الجمهورية الجزائرية الديمقراطية الشعبية

People's democratic republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of higher education and scientific research

جامعة محمد البشير الإبراهيمي - برج بوعريريج –

University Of Mohamed Al- Bachir Al -Ibrahimi - BBA

كلية الحقوق والعلوم السياسية

Faculty of law and Political Science

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر اكاديمي في الحقوق

تخصص: قانون اعلام الي وانترنت

الموسومة ب:

البحث والتحري في الجريمة الإلكترونية

من اعداد الطالبتين:

✓ بلعيالي سعيدة

✓ بلهذلي أسماء

إشراف الدكتور:

✓ سي حمدي عبد المؤمن

لجنة المناقشة:

خنتاش عبد الحق	أستاذ محاضر ب	رئيسا
سي حمدي عبد المؤمن	أستاذ محاضر قسم أ	مقررا ومشرفا
ديرم سمية	أستاذ محاضر قسم ب	ممتحنا

السنة الجامعية 2025/2024

2020 ص 27

*ملحق بالقرار رقم ...1082... المؤرخ في .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

ة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

ي أسفله.

: بلعيالي سعيدة الصفة: طالب، أستاذ، باحث طالبة .

) لبطاقة التعريف الوطنية رقم 119126655 والصادرة بتاريخ 2020/07/13 .

ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق .

ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

البحث و التحري في الجريمة

الالكترونية .

ح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية

إنجاز البحث المذكور أعلاه .

حرر بـ .ب.ع.ب.ق.ز في 2025

شوهد لأجل التصديق

السيد: المعني

بطاقة التعريف الوطنية رقم: توقيع المعني (ة)

صدر عن بتاريخ:

التفاصيل في:

2020 ص 27

*ملحق بالقرار رقم ....1082.... المؤرخ في .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

ة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

ي أسفله،

ة): بلصنديي أسماء الصفة: طالب، أستاذ، باحث طالبة

ة) لبطاقة التعريف الوطنية رقم 113613114 والصادرة بتاريخ 2024/12/02

ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

البحث والتحري في الجريمة

الالكترونية

رح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية

ي إنجاز البحث المذكور أعلاه .

