جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

خصوصية تتبع في الجريمة المعلوماتية

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: إدارة إلكترونية

من إعداد الطالب:

- بروكش هشام

تحت إشراف الأستاذ:

-نقادي حفيظ

أعضاء لجنة المناقشة

الدكتور اللقب والاسم	**الرتبة العلمية**	**جامعة الانتماء**	**رئيساً**
الدكتور اللقب والاسم	**الرتبة العلمية**	**جامعة الانتماء**	**مشرفاً ومقرراً**
الدكتور اللقب والاسم	**الرتبة العلمية**	**جامعة الانتماء**	**عضواً**

السنة الجامعية: 2024-2025

بسم الله الرحمان الرحيم

إهـــــداء

ماسلكناالبداياتإلابتسييرهومابلغناالنهاياتإلابتوفيقهوماحققناالغايةإلبفضلهفالحمدللهالذيوفقنيلتث

مينهذهالخطوةفيمسيرتيالدراسية.

اهديتخرجيإلىنفسيالطموحةجداالتيلمتخذلني

والىمنكاندعاؤهاسرنجاحيوحنانها" أميالغالية"والىمناحملاسمهبكلفخر "والدي"،

والىمنساندنيفيجميعالأوقاتداعملحظاتفرحيوالأصدقائيالذيلميتسعالمقاملذكرهم.

والى أستاذي الفاضل "نقادي حفيظ" الذي كان مشرفا في انجاز هذه المذكرة وكان معي في كل

كبيرة وصغيرة بخصوص هذا الموضوع.

شكر و تقدير

اتقدمبخالصالشكروعظيمالامتنانلكلمنساعدنافيإنجازهذاالعملالمتواضع،

وفيمقدمتهمالأستاذ الفاضل " نقادي حفيظ"الذي لميبخلعلينابتوجيهاتهونصائحهالقيّمة، وكان

له الفضل الكبير في انجاز موضوع المذكرة منذ بدايته إلى غاية نهايته،

كما نشكر الأساتذة أعضاء لجنة المناقشة الكرام رئيسا و عضوا على قبول مناقشتهم

لهذه المذكرة.

الملخص

تطرح الجريمة المعلوماتية العديد من المشاكل من ناحية القانون الإجرائي، إذ يصعب على المحققين إجراء تحقيق وجمع الأدلة الرقمية، بإتباع الإجراءات التقليدية للتحقيق: كالمعاينة، التفتيش، الضبط، ... الخ,في هذا السياق ورغبة منها في مكافحة فعالة للجريمة المعلوماتية، تبنت الجزائر أساليب جديدة للتحري، من خلال: تعديل قانون العقوبات بموجب القانون رقم 22-06 بتاريخ 20 ديسمبر 2006 عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات. وفي 2009 أصدر المشرع الجزائري القانون رقم 04-09 المؤرخ في 05 أوت سنة ،2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلاموالاتصال ومكافحتها، في هذا القانون خلق المشرع آليات جديدة خاصة للتحر ي من أجل مكافحة الجريمة المعلوماتية، إلا أن هذه الأساليب الحديثة للتحري أثارت مشكلة مدى مشروعيتها، خاصة وأنها تمس بالحقوق والحريات الأساسية للفرد والمعترف بها في الاتفاقيات الدولية، ولحل هذا الإشكال فقد وضعت شروط وضمانات يقتضي على السلطات القضائية مراعاتها عند الإذن بهذه الأساليب

Résumé:

La cybercriminalité pose de nombreux problèmes juridiques au niveau du droit processuel, car il est Difficile pour les enquêteurs de mener une enquête et la collecte de preuves numériques, conformément aux procédures traditionnelles enquête: constatations matérielles, perquisitions, saisies,etc. Dans ce contexte et animé par le souci de lutte contre la cybercriminalité, l'Algérie a adaptées des nouvelles méthodes d'investigation. Cela se traduit par : La modification du code de procédure pénale par la loi N ° 06-22 du 20 Décembre 2006 en ajutant des Novelles dispositions qui s'appliquent sur les infractions relatives aux atteintes aux systèmes de traitement automatisés de données .Et en 2009 le législateur Algérien a promulgué la loi N° 09- 04 du 05 Aout 2009 contenant les règles particulières relatives à la préventions et à la lutte contre les infractions liées au technologies de l'information et de la communication, dans cette loi le législateur a crée des novelles procédures spécifiques d'investigation pour lutter contre la cybercriminalité.

Cependant, ces méthodes modernes d'investigation soulèvent la problématique de leur légitimation surtout parce qu'elles affectent les droits et libertés fondamentaux de l'individu reconnus à l'échelle des conventions internationales .Et dans le but de résoudre cette confusion, des conditions des garanties on été imposées aux autorités judiciaires lors de l'autorisation de ces méthodes.

مـــقدمـــة

شهد العالم تطوراً مذهلاً في مجالات التكنولوجيا والاتصالات وتقنية المعلومات، حتى أصبحت مقولة "العالم قرية صغيرة "توشك على أن تكون حقيقة واقعة في أغلب الأحيان .هذه الثورة التقنية أبرزت نفسها بشكل كبير من خلال التقدم الهائل في مجال الحواسيب الآلية ومكوناتها، إلى جانب البرمجيات المتطورة المرتبطة بها .ولم يعد الاعتماد على هذه التكنولوجيا مقتصراً على الهيئات الرسمية فحسب، بل أصبح واضحاً في مختلف جوانب الحياة العامة والخاصة، لدرجة أن العنصر البشري نفسه بدأ يشتكي من استبدال الأجهزة الذكية، مثل الحواسيب والبرامج، بمجهوده البشري. وبلغ الأمر ذروته مع دخول الذكاء الاصطناعي حيز الاستخدام كبديلٍ للذكاء البشري، على الرغم من أن هذه التكنولوجيا نتاجٌ إنسانيٌّ بحت .باتت الدول تُقاس بمستوى تقدمها التكنولوجيا وقدرتها على امتلاك واستخدام التقنيات الحديثة في مختلف المجالات. ومع كل ما جلبته هذه الثورة التقنية من فوائد للبشرية، كان لها جانب مظلم أيضاً: الاستخدام غير القانوني لهذه التكنولوجيا .أصبحت التقنية الحديثة أداة هدم في أيدي الخارجين عن القانون، الذين يمارسون ما يُعرف بـ"الجريمة الناعمة"، وهي الجرائم التي لا تُراق فيها الدماء ولكنها تترك آثاراً عميقة وخطيرة. والأخطر أن هذه الجرائم تتميز بكونها عابرة للحدود، مما يتيح لمرتكبيها الهروب بسهولة من العقاب .إذ تُرتكب العديد من تلك الجرائم عبر شبكات الإنترنت، من مواقع بعيدة يصعب تتبعها .في الآونة الأخيرة، برزت ظاهرة جديدة تستدعي اهتماماً بالغاً وهي" الإجرام السيبراني "أو الجرائم المعلوماتية التي تنفذ عبر التكنولوجيا .هذا النوع من الجرائم ليس مجرد اختراق للمجتمع لكنه يشكل تهديداً حقيقياً لاستقراره وأمانه. وقد دفع ما يُمثّله هذا النوع من الجرائم من خطورة بالمشرّع الجزائري إلى التحرك، حيث تم سن تشريعات تواكب الممارسات الإجرامية المستحدثة .تضمنت هذه التشريعات نصوصاً واضحة تعاقب الجناة، كما جرى إفراد شرح موسع لها لتوضيح أركان الجريمة والظروف التي تُقام فيها، سعياً لضمان تطبيق العدالة بفعالية أكبر.

مشكلة الدراسة تكمن في التحولات الهائلة التي فرضها التطور التكنولوجي السريع والزيادة الملحوظة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، سواء كانوا أفرادًا طبيعيين أو جهات وكيانات معنوية .هذه التحولات أدت إلى ظهور نوع جديد من الجرائم المرتبطة بالتكنولوجيا، تعرف بجرائم المعلوماتية .ومع الارتفاع الملحوظ في معدلات ارتكاب هذا النوع من الجرائم مؤخرًا، بات لذلك أثر واضح على الأنظمة والقوانين، حيث أصبحت تستوجب التكيف مع طبيعة هذه الجرائم وتداعياتها وآثارها .من هنا، برزت الحاجة الماسة لتناول هذا الموضوع بالدراسة والتحليل من أجل تسليط الضوء على مفهوم الجريمة المعلوماتية، وتحديد الأسس التي تُقام عليها المسؤولية الجنائية لمرتكبيها ضمن التشريع الجزائري .وبناء على ذلك، تنبع الإشكالية المركزية للدراسة:

ما هي الآليات والإجراءات المتبعة للكشف عن الجرائم المعلوماتية في التشريع الجزائري؟ تنبثق عن هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية التي تسعى إلى تحديد المحاور الأساسية للبحث وتؤطر إجاباته بهدف تحقيق فهم أعمق للموضوع. وتتمثل هذه التساؤلات فيما يلي:

- ما المقصود بالجريمة المعلوماتية؟
-هل تمتلك الجريمة المعلوماتية أنواعًا وأهدافًا محددة؟
-ما هي الأركان التي تقوم عليها الجريمة المعلوماتية؟
-هل توجد آليات مؤسساتية مختصة للكشف عن الجرائم المعلوماتية؟
-ما هي الإجراءات المتبعة أثناء التحقيق في الجرائم المعلوماتية؟

فرضيات البحث:

- الجريمة المعلوماتية أحد صور الجرائم التقليدية.
-للجريمة المعلوماتية أنواع و أهداف.
- للجريمة المعلوماتية نفس الأركان الجريمة التقليدية.
- للجريمة المعلوماتية هيئات و آليات قانونية للكشف عنها في التشريع الجزائري

أسباب اختيار الموضوع:

من الأسباب التي دفعتني إلى اختيار هذا الموضوع وأولته اهتماماً خاصاً هو تفاقم وانتشار الظاهرة المقلقة المعروفة باسم الجرائم المعلوماتية، والتي أضحت واحدة من أبرز التهديدات على المستوى العالمي .هذه الجرائم لا تقتصر على مجرد انتهاك الخصوصية أو اختراق البيانات، بل تمتد تأثيراتها لتلحق أضراراً فادحة باقتصادات الدول، مما يفرض الحاجة الملحة إلى إنشاء أجهزة متخصصة ذات كفاءة عالية للإشراف على التصدي لهذا النوع من الجرائم، بالإضافة إلى تطوير آليات دقيقة ومُحكمة للتحقيق فيها.

كما أن موضوع الجريمة المعلوماتية، وبالرغم من أهميته الكبيرة في مجالات البحث والدراسة القانونية والتقنية، لم يلقَ حتى الآن الاهتمام البحثي الكافي. فقد عولج في دراسات كثيرة بشكل سطحي دون الدخول في العمق اللازم، وغالباً ما صُنِّف ضمن طائفة الجرائم التقليدية الأخرى دون إبراز خصوصيته وتعقيداته .من هنا تبرز الضرورة الملحة لتقديم دراسة شاملة ومتكاملة حول هذا الموضوع، سواء لمساعدة المختصين الأكاديميين على فهم أبعاده المختلفة أو لمساندة الجهات العملية التي تُعنى بتطبيق النصوص القانونية المتعلقة بالجرائم الموجهة ضد الأنظمة المعلوماتية في الميدان العملي.

- علاوة على ذلك، فإن أحد الأهداف الأساسية لدراستي هو السعي لتقديم مقاربة جديدة تجمع بين الجانبين النظري والتطبيقي لهذا الموضوع. ذلك أن معظم الدراسات السابقة اقتصرت على أحد هذين الجانبين دون محاولة الدمج بينهما، مما يُبرز حاجة فعلية لإيجاد حلول مبتكرة تجمع بين التحليل الأكاديمي والبُعد العملي لضمان معالجة شاملة ومتكاملة لهذا الملف الحيوي.

أهداف الدراسة

- تهدف الدراسة إلى التعرف ودراسة العديد من النقاط وهي
- التعرف على الجريمة المعلوماتية.

- التعرف على أهداف ارتكاب الجريمة المعلوماتية
- دراسة أركان الجريمة المعلوماتية في التشريع الجزائري
- التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية
- التعرف على إجراءات التحقيق للكشف عن الجريمة المعلوماتية.

أولاً :الأهمية العلمية

تبرز الأهمية العلمية لهذه الدراسة في تسليط الضوء على المسؤولية الجنائية لمرتكبي جرائم المعلوماتية ضمن نطاق التشريع الجزائري .يأتي هذا بالتزامن مع انتشار هذه الجريمة التي باتت تشكل خطرًا كبيرًا على الأفراد والمجتمع .من هنا، جاءت فكرة القيام بدراسة معمقة حول مسؤولية مرتكبي هذا النوع من الجرائم .ومن المأمول أن تسهم هذه الدراسة في تقديم نواة معرفية يستند إليها الباحثون ورجال القانون والمختصون في المجال القانوني لتحليل ومواجهة هذه الظاهرة.

ثانيًا: الأهمية العملية

تكمن الأهمية العملية لهذه الدراسة في تعزيز فهم ما يترتب على هذه الجرائم الحديثة من مخاطر والعمل على الحد منها داخل المجتمع .كما تهدف إلى التقليل من آثارها من خلال رفع مستوى الوعي بين مستخدمي الأجهزة الإلكترونية الحديثة بمخاطر تلك الجرائم، وتشجيعهم على تبني الحذر والحيطة أثناء الاستخدام اليومي.

حدود الدراسة

تشمل الجوانب التالية :

أولاً: الحدود الموضوعية:

تهدف الدراسة إلى تناول الموضوع من منظور قانوني علمي متكامل يركز على تحليل الجرائم المعلوماتية، مع تسليط الضوء على طبيعة المسؤولية الجنائية التي تنشأ في مواجهة هذا النوع من الجرائم الحديثة. يتم التطرق أيضاً إلى دراسة معمقة للتشريع الجزائري بوصفه إطاراً قانونياً لمحاربة الجريمة المعلوماتية بشكل خاص. لتحقيق هذا الهدف، تستعرض الدراسة بأسلوب منهجي ماهية

الجريمة المعلوماتية، من حيث تعريفها وطبيعتها القانونية، وتصنيف أنواعها المختلفة لتفصيل أنماطها الجمعية والفردية. إضافة إلى ذلك، يتم تحليل الأركان القانونية التي تقوم عليها هذه الجريمة، سواء كانت أركان مادية أو معنوية أو متصلة بوسائل ارتكابها .

وأخيراً، تركز الدراسة على العقوبات التي جاءت بها التشريعات لمواجهة الجرائم

منهج الدراسة:

اعتمد الباحث في إطار هذه الدراسة على المنهج الوصفي التحليلي، الذي يشكل قاعدة أساسية لتحديد خصائص المشكلة موضوع البحث بشكل دقيق. وقد تم التركيز خلال هذا المنهج على وصف طبيعة المشكلة وجوهرها وأسبابها العميقة، بالإضافة إلى تحليل مكوناتها والتعمق في فهم أنواعها المختلفة وأهدافها الأساسية. يهدف هذا النهج إلى استيعاب الجوانب المتعددة المرتبطة بالمسؤولية الجنائية عن الجرائم المعلوماتية في ظل التشريع الجزائري. وبفضل اعتماد هذا المنهج، تمكن الباحث من الوصول إلى مجموعة من النتائج المستندة إلى عملية تحليلية دقيقة وشاملة قدمت نظرة متكاملة حول الموضوع.

الدراسات السابقة :

●رسالة ماجستير: "اليات مكافحة جرائم تكنولوجيات الاعلام والاتصال على ضوء قانون 09/04 "بجامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق، أحمد مسعود مريم سنة 2013/2012تناول فيها الباحث الجرائم المتصلة بالتكنولوجيات العالم والاتصالو آليات مكافحتها التي جاء بها القانون .09/04

●رسالة ماجستير: "الاطار لقانوني لمكافحة الجريمة المعلوماتية في التشريع الجزائري والتشريع المقارن" جامعة باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق، عبد اللطيف معتوق، سنة ،2011/2013تناول في الباحث نظرة المشرع الجزائري ومقارنته بموقف التشريع الفرنسي والتشريعات العربية وتناول التعاون الدو لي في مجال مكافحة الجريمة المعلوماتية.

