجزائرية، في الشبكة العنكبوتية، يمكن الجمهور من رفع كل الانشغالات في الجانب الأمني والتبليغ عن كل السلوكيات اللامشروعة. وعن التكوين والتدريب أرسلت المديرية العامة للأمن الوطني سنة 2023 إطارين للتكوين في مجال الجريمة المعلوماتية بفرنسا كما تم دعوة فريق من المحققين المختصين بفرنسا في مجال جرائم المعلومات، حيث قاموا بتكوين دفعة من 22 ضابط شرطة خلال نفس السنة، كما سجلت المديرية العامة للأمن الوطني حضورها في مختلف الملتقيات والندوات الدولية التي تعالج موضوع الجريمة الإلكترونية، بهدف الاستفادة من تجارب الدول التي سبق لها التعامل مع هذه الظاهرة[2]

و الملاحظ أن هذه الدورات التكوينية والتربصات التي نظمت في هذا المجال، كانت سابقة على وجود قانون يجرم الإجرام المعلوماتي بالجزائر، و ذلك حرصا من المديرية العامة للأمن الوطني على استباق المجرمين إلى الميدان من جهة وتأهيل مصالح الشرطة القضائية للتكفل بمختلف أشكال الجرائم الإلكترونية.

ثانيا/ المديرية العامة للدرك الوطني

بدأت قيادة الدرك الوطني تطبيق برنامجها من خلال مباشرة مهامها ابتداء من سنة 2004 ، أي بعد إدراج فقرة متعلقة بمكافحة الإجرام المعلوماتي ضمن قانون العقوبات التي حددت أنماط جرائم المساس بأنظمة المعالجة الآلية للمعطيات وعقوباتها، ومن ثم تم إنشاء **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها** من أجل القضاء أو الحد مساعدة وحدات الدرك الوطني الممارسة لمهام الشرطة القضائية في البحث والتوصل إلى مرتكبي المخالفات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات وكذا المخالفات المتعلقة باستخدام الأنظمة المعلوماتية لتكنولوجيات الإعلام والاتصال، ومن أجل تحقيق ذلك يحوز أفراد المركز الذين يطاردون الجريمة المعلوماتية أحدث الأنظمة والأجهزة والبرمجيات المتطورة من أجل استخدامها في

[1] – وردة شرف الدين، الاثبات الجنائي بالادلة الرقمية، المرجع السابق ص 78.

[2] – وردة شرف الدين، الاثبات الجنائي بالادلة العلمية، المرجع السابق ص 79.

عمليات الوقاية من الإجرام المعلوماتي ومكافحته، وهذا ما يعد تحديا في حد ذاته، حيث يتعلق الأمر بحماية المنظومة الوطنية للمعلومات من خلال تطبيق القانون.

في إطار ممارسة مهامه ونشاطه، يقوم المركز بالتعاون والتنسيق مع المصالح الأمنية الوطنية وعدد من متعاطي الخدمات الهاتفية من أجل الاستجابة للطلبات التي تأتي من مختلف وحدات الدرك الوطني والمتعلقة بتشخيص والتعرف على العناوين الإلكترونية أو أرقام المرسلين محل التحقيق، كما أن المركز يتعاون مع مختلف السلطات القانونية والتشريعية في مجال طلبات التعاون مع الهيئات القانونية الدولية.

ويسعى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها الى:

- تعميم واستكمال نشر فرق المحققين في الجريمة المعلوماتية وتعميم نظام اليقظة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني.
- تكوين مجموعة مختصة في مهام أمن الأنظمة المعلوماتية وحمايتها.
-تكوين المكونين في المجال وإعداد برنامج المواد المتعلقة بالتكنولوجيات الجديدة ومكافحة الجريمة المعلوماتية على صعيد كافة مستويات التكوين.

الفرع الثاني: القطب الجزائي المتخصص بمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

في محاولة من الدولة تكييف اجهزتها المكلفة بمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال مع التحديات المفروضة وفي اطار تكميلي وداعم حتمته الضرورة تم انشاء قطب جزائي وطني متخصص يعنى بمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال لضمان فعالية اكبر للجهاز القضائي في مواجهة هذا النمط الاجرامي ودعمه، ذلك ان هذا النمط حتم نوعا من التخصص القضائي لمواجهته بالنظر لخطورته وتعقيده من جهة وطابعه التقني من جهة اخرى . انشئ هذا القطب المتخصص بموجب الامر 11/21[1] وباستقراء نصوصه نجد المشرع لم يقم بتعريف هذا القطب،

[1] – تم انشاء القطب الجزائي بموجب الامر 11/21 المتمم للامر رقم 156/66 المتضمن قانون الاجراءات الجزائية الذي استحدث الباب السادس ضمن الكتاب الاول المتعلق بمباشرة الدعوى العمومية و إجراءات التحقيق وادرج المواد من 211 مكرر 22 الى 211 مكرره 29 ضمن نصوص قانون الاجراءات الجزائية.