شوهد لأجل التصديق

السيد: _____

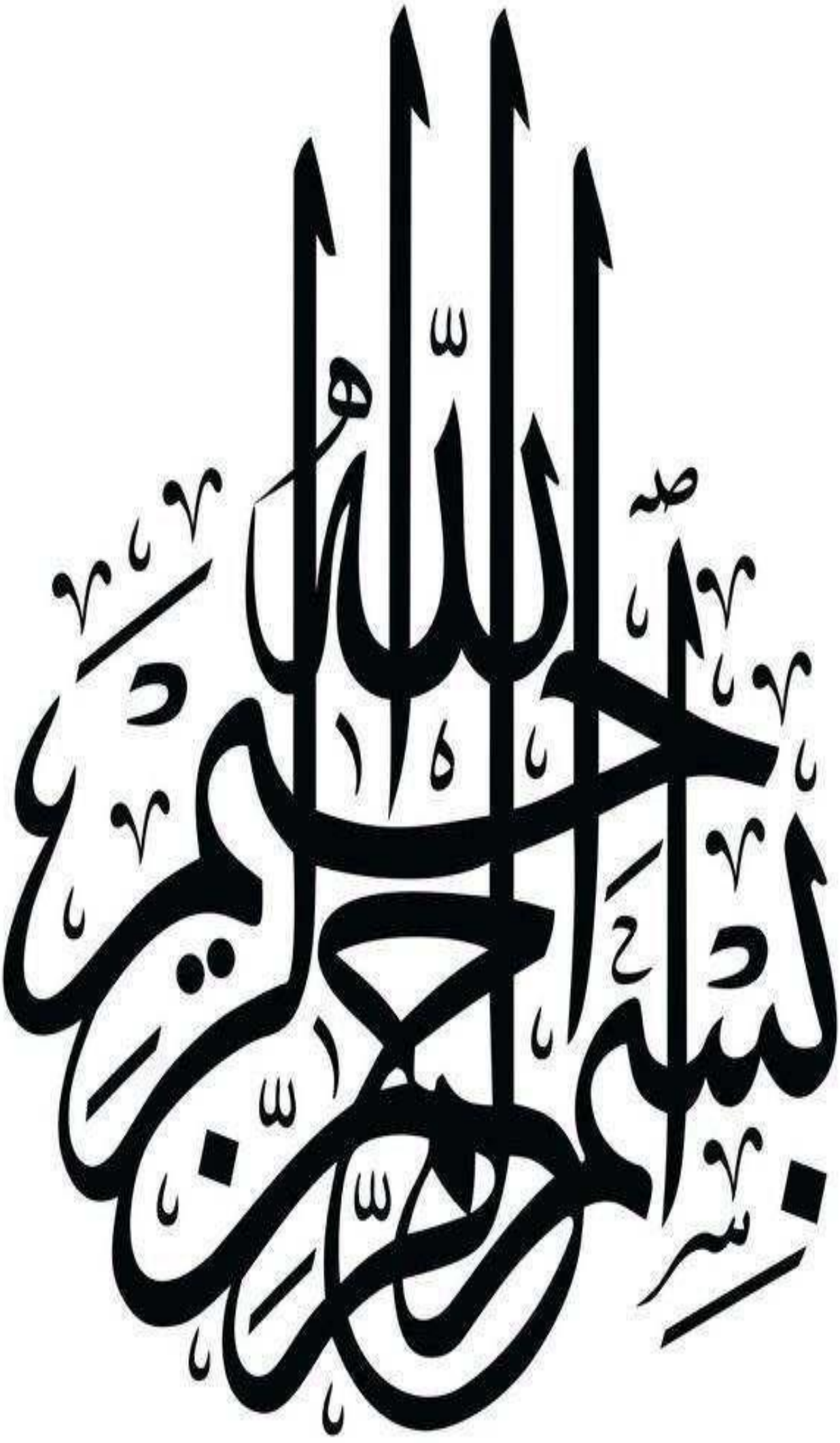
بطاقة التعريف الوطنية رقم: _____

مستخرج بتاريخ: _____

العناصر في: _____

2025.05.15

توقيع المعني (ة)


بسم الله الرحمن الرحيم

شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه أنجزنا هذا العمل المتواضع.

نتقدم بجزيل الشكر والامتنان إلى كل من ساهم في دعمنا خلال إعداد هذه المذكرة، وعلى رأسهم الأستاذ سي حمدي عبد المؤمن، الذي لم يبخل علينا بنصائحه وتوجيهاته القيّمة طوال فترة البحث.

كما لا يفوتنا أن نشكر لجنة المناقشة على تفضل قبول سيادتهم مناقشة هذه المذكرة

ونخص بالشكر أيضًا عائلاتنا الكريمة، التي كانت السند والداعم الأكبر لنا، ولكل من شجعنا ووقف بجانبنا خلال هذه الرحلة العلمية.

لكم منا جميعًا كل التقدير والاحترام

سعيدة و أسماء

إهداء

إلى من كانوا لي سندًا ونورًا في طريقي...

إلى والديّ العزيزين، من غرسا فيّ القيم، وكانا دائمًا الدافع الأول وراء كل إنجاز... شكرًا لكما من القلب.

إلى إخوتي وأصدقائي، الذين شاركوني التعب والفرح، ووقفوا بجانبي في كل لحظة... ممتن لكم دائمًا.

إلى كل من آمن بي وشجعني... أهدي هذا العمل المتواضع بالطبع،

إلى شريك دربي، وسندي في الحياة...

إلى زوجي، الذي كان دعمي الأول في كل لحظة، ورفيقي في مسيرة العلم والتعب.

شكرًا لك على صبرك، وتفهمك، ومساندتك لي في كل خطوة.

لولاك لما كان لهذا الإنجاز أن يكتمل، فلك مني كل الامتنان والحب.

أهدي لك ثمرة هذا الجهد

بلعيالي سعيدة

الاهداء

إلى من غرست فيّ القيم، وسهرت لأجلي الليالي،

إلى من كانت دعواتهم النور الذي أضاء طريقي،

إلى أمي وأبي...

كل الامتنان والحب أقدمه لكم.

إلى إخوتي وأصدقائي،

أنتم السند والدعم في كل خطوة،

شكراً لوجودكم الدائم.

إلى من شاركني الطريق،

ولكل من كان له أثر في هذه الرحلة،

أهدي هذا العمل المتواضع بالطبع،

إليك زوجي،

الذي كان دعمه لي في أوقات التعب،

أهديك ثمرة جهدي ونتاج تعبي،

فقد كنت دائمًا مصدر قوتي وإلهامي.

لك كل الشكر، وكل الامتنان

بلهذلي اسماء

مقدمة

مقدمة:

إن ما شهده العالم اليوم من تطور مثير في المجالات التكنولوجية، إنعكس على مجمل مجالات الحياة، بحيث لم يعد هناك شأن يتصل بالحياة الإنسانية، لا و له نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد.

فقد تميز العصر الحالي باختراعات هائلة على المستوى التقني بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات، حتى أصبح يعرف بقرن المعلوماتية، حيث أصبحت هذه الأخيرة وأدواتها وسائل ضرورية في العمليات البنكية أو سجلات الشركات وحتى علاقات الدول مع الأفراد، وعلى الرغم من أهمية الوسائل المعلوماتية وايجابيات استعمالها على أن الاستخدام الغير مشروع لها، قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الالكترونية او الجرائم المعلوماتية أو جرائم الانترنت، وهذه المصطلحات كلها تعبر عن مجموعة الجرائم التي تشهد الاعتداء على المعطيات بدلالتها التقنية الواسعة.[1]

إضافة الى ما سبق تتميز الجريمة المعلوماتية بصعوبة اكتشافها واثباتها بسبب ارتكابها بتقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها، وانها أيضا ذات طبيعة دولية متعدية الحدود، حيث تتجاوز الفواصل الجغرافية لعدة دول فمثلا الدراسة التي قامت بها شركة symatec وهي شركة مختصة في حماية الأنظمة والبرامج الالكترونية سنة 2010 تثبت فيها أن الاعتداءات على الأنظمة المعلوماتية واصلاحها سنويا يسبب خسارة مالية قدرها 114 مليار دولار في العالم وأن هذه الاعتداءات مست 431 مليون شخص ولعل مشكلة المكافحة الاجرائية للجريمة المعلوماتية خاصة من ناحية كيفية جمع الأدلة المعلوماتية ومدى حجيتها، وحتى تتوفر في الدليل المعلوماتي المشروعية التي شرطتها القوانين في كافة التشريعات.