لإجابة على الإشكالية الرئيسية للموضوع وما يتفرع عنها من إشكالات فرعية، تم تقسيم الدراسة إلى: مقدمة، فصلين، وخاتمة

في الفصل الأول، جرى التركيز على دراسة كافة الجوانب المتعلقة بالجريمة المعلوماتية من خلال مبحثين .تناولنا في المبحث الأول ماهية الجريمة المعلوماتية، بما يشمل تعريفها، أنواعها، وطبيعتها القانونية .أما في المبحث الثاني، فقد تمت دراسة الحماية الجنائية للجريمة المعلوماتية بالاعتماد على النصوص القانونية المختلفة .

وفيما يتعلق بالفصل الثاني، تم تخصيصه لبحث الإجراءات التحقيقية المتعلقة بالجريمة المعلوماتية، وذلك عبر مبحثين .تناول المبحث الأول الآليات والوحدات المختصة بمكافحة الجرائم المعلوماتية، بينما ركز المبحث الثاني على إجراءات التحقيق للكشف عن هذه الجرائم

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية

تمهيد:

تُمثل الجرائم الإلكترونية أحد أهم التحديات التي تواجهنا في مجتمعنا اليوم، بل وربما أشدها وطأة. لمناقشة هذه التحديات بفعالية، لا بد من تقديم لمحة عامة تُعرّف طبيعة الجرائم الإلكترونية. بعد ذلك، يجب علينا دراسة آثار المسؤولية الجنائية المترتبة على هذه الأنشطة، مما يستلزم دراسةً متعمقة لتعريف الجرائم الإلكترونية وأنواعها المختلفة أهدافها في المبحث الأول قبل التعرض إلى بحث إشكاليات المسؤولية الجنائية وتحدي المعلوماتية للقواعد العامة للمسؤولية الجنائية في المبحث الثاني.

المبحث الأول: ماهية الجريمة المعلوماتية

سوف نتطرق في هذا المبحث إلى مفهوم أنواع وأهداف الجريمة المعلوماتية (المطلبلأول)، و تحديد طبيعتها القانونية وخصائصها وأركانها (المطلب الثاني)

المطلب الأول: مفهوم، أنواع، أهداف الجريمة المعلوماتية

هناك العديد من التعريفات المختلفة للجرائم الإلكترونية، منها الضيقة ومنها الواسعة. وقد أدى ذلك إلى عدم وجود توافق في الآراء بشأن ظاهرة الجرائم الإلكترونية وإيجاد الحلول المناسبة لها.

الفرع الأول: تعريف الجريمة المعلوماتية

مع دخول أجهزة الكمبيوتر والإنترنت إلى كل جانب من جوانب مجتمعنا وحياتنا، بدأ ظهور نوع جديد من الجرائم يسمى الجرائم الإلكترونية. ومن ثم هناك حاجة إلى تعريف هذه الجرائم والتوعية بها. وسنقوم بتعريفها قانونيا وفقهيا.

أولا: التعريف الفقهي

وقد قدم الفقهاء والعلماء تعريفات عديدة تختلف باختلاف المكان الذي تنتمي إليه في العالم ومعايير التعريف نفسها. لقد حاولنا جمع معظم التعاريف المقترحة في هذا المجال. وفي التعريف المبني على موضوع الجريمة أو أحيانا على نمط السلوك الإجرامي يعرفها البروفيسور روزنبارت بأنها أنشطة غير مشروعة تهدف إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في جهاز كمبيوتر أو المنقولة من خلاله، أو كما يعرفها الفقيه سولا لوز، فهي أي نوع من الجرائم المعروفة في القانون الجنائي طالما أنها تتعلق بتكنولوجيا المعلومات. ويستند أنصار التعريف المبني على الوسائل الإجرامية في قرارهم على حقيقة مفادها أن الجريمة الإلكترونية هي استخدام أجهزة الكمبيوتر كوسيلة لارتكاب الجرائم. وتشمل هذه التعريفات ما يلي:تعريف البروفيسور جون فورستر: "السلوك الإجرامي الذي يستخدم الكمبيوتر كأداة أساسية".[1] يعرفها تادمان بأنها جميع أشكال

[1]هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 120

السلوك غير القانوني التي يتم تنفيذها باستخدام أجهزة الكمبيوتر. ونلاحظ أيضًا أن بعض القوانين والمؤسسات ذات العالقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث تبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها .كما عرفها الأستاذ" دافيد تومسن "أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي[1].

ثانيا: التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة -02الفقرة – أ -من القانون رقم 09-04المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالقول بأن " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية

"إذن وعمال بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب "المتعلقة بالجريمة هذه فنعر فها بأنها " كل السلوكيات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محال لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية."

[1] هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة ،2000، ص20

الفرع الثاني: أنواع و أهداف الجريمة المعلوماتية

أولا: أنواع الجريمة المعلوماتية

1- الجرائم التي تقع على الأشخاص: هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات

الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سالمة الجسم وفي الحرية والحق في صيانة الشرف.

2-الجريمة انتحال الشخصية:وهي جريمة قديمة جدًا تتخذ شكل العديد من الجرائم المرتكبة بالطرق التقليدية. لكن مع انتشار الإنترنت، اتخذ هذا النوع من الجرائم أشكالاً جديدة، وهي انتحال شخصية الأفراد على الشبكات الإلكترونية واستغلالها بأبشع الطرق، وسرقة البيانات الشخصية مثل العناوين وتواريخ الميلاد وأرقام الضمان الاجتماعي وغيرها، للحصول على بطاقات الائتمان وغيرها. وبهذه المعلومات، يستطيع المجرمون إخفاء هوياتهم الحقيقية والتحرك بحرية تحت أسماء مستعارة. في كثير من الأحيان يحصل المحتالون على هذه المعلومات من خلال العديد من الإعلانات على الإنترنت.

3-جريمة التحرش والملاحقة: وهي نوع جديد من الجرائم يتزايد مع كل إضافة وتحديث لبرامج الدردشة والتبادل، وهي مساحات معروفة في الفضاء الإلكتروني تسمح للمستخدمين بالتحدث مع بعضهم البعضوتشمل جرائم الملاحقة رسائل التهديد والترهيب والمضايقة , وشبه القضاة هذا السلوك الإجرامي خارج الإنترنت بالجرائم التي تهدد العامة. لا تتطلب الجريمة الإلكترونية أي

اتصال جسدي بين المجرم والضحية، مما يوحي بأنها قد يكون لها تأثير نفسي سلبي حيث أنها لا تنتج أي عنف جسدي. [1]

4- جريمة الخداع والإغراء: وهي من أشهر الجرائم الإلكترونية وأكثرها انتشاراً، خاصة بين الشباب ومستخدمي الإنترنت. ويعتمد هذا النوع من الجرائم على عامل الألفة حيث يخدع المجرمون الضحايا على أمل إقامة علاقات صداقة أو زواج عبر الإنترنت وقد تتطور الجريمة الإلكترونية إلى لقاء فعلي بين الطرفين. إن هذه الجرائم لا تعرف حدوداً، ولا يمكن تقييدها، ولا تحدها حدود سياسية واجتماعية. يمكن لأي شخص يتواصل عبر الإنترنت أن يرتكب هذه الجرائم بسهولة، وأي مستخدم ذو نوايا حسنة قد يصبح ضحية[2]

5-التشهير والقذف: مع انتشار الشائعات والأخبار الكاذبة، والتي تمتد وتؤثر على رموز الناس سواء كانت فكرية أو سياسية أو حتى دينية، ظهرت بعض المواقع الإلكترونية على شبكة الإنترنت لغرض واحد فقط، وهو خدمة هذه الشائعات والأخبار الكاذبة، بهدف التشهير بهذه الرموز وتشويه سمعتها، وتسميم عقول الناس أو محاولة ابتزاز أشخاص معينين من خلال نشر الشائعات. وأبرز وسائل ارتكاب هذا النوع من الجرائم هو إنشاء موقع على شبكة الإنترنت يحتوي على المعلومات المطلوب إدراجها أو نشرها أو إرسالها من خلال الموقع. على سبيل المثال، إرسال صور غير مناسبة أو معلومات غير صحيحة[3].

6-الجرائم المخلة بالأخلاق والآداب العامة : تُصنَّف ضمن التحديات البارزة لعصر الإنترنت، الذي يتميّز بطابعه العالمي وعدم انحصاره بمستخدم أو دولة معينة. بعض المواد التي تُعتبر غير

---

[1] منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 42 43.

[2] عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د .الطاهر موالي، سعيدة ، سنة 2015/2016، ص . 19

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص .3

أخلاقية أو مخالفة للآداب في بلد ما قد تُعد جرائم تستوجب العقاب القانوني هناك، بينما لا تُعتبر كذلك في بلدان أخرى .وتشمل هذه الجرائم أفعالًا كتحريض القاصرين على القيام بأنشطة جنسية غير مشروعة أو استغلالهم عبر الوسائل الإلكترونية، ومحاولة إغوائهم للانخراط في تلك الأنشطة، أو نشر معلومات عنهم باستخدام الحاسب الآلي بهدف دعوتهم إلى ارتكاب سلوكيات فاحشة .كما تمتد هذه الجرائم لتشمل تصوير القاصرين ضمن محتوى جنسي غير قانوني، مما يجعلها تهديدًا كبيرًا للمجتمع والأخلاق العامة[1].

ب/ الجرائم التي تقع على الأموال: تُعد الجرائم التي تقع على الأموال أحد أشكال الجرائم التي تستهدف الاعتداء على الممتلكات والحقوق المالية ذات القيمة المادية، وتشمل أيضاً الحقوق ذات الطابع الاقتصادي .وفي سياق هذا النوع من الجرائم، إذا كان الاعتداء موجّهاً نحو الأموال الملموسة المرتبطة بالحاسب الآلي، كالأجهزة نفسها أو الأسلاك والملحقات المتصلة بها، فإن تطبيق القوانين الجزائية التقليدية لا يواجه أي صعوبة تُذكر نظرًا لأن هذه العناصر تندرج ضمن تعريف "الأموال المنقولة العادية ."أما في الحالة التي يتم فيها الاعتداء على ما يرتبط بفن الحاسب الآلي من برمجيات أو أنظمة تشغيل، فإن النصوص التشريعية والقوانين السائدة تصبح عاجزة عن توفير الحماية الكافية. ويرجع ذلك إلى الطبيعة الخاصة وغير التقليدية لهذا النوع من الممتلكات الرقمية، حيث تمتاز البرمجيات والنظم بطابع مميز يتطلب وضع تشريعات حديثة تتلاءم مع خصوصيتها وتعالج قصور القوانين التقليدية في التصدي للاعتداءات عليها[2].

1- .جرائم صناعة ونشر الفيروسات: الفيروس يُعتبر نوعًا من البرامج مثل غيره من البرامج الموجودة على جهاز الحاسوب، لكنه مصمم خصيصًا بحيث يتمكن من التأثير على بقية البرامج

[1] انظر محمد أمين احمد الشوابكة، المرجع أعلاه، ص .114

[2] انظر محمد أمين احمد الشوابكة، المرجع السابق، ص .136

المثبتة على الجهاز .قد يقوم الفيروس بتحويل تلك البرامج إلى نُسخ منه أو يعمل على حذفها تمامًا، مما يؤدي إلى تعطيلها ومنعها من أداء وظيفتها[1].

2جرائم الاختراقات:الاختراق يشير إلى عملية الوصول غير المصرح به إلى أجهزة الحاسوب أو الشبكات الإلكترونية التابعة للآخرين، وذلك باستخدام برمجيات متقدمة تمكّن الأفراد ذوي الخبرة والمهارة من تجاوز التدابير والإجراءات الأمنية المصممة لحماية هذه الأنظمة .تتنوع دوافع وأهداف الاختراق استنادًا إلى الغاية التي يسعى إليها المخترق، حيث يقوم البعض بالتسلل إلى الأجهزة لغرض تحقيق أهداف محددة تختلف بحسب الظروف

المخترقون على اقتحام أجهزة الحواسيب أو مواقع الإنترنت لأسباب متعددة، منها بدافع الفضول، ومنها بغرض السرقة يعتبر الدافع الأبرز هو سرقة المعلومات القيمة التي قد تكون مستهدفة بهدف بيعها مقابل مبلغ مالي أو الاستفادة منها بطرق غير قانونية. بالإضافة إلى ذلك، قد تشمل أهداف المخترقين التلاعب بالمعلومات أو تعديلها أو إتلافها على أجهزة الآخرين .يُعتبر هذا النوع من الاختراق الأكثر خطورة، حيث يستهدف مواقع الإنترنت تحديدًا، مما يؤدي إلى تغيير تصميماتها أو تحريف محتواها. تُعرف هذه العملية باسم تغيير وجه الموقع، وتعد من بين أخطر أساليب الهجوم الإلكتروني[2].

3- .جريمة تعطيل الأجهزة والشبكات: يتعرض تعطيل أجهزة الحواسيب لآثاره من خلال البرامج التشغيلية، مما قد يسفر عن أعطال تقنية تمس المكونات الإلكترونية للجهاز .يهدف هذا التعطيل إلى منع الحواسيب والشبكات من أداء وظائفها بشكل سليم، وذلك دون الحاجة إلى تنفيذ عملية اختراق فعلية لهذه الأجهزة .وعادةً ما يتم تعطيل الأجهزة عن طريقاستخدام تقنيات

[1]منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه، ص .37

[2]منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه، ص .38

وبرمجيات تعمل على تعطيل الأنظمة أو إرباكها، مما يؤثر سلبًا على الأداء العام للأجهزة والشبكات[1].

4 –جريمة النصب والاحتيال : أصبحت مرتبطة بشكل متزايد بالتعاملات عبر الإنترنت، حيث أصبح التعاقد الإلكتروني ضرورة ملحة بسبب ما يوفره من سرعة وسهولة في التعامل .ومع ذلك، لم تخلُ هذه الميزة من الجوانب السلبية التي تمثلت في ظهور العديد من الأفعال الإجرامية المرتبطة بالنصب والاحتيال. تشمل هذه الجرائم اختراق التعاملات من خلال أساليب احتيالية جديدة يتم ابتكارها باستمرار، مما أدى إلى زيادة ملحوظة في وقوع ضحايا بين مستخدمي الإنترنت، حيث لا يزال عدد كبير منهم يتعرض لهذه العمليات الاحتيالية..

إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

ثانيا: أهداف الجريمة المعلوماتية

تهدف الجرائم المعلوماتية إلى تحقيق الوصول غير المشروع إلى البيانات والمعلومات، سواء عن طريق سرقتها، الاطلاع عليها دون إذن، حذفها، أو تعديلها بما يحقق الأغراض الإجرامية .وتشمل هذه الأهداف أيضًا الوصول غير المصرح به إلى الخوادم التي توفر المعلومات عبر شبكة الإنترنت بهدف تعطيلها أو التلاعب ببياناتها .إضافة إلى ذلك، تسعى هذه الجرائم للحصول على معلومات حساسة وسرية خاصة بالمؤسسات، البنوك، الجهات الحكومية، أو الأفراد، مما يمكّن مرتكبيها من ممارسة الابتزاز بغرض تحقيق مصالح مادية **أو سياسية .كما تسهم هذه** الجرائم في تحقيق مكاسب مادية، معنوية، أو سياسية غير مشروعة من خلال استغلال تقنيات المعلومات، كاختراق وتدمير المواقع الإلكترونية، تزوير الحسابات البنكية وسرقتها.

[1] عبد الكريم شيباني ، مرجع سابق، ص.23

المطلب الثاني: الطبيعة القانونية للجريمة المعلوماتية

قبل التطرق الى أركان الجريمة المعلوماتية يجب معرفة خصائص هذه الجريمة المعلوماتية وهذا ما سنطرق إليه في الفرع الأول والى أركانها في الفرع الثاني.