واقتصر فقط على النص على انشائه واظهار وجوده القانوني وتواجده كجهاز قضائي جزائي في التنظيم القضائي على مستوى محكمة مقر مجلس قضاء الجزائر[1] ومتناولا مرة اخرى مفهوم الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بعد ان حدد مفهومها بموجب المادة 2- ا من القانون 09-04 حرصا منه على توسيع دائرة اخرى امام ما افرزته او تفرزه التطورات التي يعرفها مجال المعلوماتية .

وتطبيقا لمبدأ الاثر المباشر او الفوري للتشريع وبمجرد النص على انشاء القطب تم العمل على تفعيله وتنصيبه خلال شهر سبتمبر 2021 اذ يقع القطب حاليا بمحكمة الدار البيضاء ويتشكل العنصر البشري للقطب من :

- **القضاة:** يضم القطب وكيل الجمهورية(جهة متابعة) تتكون من وكيل جمهورية رئيسي ووكيل جمهورية مساعد ، قاض التحقيق ورئيس القطب (جهة حكم) وجهة تحقيق تتكون حاليا من غرفتي تحقيق[2] .

- **الموظفين** : يضم القطب حاليا 8 من مستخدمي امانات الضبط وتقني سامي في الاعلام الالي و ايضا مكلفون بتنظيم الملفات و مساعدة القضاة على مستوى القطب .

كما يتشكل القطب من المصالح التالية : رئاسة امانة ضبط القطب ، مصلحة الطعون، مصلحة الجدولة، مصلحة البريد العام، مصلحة القسم الجزائي ، مصلحة تنفيذ العقوبات، امانة غرفتي التحقيق امانة رئيس القطب ومصلحة الاعلام الالي[3] .

ثانيا/ اختصاصات القطب

بالنسبة للاختصاص المحلي منح المشرع القطب اختصاصا وطنيا بنصه على ممارسة وكيل الجمهورية لدى القطب وكذا قاض التحقيق فرئيس القطب لصلاحياتهم في كامل الاقليم الوطني[4]

[1] – المادة 211 مكرر ف/22 من نفس المرسوم .

[2] – المادة 211 مكرر 23 من قانون الاجراءات الجزائية

[3] – سلمى عبد النبي، دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في مواجهة المعطيات الواقعة على المعطيات المعلوماتية، مقال منشور في مجلة الحقوق والعلوم السياسية، جامعة باتنة، المجلد 11 عدد 02 لسنة 2024 ص 21.

[4] – المادة 211 مكرر 23 من الأمر 11/21 .

بالنسبة للاختصاص النوعي فهو يختص بنوع محدد من الجرائم وهي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والجرائم المرتبطة بها وهي الجرائم التي كانت سببا في استحداثه وتواجده ضمن نسيج التنظيم القضائي في الجزائر وهو اختصاص ممنوح له ضمن كافة مراحل الدعوى العمومية، وباستقراء نصوص الامر رقم 11/21 المنشئ للقطب الجزائي نجده قد ميز في اختصاصه بين نوعين من الاختصاصات اختصاص حصري و اختصاص مشترك، **بالنسبة للاختصاص الحصري** هو الاختصاص

المنصوص عليه بموجب المادتين 211 مكرر24 و 211 مكرر 25 و يمكن التمييز من خلالها بما يلي

الحالة الأولى: وهي الجرائم المحددة بموجب 211 مكرر 24 و الجرائم المرتبطة بها .

اذا يختص القطب دون سواه بجملة من الجرائم ذات الصلة التي تمس بجملة من المصالح المحددة على سبيل الحصر بموجب نفس المادة ، والتي تتعلق بـــ:

- الجرائم التي تمس بأمن الدولة او بالدفاع الوطني .
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن او السكينة العامة أو استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية .
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- جرائم التميز وخطاب الكراهية

كما يختص القطب أيضا بالجرائم المرتبطة بتلك الجرائم، وهو أمر منطقي فمن يملك الأصل يملك الفرع، وهذا وقد تطرق المشرع لمفهوم الجرائم المرتبطة بموجب نص المادة 188 من قانون الإجراءات الجزائية[1]، وما يمكن ملاحظته أن المشرع أوكل للقطب اختصاص حصري في الجرائم

[1] – تنص المادة 188 من قانون الاجراءات الجزائية على انه " تعد الجرائم مرتبطة في الاحوال التالية :