[1] بن محمد الأمين، وسائل أساليب التحري في مجال مكافحة الجرائم الالكترونية، مذكرة لنيل شهدة الماستر، تخصص قانون قضائي كلية الحقوق، جامعة عبد الحميد بن باديس، مستغانم 2020،ص أ.

وعمدت عدة دول في سبيل مواجهة الجرائم المعلوماتية إلى وضع سياسات جنائية تتنوع بين الوقاية والمواجهة من خلال سن مجموعة من القوانين الموضوعية والإجرائية وذلك من اجل وضع حد لهذه الجرائم التي تكمن خطورتها في كونها جرائم مستحدثة وسهلة الارتكاب، نتيجة الاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات كما أن اثارها ليست محصورة في النطاق الاقليمي للدولة، فضلا على ان مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال للمعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية.

كما تستهدف الجرائم الإلكترونية محلا من طبيعة خاصة، أي المعلومات التي يحتوي عليها نظام المعالجة الآلية والذي هو عبارة عن اشارات ونبضات المعلوماتية تنساب عبر أجزاء النظم المعالجة الآلية وشبكات الاتصال العالمية بصورة آلية، والامر الذي بات يثير بعض التحديات القانونية والعملية أمام الاجهزة المعنية بمكافحة الجريمة وخاصة فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعاقب كافة المجرمين وتقديمهم للعدالة.

لقد كان ذلك بأن قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون المتضمن للقواعد الخاصة 22/06 المؤرخ في 20 ديسمبر 2006، بالإضافة الى إصداره للقانون 09/ 04 للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، ومن خلالها أوجد المشرع الجزائري طرقا اجرائية تتفق مع الطبيعة التقنية للجريمة الالكترونية.

إن دراسة الاجراءات الواجب اتباعها في مرحلة البحث والتحري، تعتبر واحدة من أهم الموضوعات الواجب دراستها كونها من الموضوعات ذات صلة وثيقة بالجريمة، والتي تمهد الطريق أمام العدالة للبدء في مرحلة التحقيق، الى ان تصل الى معاقبة الجاني. أيضا لاستيعاب هذا النوع من المخاطر المستحدثة والحد منها داخل المجتمع والتقليل من آثارها وزيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة وبأخذ الحيطة والحذر في الاستخدام أيضا لتسليط الضوء على المسؤولية الجنائية لمرتكبي جريمة المعلوماتية في التشريع الجزائري.

تهدف الدراسة الى التعرف على الجريمة المعلوماتية وأركانها وخصائصها في التشريع الجزائري كذلك على الهيئات المختصة لمكافحتها، وعلى إجراءات التحقيق التقليدية والمستحدثة للكشف عنها.

من بين الأسباب التي دفعتنا الى اختيار هذا الموضوع هو انتشار ما يعرف بالجرائم المعلوماتية بما جعلها خطرا على المستوى العالمي، ولما تلحقه من أضرار على اقتصاديات الدول مما يستوجب إقامة أجهزة كفيلة بالإشراف على مكافحة هذه الجريمة وآليات البحث والتحري فيها، بالإضافة الوقوف على حقيقة التعامل معها من الناحية الإجرائية، فالكثير من الدراسات التي عنيت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط.

وعليه نطرح الإشكالية التالية: **ما هي الآليات المتخذة من قبل المشرع الجزائري في مجال مكافحة الجريمة الإلكترونية؟**

وللإحاطة بهذه الإشكالية نطرح التساؤلات الفرعية التالية:

- ما هو مفهوم الجريمة الإلكترونية في التشريع الجزائري ؟

- ما هي الوسائل والأساليب التي أقرها المشرع لمكافحة الجريمة الإلكترونية ؟

استخدمننا عدة مناهج، منها المنهج الوصفي ويتجلى من خلال وصف طبيعة وأساليب البحث والتحري عن الجرائم المعلوماتية والمنهج التحليلي، من خلال تحليلنا وتفصيلنا لإجراءات المراقبة والترصد والتفتيش والتفاصيل المميزة للدليل الرقمي، بالإضافة إلى المنهج المقارن من خلال الإشارة إلى مجموعة من القوانين الأجنبية.

وجاءت دراستنا في فصلين كاملين، في الفصل الاول تناولنا فيه الاطار الموضوعي للجريمة المعلوماتية مفهومها، خصائصها، وأنواعها، وأركانها، وفي الفصل الثاني تطرقنا الى اجراءات ووسائل التحري في الجرائم المعلوماتية الإجراءات التقليدية والمستحدثة للتحري بهذا النوع من الجرائم التي نص

عليها قانون 04 / 09 المؤرخ في 14 شعبان 1430 موافق ل 5 أوت 2009 المتضمن مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال.