الفرع الأول: خصائص الجريمة المعلوماتية

تختلف الجريمة المعلوماتية بشكل عام عن الجريمة التقليدية من جوانب متعددة، سواءً من حيث الخصائص العامة التي تميزها، أو الدوافع التي تقف وراء ارتكابها، وكذلك الأساليب المستخدمة في تنفيذها .ومن أبرز السمات التي تنفرد بها:

أولا: صعوبة اكتشاف الجريمة المعلوماتية

الجرائم المرتبطة باستخدام الإنترنت تتمتع بطبيعة فريدة تجعلها خفية ومستترة في معظم الأحيان، وهو ما يجعل اكتشافها أمراً بالغ الصعوبة الضحية غالباً ما يكون غير مدرك لوقوع الجريمة، حتى وإن حدثت أثناء تواجده على الشبكة يعود ذلك إلى المهارات الفنية العالية التي يمتلكها مرتكب الجريمة، والتي تتيح له تنفيذ أفعاله بدقة متناهية .وتظهر هذه الجرائم من خلال أساليب متعددة مثل إرسال الفيروسات التي تعطل الأجهزة، وسرقة الأموال أو البيانات الشخصية وحذفها أو إتلافها بالكامل، بالإضافة إلى التجسس على المعلومات الخاصة، وسرقة المكالمات، وغيرها من الأنشطة الإجرامية المعقدة .تتميز وسائل التنفيذ المستخدمة في هذه الجرائم بالطابع التقني المتقدم، مما يضفي عليها مستوىً مرتفعاً من التعقيد الذي يجعل ملاحقتها أمراً شاقاً[1].

بالإضافة إلى ذلك، فإن الجزء الأكبر من هذه الجرائم لا يتم الإبلاغ عنها حتى عند اكتشافها، نظراً لخوف الضحايا من فقدان ثقة عملائهم أو الإضرار بسمعتهم .وتجدر الإشارة إلى أن

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، ص.32

المجرمين يستطيعون تدمير الأدلة الرقمية التي يمكن أن تُستخدم لإثبات الجريمة في غضون أجزاء من الثانية، مما يضاعف من صعوبة ملاحقتهم ومحاسبتهم قانونياً[1].

ثانيا: صعوبة إثبات الجريمة المعلوماتية

تُعد الجريمة المعلوماتية من التحديات الحديثة التي تواجه السلطات نظراً لطبيعتها الخاصة والمختلفة عن الجرائم التقليدية. فهي تحدث داخل بيئة افتراضية تعتمد على الحاسوب وشبكة الإنترنت، بعيدة كل البعد عن الواقع المادي الملموس الذي اعتادت أجهزة الأمن التعامل معه. هذه البيئة الرقمية التي تُشكل مسرح الجريمة تجعل عملية تحديد الأدلة وجمعها أمرًا بالغ التعقيد.

فالتعامل مع هذا النوع من الجرائم يحتاج إلى أدوات وتقنيات متطورة لفهم وتحليل البيانات الرقمية التي يمكن أن تكون مبعثرة أو مخفية بطريقة متقنة، وهو ما يزيد من صعوبة عمل سلطات الأمن وأجهزة التحقيق التي تجد نفسها أمام تحدٍّ مستمر لضمان تحقيق العدالة والقبض على الفاعلين في هذا المجال الملتبس.

إن هذه الجرائم، نظرًا للطبيعة التقنية المعقدة التي تتطلبها في ارتكابها، تحتاج بالمثل إلى تقنيات متقدمة لاكتشافها ومواجهتها .كما أنها تستدعي أساليب تحقيق وتعامل خاصة، وهو ما لم يتحقق بشكل كافٍ في الأجهزة الأمنية والقضائية لدينا، بسبب نقص المعرفة والمهارات في هذا المجال. هذا الوضع يتطلب توجّهًا نحو التخصص في مجال التقنية لتقوية منظومة الأمن والقضاء وتحصينها ضد هذا النوع من الجرائم .القوانين التقليدية أصبحت غير قادرة على مواجهة التحديات التي يفرضها التطور السريع في المجال التكنولوجي، مما يستلزم إعادة النظر لتعزيز التصدي للجريمة المعلوماتية[2].

---

[1] نهال عبد القادر المومني، الجرائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع، ص56.

[2] محمد عبيد الكعبي، مر جع سابق، ص.40

ثالثا: أسلوب ارتكاب الجريمة المعلوماتية

تتميز الجرائم المعلوماتية بأساليب تنفيذها التي تختلف بشكل واضح عن الجرائم التقليدية. فبينما تعتمد الجرائم التقليدية على استخدام القوة البدنية، مثل الكسر أو الخلع كما يظهر في جرائم السرقة[1]، تتطلب الجرائم المعلوماتية مهارات تقنية واستخدام شبكة المعلومات الدولية (الإنترنت). يقوم المجرم في هذا النوع من الجرائم بتوظيف خبراته التقنية وقدرته على تحليل واستغلال الثغرات لاختراق الخصوصيات أو تنفيذ أفعال إجرامية متنوعة، مثل التجسس أو استغلال القُصّر . ويُلاحظ أن هذه الجرائم لا تعتمد على العنف الجسدي أو سفك الدماء، بل تتحقق عبر استغلال الكفاءة التكنولوجية والتخطيط المعقد.

رابعا: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

تعد الجريمة المعلوماتية من الجرائم التي تعتمد في الغالب على جهود جماعية لتتحقق، حيث عادة ما يتم تنفيذها من خلال تضافر جهود مجموعة من الأشخاص الذين يتشاركون

الأدوار لتحقيق هدفهم بالإضرار بالجهة المستهدفة .في هذا النوع من الجرائم، يبرز دور شخص متخصص في تقنيات الحاسوب وشبكات الإنترنت، يمتلك المهارات الفنية والتقنية اللازمة للقيام بالجزء الفني المتعلق بالمخطط الإجرامي .إلى جانبه، يُشترك عادة بشخص آخر إما من داخل المحيط القريب أو من خارج المؤسسة أو الجهة المستهدفة، ويتولى هذا الشخص مسؤولية تسهيل عملية التلاعب بالتفاصيل الضرورية وضمان تحويل المكاسب التي تتحقق من الجريمة إلى وجهات محددة. هذا التعاون المنظم بين الأطراف يظهر مدى تعقيد واحترافية هذه النوعية من الجرائم، مما يجعل التصدي لها وتحديد المسؤوليات فيها أمرًا يحتاج إلى تقنيات متقدمة وتحقيقات دقيقة[2].

---

[1] نهال عبد القادر المومني، مرجع سابق، ص .58-57

[2] حمد عبيد الكعيبي، المرجع السابق، ص .42

خامسا: خصوصية مجرمي المعلوماتية

يُطلق على الشخص الذي يقوم بارتكاب الجرائم المتعلقة بالمجال المعلوماتي تسميات مثل المجرم الإلكتروني أو المجرم المعلوماتي. هذا النوع من المجرمين يتميّز بخصائص وسمات فريدة تُميّزه بوضوح عن مرتكبي الجرائم التقليدية، الذين يُعرفون بالمجرمين التقليديين .ففي حين أن الجرائم التقليدية غالبًا لا تتطلب مستوى عاليًا من التعليم أو المعرفة التقنية من مرتكبيها، فإن الأمر يختلف جوهريًا في حالة الجرائم المعلوماتية .يُصنّف هذا النوع من الجرائم غالبًا ضمن الجرائم التقنية أو الفنية، وذلك لأنها تعتمد بصورة أساسية على الفهم العميق للتكنولوجيا والاطلاع على تقنيات المعلومات والاتصال الحديثة. من هذا المنطلق، نجد أن مرتكبي الجرائم المعلوماتية يمتلكون في معظم الأحيان قدرات فنية ومهارات معرفية متقدمة، تمكّنهم من اختراق النظم الرقمية أو استغلال الثغرات التقنية بكل

دقة واحترافية .وهذا الاختلاف الجوهري بين طبيعة الجرائم وأنواعها ينعكس كذلك على نوعية المجرمين أنفسهم، حيث إن المجرم المعلوماتي غالبًا ما يكون شخصًا ملمًا بالتطورات التكنولوجية والمعرفية، مما يجعل نشاطاته الإجرامية أكثر تعقيدًا وصعوبة في الاكتشاف مقارنة بالجرائم التقليدية التي تعتمد غالبًا على أساليب تنفيذ مباشرة وواضحة[1].

سادسا: الجريمة السيبرانية جريمة عابرة للحدود

مع ظهور شبكات المعلومات، لم تعد هناك حواجز واضحة أو ملموسة تعيق انتقال البيانات بين الدول. فقدرة الحواسيب وشبكات الاتصال على نقل كميات هائلة من المعلومات وتبادلها بين أنظمة متباعدة بمسافات شاسعة أسفرت عن حقيقة مفادها أن جريمة سيبرانية واحدة قد تترك آثارها في أماكن متعددة داخل دول مختلفة وبالتزامن

[1]- نهال عبد القادر المومني، مرجع سابق، ص .57-58

الفرع الثاني: أركان الجريمة المعلوماتية

الجريمة التي يتم ارتكابها عبر الإنترنت تُعد من الأنواع الحديثة والمميزة التي تعتمد على الفضاء الافتراضي كبيئتها الرئيسية لوقوع الأفعال غير المشروعة، وهذا يجعلها تختلف في بعض الخصوصيات عن الجرائم التي تحدث في العالم التقليدي أو المادي .ومع ذلك، لا يمكن إنكار أن هناك نقاط تلاقي وتشابه بين هذين النوعين من الجرائم، خاصة فيما يتعلق بالركائز الأساسية التي تُعرِّف كل منهما. فعلى الرغم من الطابع الرقمي للجريمة الإلكترونية، إلا أنها تتشارك مع الجريمة التقليدية في مجموعة من العناصر الرئيسية، أولها وجود فعل غير مشروع يُرتكب بهدف تحقيق غاية معينة تتناقض مع القانون والنظام. بالإضافة إلى ذلك، هناك العنصر البشري المتمثل في مرتكب الجريمة، أي الشخص الذي يعمل على تنفيذ هذا الفعل بطريقة تنتهك القوانين المعمول بها. انطلاقاً من هذه النقاط المشتركة، يمكننا التعمق أكثر في تحديد وتحليل الأركان الأساسية التي تقوم عليها الجريمة الإلكترونية، مما يساعدنا على فهم هذه الظاهرة بشكل أعمق وتطوير أساليب فعّالة لردعها والحد من تداعياتها.

أولا: الركن الشرعي

الركن الشرعي للجريمة يُفهم على أنه وجود نص قانوني رسمي صريح يجرم الفعل المعني ويحدد العقاب المترتب عليه وقت وقوع هذا الفعل .يرتكز هذا الركن على مبدأ هام يحظر ملاحقة الأشخاص عن أفعال ارتكبوها قبل صدور نص التجريم المرتبط بها، أو عن أفعال ارتكبت بعد إلغاء النص المجرّم لها .إضافة إلى ذلك، لا يصح قياس أو إسقاط التجريم على أفعال لم ينص عليها المشرّع بشكل مباشر، حتى وإن وُجدت تشابهات كبيرة بين تلك الأفعال وأخرى نص القانون على تجريمها سواء من حيث الدوافع، أو النتائج، أو الفاعلية، أو العناصر المكونة للجريمة .يستمد هذا المبدأ قوته من ضرورة احترام الحدود التي وضعها المشرع، حيث يُمنع بشكل قاطع التوسع في تفسير النصوص الجزائية بما يتجاوز نطاق مدلولها الواضح والصريح .وعلى هذا النحو، يجب على

القضاة الالتزام الحرفي بدلالات النصوص القانونية والتمسك بمضامينها[1]، دون الخروج عنها أو تحميلها معانٍ إضافية.يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري وال مجال إهمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم [2]

يمثل الركن الشرعي في الجريمة العنصر القانوني الذي يكتسب الفعل من خلاله صفته غير المشروعة، والتي تجعل من السلوك المنسوب للجاني جريمة يعاقب عليها القانون .يتألف هذا الركن من عنصرين رئيسيين لا بد من تحققهما :

-يجب أن يكون الفعل متطابقا مع نص التجريم الوارد في القوانين أو النصوص التشريعية السارية.

-يجب ألا يكون الفعل المرتكب مشمولا أو مستفيدا من أحد أسباب الإباحة التي ينص عليها القانون .حين نتحدث عن مطابقة

الفعل لنص التجريم، فإن هذا يعني ضرورة أن تكون التصرفات أو الأفعال التي قام بها الجاني تتطابق بشكل صريح ومباشر مع تلك الأفعال التي حددتها النصوص التشريعية كجرائم معاقب عليها. هذا التطابق يضمن تأطير الجريمة قانونياً وعدم إخضاعها للتفسيرات الشخصية أو الاجتهادات غير المستندة إلى القانون .أما بالنسبة لشرط ألا يخضع الفعل لسبب من أسباب الإباحة، فإن هذا العنصر يشير إلى أنه لا يمكن اعتبار أي فعل مجرماً إذا كان مرتكب الفعل محمياً بأحد أسباب التبرير التي يجيزها المشرع. وبما أن أسباب الإباحة تنفي الصفة الإجرامية عن السلوك، فإن القضاء يتوقف عند دراسة مدى انطباقها في كل حالة على حدة. وفي هذا السياق،

[1] أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان ،2014 ص.45

[2] حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، ب يروت،2014 ص.

أشارت اجتهادات المحكمة العليا إلى أن تطبيق نظرية العقوبة المبررة يستند إلى وجود نص قانوني واضح يحدد نفس العقوبة ويشرح شروط فرضها، مما يعزز مبدأ العدالة واليقين التشريعي[1].

ثانيا: الركن المادي

الركن المادي للجريمة يعد أحد العناصر الأساسية التي تُبنى عليها الأركان الأخرى، ويعبر عن المظهر الخارجي الواقعي للسلوك المجرّم من حيث كونه فعلًا أو امتناعًا عن فعل يصدر عن إنسان يتمتع بالعقل والإدراك .يعكس هذا الركن الجانب الحسي للجريمة، إذ يتجسد في عمل إيجابي مباشر، كارتكاب فعل محظور صراحة بموجب القانون، أو في تقاعس سلبي يتمثل في الامتناع عن أداء فعل يُفترض قانونًا وجوب القيام به. الهدف النهائي لهذا السلوك يكمن في إحداث ضرر أو تهديد بإلحاق ضرر بحق محمي، سواء كان هذا الحق متعلقًا بالفرد أو المجتمع بأسره، وهو ما يحظى بضمانة وصيانة من الدستور والقوانين.

وفي هذا السياق، يوضح الدكتور رضا فرح أن الركن المادي يمكن تحليله وتقسيمه إلى ثلاثة عناصر رئيسية، يترابط كل منها بالآخر ويعمل بشكل جماعي لتكوين الإطار العام للجناية أو الجنحة.

هذه العناصر هي:

– السلوك الإجرامي: وهو النشاط المحظور الذي يتجسد في فعل أو امتناع يشكل انتقالًا مباشرًا للتعدي على حقوق يحميها القانون.

– النتيجة الإجرامية:وهي الأثر الفعلي الذي يترتب على السلوك الإجرامي، والذي قد يتمثل في إلحاق ضرر مادي أو معنوي بالمصلحة المحمية قانونًا.

– العلاقة السببية:وهي الرابط الواضح والمباشر بين السلوك الإجرامي والنتيجة الناجمة عنه، بحيث يُثبت بشكل لا يقبل الشك أن النتيجة لم تكن لتقع لولا وقوع ذلك السلوك .

[1] بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص.95-94

هذه العناصر الثلاثة معًا تشكل البنية الأساسية للركن المادي، حيث لا يمكن تصور اكتمال الجريمة من دون توافرها مجتمعة وبصورة مترابطة ومنسجمة.

أ–السلوك الإجرامي: هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة المعلوماتية يمكن أن نجده بنوعيه السلوك الإيجابي أو السلبي .ال ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بال شك صعوبات كثيرة [1].

ب– النتيجة الإجرامية: يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى[2]

ج– العلاقة السببية بين الفعل والنتيجة: تتمثل العالقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد[3]

ثالثا: الركن المعنوي

الركن المعنوي للجريمة المرتكبة في الفضاء الإلكتروني يعتمد بشكل أساسي على توافر نية الجرم لدى الجاني، وهذه النية تتجسد في توجه إرادته نحو القيام بأفعال غير مشروعة يحظرها ويجرمها القانون .

---

[1] أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص51 .52-

[2] بلعلبات إبراهيم، المرجع السابق، ص .18

[3] سامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص .59-58

من أمثلة هذه الأفعال انتحال شخصية مزود الخدمة عبر الإنترنت أو سرقة البيانات الحساسة كأرقام البطاقات الائتمانية .ولإثبات هذا الركن، لا يقتصر الأمر على مجرد توفر النية، بل يجب أن يتمخض عن هذه الأفعال نتيجة ملموسة تحمل صفة الجريمة المقررة قانونًا[1].