أ/ اذا ارتكبت في وقت واحد من عدة اشخاص مجتمعين

المتصلة بتكنولوجيا الإعلام والاتصال الأكثر خطورة بالنظر لمحل الاعتداء الذي ينصب على مصالح بالغة الأهمية كأمن الدولة، الدفاع الوطني، السكينة العامة، استقرار المجتمع، وكذا على بعض صور الاعتداءات العظيمة الأثر إن صح القول، والتي تم النص على تجريمها بموجب التعديلات الأخيرة التي عرفها قانون العقوبات، أو نصوص التجريم الخاصة، والتي من شأن تكنولوجيات الإعلام والاتصال المتوافرة والمتطورة التسهيل من ارتكابها، وتوسيع نطاق آثارها[1] .

الحالة الثانية: الجرائم المبنية بموجب نص المادة 211 مكرر 25، والجرائم المرتبطة بها:إذا يختص القطب دون سواه أيضا بالجرائم ذات الصلة الأكثر تعقيدا والجرائم المرتبطة بها، هذا وقد حددت الفقرة الثانية من نفس المادة مفهوم تلك الجرائم تعقيدا وبينته[2].

وما يمكن الإشارة إليه في هذا الصدد، أن المشرع إذا كان قد منح القطب اختصاص حصري في الحالات المحددة في المادة 211 مكرر 24 بالنظر لأهمية المصالح الواقع عليها الاعتداء، فمن باب أولى منحه نفس الاختصاص الحصري في الجرائم الأكثر تعقيدا، كونه الأقدر على مواجهتها بالنظر لتخصصه، وتفرغه لها دون غيرها وانفراده بها، وكنوع من توزيع الاختصاص بين مختلف الجهات القضائية المجندة لهذا النوع من الإجرام[3] .

ب/ اذا ارتكبت من اشخاص مختلفين حتى في اوقات متفرقة وفب اماكن مختلفة ولكن على اثر تدبير اجرامي سابق بينهم

ج/ اذا كان الجناة قد ارتكبوا بعض هذه الجرائم للحصول على وسائل ارتكاب الجرائم الاخرى او تسهيل ارتكابها او اتمام تنفيذها او جعلهم في مأمن من العقاب

د/عندما تكون الاشياء المنتزعة او المختلسة او المتحصلة عن جناية او جنحة قد اخفيت كلها او بعضها "

[1] – سلمى عبد النبي، المرجع السابق ص 23 .

[2] – نصت المادة 211 مكرر 25ف/2 من الأمر 11/21 على انه " يقصد بالجريمة المتصلة بتكنولوجيا الاعلام و الاتصال الاكثر تعقيدا، بمفهوم هذا القانون الجريمة التي بالنظر الى تعدد الفاعلين او الشركاء او المتضررين او بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة او جسامة اثارها او الاضرار المترتبة عليها، او لطابعها المنظم او العابر للحدود الوطنية او لمساسها بالنظام و الامن العموميين، تتطلب استعمال وسائل تحري خاصة او خبرة فنية متخصصة او اللجوء الى تعاون قضائي دولي " .

[3] – سلمى عبد النبي، المرجع السابق ص 23 و 24 .

اما بالنسبة للاختصاص المشترك فقد أشارت إليه أحكام المادة 211 مكرر 27 من قانون الإجراءات الجزائية، ويقصد به الاختصاص المشترك بين القطب وبين الاختصاص المحلي لمحكمة سيد أحمد قسنطينة، ورقلة، ووهران، بمناسبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو أمر منطقي جدا، لان من يملك الكل يملك الفرع، بالنظر لمفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال الاشمل، وأن هذه الأخيرة من اختصاص القطب، بل هي سبب استحداثه ضمن التنظيم القضائي الجزائي.

ولن يتأت فهم هذه إلا من خلال ضبط وربط حدود كل من الاختصاص الإقليمي أو المحلي فالاختصاص النوعي، ذات الصلة، في الذهن، مع الأخذ بعين الاعتبار طبيعة هذه الجرائم التي لا يمكن في كثير من الأحيان حصرها في نطاق اختصاص محكمة واحدة، وإنما يتعداه إلى نطاق اختصاص العديد من المحاكم، أو جميع محاكم الجمهورية، كما قد يتعدى الحدود الوطنية .

وبالنسبة لمسألة تزامن الاختصاص تطرق المشرع من خلال الامر 11/21 لمسألة بالغة الأهمية هي مسألة تزامن الاختصاص، الناتج لا محال عن جملة من التعديلات التي مست قانون الإجراءات الجزائية، بمناسبة مجابهة جملة من الجرائم النوعية والمستحدثة ومن بينها الجرائم ذات الصلة، وفرق من هذا الصدد بين حالتين هما:

الحالة الأولى: نصت وهي حالة تزامن مع اختصاص القطب مع اختصاص القطب الاقتصادي والمالي إذا فصل فيها المشرع محددا للاختصاص بشأنها لهذا الأخير[1] .