الفصل الأول :

الإطار الموضوعي للجريمة المعلوماتية

الفصل الاول: الإطار الموضوعي للجريمة المعلوماتية

تعد الجرائم المعلوماتية من الجرائم المستحدثة التي ظهرت في العصر الحديث والسبب في ذلك يرجع الى ارتباط هذه الجرائم بوسائل التقنيات الحديثة والمتمثلة في أجهزة الكمبيوتر وشبكات الانترنت والمواقع المعلوماتية ، ولقد أدى الانتشار الكبير للتكنولوجيا الحديثة الى زيادة اهتمام الباحثين والمختصين من ميادين عدة، بهذا الموضوع مما ادى الى تنوع تعاريفها ومسمياتها ومن ثم صعوبة ايجاد تعريف جامع مانع لها فهي تعتبر من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطوراتها التي ارتبطت بتقنية المعلومات فقد اصطلح على تسميتها بداية بإساءة استخدام الكمبيوتر ثم جرائم تقنية المالية إلى جرائم الهاكرز جرائم الانترنت والجدير بالذكر إن مصطلح الجريمة المعلوماتية استخدم نسبة قليلة جدا فالاستخدام الاكثر شيوعا في التشريعات " جرائم الكمبيوتر " جرائم الاتصالات الالكترونية " جرائم تكنولوجيا المعلومات" والجريمة ذات التقنية العالية ".

المبحث الاول: مفهوم الجريمة المعلوماتية

وسنحاول من خلال هذا المبحث من دراستنا تفصيل الإطار المفاهيمي لهذه الجريمة من خلال تطرق لمفهومها وأركانها.

المطلب الاول: تعريف الجريمة المعلوماتية

سيتم التطرق في هذا المطلب إلى تعريف الجريمة المعلوماتية وأركانها.

الفرع الاول: التعريف الفقهي للجريمة المعلوماتية

عرفها الفقيه تاديمان ، بأنها، كل اشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي، وفي ذات الاتجاه عرفها البعض بانها، الجرائم التي يكون قد وقع

في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسوب وبعبارة اخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابياً أكثر منه سلبياً.[1]

وينتقد البعض التعريف السابق لكونه يقوم في الأساس على العمل الرئيسي المكون لها وليس فقط على الوسائل المستخدمة فيها. ذلك أنه لا يمكن ان يطلق على جريمة ما انها من جرائم الحاسب الآلي لمجرد ان الحاسب قد استخدم في ارتكابها.[2]

ايضا هناك من تبنى اتجاه تعريف موسع واخر تبنى اتجاه تعريف ضيق فقد قدموا ايضا عدة تعريفات منها: [3]

هي كل فعل او امتناع عمدي ينشأ عن الاستخدام الغير مشروع لتقنية المعلومات بهدف الإعتداء على الأموال او الأشياء المعنوية.

كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الجاني.

عمل او امتناع يأتيه الانسان اضرار بمكونات الحاسوب وشبكة الاتصال الخاصة بها التي يحميها القانون يفرض لها عقابا.

إن التعاريف السابقة تنطوي على توسيع كبير للمفهوم الجريمة الالكترونية اذ يأت على هذا التوسع أنه من شأنه أن يسقط وصف الجريمة الالكترونية على افعال قد تكون على ذلك لمجرد مشاركة الحاسوب في نشاط الاجرامي وبعض الجرائم كسرقة الحاسب الالي والاقراص المضغوطة مثلا

---

[1] – شريف حسين محمد، القانون الواجب التطبيق على الجريمة الإلكترونية، دار المصرية للنشر والتوزيع، مصر، 2025، ص20.

[2] – المرجع نفسه، ص20.

[3] –خالد ممدوح إبراهيم، الفن التحقيقي الجنائي في الجرائم الالكترونية، ط الاولى، دار الفكر الجامعي للنشر، الاسكندريه، 2009.

لا يمكن اعطائها وصف الجريمة المعلوماتية لمجرد ان الحاسوب أو أحد مكوناته المادية كان محلا لفعل الاختلاس.

أما بالنسبة للاتجاه الذي تبنى التعريف الذي قد عرف الجريمة المعلوماتية بأنها كل فعل غير مشروع يكون العلم وتكنولوجيا الحاسب الالي بقدر كبير، لازم لارتكابه من ناحية ملاحقته وتحقيقه من ناحية اخرى.[1]

الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا.

الجريمة التي تكون متطلبا لاختراقها ان تتوفر على تفاعلها معرفه تقنية الحاسب ما يعرف على هذه التعريفات أيضا حاضر على الاحاطة بأوجه ظاهرة الاجرام المعلوماتي فالبعض من فقراء الاتجاه ركزوا على معيار موضوع الجريمة، والبعض الاخر ركزوا على وسيلة ارتكابها، والبعض الاخر على معيار النتيجة.[2]

ايضا تعرف بانها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليه فعليه داخل نظام الحاسوب وبعباره اخرى تلك الجرائم التي يكون دور الحاسب فيها ايجابيا وأكثر سلبيا.

فهو تعريف اخر للفقيهين في الفعل الغير مشروع التي يتسبب في ارتكابه الحاسب الالكتروني وهذا التعريف ينتقد لأنه ينطوي على توسع كبير في مجال الجريمة المعلوماتية لأنه يرى أنه بمجرد مشاركته الحاسب الالي تقوم جريمة وتتوصف بالمعلوماتية.