وبالتالي، فإن إرادة الجاني تكتسب الصفة الإجرامية عندما تتداخل مع الفعل غير المشروع الذي يظهر نية تعمد ارتكاب الأذى، مع علمه المسبق بالنتائج الضارة والخطيرة التي قد تترتب على تلك الأفعال. وهذا الإدراك يجعل الجاني يتحمل المسؤولية الكاملة عن أفعاله، نظرًا لوعيه بمدى خطورتها وانعكاساتها السلبية على الضحايا والمجتمع ككل[2].

المبحث الثاني: الحماية الجنائية من خلال النصوص القانونية

في هذا المبحث سوف نتطرق إلى موقف المشرع الجزائري من الجريمة المعلوماتية (المطلب الأول)، جرائم الاعتداء الماسة بالأنظمة المعلوماتية (المطلب الثاني)

المطلب الاول: موقف المشرع الجزائري من الجريمة المعلوماتية

لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات لما كان فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 04/15 المؤرخ في 10/11/2004 المتمم

والمعادل للأمر 66/156 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة.

---

3 [1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جر ائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان،2011 ص-74. 73

[2] حنان ريحان مبارك المضحاكي، المرجع السابق، ص .107

لذلك فقد آثار المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محال لها (الفرع الأول). ثم في مرحلة الحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 09/04 المتضمن الوقاية من هذه الجرائم ومكافحتها (الفرع الثاني)

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

اعتمد المشرع الجزائري مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات "لتوصيف الجريمة المعلوماتية، حيث اعتبر أن النظام المعلوماتي، بمفهومه الشامل، يشمل كل من المحتوى المادي والمكونات غير المادية المرتبطة به، هو محور هذه الجريمة وأساس تشخيصها. يُعد نظام المعالجة الآلية للمعطيات العنصر الأساسي والشرط الابتدائي الواجب توافره من أجل تحليل وجود أو عدم وجود أركان أي جريمة تتعلق بالاعتداء على هذا النظام .وبناءً عليه، إذا تبين غياب هذا الشرط الأساسي، فإن البحث في مدى تحقق عناصر الجريمة يصبح غير ذي جدوى، لأن توفر النظام يُعتبر شرطًا جوهريًا لتحقيق الأركان الأخرى .ومن المهم الإشارة إلى أن مكونات النظام المعلوماتي غير المادية تختلف في طبيعتها، فهي قد تكون مخزنة داخل النظام، أو يتم نقلها منه، أو تُرسل إليه من مصدر خارجي .هذا التباين يفرض الحاجة إلى دراسة دقيقة وشاملة لمفهوم نظام المعالجة الآلية للمعطيات .يتطلب الأمر توضيح ماهية هذا النظام، وما يشتمل عليه من عناصر مادية وغير مادية، لفهم الأساس القانوني الذي يستند إليه المشرع في تحديد الجرائم المعلوماتية. مثل هذه الدراسة تسهم في تحديد النطاق الدقيق للحماية القانونية التي تُمنح لهذه الأنظمة وتعزز من أدوات مكافحة الجرائم الإلكترونية في العصر الرقمي الراهن

أولا: المقصود بنظام المعالجة الآلية للمعطيات[1]

إن معالجة البيانات تمثل عملية تتطلب وجود آلية محكمة ومنظمة تعمل على جمع وتوفير المعلومات الضرورية وإجراء العمليات اللازمة لتحليلها ومعالجتها بفعالية ودقة. نتيجة لهذه الحاجة الملحة، برزت ضرورة تطوير إجراءات وأدوات متخصصة تسهّل تحقيق هذه الوظيفة، مما أدى إلى نشوء مفهوم نظم المعلومات المبنية على التقنيات الحاسوبية .يُطلق على هذه النظم مصطلح "نظم المعلومات المحوسبة"، وهي أنظمة تعتمد بشكل أساسي على تكامل الأجهزة المادية (الهاردوير) والبرمجيات (السوفتوير) للحاسوب بهدف معالجة كميات كبيرة من البيانات، تنظيمها، ثم استرجاع المعلومات المطلوبة بدقة وفي الوقت المناسب لتلبية احتياجات المستخدمين أو المؤسسات. هذه النظم توفر حلولاً مرنة وفعّالة تُسهم في تحسين جودة العمل وتسريع العمليات المرتبطة بإدارة وتحليل المعلومات.

شهدت السنوات الأخيرة تطورًا تقنيًا هائلًا في عالم تكنولوجيا المعلومات، حيث اتسعت مهام هذا المجال لتشمل جمع وتوفير ومعالجة وتبادل المعلومات بشكل متزامن. هذا التقدم التقني أدى إلى ظهور مفهوم جديد ومبتكر يعرف باسم نظام المعالجة الآلية للمعطيات .وُجد هذا النظام في الأساس كرد فعل طبيعي لحاجة ملحة ظهرت مع تداخل وتكامل تقنيات نظم المعلومات مع تقنيات الاتصالات عن بعد، مما أوجد بيئة تقنية موحدة تهدف إلى تعزيز الكفاءة في التعامل مع البيانات والمعلومات .يعرف نظام المعالجة الآلية بأنه عبارة عن مجموعة من العمليات والنظم المترابطة التي تعتمد على أساليب منظمة لجمع وفرز وتصنيف البيانات، ثم معالجتها وتحويلها إلى معلومات ذات قيمة معرفية. هذه المعلومات يمكن استرجاعها واستخدامها من قبل الإنسان في أي وقت يحتاج إليها، سواء كان ذلك لاتخاذ قرار، أو تنفيذ مهمة معينة، أو أداء وظيفة محددة، مما يجعل دوره محوريًا في دعم عملية اتخاذ القرار المبنية على أسس معرفية .ومع اتساع استخدامات

[1]سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، جامعة الحاج لخضرباتنة، سنة دراسية ،2102/2013 ص .43-42

هذه الأنظمة التقنية، أصبح من الضروري وجود إطار قانوني يحميها من أي تهديدات أو اعتداءات تستهدف أمنها وسلامتها. ولهذا السبب، وفي سياق مراجعة قانون العقوبات الجزائري وإدخال تعديلات عليه، أضيف قسم جديد تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات". لكن الملاحظ على هذه الإضافة هو أن المشرع الجزائري، بالرغم من إدراجه هذا القسم وصياغته لأشكال متعددة للحماية من الاعتداءات التي قد تطال هذه الأنظمة، لم يقدم تعريفًا واضحًا ومباشرًا لنظام المعالجة الآلية للمعطيات، تاركًا بذلك مفهومه مفتوحًا وقابلاً للتأويل. هذا الأمر يثير تساؤلات حول كيفية تحديد نطاق الحماية القانونية الممنوحة لهذه الأنظمة في ظتم تكليف مهمة تحديد وتعريف هذا المفهوم للفقه، مستندًا في ذلك إلى النهج الذي اعتمده المشرع الفرنسي .فقد اتبعت الجمعية الوطنية الفرنسية موقفًا مشابهًا عندما قررت عدم الإبقاء على التعريف الذي اقترحه مجلس الشيوخ الفرنسي ضمن إطار النظام الخاص بالمعالجة الآلية، وذلك أثناء تعديلها لقانون العقوبات. في النهاية، تم حذف ذلك التعريف

من النص النهائي، وهو ما يعكس توجّهًا محددًا نحو تبسيط أو إعادة صياغة التشريعات بطريقة لا تتعارض مع المفاهيم القانونية الأساسية.

ثانيا: مدى اشتراط الحماية التقنية للنظام المعلوماتي[1]

طرح الفقه القانوني قضية ذات أهمية بالغة فيما يتعلق بجرائم الاعتداء على نظم المعالجة الآلية للمعطيات .تمحورت هذه القضية حول مسألة اشتراط وجود حماية تقنية للنظام المعلوماتي كشرط ضروري لحمايته من الناحية الجزائية .وفي هذا السياق، انقسمت الآراء الفقهية إلى اتجاهين رئيسيين .الاتجاه الأول، وهو الرأي الغالب في الفقه الفرنسي، يرى أنه لا يشترط وجود حماية تقنية للنظام المعلوماتي لقيام جريمة الاعتداء عليه .وفقاً لهذا الرأي، لغياب تعريف دقيق ومحدد

[1]سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص.45

فإن نظام الحماية التقنية ليس سوى عاملاً إضافياً يساهم في تعزيز مستوى الأمان، إلا أن عدم توفره لا يعد مبرراً لاستبعاد المسؤولية الجنائية عن منتهكي النظام. وبهذا يُركز هذا الاتجاه على عنصر سوء النية المعلوماتية، إذ يُنظر إلى الانتهاك غير المشروع للنظام على أنه يكفي لإثبات القصد الجنائي .وبالتالي، فإن الحماية التقنية تُعتبر مجرد وسيلة لتعزيز الأمن، لكنها ليست شرطاً جوهرياً لإثبات الجريمة .من جهة أخرى، تبنى الاتجاه الثاني رأياً مخالفاً ينص على ضرورة وجود نظام أمني فعال لحماية النظام المعلوماتي ليتم الاعتراف بتجريم أي اعتداء عليه .يستند أنصار هذا الرأي إلى عدة حجج، منها أن وجود اعتداء على النظام الأمني يعتبر أساساً لإثبات قيام الجريمة المعلوماتية، وأن عدم وجود هذا الاعتداء يجعل من الصعب تصور وقوع الجريمة أصلاً .كما يؤكدون أن القضاء لا يفترض معاقبة على اعتداء طالما لم يتخذ صاحب الحق إجراءات لحمايته .بالإضافة إلى ذلك، يرون أن تغاضي هذا الشرط يؤدي إلى توسيع نطاق التجريم بشكل غير عقلاني، حيث يصبح كل دخول غير مشروع جريمة، وهو ما يتعارض مع مفاهيم العدالة والاعتدال .

ومع ذلك، يمكن القول إن هذا الشرط في الوقت الراهن قد أصبح شبه فاقد للأهمية العملية بسبب التقدم التقني الهائل. فغالبية النظم المعلوماتية أصبحت محمية بواسطة تقنيات حديثة وذات كفاءة عالية بشكل افتراضي، بل ظهرت شركات متخصصة تقدم خدمات حماية متطورة لأنظمة المعلومات .وعلى الرغم من أهمية الحماية التقنية كخط دفاع أساسي، فإنها تظل غير كافية بمفردها للحد من الجرائم الماسة بنظم المعالجة الآلية للمعطيات. ومن ثم، يبقى من الضروري استكمالها بإطار قانوني جزائي رادع يضمن عدم الإفلات من العقاب ويردع مرتكبي الجرائم في هذا المجال المتطور.

[1] سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص .43-42

الفرع الثاني: المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]

إنه وقبل صدور القانون رقم 09/04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية.

هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون09/04 تعريفا موسعا للجرائم المعلوماتية واعتبر أنما تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محال للاعتداء بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة الارتكاب.

ويذهب بعض الفقه الجنائي إلى القول بأن هذه الطائفة الأخيرة تشكل أهم الجرائم التي تتصل بالمعلوماتية وأكثرها إثارة للمشكلات القانونية، فهي تتكون بصفة عامة من بعض الجرائم التقليدية التي يتم ارتكابها بواسطة المعلوماتية فتكتسب داخل هذا الإطار خصائص جديدة لارتباطها بالحاسب الآلي والنظم المعلوماتية تتميز عن الصورة التقليدية لها وتؤدي بالتالي إلى صعوبة تطبيق النصوص التقليدية عليها وهي في ثوبها الجديد، ومن هذه الجرائم على سبيل المثال يمكن أن نتصور ارتكاب جرائم إرهابية، جرائم التزوير أو جرائم أخلاقية ... بواسطة منظومة معلوماتية

[1] سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص .43-42

المطلب الثاني: جرائم الاعتداء الماسة بالأنظمة المعلوماتية

حاول المشرع الجزائري خلال الفترات الأخيرة من الزمن تدارك الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني، فقام بتعديل أحكام قانون العقوبات الجزائري، بموجب القانون رقم 15-04[1] ، مستحدثا فيه مجموعة من النصوص، التي جرم من خلالها كل الأفعال والسلوكيات المرتبطة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها جزاء.

ويمكن الإشارة قبلها، إلى تعريف الجريمة المعلوماتية أو الجريمة السيبرانية أو جريمة الفضاء الإلكتروني مثلما يسميها البعض، وهي جريمة يستخدم الحاسوب في ارتكابها، وهي عبارة عن مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وسواء كان ذلك بطريقة مباشرة أو غير مباشرة، والمهم في ذلك هو استخدام وسائل الاتصال الحديثة بشأنها من كمبيوتر، أو أية آلة ذكية أخرى.

الفرع الأول: الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

تتمثل الصورة البسيطة للاعتداء على نظام المعالجة الالية للمعطيات في شكل الدخول أولا أو البقاء ثانيا غير المرخص بهما.

أولا: الدخول غير المرخص به

تنص المادة 394 مكرر من قانون العقوبات الجزائري أنه: »**يعاقب بالحبس من ثالثة أشهر إلى سنة وبغرامة من 500000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك** .«

يفهم من نص المادة أعاله، أن الجزاء عن مثل هذه المخالفات يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول، وطبعا هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط.

---

[1]قانون رقم 15-04 مؤرخ في 10 نوفمبر،2004 يتضمن قانون العقوبات، جريدة رسمية عدد ،71 لسنة ،2004 معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر ،07 المضافة بموجب القانون نفسه

ما يوقع كما يفهم من البند نفسه أن المشرع ال يعاقب على الفعل الكامل، أي على الجريمة التامة، العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي ال تشترط لقيامها تحقق النتيجة الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألا يكون الدخول صدفة أو خطأ .وتجدر الإشارة هنا، إلى أن المشرع الجزائري لم يشترط في البند أعاله، طبيعة خاصة لهذا النظام، أي أن المادة 394 مكرر لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية، وبدون أي استثناء .وبذلك يكون مشرعنا قد أصاب بشكل كبير في تنظيمه لهذه المسألة، حيث وبتمييز المشرع بين تجريم الدخول غير المرخص به إلى نظام معلوماتية محاط بحماية فنية وعدم التجريم للدخول غير المرخص به إلى نظام غير محاط بحماية فنية، سيؤدي حتما إلى فتح المجال للمجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء، بحجة أن النظام المعتدى عليه غير محاط بحماية فنية، وبذلك، فيكون المشرع قد أحسن فعال عندما لم يفصل بين النظام المحاط بالحماية الفنية، وذلك النظام غير المحاط بها.

ثانيا: البقاء غير المرخص به يقصد بالبقاء غير المرخص به هنا، الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص[2] .ولقد سوى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وذلك على غرار ما اتخذه المشرع الفرنسي في منظومته[1] الجزائية، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثالثة (03) أشهر إلى سنة، وغرامة مالية من 50000 دج إلى 100000 دج ويعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يحتمل صورتين مختلفتين هما :

-تتمثل الصورة الأولى، في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية ن كان خطأ أو للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى صدفة، غير انه وبتفطن الفاعل للوضع وبدال من الانسحاب أو مغادرة النظام فورا، فإنه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به – .بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشأن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله .والإشكال الذي يمكن أن يثيره هذا الاجتماع والتداخل للسلوكين من دخول إلى النظام والبقاء فيه، هو تحديد النطاق الزمني لكل واحدة منها، بمعنى متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟

ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة البقاءتكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام[1]

ومهما يكن من أمر، فإن المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى الدخول ثم إلى البقاء، وكأن المشرع يصنف الأولى بجريمة وقتية كون فترة استمرارها قصيرا جدا والأخرى بجريمة مستمرة، مقارنة بالأولى

الفرع الثاني: الصور المشددة للاعتداء على نظام المعالجة الآلية للمعطيات

يشدد المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، وذلك بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات، التي تنص أنه: »... تضاعف

[1] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007، ص1

العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج[1].»تبعا لذلك، فإن المادة تحدد ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية وهما :

-حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام.