الحالة الثانية: وهي حالة تزامن اختصاص القطب مع اختصاص محكمة مقر جلس قضاء الجزائر بمناسبة تمديد الاختصاص من جرائم الإرهاب والجريمة المنظمة عبر الوطنية إذا يؤول الاختصاص أيضا لهذه الأخيرة تطبيقا لأحكام المادة[2] .

وتعليقا على مسألة تزامن الاختصاص المتضمنة في نص المادتين المشار إليهما أعلاه، فيمكن تصور ذلك في الحالة التي ترتكب فيها الجرائم المشار إليها أعلاه والتي يختص بها القطب الجزائي الاقتصادي والمالي أو محكمة مقر مجلس قضاء الجزائر باستعمال تكنولوجيا الإعلام والاتصال ويذلك

[1] – المادة 211 مكرر28 من قانون الإجراءات الجزائية

[2] – المادة 211 مكرر 29 من الامر 11/21 .

تكون مسألة التخلي لصالحهما مسألة طبيعية ومنطقية للغاية كون تلك التقنيات المستعملة مجرد وسيلة أو مسهلة فقط لارتكابها ويبقى الفعل الرئيسي من اختصاصهما.

ثالثا/ إجراءات اتصال القطب الجزائي الوطني بملف الدعوى.

بعد تعرفنا على النظام القانوني للقطب واختصاصاته، يثور التساؤل عن كيفية توصل القطب بالملف، وإخطاره بالجرائم التي يختص بها، وفي هذا الصدد، ومرة أخرى ميز لمشرع من حالتين، فرق من خلالهما بين إجراءات إخطاره في قضايا الاختصاص المشترك.

1/ كيفية الإخطار في قضايا الاختصاص الحصري.

تطبيقا لاحكام المادة 211 مكرر 26، والإحالة الواردة بموجب أحكامها بعد أن تقوم مصالح الضبطية القضائية بإعداد محاضر التحريات الأولية، ترسل تلك المحاضر إلى وكيل الجمهورية بالقطب، حينها يتلقون التعليمات مباشرة منه بطبيعة الحال، بما له من صلاحيات إدارتهم طبقا للقانون بخصوص الجرائم ذات الصلة، وإذا ما تبين له أن تلك الواقع أنها ليست ضمن اختصاصه فإنه يتخلى عنها بموجب مقرر تخلي لصالح وكيل الجمهورية المختص إقليميا.

وهو الأمر المنطبق أيضا على قاضي التحقيق بالقطب، في حال تفتح تحقيق، إذا ما تبين له أن الواقائع المخطر بها ليست من اختصاصه، فإنه لا يحقق فيها ولا يصرح بذلك عن طريق إصداره لأمر بغير الاختصاص بشأنها.

وتطبيقا للأثر الفوري للقانون الإجرائي، إذا تم إيداع محاضر التحقيق الابتدائي المتعلقة بها أمام نيابات الجمهورية المختصة محليا فإن الاختصاص يتحول وجوبا لوكيل الجمهورية لدى القطب، إذا كانت القضايا مطروحة على جهتي التحقيق أو الحكم يصبح قضايا التحقيق والحكم غير مختصين محليا وتحول الملفات للقطب أو مجلس قضاء الجزائر بحسب الحالة[1] .

[1] – سلمى عبد النبي، المرجع السابق ص 25 .

2/ كيفية الإخطار في قضايا الاختصاص المشترك.

تطبيقا لأحكام المادة 211 مكرر 27، وما تضمنته من إحالات، فإنه وفي هذا النوع من القضايا يقوم وكلاء الجمهورية المختصين محليا بإرسال نسخة من المحاضر المعدة إلى وكيل الجمهورية لدى القطب دون أن تتضمن تقاريرهم إبداء أي رأي، بل يتعين الاكتفاء بعبارة على سبيل الإخبار فحسب.

هذا الأخير، وإذا ارتأى أن الجريمة تدخل ضمن اختصاصه وتمسك بالقضية، عندها يصدر وكيل الجمهورية المختص إقليميا مقررا بالتخلي، أما إذا كانت الدعوى في مرحلة التحقيق القضائي في الأمر بالتخلي في هذه الحالة يصدره قاضي التحقيق لصالح قاضي التحقيق بالقطب[1].

[1] – سلمى عبد النبي، نفس المرجع ص 26.