---

[1] – مهداوي حنان، التعليم القانوني للجريمة الالكترونية في التشريع الجزائري، **مجلة الفكر القانوني والسياسي** كلية الحقوق والعلوم السياسية، جامعة محمد الامين دباغين سطيف 2، المجلد عدد 2، 2022 ص ص 61،62.

[2] _ المرجع نفسه، ص ص 61،62.

وعرفها فريق آخر من الفقه بأنها كل فعل متعمد أيا كانت صلته بالمعلوماتية نشأ فيه خسارة تلحق بالمجني عليه او كسب يحققه الفاعل.[1]

ولم يقتصر الفقه على وضع التعريفات بل ساهمت الهيئات والمؤسسات المهتمة بدراسة الجريمة المعلوماتية بوضع تعريف لها ويعرف خبراء التعاون الاقتصادي والتنمية الجرائم المعلوماتية بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية لبيانات أو نقلها.[2]

ايضا يرى بعض الفقهاء بأن الجريمة المعلوماتية هي فعل يسبب بأثر جسيم الأفراد أو الجماعات أو المؤسسات بهدف ابتزاز الضحية وتشويه سمعته من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الانترنت.

ايضا تعتبر نشاط اجرامي يستهدف جهاز كمبيوتر أو شبكة كومبيوتر أو جهاز متصل بالشبكة وتقع معظم هذه الجرائم المعلوماتية على أيدي لصوص أو معترفين يودون كسب المال وتكون الأسباب سياسية أو شخصية وهم ذوي مهارات نفسية عالية.[3]

الفرع الثاني: التعريف القانوني للجريمة المعلوماتية

أولا: موقف المشرع الجزائري

استعمل المشرع الجزائري للدلالة على الجريمة المعلوماتية ، بداية مصطلح "جرائم المساس بأنظمة المعالجة الآلية للمعطيات" وذلك بعد استخدامها بموجب القانون 04_15المعدل والمتمم للأمر 66_ 156 المتضمن قانون العقوبات، ثم بعد ذلك استعمل مصطلح الجرائم المتصلة

---

[1] _ ايمن عبد الله الفكري، **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية**، مكتبة القانون والاقتصاد، الرياض، 2014، ص ص95 - 97.

[2] – عدنان علي طياش، **الإنترنت في العصر الحديث وذكاء الاصطناعي والجريمة الالكترونية**، الكتاب 3، ط 1، 2022، ص ص 88، 93.

[3] _ المرجع نفسه، ص ص 88-93.

بتكنولوجيا الإعلام والاتصال، وذلك بموجب القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال يحث عرفها في المادة 2.

يلاحظ على هذا التعريف أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهي المنظومة المعلوماتية أو نظام للاتصالات المعلوماتية وثانيها معيار موضوع الجريمة وهي المساس بأنظمة المعالجة الآلية للمعطيات ومن خلال النص القانوني المذكور نجد أن المشرع قد أحال الى قانون العقوبات وبالتالي كل الأفعال المجرمة في المواد من 394مكرر إلى 344مكرر 8 ،تشكل موضوعا للجريمة المعلوماتية ،وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات ،كما حدد المشرع نطاق الجريمة الإلكترونية وذلك من خلال إقراره بأنها، ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه وهذا ما يوسع من نطاقها في القانون الجزائري.[1]

[1] – **القانون 04/09 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، ج ر، ع47، المؤرخ في 05 أوت 2005.

ثانيا: الطبيعة القانونية للجريمة المعلوماتية

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات, على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد ,مما يؤدي إلى ارتكاب الفعل والسبب في ذلك توسع بنوك المعلومات بأنواعها دلالة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة ،على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة المعلوماتية للبيانات، سواء كان في تجميعها أو تجهيزها أو في إدخالها إلى الحاسب الالي المرتبط بشبكة الإنترنت ،ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال معالجة النصوص وصعوبة التكيف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة ،بحث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة ،وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الاثبات ومتابعة مرتكبها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[1]

- الأدلة الإلكترونية غالبا ما تكون رقمية مما تتطلب تقنيات متخصصة لجمعها وتحليلها

- يمكن تنفيذ الجرائم المعلوماتية في ثوان محدودة.

- لها تأثير واسع النطاق ويمكن أن تصيب ملايين الأفراد والمؤسسات

- ترتكب باستخدام وسائل مسطورة لإخفاء هوية الجنّات

- الجريمة المعلوماتية تتم عادة بجوانب أكثر من شخص على ارتكابها إصرار الجاني عليه وغالبا ما يشترك في إخراج الجريمة إلى خير الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم الجانب الفني من المشروع الإجرامي وشخص آخر من محيط أو من خارج المؤسسة الجاني عليها لتخطية عملية التلاعب وتحويل المكاسب.

---

[1] - بوضياف اسمهان "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، جامعة محمد بوضياف مسيلة، مارس 2018 ص353.

– تدني نسبة الإبلاغ عن الجريمة من طرف الجاني عليه خاصة في حالة شركات ومؤسسات. بنوك وهو بنك marchant bank city وهو بنك في بريطانيا لسرقة ثمانية مليون جنيه من احدى ارصدته الى رقم في سويسرا وثم ضبط الفاعل يسحب المبلغ المسلوب والمسروق وبدلا من محاكمته قام البنك بدفع مليون جنيه له بشرط التزام الفاعل بعدم الاعلام عن جريمته واعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الامن بحاسوب البنك الرئيسي غالبا ما تكون الخسائر القادمة للمجني عليه.