-ويتحقق الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة و إعاقته عن الأداءوتجدر الإشارة هنا، إلى أن الصورة البسيطة للاعتداء على النظام المحددة في المادة 394 مكرر 01السابقة لم تشترط البحث في النتيجة الإجرامية، بينما وباستقرار الفقرة 02 من المادة 394 مكرر يفهم أن النتيجة الإجرامية واجبة الإثبات، فيجب إثبات المحو أو التعديل أو التخريب للإقرار بالصورة المشددة للجريمة ال كنا بصدد الصورة الأولى والبسيطة لا أكثر، ولقد أصاب المشروع مجددا في تشديده للعقاب هنا، والهدف -طبعا- هو الحد من تفاهم الإجرام المعلوماتي وما يرتبه من أضرار بالغة ووخيمة على الفرد والمجتمع والدولة

1خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010، ص.123.

خلاصة الفصل:

ماسبقفإنالجريمةالمعلوماتيةجريمةمستحدثةتستهدفلاعتداءعلىالمعطياتبدلالتهاالتقنيةالواسعةأوالاستعانةبهاالارتكابجرائمتحاكيالجرائمالتقليديةفيالعالمالافتراضية،وفيهذاالفصلتمتناولتعريفالجريمةالمعلوماتيةوذلكحسبالاتجاهاتالقانونية،ثمبعدذلكتمتحديدالطبيعةالقانونيةلهاثمتبيانخصائصها،بالإضافةإلىالهدفمنارتكابها،ثمتمالتعريجبعدذلكإلىاستيضاحموقفالتشريعالجزائريمنالجريمةالمعلوماتيةمنخلالالنصوصالقانونيةالموضوعةلمواجهةهذهالجريمة،والصورالتيجاءتهذهالنصوصالقانونية،وفيالأخيرإبرازأهمصورهذهالجريمة

الفصلالثاني :

إجراءاتالتتبعفيالجريمةالمعلوماتية

تمهيد:

الجريمة المعلوماتية يرتكبها جناة ذو يصفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكلها تقدما لجاني فيفهم تكتيكالعمل في الحسابات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون أن يتم الاهتداء إليه، ألنها ليترك آثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب إلقاء القبض عليه لم رتكبيها وللتعرف أكثر على الآليات والإجراءات المتبعة لملاحقينا لكشف عنها تها لجرائم التي تتخذ للكشف عن هذه الجريمة، تم التطرق لوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجرائم المعلوماتية على المستوى الوطني في المبحث الأول، وإجراءات القانونية التحري للكشف عن الجريمة المعلوماتية في المبحث الثاني.

المبحث الأول: يركز على الوحدات المتخصصة التي تتولى إجراءات البحث والتحقيق في الجرائم المعلوماتية:

سنستعرض من خلال أهم أبرز الهيئات والوحدات التي تُعنى بمكافحة هذا النوع من الجرائم، والمسؤولة عن تنفيذ مهام الوقاية والمو اجهة نظرًا لتخصصها الاستثنائي.

تتميز هذه الوحدات بتشكيلتها البشرية الخاصة التي تضم محققين يتمتعون بصفة ضباط شرطة قضائية بالإضافة إلى برة واسعة في مجالات النظم المعلوماتية والإجرام السيبراني.

هذا التأهيل المزدوج يتيح لهم القيام بمهام البحث والتحقيق في الجرائم المعلوماتية بكفاءة عالية، سواء كانت هذه المهام متحت إشراف وكيل الجمهورية أو قاضي التحقيق، الذين غالبًا ما يفتقرون للخبرة التقنية العميقة في هذا المجال.

المحققون المتخصصون في هذه الوحدات يستخدمون تقنيات معلوماتية دقيقة تتطلب خبرة متقدمة ومهارة في التعامل مع هذه الضمانة وفعالية عملياتا لبحث والتحري.

يُعتبر من أبرز رموز هذه الجهود الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي سنناقش ها في المطلب الأول.

كما تشمل الأجهزة الأمنية الأخرى المعنية بمكافحة الجرائم المعلوماتية، سواء التابعة لجهاز الأمن الوطني أو لقيادة الد ركالوطني، والتي سيتم تناولها في المطلب الثاني.

المطلب الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى السنة 2009 وبالضبط منذ تاريخ 05 أوت 2009 تاريخ صدور القانون 04-09 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بحيث جاء في نص المادة 13

من القانون علما أنه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تحدد تشكيل ة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم وقد استلزم الأمر لصدور التنظيم الذي طرحته نص المادة 13 السالفة الذكر الانتظار لمدة 06 سنوات كاملة، أين صدر المرسوم الرئاسي رقم 268-15 بتاريخ 08 أكتوبر 2015 ضمن العدد الثالث

والخمسين 53 للجريدة الرسمية، والذي تضمن في فصوله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية. للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

الفرع الأول: التعريف بالهيئة واختصاصاتها

أولا : التعريف بالهيئة

تعتبر " الهيئة " كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون 04-09 وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية

ثانيا :اختصاصات الهيئة

بين الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام الأساسية التي تتكلف بها الهيئة وهي وعلى سبيل الحصر مهام الهدف منها هو الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي:

1. اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال
2. تعزيز وتفعيل الجهود والإجراءات المتعلقة بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال، مع الترك يز على تنسيق التدابير لمكافحتها بشكل فعال ومستدام .
3. تقديم الدعم اللازم للسلطات القضائية وأجهزة الشرطة القضائية في مجال مكافحة الجرائم الإلكترونية، وذل كمن خلال تزويدها بالمعلومات الدقيقة والخبرات الفنية والقضائية اللازمة لتطوير أدائها
4. ضمان إجراء مراقبة وقائية شاملة لمنظومة الاتصالات الإلكترونية بهدف الكشف المبكر عن الجرائم المتصلة بالإر هاب والتخريب وأي أنشطة تهدد أمن الدولة، مع الالتزام بالقيام بهذه المهمة تحت إشراف قاضٍ مختص حسب الاخت صاص الحصري المنظم لهذا العمل
5. جمع وتوثيق البيانات الرقمية بشكل دقيق، وتسجيلها وحفظها وفق المعايير المعتمدة، مع تحديد مسارها بدقة ل ضمان استخدامها كمستند اموثوق فيه في الإجراءات القضائية المختلف

6. دعم جهود التكوين والتدريب المتخصص للمحققين في مجال التحريات التقنية، وتزويدهم بالمعرفة والمهارات اللازمة للتعامل مع الجرائم المتعلقة بتكنولوجيا المعلومات بكفاءة عالية.
7. العمل على تطوير وتوسيع التعاون مع المؤسسات والهيئات الوطنية المختصة بمكافحة الجرائم السيبرانية والاستفادة من إمكانياتها وخبراتها لتعزيز الجهود المشتركة في هذا المجال
8. تنفيذ الطلبات القانونية الرسمية الصادرة عن الدول الأجنبية وفقا لأطر والبروتوكولات المعتمدة، مع السعي لتطوير آليات تبادل المعلومات والتعاون الدولي لملاحقة الجرائم المعلوماتية بشكل أكثر فعالية
9. المشاركة الفعالة في تحديث ومراجعة القوانين والمعايير القانونية المتعلقة بمجالات اختصاص مكافحة الجرائم التقنية، بما يتماشى مع التطورات المستجدة في هذا الميدان لضمان فعالية الأطر التشريعية والتنظيمية.

الفرع الثاني: تشكيلة الهيئة وطبيعة عملها

أولا: تشكيلة الهيئة الإدارية

تتألف الهيئة من هيكلين رئيسيين هما:

لجنة الإدارة والمديرية العامة، حيث تشكلا للجنة الإدارة العمود الفقري لتوجيه الهيئة واتخاذ القرارات الإستراتيجية.

تتكون لجنة الإدارة من عدد من الشخصيات البارزة ذات المسؤوليات الرفيعة، وعلى رأسهما الوزير المكلف بالعدل الذي يتولى رئاسة اللجنة، بالإضافة إلى الوزير المكلف بالداخلية، والوزير المسؤول عن التكنولوجيات الحديثة والإعلام والاتصال، وقائد الدرك الوطني، ومدير الأمن الوطني.

كما تضم اللجنة في هيكلها ممثلين اثنين، أحدهما يمثل رئاسة الجمهورية والآخر يمثل وزارة الدفاع، إلى جانب قاضيين من المحكمة العليا الذين يساهمون بخبراتهما القانونية.

فيما يتعلق بالمديرية العامة، فإنها تُدار بواسطة مدير عام يتم تعيينه بموجب مرسوم صادر عن رئاسة الجمهورية.

تُناط بهذه المديرية العامة مجموعة من المهام الحيوية التي تشمل، على سبيل المثال، إعداد وتنسيق برامج عمل الهيئة، دراسة مشروع الميزانية بدقة واحترافية لضمان تحقيق الأهداف المرجوة، وأيضًا تتولى مسؤولية تقديم تقارير دورية وشاملة عن نشاطات الهيئة وتطوراتها.

يلعب كل من هذه المكونات دورًا تكاملياً لضمان تحقيق رؤية الهيئة وتنفيذ إستراتيجيتها بكفاءة وفعالية .

ثانيا : تشكيلية الهيئة التقنية

إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتقسم منحيث مهامها وتشكيلتها بالطابع التقني، باعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية وبمكافحة الجرائم المعلوماتية وهذه المديريات هي:

- 1 مديرية المراقبة الوقائية واليقظة الإلكترونية : لميشر الأمر الرئاسي 15-261 إلى تشكيلة هذه المديرية، غير أنه ومن خلال التحليل نص المادة 18 منه يمكننا تحديد تشكيلتها في مجموعة منضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، منسلكا الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية لاستعلام والأمن، يعينون بموجب قرار اتمشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك, تعمل هذه المديرية على إنجاز المهام التالية:

-

تنفيذ مهام المراقبة الوقائية للاتصالات الإلكترونية، بالإضافة إلى إجراء التفتيش والحجز داخل الأنظمة المعلوماتية في الحالات المتعلقة بجرائم الإرهاب أو التخريب، والجرائم التي تهدد أمن الدولة، معضرورة الحصول على إذن خطي من السلطة القضائية وتحت إشراف القاضي المختص.

- نقل المعلومات التي تجمعها إلى السلطات القضائية وأجهزة الشرطة المختصة

-

تنفيذ طلبات التعاون القضائي الدولي ضمن نطاق اختصاص الهيئة، وجمع البيانات الضرورية لتحديد مواقع مرتكبي الجرائم الإلكترونية والتعرف عليهم.

- جمع المعلومات وتوظيفها بالشكل الأمثل مثل حجر الزاوية في مجال الكشف عن الجرائم المعلوماتية.

إذ تتولى الجهات المعنية تحصيل كافة البيانات المتعلقة بالجرائم الإلكترونية وتحليلها بعمق، بهدف تتبع الأنشطة المشبوهة و تقديم أدلة دامغة تساهم في كشف هوية الفاعلين والمتورطين، مما يسهم في تعزيز الأمن الرقمي.

-

إضافة إلى ذلك، فإن الانخراط في حملات التوعية الموجهة للجمهور حول المخاطر المتزايدة المرتبطة باستخدام تكنولوج

يا الإعلام والاتصال يساهم في رفع مستوى الوعي العام، ويحذر من التهديدات المتنوعة التي قد تواجه المستخدمين، بدءًا من الاحتيال الإلكتروني وصولًا إلى جرائم سرقة الهوية وانتهاك الخصوصية.

-

كما يتمثل دور المديرية بشكل مباشر أو بناءً على طلب السلطات القضائية ومصالح الشرطة القضائية في تزويد هذه الجهات بمعلومات دقيقة وموثوقة تتعلق بالجرائم المعلوماتية.

هذا التعاون الحيوي بين الجهات التقنية والقانونية يهدف إلى تمكين المؤسسات المختصة من اتخاذ الإجراءات المناسبة بسرعة وكفاءة.

-

بناءً على المهام المكلفة بها هذه المديرية والأدوار المحورية التي تؤديها، يمكن وصفها بأنها القلب النابض والمركز العملياتي للمؤسسة، حيث تتحمل مسؤولية الإشراف التقني على كافة الجوانب المتعلقة بالبحوث والتحقيقات في الجرائم المعلوماتية.

دورها لا يقتصر فقط على المعالجة التقنية للبيانات المتعلقة بالجرائم، بل يتعدى ذلك ليشمل إدارة مركز العمليات التقنية بكفاءة، إلى جانب الإشراف على الملحقات الفنية والخدمات المرتبطة بها. --

هذا التخصص التقني وجودها في صلب العمل التنظيمي يعكس بوضوح مدى تأثيرها المحوري في توجيه الجهود الرامية إلى الوقاية من الجرائم المعلوماتية أو مكافحتها.

تعزيزًا لذلك، فإن استراتيجياتها العملية والتنظيمية تُظهر قدرتها على تقديم حلول مبتكرة وسريعة للتحديات التي تفرضها الجرائم الإلكترونية المتسارعة .

2- مديرية التنسيق التقني: لمينص المرسوم الرئاسي 15-261 على تشكيلة مديرية التنسيق التقني مما يترك المجال للقول بأنها تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل والدفاع والداخلية على شاكلة مديرية المراقبة الوقائية واليقظة الإلكترونية، غير أنها تختلف عنها من حيث المهام الموكلة إليها، فتتمثل مهامها أكثر في الدور الوقائي والإعلامي من خلال توليها:

1. إنجاز الخبرات القضائية في مجال اختصاص الهيئة
2. تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.

3. إعدادا لإحصائيات الوطنية للإجرام المعلوماتي.

4. إدارة وتشغيل المنظومة المعلوماتية

من خلال استعراض الهيكل العام للهيئة ومجمل المهام الموكلة إليها، يظهر بوضوح حجم الإدراك لدى السلطة التشريعية بضرورة تعزيز وتحفيز دور الهيئة في التصدي للجرائم المعلوماتية والوقاية منها، حتى وإن جاء ذلك التدخل متأخرًا نسبيًا. فالوتيرة المتسارعة التي تتوسع بها تطبيقات تقنيات المعلومات في مختلف جوانب الحياة الاجتماعية والمؤسسات الحكومية في الجزائر أوجدت حاجة ملحة لمثل هذا الدور. هذه التطورات التكنولوجية لم تقتصر على تحسين خدمات المجتمعات المحلية، بل جاءت أيضًا محملة بتحديات كبيرة، أبرزها التزايد المستمر في التهديدات التي تستهدف سلامة الأنظمة المعلوماتية. ومع ارتفاع مخاطر الاعتداءات الإلكترونية، والتي تمثل بدورها خطرًا حقيقيًا على أمن وحماية البيانات، سواء تلك المخزنة في المنظومات الرقمية أو أثناء تداولها بين الأطراف المختلفة، تتعاظم الحاجة إلى جهود وقائية قوية وإجراءات صارمة لمكافحة الجرائم السيبرانية المتزايدة التي باتت تشكل ظاهرة مقلقة في العصر الرقمي الحديث.

المطلب الثاني: الأجهزة الأمنية

تضم الأجهزة الأمنية كل من جهاز الأمن الوطني والذي سنتطرق له في الفرع الأول، وجهاز الدرك الوطني في الفرع الثاني.

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

في سياق تطبيق سياسة أمنية فعالة، تسخّر مديرية الأمن الوطني كافة مواردها البشرية والتقنية المتاحة للتصدي لمختلف أنواع الجرائم، لا سيما الجرائم المستحدثة مثل الجرائم السيبرانية .تُعد هذه

الأخيرة نتاجاً للتطور الحاصل على المستويين الدولي والوطني في مجالات تكنولوجيا المعلومات والاتصال .ويأتي هذا الجهد بهدف حماية المصلحة العامة وضمان سلامة المصالح الخاصة المرتبطة باستخدام هذه النوعية من التكنولوجيا.

أولا :على المستوى المركزي

اتخذت المديرية العامة للأمن الوطني خطوات هامة لتحديث هيكلها التنظيمي بهدف تأسيس وحدات متخصصة تُعنى بمكافحة أنواع محددة من الجرائم بشكل دقيق وفعال .وفي هذا الإطار، عملت المديرية العامة للشرطة القضائية على إنشاء مصلحة مختصة تعنى بمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، وأُطلق عليها اسم نيابة مديرية مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال. بالإضافة إلى ذلك، جرى استحداث نيابة مديرية الشرطة العلمية والتقنية التي تمثل ركيزة أساسية في هذا المجال عبر توفير مصالح عملية مكرسة لخدمة هذا الهدف . تشمل المهام الرئيسية لهذه المصالح إجراء عمليات البحث والتحري والتحقيق الشامل فيما يتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مما يضمن تغطية شاملة ومهنية لكافة القضايا الحديثة والمعقدة في هذا المجال. ومن بين أبرز هذه الوحدات المتخصصة، المخبر المركزي للشرطة العلمية، الذي يُعد مقرُّه بالعاصمة الجزائرية الركيزة الفنية والتقنية لتقديم الدعم الكامل في مسار التحقيقات وتحليل الأدلة الرقمية والتكنولوجية .تسهم هذه الهيكلية المتطورة في تعزيز الكفاءة وقدرة الأجهزة الأمنية على مواجهة التحديات الناجمة عن الجرائم المعلوماتية التي أصبحت تتطور بصفة مستمرة مع التطورات التكنولوجية المتسارعة.