الخاتمـــــــــــــــــــــــــــــــــة

إن الجريمة محل الدراسة المسماة على صفحات هذه الأطروحة بالجرائم الالكترونية ما هي الا شكل من أشكال الجرائم المستحدثة وانعكاس مباشر لثورة تكنولوجيا المعلومات والإتصالات ، تثير هذه الجرائم عديد الاشكالات من الناحية الموضوعية والاجرائية كونها جرائم مستحدثة ومتجددة تختلف عن الجرائم التقليدية المنصوص عليها بقانون العقوبات، مما قد يؤدي الى افلات المجرمين من العقاب لعدم وجود نص قانوني يجرم الفعل المرتكب عملا بمبدأ الشرعية الذي ينص على أنه (لا جريمة ولا عقوبة ولا تدبير أمن إلا بقانون) لذا تبلورت فكرة وضع نصوص قانونية خاصة تكافح هذا النوع من الاجرام من اجل ذلك سعى المشرع الجزائري إلى اتخاذ الإجراءات والتدابير اللازمة لمواجهة هذه الجريمة .

وبعد تخصيص هذه الدراسة لاليات مكافحة الجرائم الالكترونية في التشريع الجزائري تم التوصل إلى جملة من النتائج وتقرير بعض التوصيات نعرضها كما يلي:

أولا –نتائج الدراسة:

يمكن إجمال نتائج الدراسة في النقاط التالية :

1/ تبنى المشرع الجزائري في الامر رقم 15/04 المعدل لقانون العقوبات التعريف الضيق للجريمة الالكترونية والقائم على معيار موضوع الجريمة وحصر مفهوم الجريمة في الاعتداءات الماسة بالأنظمة المعلوماتية، ولكنه لم يقدم تعريفا للمساس بأنظمة المعالجة الآلية للمعطيات، ولكن بصدور القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من جرائم تكنولوجيات الإعلام والاتصال وسع من مفهوم الجريمة الالكترونية واطلق عليها تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث عرفها في المادة 02 منه على أنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

2/ اختلف المشرع الجزائري في أسلوب المعالجة التشريعية للجرائم الالكترونية وكان ذلك من خلال التعديل في قانون العقوبات حيث تمم المشرع الجزائري قانون العقوبات الفصل الثالث من الباب الثاني من الكتاب بالقانون 04/15 المؤرخ في 10 نوفمبر 2015 بقسم سابع مكرر 01 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" احتوى على أهم الجرائم التي تستهدف الأنظمة المعلوماتية، كما استحدث قوانين خاصة تنص على هذه الجرائم من بينها : القانون المتعلق بالتامينات

الخاتمـــــــــــــــــــــــــــــــــــــــة

الاجتماعية،القانون المتعلق بحقوق المؤلف والحقوق المجاورة، القانون المتعلق بالتوقيع والتصديق الإلكترونيين، القانون المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وغيرها من النصوص المتفرقة المندرجة ضمن قوانين مختلفة تنص على أنواع من الجرائم الالكترونية والعقوبات المقررة لها .

3/ نص المشرع الجزائري على أحكام إجرائية خاصة بموجب القانون 22/06 المعدل لقانون الاجراءات الجزائية تندرج ضمنها مكافحة الجرائم الالكترونية تتمثل في إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب وقيد المشرع السلطات القضائية المختصة الإذن بها في حال إذا اقتضت ضرورات التحري والتحقيق في جرائم محددة على سبيل الحصر ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

4/ بصدور القانون 09 – 04 المتعلق بالقواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها أرسى المشرع بموجبه قواعد إجرائية جديدة وإستثنائية تتوافق وطبيعة الجرائم الالكترونية، ولها القدرة على التعامل مع الدليل الالكتروني الناجم عنها وتتمثل في اجراءات الاتصالات الإلكترونية وإجراءات تفتيش المنظومات المعلوماتية وحفظ المعطيات المتعلقة بحركة السير، وايضا إعتراض المعطيات المتعلقة بمحتوى الإتصالات.

5/ تضمن المرسوم الرئاسي رقم 06 – 348 المؤرخ في 05 أكتوبر 2006 تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ويعمل على حل مشكلة تنازع الإختصاص الجنائي الداخلي.

6/ تم انشاء ما يسمى بـــــــــــ القطب الجزائي المتخصص بموجب الامر 11/21 المعدل لقانون الاجراءات الجزائية يختص بنوع محدد من الجرائم وهي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والجرائم المرتبطة بها وهي الجرائم التي كانت سببا في استحداثه وتواجده ضمن نسيج التنظيم القضائي في الجزائر وهو اختصاص ممنوح له ضمن كافة مراحل الدعوى العمومية.