– ذاتية الجريمة المعلوماتية برز بوضوح في أسلوب ارتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من هذا الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر وتقليد لمفاتيح كما هو الحال في جريمة السرقة وتحتاج كذلك إلى وجود شبكة المعلومات الدولية «الأنترنت» مع وجود مجرم يوظف خبراته وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير للتغرير بالقاصرين.[1]

[1] – كلتوم دهان، فاطمة دهان، **إجراءات البحث، والتحري في الجريمة المعلوماتية**، مذكرة مقدمة ضمن متطلبات شهادة ماستر أكاديمي، حقوق تخصص قانون جنائي وعلوم جنائية، جامعة غرداية 2022 ص ص 14-16.

المطلب الثاني: خصائص الجريمة المعلوماتية

نظراً للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا ما يجعلها تتميز عن التقليدية بمجموعة من الخصائص أو السمات والتعرف على خصائصها يساعد في إيجاد الحلول لمكافحتها ومن خصائصها _الجرائم الإلكترونية ترتكب في أي مكان في العالم وأشهد أن ضحاياها في دول أخرى دون الحاجة إلى وجود الجاني في مكان الجريمة.

الفرع الأول: صعبة الإثبات

تتميز الجريمة المعلوماتية عن الجرائم التقليدية بأنها صعبة الإثبات. وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة وغياب الدليل الرقمي، (بصمات، تخريب، شواهد مدية) وسهولة محو الدليل أو تدميره في زمن مثناه القصر يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة.

لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الآلي الإلكتروني إلى أي عنف أو جثث أو سفك الدماء أو آثار اقتحام سرقة الأموال، وأنما هي بيانات ومعلومات تغير أو تعدل أو تمحى كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الإلكتروني. لذا يكون من الصعب اكتشافها ومن تم تطبيق الجزاء الجنائي على مرتكباها ويتعلل بارتكابها وجود جهاز إلكتروني ومعرفة تقنية استخدامه إنما يميزها عن غيرها من الجرائم وجود علم كافي الجوانب النفسية للتقنية لاستخدام الحاسب الآلي و الانترنت وتعتبر العلاقة بين مدى الدراية بالجوانب النفسية والتقنية للحاسب وبين الجريمة الإلكترونية علاقة طردية.[1]

فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب زاد استخدام خبرتهم بشكل غير مشرف وأثبت الواقع العلمي أن الجرائم الإلكترونية قد ترتكب من خلال الهواتف المحمولة، عند

[1] – بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية، مرجع سابق، ص 356.

ظهور أجهزة الهاتف الذكية التي هي في الحقيقة عبارة عن أجهزة الكمبيوتر صغيرة والتي من خلالها تتم الاتصال بشبكة الانترنت ويسهل التخزين ونقل المعلومات من خلالها وليس كما ذكر بعض الباحثين بأن الحاسب الآلي هو الأداة الوحيدة التي في ارتكاب الجريمة المعلوماتية ويمكن علاج المشكلة السابقة من خلال وجود برامج حماية على كل أجهزة الحاسب سواء المنزلية أو المتوافرة في الأماكن العامة لضمان الحفاظ على الاسرار الشخصية والمهنية وعدم جعل الجهاز متصل بالأنترنت والتيار الكهربائي خارج وقت الاستخدام له لأن مرتكب فيه الجرائم في الغالب شخص يتميز بالذكاء والدهاء وذو مهارة تقنية عالية. [1]

وهناك أيضا من يرى بان اكتشاف هذه الجرائم يكون بمحض الصدفة بمادة ويعود السبب في ذلك الى عدم ترك اي اثر خارجي بصورة مرئية بالإضافة الى قدرة الجاني على تدمير دليل الادانة في اقل من ثانية واحدة ومما نزيد في صعوبة اثبات هذه الجرائم ايضا ارتكابها عادة في اثناء وعدم وجود اي أثر كتابي لما يجري خلال تنفيذها من عمليات او افكار اجرامية لان غياب الدليل الفيزيقي فيها. [2]

لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الإلكتروني أي عنف أو جثث أو سفك الدماء أو آثار اقتحام لسرقة الأموال وإنما هي بيانات ومعلومات تفسر أو تعدل أو تمحى كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الآلي الإلكتروني.

فالكشف عن هذه الجرائم يتم عن طريق فحص والتحقيق أو عن طريق الشكاوي التي يقدمها المجني عليهم فجهات التحتية لما تصل إلى تلك المعرفة أو الخبرة التي تمتلكها مال التحقيق في الجرائم التقليدية لأن الأمر يتطلب معرفة واسعة وحاصلة كاملة بهذه التكنولوجيا الحديثة. [3]

[1] - بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية، مرجع سابق، ص 356.
[2] كلتوم دهان، فاطمة دهان، مرجع سابق ص 14-16.
[3]– الشيخ حذيفة بن حسين القحطاني، **الجرائم الالكترونية احكام وضوابط**، د د ن، د ب ن، 2025، ص ص14-15.