ثانيا: على المستوى الجهوي

على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية ، تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية"[1]

والتي لم تكن عند استحداثها سنة 2004 سوى قسم، غير أنا لارتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الانتشار المتزايد لتقنية المعلومات ية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي :

1- قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

2- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

3- قسم تحليل الأصوات.

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم معناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الاطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلومات .[2]

ومن مهام هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الإلكترونية، وذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة والمعلومات الرقمية على مختلف أشكالها:

ملفات، رسائل الكترونية، برامج، صور ...، هذا البحث يتم عن طريق استعمال البرامج

ووسائل خاصة تمكننا من استرجاع كل المعطيات المحذوفة، والاطلاع على محتوى كل الوسائط الرقمية

[1] مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن نيابة مديرية الشرطة العلمية و التقنية – مديرية الشرطة القضائية– المديرية العامة لألمن الوطني – ص .03-02

[2] حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص.180

تلعب الوحدة دورًا حيويًا في الكشف عن أسرار الجرائم المعلوماتية من خلال الإجراءات المختلفة التي تقوم بها، سواء أثناء مرحلة البحث والتحري أو خلال مرحلة التحقيق القضائي.

في مرحلة البحث والتحري، يتعاون أعضاء الوحدة مع فرق مكافحة الجرائم المعلوماتية المنتشرة في مختلف مديريات الأمن الوطني لتلبية استجابة هؤلاء لطلبات عناصر الشرطة أو ما يُوجه إليهم من وكيل الجمهورية أو قاضي التحقيق على شكل أوامر قضائية، بهدف تقديم الدعم اللازم أثناء معاينة مسرح الجريمة وحجز الأدلة الموجودة .أما في مرحلة التحقيق القضائي، يقتصر دور الوحدة على الخبرة التقنية، حيث تقدم تقارير فنية استجابة لطلبات وكيل الجمهورية أو قاضي التحقيق .تُعِد هذه التقارير بناءً على تحليل الأدلة المحجوزة بهدف استخراج البيانات الإلكترونية منها .قد يشمل ذلك فحص محتويات الأقراص الصلبة لأجهزة الكمبيوتر المستخدمة في الجريمة، أو أجهزة الضحايا، بالإضافة إلى تحليل مختلف أنواع وأشكال وسائل التخزين الإلكترونية .تسعى هذه التحليلات إلى تحديد المواقع التي تم اختراقها وتحديد المواقع الجغرافية وعناوين المتورطين، باستخدام تقنيات مادية متطورة وحديثة ذات كفاءة عالية .وفي الختام، فإن المديرية العامة للأمن الوطني تُظهر اهتمامًا كبيرًا بمكافحة الجرائم المعلوماتية، ما يعكس التزامها بتعزيز الأمن الإلكتروني ومواجهة التحديات الناتجة عن التطورات التكنولوجية[1].

ثالثا: على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، خلقت المديرية العامة للأمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرائم المعلوماتية على مستوى مصالحها بأمن والولايات ، يتمثل دورها في تلقي الشكوى والبحث والحقيق في الجرائم المعلوماتية وتقريب الإدارة من المواطن.

---

[1] حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص.181

الفرع الثاني: الوحدات التابعة للدرك الوطني

تضع قيادة الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية وهي تباعا:

1قيادةالدركالوطنية

2.الوحداتالإقليمية.

3.الوحداتالمشكلة

4.الوحداتالمتخصصةوحداتالإسناد.

5.هياكلالتكوين.

6.المعهدالوطنيللأدلةالجنائيةوعلمالإجرام.

7.المصالحوالمراكزالعلميةوالتقنية.

8.المصلحةالمركزيةللتحرياتالجنائية.

9.المفرزةالخاصةللتدخل

تعملمؤسسةالدركالوطنيجادةإلىالتطلعبمختلفالجرائمالمرتكبةعلىشبكةالإنترنتوهذاالتسهيلمهمةالبحثوالمعاينةوالتفتيشفيأنظمةالحواسيبوالعملعلىمراقبةمختلفالشبكاتوبالتاليفقدتموضعمصالحالشرطةالقضائيةالتابعةللدركالوطنيفيخدمةهذهالأهداف،وذلكحسبالاختصاصوالصلاحياتوطبيعةالجريمةإلىثالث 03 مستوياتمركزية،جهوية،محلية[1].

[1]الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2019 – الرابط الإلكتروني:
http://www.mdn.dz/site_cgn/index.php?L=ar&p=undefined

أولا: علىالمستوىالمركزي:

تعملمصالحالدركالوطنيمنخلالأجهزتهاالمركزيةعلىمكافحةالجرائمالمعلوماتيةودعمأعمالالبحثوا لتحقيقبشأنهامنخلالالهيئاتالتالية:

1–مديرية الأمن العمومي والاستغلال: وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

2–المصلحة المركزية للتحريات الجنائية:وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال[1]

3–المعهد الوطني للأدلة الجنائية وعلم الإجرام: يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 04-183 بتاريخ: 26 جوان ،2004 في إطار عصرنة قطاع الدرك الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعاينة وذلك بمختلف دوائره، بما فيها دائرة الإعلامالآليوإلكترونيك، التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية، و ن الخدمة الأساسية التي يقدمها هذا المعهد في هذا الشأن – :القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة بما فيها تلك المتعلقة بالجرائم المعلوماتية.

–تطبيق مناهج تقنية وعلمية متقدمة في جمع وتحليل الأدلة المستخرجة من مسارح الجريمة.

– تأمين المساندة العلمية للتحقيقات المعقدة، وخصوصاً تلك المتعلقة بالجرائم الإلكترونية.

– المساهمة في الأبحاث والدراسات الوقائية بهدف تقليل معدلات الجريمة بجميع أشكالها، بما يشمل الجرائم المعلوماتية.

[1]معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – البيض – الجزائر.

يمثل المعهد الوطني للأدلة الجنائية وعلم الإجرام جهة محورية تُعنى بإجراء التحاليل وتقديم الخبرات في مجال علم الإجرام، وذلك ضمن إطار وضع استراتيجيات فعالة لمكافحة الجريمة[1]

4- مركز الوقاية من جرائم الإعلامالآلي والجرائم المعلوماتية:

تم تأسيس هذا المركز حديثًا ليصبح بمثابة نقطة الاتصال الوطنية في مجال دعم جهود البحث والتحقيق في الجرائم المعلوماتية .يضطلع المركز بتقديم الدعم التقني للمحققين، ويساهم بفعالية في توجيه مسارات التحقيق المتعلقة بتكنولوجيا المعلومات والاتصال .يتميز بطبيعته التقنية ويعمل تحت إشراف مديرية الأمن العمومي واستغلال الموارد التابعة لقيادة الدرك الوطني، مع تنفيذ المهام المسندة إليه بأعلى المستويات المهنية.

1-العمل على ضمان مراقبة دائمة ومستدامة لشبكة الإنترنت بهدف تعزيز الأمن الرقمي وتوفير حلول سريعة لأي تحديات تقنية أو أمنية قد تطرأ.

2-تنفيذ عمليات مراقبة دقيقة للاتصالات الإلكترونية وفق الأطر القانونية المحددة، بما يخدم احتياجات وحدات الدرك الوطني والجهات القضائية ويضمن احترام القوانين المعمول

3-تقديم الدعم اللازم للوحدات الإقليمية التابعة للدرك الوطني في مجال معاينة الجرائم المتعلقة بمجال تكنولوجيا الإعلام والاتصال، مع تسليط الضوء على جمع وتحليل الأدلة المتاحة عبر شبكة الإنترنت لتسريع عمليات التحقيق.

4-الإسهام في إجراء التحقيقات الأمنية والتحريات الإلكترونية عبر شبكة الإنترنت بما يعزز من فعالية وحدات الدرك الوطني ويدعم السلطات القضائية في كشف النشاطات المشبوهة ومكافحة الجرائم الإلكترونية بطريقة احترافية ومتكاملة.

[1]الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 مارس 2019 – الرابط الإلكتروني:

http://www.mdn.dz/site_cgn/index.php?L=ar&p=undefined

إذن تعتبر هذه الهيئات التابعة للدرك الوطني مسؤولة عن تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوم سناد ونقاط وصل بين مختلف اتية، وذلك على نطاق وطني بحيث تعتبر هيئات دعم الوحدات الأخرى المتخصصة والتي توجد كذلك على مستويات أدنى منها الجهوية والمحلية.

ثانياً :على المستوى الجهوي

تضطلع المصالح الجهوية التابعة للشرطة القضائية المنضوية تحت لواء الدرك الوطني بدور محوري يتمثل في التنسيق الفعّال بين مختلف الوحدات المتخصصة في مجال الشرطة القضائية .يُضاف إلى هذا الدور المهم تقديم الدعم اللازم لهذه الوحدات من خلال توفير الوسائل التقنية والخاصة التي تتيح تنفيذ التحريات والأبحاث المعقدة، لاسيما في المجالات المستجدة مثل الجرائم المعلوماتية التي تتطلب إمكانيات متقدمة ومهارات عالية .ويُبرز الدرك الوطني أهمية بارزة في ميدان الشرطة القضائية، وذلك بالنظر إلى الانتشار الجغرافي الواسع لوحداته الذي يغطي كامل التراب الوطني بلا استثناء .كما تُعزز مكانته الإمكانيات المادية الكبيرة المسخّرة لخدمته، بالإضافة إلى العدد الكبير من الأفراد المؤهلين الذين يساهمون بشكل فعال في أداء مهامهم المختلفة. لا يمكن تجاهل الصلاحيات القانونية الواسعة التي منحها القانون لعناصر الدرك الوطني، والتي تُفيد في تسهيل إنجاز مهامهم بشكل دقيق وفعّال. ويتوزع أفراد الدرك الوطني في الواقع، بناءً على رُتبهم ومهامهم الوظيفية، ضمن فئتين رئيسيتين هما ضباط وأعوان الشرطة القضائية، مما يبرز التدرج والتخصصية في أداء العمل[1].

ثالثا: على المستوى المحلي

يمتلك الدرك الوطني وحدات متخصصة تُعرف بفصائل الأبحاث، والتي تضم أفرادًا يتمتعون بخبرات متميزة ومهارات متقدمة في مجال الشرطة القضائية .تُعنى هذه الفصائل،

1حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص.180

على وجه الخصوص، بمواجهة ومكافحة الأنواع البارزة والخطيرة من الجرائم المنظمة، مثل الجرائم الإلكترونية التي تشكل تهديدًا متزايدًا .ويُنفَّذ ذلك من خلال إجراء تحقيقات دقيقة ومعمقة تتطلب أساليب بحث وتحري معقدة ومحترفة .تساهم هذه الوحدات ذات الطابع التخصصي في دعم وتعزيز جهود البحث والتحري التي تبذلها الفرق الإقليمية التابعة للدرك الوطني، مما يسهم في تحسين كفاءة العمليات وتوسيع نطاقها. وقد أتاح هذا النهج إنشاء خلايا متخصصة في مكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات داخل كل مجموعة ولائية، مما يعكس استجابة فعالة لمتطلبات العصر الحديث وتطور المنظومة التكنولوجية، ويضمن مواجهة فعالة لهذه التهديدات المتجددة بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير الخلايا المتخصصة في مجال أعمال البحث والتحقيق في هذا النوع من الجرائم [1]

المبحث الثاني: إجراءات القانونية التحري للكشف عن الجريمة المعلوماتية

1حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص.180

تنقسم الإجراءات القانونية من أجل الكشف عن الجريمة المعلوماتية الى إجراءات كلاسيكية وهذا ماسنتطرق إيه في المطلب الأول،وإجراءات حديثة للكشف عن الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية

تتمثل إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية في جميع الإجراءات التي يمكن إيجادها في الجرائم التقليدية وهي المعاينة والتفتيش، وعليه سوف نبرز هذه إجراءات فيما يلي:

الفرع الأول: معاينة مسرح جرائم الماسة بأنظمة المعلوماتية

عندالحديثعنالإجراءاتالتقليديةللتحريبهدفالكشفعنالجرائمالمعلوماتية،فإنالخطوةالأولىتتمثلفيمعاينةمسرحالجريمةالمعلوماتية. يشيرهذاالمفهومإلىالإجراء

فحص ميداني يتضمن مراقبة وتحديد حالة مكانٍ معين أو شخصٍ أو شيءٍ ما بهدف التحقق من حالته الراهنة، وضبط كل ما يمكن أن يسهم في استجلاء الحقيقة[1].هذا الإجراء يُعتبر وسيلةً هامة لتوثيق حالة المواقع أو الأشخاص وكل ما يمكن أن يكون له دور في كشف ملابسات الحقيقة . تستلزم هذه المعاينة انتقال ضابط الشرطة القضائية إلى الموقع المحدد لإجراء الفحص الميداني، حيث يعمل على توثيق ووصف الوضع القائم للمكان وكل ما يحتويه من أشخاص أو أشياء يمكن أن تعين على توضيح الحقيقة، بهدف كشف طبيعة الجريمة موضوع التحقيق.

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات بما فيها التشريع الجزائري في المادة 61 من قانون الإجراءات الجزائية الجزائري، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراء وجوبيا في الجنايات وجوازي في الجنح، وهي قد تتم في مكان عام أو مكان خاص، فإذا كانت في

[1] حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص.180

مكان عام؛ الضابط الشرطة القضائية ال يحتاج إلى إذن من النيابة العامة بإجرائها، أما إذا كانت بمكان خاص؛ فلابد لصحتها، من رضا صاحب المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.ولمعاينة مسرح الجرائم المعلوماتية، يجب التفرقة بين حالتين:

أولا: معاينة الجرائم الواقعة على المكو نات المادية للحاسوبHardware

.تُعتبر مكونات الحاسوب ذات الطابع المادي والمحسوس، مثل شاشة العرض، ومفاتيح التشغيل، والأقراص، وغيرها من الأجزاء الملموسة، من العناصر التي لا تشكل أي تعقيد يُذكر عند التعامل معها .فهي تسمح لضابط الشرطة القضائية بإجراء عمليات المعاينة بسهولة والاحتفاظ بما يلزم من أشياء تُصنَّف كأدلة مادية تُسهم في كشف ملابسات الجريمة وتقديم الدعم لتحقيق العدالة.

ثانيا :تحليل ومعاينة الجرائم المتعلقة بالمكونات الرقمية غير المادية أو المرتبطة باستخدامهاsoftware

مثل الجرائم التي تستهدف برامج الحاسوب وبياناته، تُعدُّ من القضايا التي تثير إشكاليات متعددة معقدة .هذه الإشكاليات تتسبب في إعاقة فعاليات عملية المعاينة وتُحدُّ من فائدتها المرجوة، ويمكن إبراز أهم التحديات التي تواجه هذا النوع من الجرائم فيما يلي – :الصعوبة الأولى تكمن في كون الجرائم التي تستهدف المكونات غير المادية للحاسوب لا تخلف عادة آثاراً مادية واضحة يمكن الاستدلال عليها أو جمعها بسهولة .فالمكونات البرمجية بطبيعتها ليست ملموسة، مما يجعل عملية تحليل مسرح الجريمة ومكوناته أكثر تعقيداً – .التحدي الثاني يتمثل في العدد الكبير من الأفراد الذين قد يمرون بمسرح الجريمة خلال الفترة الزمنية الفاصلة بين وقوع الجريمة واكتشافها.

غالباً ما تمتد هذه الفترة لفترة طويلة، وهو ما يتيح فرصة كبيرة لتعديل الموقع، أو العبث بالآثار التي يمكن أن تكون حيوية في التحقيق .قد يؤدي ذلك إلى تشويه الأدلة الرقمية المرتبطة بالحاسوب أو حتى فقدانها بالكامل، مما يسهم بشكل كبير في تعقيد عملية التعرف على وقائع الجريمة وتحديد المسؤولين عنها .