ثانيا/ التوصيـــــات

من خلال النتائج المتوصل اليها يمكن اقتراح جملة من التوصيات نوجز اهمها فيما يلي:

1/ يستحسن أن يسن المشرع قانون موحد لمكافحة الجرائم الالكترونية يشمل كافة النصوص الموضوعية والإجرائية ليكون هذا القانون بمثابة مرشد قانوني خاص بمكافحة هذه الجرىمة، مما ىسهل عمل السلطات القضائية فىما تثىره النصوص المتفرقة من صعوبة معرفة صدورها ومن إمكانية تناقضها في بعض الاحيان، كما يساعد كل الجهات المعنىة من طلبة ومحامىن وفقهاء قانونىىن وأساتذة جامعىىن من الإلمام بكل ما ىخص هذا النوع المستحدث من الجرائم.

2/ ضرورة إجراء دورات تكوينية متواصلة للشرطة والقضاة لغرض تحيين معارفهم ومواكبة التطورات التكنولوجية في مجال مكافحة الجرائم الالكترونية والإلمام بالتقنيات والأساليب المتطورة التي يستخدمها المجرمون .

3/ تشجيع البحوث والدراسات العلمية المتعلقة بالجرائم الإلكترونية بصفة عامة سواء ما تعلق منها بالجانب الموضوعي او الإجرائي واعتماد نتائج هذه الدراسات عند إصدار التشريعات الوطنية.

قائمة المصادر والمراجع

قائمة المراجع باللغة العربية

أولا / النصوص القانونية :

1/ الأمر رقم 156/66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم .

2/ الأمر رقم 155/66 المؤرخ في08 يونيو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

3/ امر رقم 03-05 مؤرخ في 19 يوليو سنة 2003يتعلق بحقوق المؤلف والحقوق المجاورة .

4/ القانون 01/08 المؤرخ في 23 يناير 2008 المتعلق بالتأمينات الاجتماعية .

5/ القانون رقم 15/ 04 المؤرخ في 10 فيفري2015 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكترونيين

6/ القانون رقم 04/18 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية.

7/ القانون 07/18 المؤرخ في 10 يونيو 2018 المتعلق ب حماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

8/ قانون عضوي رقم 14/23 المؤرخ في 27 غشت 2023 يتعلق بالاعلام .

ثانيا /المراسيـــم :

1/ المرسوم الرئاسي رقم 04 / 183 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام، الجريدة الرسمية رقم 41 المؤرخة في27 جوان 2004 ..

2/ المرسوم الرئاسي رقم 432/04 المؤرخ في 29 ديسمبر 2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية رقم 84 مؤرخة في 29 ديسمبر2004 .

قائمة المصادر والمراجع

ثانيا / الكتب والمؤلفات القانونية :

1/ محمد الفيومي، مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، المكتب الجامعي الحديث،الإسكندرية، مصر 1998 ص علي جعفر جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنـــــــــــــــة منشورات زين الحقوقيـــــــــــــــــــــــة، د ب ن 2013

2/ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعةالجديدة، الإسكندرية 2009

3/ أسامة أحمد المناعسة وجلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة – وفقا لقانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 ، ط 2، دار الثقافة للنشر والتوزيع، عمان .

4/ هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية – معلقا عليها – طبعة أولى دار النهضة العربية القاهرة، 2011 .

5/ أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندريـــــــــــــــــة 2015 .

6/ عبد الغني مصطفى و فاطمة بوجيري، مقدمة في الانترنت، مؤسسة لورد العالمية للشؤون الجامعية، البحرين 2006 .

7/ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، طبعة أولى، مطابع الشرطة، القاهـــــــرة 2009 .

8/ عبد الرحمان خلفي، الاجراءات الجزائية في التشريع الجزائري والمقارن، الطبعة الثانية، دار بلقيس، الجزائـــر 2016

9/ نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي، دار هومه، الجزائر 2013 .

10/ عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية – شبكة الأنترنت، شبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات – دراسة قانونية مقارنة – طبعة أولى، دار الثقافة للنشر والتوزيع 2011 .

قائمة المصادر والمراجع

11/ محمد أمين الشوابكة، جرائم الحاسوب و الأنترنت – الجريمة المعلوماتية – طبعة أولى، دار الثقافة للنشر والتوزيع 2007 .

12/ عامر محمود الكسواني، التجارة عبر الحاسوب، دار الثقافة للنشر والتوزيع، الأردن 2008 .

13/ حنان ريحان مبارك المضحكي، الجرائم المعلوماتية – دراسة مقارنة – طبعة أولى، منشورات الحلبـــــــــــــي الحقوقية 2014 .