الفرع الثاني: عابرة للحدود

باعتبار الجريمة المعلوماتية تقوم في بيئة فضائية معلوماتية مفتوحة عابرة للحدود من خلال السرعة التي تنقسم بها هذه الأخيرة في تنفيذ الجرم بنقل المعلومات بين الدول معها، اختلفت المسافة لفهم الامر الذي جعل مرحلة البحث عن الجاني لجرائمه عبر الحدود لتقتضي من الناحية العلمية ان يتم نطاق دولة اخرى فاهم ما يميز الجرائم المعلوماتية هو عبورها للحدود الدولية لسهولة حركة الافعال المعلوماتية. [1]

تعبر تقنية الانترنت كما أنها ترتكب عن طريق الحاسب الآلي عن طريق الشبكات الدولية وتحقق لدورها نتائج إجرامية في دولة أخرى كما أنه يعد مسافات تشكل عدة إشكاليات من بين أهمها وجود أجزاء التحقيق وملاحقة المتهمين بمبدأ سيادة الوطنية للدولة إشكالات الاختصاص القضائي والقانون الواجب النطاق على هذا النوع من الجرائم باعتبارها جرائم غير ملموسة.[2]

مثال: هذه الجرائم قضية *RN thapsa* وفيها قام مبرمج انجليزي يعمل لدار بنك بالكويت بالتلاعب في معطيات النظام الحاسب الآلي الخاص بالبنك وذلك عن طريق الخصم من ارصدة العملاء تم الايداع في حسابه الخاصة وبعد عودته الى انجليترا طلب من البنك تحويل الحساب الخاص الى عدة حسابات بنكية في انجليترا فقام البنك بذلك حركم الفاعل بتهمة الحصول على اموال التغيير بالطريق الاشكالي وحكم عليه بعقوبة السجن طعن في الحكم اشداد على عدم الاختصاص القضاء الانجليزي لأنه فعلي السحب والايداع قد تم في الكويت لأنه في انجلترا لكن محكمة الاستئناف رفضت طعنه وردت بان النشاط الاجرامي للمتهم لم يكتمل الى بعد الطلب

[1] الشيخ حذيفة بن حسين القحطاني، المرجع السابق، ص16 .
[2] _ ايمن عبد الله الفكري، مرجع السابق، ص95 - 97.

الذي تقدم به الى مدير البنك بالتحويل وما اسفل عنه هو من حصوله على الاموال محل النشاط الاجرامي بواسطة البنوك الانجليزية. [1]

في الكويت، لا في إنجلترا، لكن محكمة الاستئناف رفضت طعنه وردت بأن النشاط الاجرامي للمتهم لم يكتمل بعد الطلب الذي تقدم به إلى مدير البنك بتحويله وما أسف عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية، ولهذا فمكافحة هذه الجرائم تتطلب تعاونا كثيفا بين الدول وتوافق كبيرا بين تشريعاتها.[2]

المطلب الثالث: أنواع الجريمة المعلوماتية

نظرا لصعوبة حصر أنواع الجرائم المعلوماتية بصورة دقيقة تعددت محاولات تحديد أنواعها فهناك من قسمها على أساس معيار الأداة استعملت في ارتكاب الجريمة (الحاسب الآلي) وهناك من قسمها بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية ومدى اتفاقها أو اختلافها من القواعد التي تحكم القانون الجنائي بالإضافة إلى اتجاه ثالث قسمها بالاعتماد على محل الجرائم المعلوماتية التي تنصب على معطيات الحاسوب بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة وهذا الآخر يعود الاتجاه الراجح في تقسيم الجرائم المعلوماتية اذ صنفها ضمن طائفتين الأولى تمثل الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي والأخرى الجرائم الواقعة على النظام المعلوماتي.

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

أولا: الواقعة على أشخاص

---

[1] _ دیابلو محمد نجیب، **الجريمة الالكترونية وجهة الدليل الرقمي في الاثبات الجنائي**، ط01، المركز التجاري الشرق أدنى للدراسات الاستراتيجية المملكة المتحدة بريطانيا، 2024 ص ص44، 46.

[2] – محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مراجعتها، **مجلة دراسات وأبحاث**، كلية الحقوق ولأداء العلوم الاجتماعية، جامعة 8 ماي 1945 قالمة، 2009، ص ص 375-376.

الأفعال الواقعة بواسطة الجريمة المعلوماتية هي انتهاك حرمة الحياة الخاصة الأفراد عن طريق تفسير البيانات الشخصية للفرد أو محوها من طرق شخص غير مؤهل بذلك او نشر المعلومات تخص حياة الفرد على العالم ويكون العالم على اطلاع عليها من يؤدي بأضرار نفسية للضحية حيث انه اصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من اسرار حياة الانسان التي اصبح التحصيل عليها بسهولة ولسرعة النظر إلى التطورات التكنولوجية في مجال المعلومات التي شهدها العالم في الفترة الأخيرة بالنظر لعلاقة الحياة الخاصة للإنسان مع تقنية حديثة وقد عاتب المشرع الجزائري الاعتداء على حرمة الحياة الخاصة بموجب المادة 303 [1]مكررا من قانون العقوبات الجزائري على أنه يعاقب بالحبس من 8 أشهر إلى3 سنوات وبغرامة مالية من 50،000 دج إلى3000.000 وذلك إذا قام بالتخاطب أو تسجيل أو نقل مكالمة أو أحاديث خاصة أو سرية أو نقل صورة لشخص في مكان خاصة دون إذن صاحبها أو رضاه.