أما لإنجاح عملية المعاينة والتحقيق الفعال في الجرائم المتصلة بالمعلوماتية، فإن الخبراء يقدمون مجموعة من التوصيات التقنية والإرشادات الواجب اتباعها لضمان تحقيق أفضل النتائج وتجنب خسارة الأدلة. من أبرز هذه الإرشادات:

– يجب توثيق الأجهزة الإلكترونية ذات العلاقة توثيقاً كاملاً ودقيقاً. يتضمن ذلك تصوير جهاز الحاسوب وما يتصل به من أدوات أو أجهزة ظرفية أخرى، وتوثيق محتوياته بالكامل. كما ينبغي أن يشمل التصوير مسرح الجريمة بشكل عام، مع إيلاء اهتمام خاص للأجزاء الخلفية للأجهزة وكافة ملحقاتها، لتجنب إغفال أي تفاصيل قد تكون ذات أهمية.

– يُوصى أيضاً بتسجيل معلومات شاملة حول الزمان والمكان لكل صورة يتم التقاطها .هذه التفاصيل الزمنية والمكانية تُعتبر مهمة لتحليل تسلسل الأحداث وربط الأدلة بالسياق الزمني للجريمة، مما يساعد في تعزيز مصداقية الأدلة وتحقيق رؤية متكاملة للأحداث .وباختصار، فإن التعامل مع الجرائم الرقمية يتطلب مستوى عالياً من الدقة والحرص، واتباع قواعد تقنية صارمة لضمان الحفاظ على الأدلة والاستفادة منها في كشف ملابسات الجرائم والدعوة إلى تحقيق العدالة

– ينبغي توثيق وفحص حالة توصيل الكابلات الكهربائية الخاصة بالحاسوب، والتي ترتبط بمكونات النظام، لتسهيل عملية المقارنة والتحليل عند تقديم الموضوع أمام المحكمة.

– ضرورة التريّث قبل نقل أي مادة معلوماتية من موقع الجريمة، لضمان إجراء الاختبارات اللازمة والتأكد من عدم وجود أي حقول مغناطيسية في البيئة المحيطة .هذا الإجراء يهدف إلى حماية البيانات المخزنة ومنع أي تلف أو حذف للمعلومات المسجلة.

–إعداد مخطط تفصيلي شامل للمنشأة التي وقعت فيها الجريمة يعد خطوة أساسية لفهم الوضع وتحليل الأحداث. يتضمن هذا المخطط رسمًا دقيقًا ومُفصّلاً للمنشأة يوضح توزيع المواقع والمرافق بداخلها، بالإضافة إلى تحديد الأماكن الرئيسية التي ترتبط مباشرة بالجريمة. بالإضافة إلى ذلك، يجب إعداد كشف مفصل يُدرج أسماء جميع المسؤولين المرتبطين بالمنشأة، مع توضيح الأدوار والمهام الموكلة لكل فرد منهم، وذلك لضمان التحديد الدقيق للمسؤوليات .يهدف هذا الإجراء

الشامل إلى تقديم تصور واضح ومتكامل يعزز من عملية التحقيق ويوفر مرجعية يمكن الاعتماد عليها لتحليل الأحداث وربط المعلومات المتعلقة بالجريمة بشكل منهجي ومنظم[1]

الفرع الثاني: تفتيش الأنظمة المعالجة الآلية للمعطيات وضبطها

يهدف التفتيش في الأساس إلى ضبط الأدلة المادية التي يمكن أن تسهم في كشف ملابسات الجريمة وبيان حقيقتها. يتمثل جوهر هذا الإجراء في الحصول على المصادر التي ترتبط بشكل مباشر بالجريمة، مما يجعل كل ما يتم ضبطه أو مصادرته من قبل ضابط الشرطة القضائية بعد إجراء عملية التفتيش يمثل الأثر المباشر لعملية التفتيش ذاتها .عليه، فإن عملية الضبط لا تقتصر على كونها مجرد إجراء تكميلي، بل هي جزء محوري وأساسي من إجراءات التحقيق الجنائي، خاصة فيما يتعلق بالجرائم المعلوماتية .يتمثل ذلك في السيطرة الفعلية على الأدلة المتعلقة بالجريمة وحجزها كمصدر موثوق للمعلومات والتحقق منها، إلى جانب المحافظة عليها لضمان عدم المساس بها حتى يُستفاد منها في سياق التحقيق[2]. تتجلى الأهمية الكبرى لهذه العملية في تعزيز الجهود الرامية لتحصيل دليل قوي يدعم سير التحقيقات ويثري الأدلة المتاحة للوصول إلى الحقيقة. الهدف الرئيسي من ذلك هو توثيق واقعة معينة يمكن الركون إليها قانونيا واستعمالها أمام القضاء بما يخدم مصلحة التحقيق بطريقة موثوقة وعادلة .سنقوم في الأقسام التالية بإبراز الجوانب المختلفة لهذه العملية والتفصيل في مدى تأثيرها وكفاءتها في دعم السعي وراء العدالة.

---

[1]طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر،1 ،2012-2011ص .131

[2]يمثل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المادية: وهي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة، وحدة الحاسوب والمنطق، الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة، أنظر: طارق إبراهيم الدسوقي عطية، امن المعلوماتي ، دار الشر الجديدة الإسكندرية، سنة ،2009 ص 441

اولاً :تفتيش أنظمة المعلوماتية

يُقصد بعملية التفتيش هنا فحص المكونات المادية وأنواعها المختلفة بهدف العثور على أي دليل يتعلق بجريمة معلوماتية وكشف حقيقتها .هذا النوع من التفتيش يتم ضمن إطار التفتيش التقليدي وفقاً للإجراءات القانونية السارية .إلا أن هناك حالات خاصة تستدعي أساليب تفتيش محددة لهذه المكونات، وأبرزها :

الحالة الأولى:عندما تكون هذه المكونات موجودة في مكان خاص، كالمنزل الخاص بالمتهم أو أحد ملحقاته .في هذه الحالة، تُطبق القواعد المطبقة على تفتيش المسكن، مع الالتزام بجميع الضمانات القانونية المعمول بها في التشريعات المختلفة.

الحالة الثانية :إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن[1].

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية في حالة الحواسيب الآلية المحمولة في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها ال يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات.

ثانيا :تفتيش نظم الحاسوب المنطقية أو المعنوية

يعرف الكيان المنطقي للحاسوب بأنه: ''مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات ".وقد حذا المشرع الجزائري في المادة 47 الفقرة

[1]طرشي نورة، المرجع السابق، ص .115-

الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: ''إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليال أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك[1]''.

ثالثا :القواعد الشكلية لتفتيش نظم المعلوماتية

أ- إجراء التفتيش بحضور أشخاص معينين بالقانون: من بين هذه الأشخاص المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية-القائم بالتفتيش-ا ذا تعذر ، حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة45 من قانون الإجراءات الجزائية الجزائري، على أنه: "ال تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات."

ب- إعداد محضر خاص بالتفتيش: عملية إعداد محضر خاص بعملية التفتيش تعد خطوة ضرورية وأساسية لضمان توثيق كل ما يحدث خلال إجراء التفتيش، وهي تتطلب تكليف الشخص المسؤول عن التفتيش بمهمة محددة تتضمن اصطحاب كاتب مختص .يقوم هذا الكاتب بتولي مهمة تدوين محضر متكامل وشامل يشتمل على جميع الأحداث والوقائع التي يتم رصدها أثناء التفتيش بالتفصيل الدقيق. يتم تسجيل هذه الوقائع بشكل منظم ودقيق بما يشمل كافة البيانات المتعلقة بعملية التفتيش، مع الإشارة إلى الأشياء والوثائق التي يتم ضبطها .يجب أن يتسم المحضر بالشفافية والمصداقية، حيث تمثل هذه التفاصيل عنصراً رئيسياً لضمان توثيق العملية بأعلى

[1]طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة الإسكندرية، سنة ،2009 ص385.

درجات الأمانة والتدقيق، وذلك بهدف الحفاظ على النزاهة وتحقيق العدالة في كافة مراحل التحقيق.

ت– إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده:تعد إجراءات تنفيذ عمليات التفتيش على نظم الحاسوب الآلي ذات طبيعة خاصة وفريدة تميزها عن غيرها من العمليات، وذلك نظراً للحساسية العالية التي تنطوي عليها عند التعامل مع الأجهزة الإلكترونية والبرامج المثبتة عليها . ولضمان تنفيذ هذه الإجراءات بأعلى درجات الدقة والكفاءة، يجب أولاً تحديد نوع النظام المستهدف بالتفتيش بشكل دقيق ومحدد .هذا الأمر يتطلب أن يتمتع المسؤول عن عملية التفتيش بخلفية معرفية واسعة وإلمام شامل بمفاهيم وتقنيات علوم الحوسبة والمعلوماتية، مما يتيح له القدرة على فهم وإدراك تفاصيل النظم التي سيتم تفتيشها بشكل عميق. بالإضافة إلى ذلك، من الضروري، في كثير من الأحيان، اللجوء إلى الخبراء المتخصصين في النظام المحدد والاستعانة بهم للإسهام الفعال في عملية تنفيذ التفتيش. هؤلاء الخبراء يمكنهم تقديم الدعم والاستشارة الفنية التي تعزز من جودة ونجاح العملية .وبالتالي، تتضمن هذه الإجراءات مزيجاً متكاملاً من التخطيط المدروس والتعاون المهني بين الفِرق، بما يضمن تنفيذ التفتيش بصورة احترافية تحقق الأهداف المرجوة بأعلى مستوى من الدقة والفاعليةومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي.

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

- ضرورة اتخاذ التدابير اللازمة لتأمين وحماية مسرح الجريمة، وذلك يشمل ضمان فصل التيار الكهربائي عن الموقع المستهدف بالمعاينة .كما يتعين تعطيل أي أجهزة تدعم الشبكة الإلكترونية المرتبطة بالمكان، بهدف إيقاف قدرة الجاني على التدخل أو تنفيذ أي تصرف قد يؤثر على الأدلة والبصمات المتواجدة في موقع الجريمة، وبالتالي حماية سلامة التحقيق.

- إبعاد المتهم عن موقع النظام في حال كان يتواجد على مقربة منه، وذلك بهدف ضمان سلامة الإجراءات وتحقيق الحيادية الكاملة خلال سير التحقيقات أو اتخاذ القرارات المتعلقة بالقضية.
- تجنب تماماً لمس لوحة المفاتيح، لأن القيام بذلك قد يؤدي إلى الحاجة لاستخدام برامج إضافية قد تكون إما معقدة في التعامل أو غير موثوقة وتحتوي على عناصر احتيالية، مما يزيد من مخاطر الاستخدام ويُعقد العملية بشكل غير مرغوب فيه.

المطلب الثاني :إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية

في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون 06/22 المؤرخ في 20/12/2006 الذي جاء فيه إجراءات مستحدثة للكشف عن للجرائم الماسة بأنظمة المعالجة للمعطيات وهي:

الفرع الأول: الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

منح المشرع الجزائري ضباط الشرطة القضائية صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كجزء من التدابير التي تهدف إلى الكشف عن الجرائم المرتبطة بالمجال المعلوماتي . وتُنفَّذ هذه الإجراءات بأسلوب سري يهدف إلى تعزيز فعاليتها في مواجهة هذه الجرائم .ومع ذلك، يثير هذا التفويض جدلاً واسعاً بسبب تعارضه الظاهر مع القوانين والنصوص المعتمدة التي تضمن حماية الحق في الخصوصية والحياة الشخصية، مما يفتح مجالاً لمناقشات حول التوازن بين الأمن العام واحترام الحقوق الفردية.[1]

تصوير الأشخاص، سواء كان فردًا أو مجموعة، عادةً يتم من خلال التقاط صور لهم أثناء وجودهم في أماكن خاصة أو عامة .يُستخدم هذا النوع من الوسائل بشكل متزايد في العديد من البيئات، بما في ذلك المناطق السكنية والمرافق الخاصة والعامة، لأغراض متعددة، بعضها قد يكون مشروعًا والآخر يحتمل أن يستثير الجدل حول المساس بالخصوصية .أما فيما يتعلق بتسجيل الأصوات،

فيتم ذلك بطرق متنوعة وبتقنيات متطورة .إحدى هذه الطرق تشمل مراقبة الهواتف وتسجيل المحادثات التي تُجرى عبرها، كما أن هناك وسائل أخرى تعتمد على استخدام ميكروفونات متقدمة تمتاز بحساسيتها العالية، مما يسمح لها بالتقاط أدق الأصوات وتحويلها إلى تسجيلات محفوظة بأجهزة متخصصة. بالإضافة إلى ذلك، قد تتم عملية التسجيل من خلال التقاط إشارات الاتصال السلكي أو موجات الإرسال الإذاعي، وهي وسائل تطورت لتصبح أكثر كفاءة وأسهل استخدامًا في مختلف الظروف.

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 09/04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلاموالاتصال ومكافحتها ، أنه: ”مع مراعاة الأحكام القانونية التي تخص سرية المراسلاتوالاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

اضافة إلى أن القاعدة القانونية الأساسية تنص على أن كل متهم بريء حتى تثبت إدانته بحكم قضائي نهائي، يبرز تساؤل مشروع حول مدى جواز اللجوء إلى وسائل تقنية مثل التسجيل الصوتي، أو اعتراض المراسلات الإلكترونية، أو حتى التقاط الصور في الأماكن العامة أو الخاصة، بهدف إثبات أو نفي الاتهام الموجه إلى المشتبه فيه .هذه الوسائل، رغم فعاليتها المحتملة في جمع الأدلة، تثير جدلاً واسعاً، ليس فقط لأنها قد تتعدى على خصوصيات المتهم، بل قد تمس أيضاً بالأشخاص المحيطين به

من أقارب أو أصدقاء أو زملاء .فيما يتعلق بالجانب القانوني والإجراءات المتبعة، يفرق الفقه القانوني بين مصطلحين رئيسيين: اعتراض المكالمات الهاتفية ومراقبة الخط الهاتفي. في الحالة الأولى،

يتم اعتراض المكالمات دون علم أو موافقة الطرف المعني، مما يمثل تعدياً محتملاً على حرمة الخصوصية الشخصية. أما في الحالة الثانية، فإن مراقبة الخط الهاتفي تتم بموافقة مسبقة من صاحبه، أو بناءً على طلب واضح منه. ومع ذلك، يخضع كلا الإجراءين عادةً لسلطة الهيئة القضائية التي تقوم بمراجعة طلب الرقابة الهاتفية بعناية والتأكد من استيفاء الشروط القانونية اللازمة. كما يتم تحقيق ذلك من خلال تسخير التعاون مع الجهات المختصة مثل مصالح البريد والاتصالات .هذه القضايا تفتح الباب أمام نقاش أوسع يتعلق بالتوازن بين حق الفرد في الخصوصية وبين مصلحة العدالة العامة في الوصول إلى الحقائق وإنفاذ القانون بطرق تتسم بالشرعية والإنصاف .لذلك، يبقى السؤال المطروح حول ضرورة الالتزام بمعايير دقيقة وشروط صارمة عند استخدام هذه الوسائل التقنية، لضمان عدم تجاوز الحدود المشروعة وحماية حقوق الأطراف كافة

ويعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية .لكن مع ذلك، نجد المشرع حاول يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط والت ازم أعوان وضباط الشرطة القضائية القائمين وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، بالإجراء السر المهني، وفيما يلي نتولى شرح كال الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة ، وهو ما سنشير إليه على النحو التالي[1]:

أولا: مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 09/04 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة".ينبغي أن يحتوي الإذن الصادر للقيام بعمليات التقاط الاتصالات على مجموعة من العناصر البالغة الأهمية التي تسهل التمييز والتعرف على الاتصالات المستهدفة. يشمل ذلك تحديد الأماكن المقصودة، سواء كانت هذه الأماكن ذات طبيعة سكنية أو غير سكنية. كما يلزم الإذن بتوضيح نوع الجريمة التي استوجبت اتخاذ مثل هذه التدابير الاستثنائية، بالإضافة إلى تحديد المدة الزمنية التي ستستغرقها هذه الإجراءات. على هذا النحو، لا يمكن استخدام الإذن الصادر من وكيل الجمهورية لغايات التحقيق في جريمة معينة لتبرير التحقيق في جريمة أخرى ما لم يتم إصدار إذن جديد يلائم تلك الحالة، كما يجب أن يوضح الإذن جميع الأماكن التي سيتم فيها وضع الأجهزة التقنية اللازمة لتنفيذ عملية التقاط وتسجيل المحادثات الصوتية بدقة متناهية سواء كانت تلك المحادثات تتم من قِبَل شخص واحد أو تتضمن عدة أشخاص .خلال مباشرة أعمال التحريات أو التحقيقات، يقوم ضابط الشرطة القضائية الذي حصل على الإذن أو الذي عُهد إليه من قبل القاضي المختص بتحرير تقرير مفصل بشأن كل عملية تتم لاعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور. يتناول التقرير كذلك تفاصيل وضع الأجهزة التقنية وعمليات الالتقاط والتسجيل، سواء كان ذلك صوتيًا أو مرئيًا .ويجب أن يتضمن هذا المحضر تواريخ وأوقات دقيقة لبداية ونهاية كل عملية، ما يضمن وضوحًا لا لبس فيه بشأن البيانات والمعلومات المدونة . تُعد هذه الدقة ضرورية لضمان موثوقية الوثائق، ويُوقع محرر المحضر في نهايته كإجراء رسمي يؤكد صحته .عقب ذلك، يقوم ضابط الشرطة القضائية المخوَّل أو المكلف بمراجعة وتصنيف المراسلات أو الصور أو التسجيلات الصوتية واختيار ما يمكن أن يوفر أدلة مفيدة تُسهم في توضيح الحقيقة .