14/ طارق عفيفي صادق أحمد، طارق عفيفي صادق أحمد، الجرائم الإلكترونية – جرائم الهاتف المحمول – دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، المركز القومي للإصدارات القانونية، القاهرة 2011 .

15/ سعد جاد الله حيدر، النظام القانوني لعقد الإتصالات الحديثة " الهاتف النقال " دار الكتب القانونية، 2012 .

16/ هالة محمد عنبة، دليل تطبيقات الحاسب والأنترنت والهاتف الجوال في الإدارة والتسويق، المنظمة العربية للتنمية الإدارية 2009 .

ثالثا/ المقـــالات :

1/ سلمى عبد النبي، دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في مواجهة المعطيات الواقعة على المعطيات المعلوماتية، مقال منشور في مجلة الحقوق والعلوم السياسية، جامعة باتنة، المجلد 11 عدد 02 لسنة 2024 .

2/ عبد المحسن بدوي محمد أحمد، الجرائم المعلوماتية، مقال منشور ضمن مجلة الأمن و الحياة عدد 335 ، جامعة نايف العربية للعلوم الأمنية، الرياض1431 .

3/ زيوش عبد الرؤوف وزغيشي مصطفى، الجرائم الالكترونية الاقتصادية–المفهوم والدوافع–مقال منشور في مجلة الدراسات القانونية والاقتصادية، عدد01، مجلد07 ، سنة 2024 .

4/ سمير شعبان، الجريمة الالكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم مقال منشور في مجلة دراسات وابحاث، المجلة العربية للأبحاث فى العلوم الإنسانية والإجتماعية ، عدد 01 سنة 2019.

5/ حابت امال،الجريمة المعلوماتية في التشريع الجزائري بين قانوني 15/04 و 04/09 مقال منشور في مجلة هيرودوت للعلوم الانسانية والاجتماعية مجلد 07، عدد 25، لسنة 2003.

قائمة المصادر والمراجع

6/ نعيمة داودي، الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها) مقال منشور في مجلة مهد اللغات مجلد 02، عدد01 لسنة 2020 .

7/ بعجي عبد النور، الإرهاب الالكتروني، بين عولمة الجريمة وضرورة المكافحة، مقال منشور في مجلة الدراسات والبحوث القانونية ، المجلد 07، العدد 02 سنة 2022 .

8/ صابرين يوسف عبد الله، دور الأدلة المرئية في الإثبات الجنائي، مقال منشور في مجلة كلية الحقوق جامعة النهرين المجلد 19، العدد 2، 2017 .

9/ اجعود سعاد، الحماية الجزائية لتكنولوجيا الاعلام والاتصال في التشريع الجزائري – دراسة على ضوء النصوص المستحدثة "– مقال منشور في مجلة الرسالة للبحوث الانسانية، مجلد 07، العدد 04 لسنة 2022 .

10/ بطيحي نسمة، جريمة الدخول او البقاء غير المشروع ، مقال منشور في مجلة الفقه القانوني والسياسي، جامعة ابن خلدون تيارت، المجلد 01 ، العدد 01 .

11/ فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مقال منشور في مجلة العلوم الانسانية، عدد 33، جوان 2010.

12/ شول بن شهرة و بن بادة عبد الحليم، الآليات القانونية والمؤسساتية للوقاية من الفساد ومكافحته مقال منشور في مجلة جيل للأبحاث القانونية المعمقة، العدد 8، نوفمبر 2016

13/ رابح وهيبـــــــــــــة، التسرب في التشريع الإجرائي الجزائري، مقال منشور ضمن مجلة جامعة القدس المفتوحة للأبحاث والدراسات العلىا، جامعة القدس المفتوحة، العدد السادس والثلاثون، الجزء الأول، فلسطين 2015 .

14 / وداعي عز الدين، التسرب كأسلوب من أساليب البحث و التحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، مقال منشور في المجلة الأكاديمية للبحث القانوني، مجلد 16 عدد 02، 2017 .

15/ نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مقال منشور في مجلة الأندلس للعلوم الإنسانية والاجتماعية، المجلد 15، العدد 15، أفريل 2018 .

16/ خرشي امال، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، مقال منشور في مجلة الابحاث القانونية والسياسية، المجلد 04، عدد 01 لسنة 2022 .

قائمة المصادر والمراجع

رابعا/ الملتقيات

1/ مصطفاوي عبد القادر، الشرطة الوطنية ومكافحة الجريمة المعلوماتية، بحث مقدم الى فعاليات الملتقى الدولي حول محاربة الجريمة المعلوماتية ، مركز البحوث القانونية والقضائية، الجزائر من 5 الى 6 ماي 2010.