يتم تضمين هذه المواد في ملف القضية المتعلقة بالمتهم .في حال كانت هناك محادثات أو مكالمات تتم بلغات أجنبية، فإنه يتم نسخها وترجمتها باستخدام مختص يُكلف خصيصًا لهذا الغرض، لضمان استيعاب كامل ودقيق لجميع المحتويات ذات الصلة بمجرى التحقيق

ثانيًا :الالتزام بالسر المهني

.1تُعتبر إجراءات التحري والتحقيق ذات طبيعة سرية، ويأتي هذا الالتزام كجزء من الضمانات الممنوحة للمتهم .السرية هنا تعني أن كل من يضطلع بالتحري أو يُكلّف بإجراءات التحقيق أو يساهم فيها مُلزم بحفظ السر المهني بالحد الأقصى الممكن

.2 .لم تعد السرية هدفًا لإضعاف موقف المتهم أو تضييق الخناق عليه كما كان يُعتقد سابقًا، بل أصبحت أداة أساسية لحماية الحريات الفردية .

.3المشرّع أكد بشكل واضح على أن هذه الإجراءات يجب أن تتم مع احترام مبدأ السر المهني، بحيث لا يُعتدى عليه بأي شكل .فالضابط المكلف بمهمات مثل اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، ملتزم قانونيًا بعدم إفشاء ما اطلع عليه .

.4يُلزم القانون باتخاذ التدابير اللازمة لضمان الحفاظ على السر، وقد نص قانون الإجراءات الجزائية على الطبيعة السرية لهذه العمليات، إلا في الحالات التي يُحدد فيها القانون خلاف ذلك، شريطة أن لا يتم المساس بحقوق الدفاع.

.5 كل من يشارك في هذه الإجراءات مُلزم بحفظ السر المهني وفقًا للشروط المحددة في قانون العقوبات، حيث يُواجه عقوبات صارمة إن تم انتهاك هذا المبدأ.

على هذا النحو، تُجرى عمليات التحري عن الجرائم المتعلقة بأنظمة معالجة المعطيات الآلية في إطار من السرية المطلقة .يُمنع تمامًا إبلاغ المشتبه به أو أي شخص آخر بتلك التحريات .كما يُحظر على الضباط المأذون لهم أو المكلفين الكشف عن محتوى محاضر التحريات لأي جهة كانت، وإلا تعرّضوا للمساءلة الجنائية بتهمة إفشاء السر المهني .من هنا، يصبح واجبًا على ضباط الشرطة

القضائية وفرق العمل تحت إشرافهم ألا ينقلوا أو يكشفوا عن أي معلومات حصلوا عليها أثناء أداء مهماتهم، حفاظًا على سمعة المواطنين التي يجب ألا تبقى عرضة لأية بيانات غير مؤكدة

الفرع الثاني :آلية التسرب أو الاختراق

تعد تقنية التسرب واحدة من الابتكارات القانونية التي أضافها المشرّع الجزائري عند تعديل قانون الإجراءات الجزائية في عام 2006، وذلك لمواجهة الضرورات التي تفرضها عملية التحري والتحقيق في الجرائم المحددة بالمادة (65 مكرر 5)ومنح القانون وكيل الجمهورية الصلاحية تحت إشرافه المباشر للإذن بتنفيذ عملية التسرب، شرط الالتزام بمجموعة من الشروط الدقيقة .يتعين على الضابط المكلف بالتسرب الحصول على إذن كتابي من وكيل الجمهورية المختص، بحيث تُنفذ العملية تحت رقابته ومتابعته المستمرة. وإذا قرر ضابط الشرطة القضائية مباشرة هذه الإجراءات، يتوجب عليه بدايةً إخطار وكيل الجمهورية وإعداد إذن مكتوب يشمل جميع التفاصيل المتعلقة بعملية التسرب .بالإضافة إلى ذلك، يجب أن يُوضح الإذن هوية ضابط الشرطة القضائية المسؤول عن تنسيق العملية. يُعتبر غياب الإذن الكتابي الذي يستوفي التزامات القانون سببًا للبطلان المطلق، حيث يصبح الإجراء باطلاً قانونياً .أما بخصوص عملية التسرب، فهي تقوم على مبدأ اندماج ضابط أو عون الشرطة القضائية بتوجيه مباشر من ضابط الشرطة القضائية المسؤول عن التنسيق، بهدف إيهام المشتبه بهم بأنه جزء منهم

أو شريك في أنشطتهم الإجرامية .وعليه، يُكلَّف المأذون له بإجراء عملية الاختراق بمراقبة المشتبه فيهم وتوثيق تحركاتهم، أو التوغل في جماعاتهم لإقناعهم بأنه أحد أفرادها، مما يتيح كشف أنشطتهم الإجرامية عن قرب .لضمان فعالية العملية، يُسمح لضباط وأعوان الشرطة القضائية باتخاذ هوية مستعارة واستخدامها أثناء عملية التسرب. بل ويمكن لهم، إذا دعت الضرورة القصوى، ارتكاب بعض الجرائم المرتبطة بالعملية دون أن تترتب عليهم أي مساءلة جنائية .وتأتي هذه الاستثناءات لضمان تحقيق الهدف الأساسي من التسرب، وهو مراقبة المشتبه فيهم وتفكيك أنشطتهم الإجرامية مع الالتزام التام بإخفاء الهوية الحقيقية لضمان نجاح المهمة بأعلى درجات الكفاءة

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال.

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسبابإلا لرؤسائهم السلميين، لان هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة 65(مكرر 16) بأن نصت صراحة أنه:"لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات ".كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى واذا تسبب الكشف عن الهوية في أعمال خمس سنو ات وبغرامة من 50000 دج إلى 2000000 دج، عنف أو ضرب وجرح أحد هؤلاءالأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغرامة من 200000 دج إلى 500000 واذا تسبب هذا دج، الكشف في وفاة أحد هؤلاءالأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500000 إلى 1000000 دج .

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم و النجاحّ يحرضوا المشتبه في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان

المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه الارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

خلاصة الفصل

ما سبق تم التطرق في هذا الفصل الى الأجهزة المختصة المكافحة للجريمة المعلوماتية متمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال، الأجهزةالأمنية سواء الامن الوطني أو الدرك الوطني سواء على المستوى الوطني أو الجهوي أو المحلي، ثم بعد ذلك تم التطرق الى الإجراءات القانونية للتحري من أجل الكشف ومكافحة الجريمة المعلوماتية، التي تكمن المحقق من التعرف على الجاني وتوقيفه وتقديمه أمام النيابة العامة لأخذ جزاءه.

خاتمة

الخاتمة

يتضح من خلال ما تم استعراضه وتحليله سابقًا أن الجريمة المعلوماتية تعتبر من أبرز القضايا الحساسة والمعقدة في العصر الحديث، وذلك نظرًا لخطورتها المتزايدة وتأثيرها المدمر على مختلف الأصعدة الاجتماعية والاقتصادية وحتى الأمنية .لهذا السبب، تستدعي دراسة هذه الظاهرة اهتمامًا كبيرًا ومعمقًا لفهم آلياتها وتعقيداتها بشكل أفضل، وهو ما دفع الجهات المعنية للتصدي لها من خلال اعتماد عدة تدابير وقوانين لمكافحتها على الصعيد الوطني. في هذا السياق، كان المشرع الجزائري سبّاقًا في إدراك الحاجة إلى سد الفجوة التشريعية المتعلقة بمواجهة الجرائم المعلوماتية، حيث بادر إلى تعديل النصوص القانونية ذات الصلة ولا سيما قانون العقوبات .كما عمل على إصدار قانون خاص تحت رقم 04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كل ذلك بهدف تقليص انتشار هذه الجرائم التي باتت عابرة للحدود بفعل الطبيعة الرقمية التي تميزها .من خلال الدراسة والتحليل، يمكن تلخيص أبرز النتائج المستخلصة على النحو التالي:

1.تعد الجرائم المعلوماتية واحدة من الجرائم المستحدثة التي تمثل تحديًا عالميًا بسبب طبيعتها العابرة للحدود، ما يجعل التعاون الدولي عنصرًا أساسيًا لمواجهتها .

2.تختلف الجرائم المعلوماتية عن الجرائم التقليدية بصفات فريدة، حيث تتميز بصعوبة كشفها وإثباتها مقارنة بالجرائم التقليدية، وهو ما يسهم في قلة حالات الإبلاغ عنها

3.لا تتطلب الجرائم المعلوماتية استخدام العنف التقليدي؛ بل تعتمد على الحنكة والذكاء وسرعة التنفيذ والمهارة العالية في التعامل مع التكنولوجيا الحديثة، وهو ما يجعل المجرم المعلوماتي شخصية متميزة بهذا المجال.

4.تتشابه الجرائم المعلوماتية مع غيرها من الجرائم من حيث وجود القصد الجنائي، ولكنها تتطلب تخصصًا إضافيًا لفهم دوافع مرتكبيها وطرق تنفيذها .

5.بادرت الدولة الجزائرية إلى اتخاذ خطوات قانونية سريعة وفعالة من أجل التصدي لهذه النوعية من الجرائم وذلك من خلال إصدار قوانين رادعة وتسخير الموارد البشرية المدربة والمتخصصة بهدف الحفاظ على الأمن العام وحماية المواطنين من آثار هذه الآفة الرقمية .

6.أظهر المشرع الجزائري وعيًا متزايدًا تجاه خطورة الجرائم المعلوماتية من خلال إجراء تعديلات شاملة في القوانين الوطنية مثل قانون العقوبات وقانون الإجراءات الجزائية بالإضافة إلى إصدار قانون 09/04 .ومع ذلك، فإن هذه الجهود، رغم أهميتها، لا تزال بحاجة إلى مزيد من التطوير والتعزيز لمواكبة النمو المتسارع لهذا النوع العصري والمتجدد من الجرائم .يتطلب هذا الموضوع اهتمامًا مستمرًا ومرونة تشريعية وتقنية لمواكبة التغيرات السريعة في مجال التكنولوجيا الرقمية والاتصالات، مما يساعد على سد الثغرات القانونية وتقليل فرص استغلالها من قبل المجرمين الرقميين.

اما فيما يتعلق بالاقتراحات التي يمكن تقديمها لمعالجة التحديات المتعلقة بجرائم المعلوماتية، فإنه يمكن تلخيصها على النحو التالي :

أولا: نقترح من وجهة نظرنا أن يقوم المشرع بوضع تعريف قانوني واضح ومحدد لهذا النمط الجديد والمستجد من الجرائم الإلكترونية .بالنظر إلى تسارع انتشاره وتزايد مخاطره، يصبح من الضروري تعريفه بشكل دقيق، بحيث تتم الإشارة إلى طبيعته ونوعيته، لتجنب الوقوع في الأخطاء عند التكييف القانوني لهذه الجرائم والمعالجة القانونية لها

ثانيا:ضرورة تطوير المشرع لمنظومة التشريعات القانونية بما يتماشى مع التطورات المتزايدة والمتلاحقة في هذا النوع من الجرائم .فالتقنيات الحديثة المستخدمة في ارتكاب هذه الجرائم تتطلب منظومة تشريعية مرنة تواكب التحولات الرقمية السريعة

ثالثا: إنشاء أقسام متخصصة داخل المؤسسات القضائية والأمنية تعنى بالجرائم المعلوماتية. وجود جهات مختصة يقدم إطارًا أكثر كفاءة لمكافحة هذه الجرائم .

رابعا: تخصيص قوة شرطة جنائية مؤهلة، تضم خبراء ومتخصصين في مجال الإنترنت والبيانات الرقمية. إن وجود كفاءات مدربة ومتمرسة يساهم في تحسين قدرة السلطات على مكافحة هذه الجرائم بكفاءة عالية .

خامسا: ينبغي على المشرع أن يستثمر في توفير وسائل وأجهزة حديثة ومتطورة لأغراض التحقيق والقمع الفعال للجرائم المعلوماتية. توفير هذه الموارد التقنية المتقدمة سيساعد بشكل كبير في تتبع الجريمة وحل ألغازها

سادسا: أهمية السعي لعقد اتفاقيات دولية تتعلق بالجرائم المعلوماتية، والعمل على تعزيز التعاون الدولي لملاحقة مرتكبي هذه الجرائم العابرة للحدود .هذا التعاون سيتيح للدول مواجهة التحديات المشتركة بروح تكاملية

سابعا: قيام السلطات المختصة بزيادة حملات التوعية الشاملة التي تستهدف الأفراد والمجتمع ككل لرفع مستوى الوعي بخطورة هذه الجرائم وطرق تجنب الوقوع ضحية لها. هذه الحملات ستكون أداة فعالة لتمكين المواطنين من اتخاذ الحيطة والحذر .وعلى ضوء ما تم الإشارة إليه، يمكن استخلاص أن جريمة المعلوماتية هي بطبيعتها جريمة معقدة وعابرة للحدود، مما يجعل إثباتها أمرًا صعبًا في كثير من الحالات. لذا نقترح أن يتم إجراء دراسات معمقة مستقبلية تتناول رؤية المشرع الجزائري لهذه الظاهرة الإجرامية مقارنة بالتشريعات المعمول بها في الدول العربية والغربية. إضافة إلى دراسة مدى مساهمة الجهود الدولية المبذولة للقضاء على هذه الجرائم وتحقيق العدالة .في الختام، أرجو أن أكون قد وفقت في معالجة الموضوع بما يليق بأهميته وحجمه. فإن أصبت فهذا من توفيق الله، وإن أخطأت فلكل مجتهد نصيب.

قائمة المصادر والمراجع

أولا: المصادر

1_**القوانين:**

_القوانين العادية:

1-أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية 2006

2-أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014

3-آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007

4-أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004

5-بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007

6-خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010

7-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007

8- كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000

9-محمد أمين احمد الشوابكة، جرائم الحاسوب الأولىوالإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004

10-محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009

11-محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008

12-محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، سنة 2008.

13-منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

14-نهال عبد القادر المومني، الجر ائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع .

15-هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهر ة، 1992.

16-هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، .

القوانين والاوامر :

1-دستور 1996

2-القانون رقم 15-04 مؤرخ في 10 نوفمبر،2004 يتضمن تعديل قانون العقوبات .

3-القانون رقم 06/23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية

4-القانون رقم 04-09 المؤرخ في 05 اوت ،2009 يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلاموالاتصال ومكافحتها .

5-المرسوم الرئاسي 261-15 الذي يحدد تشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلاموالاتصال ومكافحتها.

المواقع الأنترنت :

الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 مار س 2019 – الرابط

http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined:

الإلكتروني

.

فهرس المحتويات