خامسا/ اطروحات الدكتوراه

وردة شرف الدين، الإثبات الجنائـــــــــــي بالأدلة الالكترونية – دراسة مقارنة – أطروحة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة بسكرة 2016 / 2017 .

علالـــــــي أمينة، مكافحة الجرائم العابرة للحدود المرتكبة بتقنية المعلومات، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة عنابة 2019 .

[1]– نادية سلامي، اليات مكافجة التجسس الالكتروني، اطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الجنائي جامعة العربي التبسي – تبسة 2019/2018 .

سادسا/ مذكرات الماجستير

1/ رصاص فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شهادة ماجستير في القانون العام جامعة أبي بكر بلقايد – كلية الحقوق والعلوم السياسية، تلمسان 2012/2011 .

2/ سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011/2010 .

سابعا / المواقع الالكترونية

1/ مقال بعنوان : ماهي الكاميرا الرقمية وماهي أنواعها ؟ منشور على الموقع الالكتروني التالي http://Lightfragrance.wordpress.com

2/ يونس عرب، جرائم الكمبيوتر والإنترنت– المعنى والخصائص والصور واستراتيجية المواجهة القانونية– انظر الموقع الالكتروني http://www.abhatoo.net.ma

3 / شبكات الند للند، مقال منشور على الموقع الإلكتروني:www.bossla.com

4/ بن دراح علي ابراهيم، محاضرات في الجرائم المعلوماتية مقدمة لطلبة السنة الثانية ماستر– تخصص قانون جنائي وعلوم جنائية– المركز الجامعي بأفلو 2021/2020 منشورة على الموقع الالكتروني :

قائمة المصادر والمراجع

https://www.cu-aflou.dz › DocPdf › publications

ثامنا/ المعاجم والقواميس

1/ المعجم الوسيط، مجمع اللغة العربية، مكتبة الشروق الدولية 2004 ص 171، نسخة إلكترونية متوفـــــــرة علـــــــــــــــــى موقع المكتبة الوقفية للكتب المصورة www.waqfeya.comتاريخ الزيارة 2025/01/06 ساعة الزيارة 13.41

2/ معجم المعاني الجامع، متوفر على العنوان الإلكتروني www.almaany.com

المراجع باللغة الأجنبية

/1 chawki wahab and mouhamed wahab ، echnology Is a Double-Edged Sword: Illegal Human Trafficking in the Information Age p19.web sit:www.DROIT-TIC.fr

ملخص:

في ظل التحول الرقمي المتسارع، أفرز الواقع المعاصر نمطًا جديدًا من الجرائم يُعرف بالجرائم الإلكترونيـــة، وهـــي أفعال غير مشروعة تُرتكب عبر الوسائط التكنولوجية ووسائل الاتصال الحديثة. وقد أضحى هذا النوع مـــن الجـــرائم يشكل تحديًا حقيقيًا أمام المنظومات القانونية، نظرًا لطبيعته غير التقليدية وصعوبة تتبعه أو تحديد مرتكبيه بدقة. وإزاء هذه التهديدات، برزت الحاجة الماسة إلى تطوير ترسانة قانونية مرنة وفعالة تُواكب هذا التطور التكنولوجي، وتُحـــدد المسؤوليات، وتُعزز آليات الوقاية والزجر.

وفي هذا السياق، سعت الجزائر إلى مجاراة هذا التحول من خلال إصدار القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تضمن هذا النص القانوني أحكامًا مهمة تتعلق بتجريم الأفعال الإلكترونية، وضوابط التحري والتحقيق، وآليات التعاون بـــين السلطات المختصة.

وتأتي هذه الدراسة في إطار محاولة تحليل الإطار القانوني المنظم للجرائم الإلكترونية، مع التركيز على خصوصياتها القانونية وإشكالات إثباتها وملاحقة مرتكبيها في بيئة افتراضية عابرة للحدود.

Abstract:

In light of the accelerating digital transformation, contemporary reality has given rise to a new type of crime known as cybercrime, which is an illegal act committed through modern technological media and communication tools. This type of crime has become a real challenge for legal systems, given its unconventional nature and the difficulty of tracking and accurately identifying perpetrators. In the face of these threats, there is an urgent need to develop a flexible and effective legal framework that keeps pace with this technological development, defines responsibilities, and strengthens prevention and retribution mechanisms.

In this context, Algeria sought to keep pace with this transformation by issuing Law No. 09-04 of August 5, 2009, concerning the special rules for preventing and combating crimes related to information and communication technologies. This legal text includes important provisions related to the criminalization of electronic acts, controls for investigation, and mechanisms for cooperation between competent authorities.

This study attempts to analyze the legal framework governing cybercrime, focusing on its legal specificities and the challenges of proving and prosecuting perpetrators in a virtual, cross-border environment.