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

أولا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الائتلاف العمدي أو العبث بمفاتيح التشغيل مما يترتب عليها خسائر كبيرة ولقد حدث هذا التنوع من الجرائم لفرنسا وادى إلى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقدرت ب5 ملايين فرنسي.

[1] – **المادة 303 من الأمر 66–155 المتضمن قانون العقوبات الجزائري**، المعدل والمتمم بموجب القانون 24-06 المؤرخ في 28 أفريل 2024.

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

حيث يتم بواسطة الاحتيال وادخال معطيات في نظر المعالجة الآلية للمعطيات او اتلافها او حذفها او تغيير المعطيات المدرجة.

ولقد عالج المشرع الجزائري هذا النوع من الجرائم من خلال نص 394 مكرر من قانون العقوبات التي تنص على انه يعاقب بالحبس من 6 اشهر الى ثلاث سنوات وغرامه مالية تقدر بثمن5000,00 إلى 20,000 دج كل من أدخل بطريقة الغش المعطيات يتضمنها. [1]

يعرف البعض الاتلاف بأنه هو ذلك الفعل الذي يجعل الشيء غير صالح للاستعمال أو بإعدام صلاحيته أو بإعدام صلاحيته أو تعطيله سواء بصفة كلية أو جزئية.

ثالثا: الجرائم الواقعة على البرامج المعلوماتية

وتقسم هذه الجرائم بدورها الى الجرائم الواقعة على البرامج التطبيقية عن طريقة تحديد البرنامج اولا من ثم التلاعب به او تعديله لمن اتلفها قيام احد المبرمجين الأمريكيين بتعديل برنامج بإضافة دولار واحد على حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به اطلق عليه اسم zz wik[2]

المبحث الثاني: خصوصية اركان الجريمة المعلوماتية

لكي يمكن القول بوجود جريمة ما فإن المشرع يتطلب كأصل عام ضرورة وجود ركن مادي وركن معنوي وشرعي فيها ، وبغير الركنين لا يمكن القول بوجود جريمة.

[1] – المادة 394 من قانون العقوبات، المصدر السابق.

[2] – بوضياف اسمهان، مرجع سابق، ص 356.

المطلب الأول: خصوصية الركن الشرعي

سنتطرق في هذا المطلب الى خصوصية الركن الشرعي في التشريع الجزائري.

الفرع الأول: الركن الشرعي في التشريع الجزائري

يقصد به الصفات غير المشروعة للفعل، حيث يكون هناك قاعدة تجريمية وعقوبات مفروضة على الجرائم المعلوماتية المرتبطة بأنظمة المعلومات وذلك تحقيقا لمبدأ الجريمة ولا عقوبة إلا بنص فإذا انتفى التجريم انتفت من مرتكبها المسؤولية الجزائية، يعد هذا المبدأ ضمانا لمصلحة الأفراد فهو الحامي الحقيقي لحقوق الأفراد وكفالة الحريات الفردية لملاحقة الأفعال وتوقيع العقاب يجب أن ينتج من قوانين صادرة من السلطة التشريعية تجرم الأفعال وتعاتب مرتكبيها.

أول نص تشريعي جزائري في مجال الإجرام المعلوماتي لم يظهر في قانون العقوبات إلا في 26 جويلية 2001 بموجب القانون رقم 01-09 المواد 144 مكرر و 146 مكرر و 144 مكرر 2 و 146 من قانون العقوبات الجزائري والمتعلق بجريمة القذف والسب والإهانة إزاء رئيس الجمهورية أو فيما يخص دين الإسلام والرسول" صلى الله عليه وسلم" ، وباقي الأنبياء أو ما هو معلوم من الدين أو ضد الهيئات المؤسسة أو الهيئات العمومية، ومن خصوصيات المادة 144 مكرر ق.ع أن المشرع أدرج فيها لأول مرة مصطلح .... وسيلة الكترونية أو معلوماتية .... التي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلومات والانترنت بالإضافة إلى المواد 144 مكرر 1 و 2 و 146 قانون العقوبات الجزائري. [1]

[1] _ شلاخ لطيفة، **انتشار الجريمة الالكترونية الماسة بالأشخاص في الهيئة الجزائرية**، دراسة ميدانية لبعض مستخدمي مقاهي النت بمدينة المسيلة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف – المسيلة، ماي 2017، ص 14.

ولقد ورد العقاب في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحتها تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04/15 المؤرخ في 10 نوفمبر 2004 في الفصل السابع مكرر من المواد 394 مكرر إلى 394 مكرر.7[1]

ولقد كان تعديل هذا القانون بموجب القانون رقم 09/04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [2]

ثانيا: خوصصة الركن الشرعي تشريعات المقارنة

إن الجريمة هي نتيجة الأعمال العادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الصادرة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه [3]

القاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون. [4]

---

[1] _ بموجب المواد من 394 مكرر إلى 394 مكرر 7 من القانون 04/15، مصدر سابق ، ص ص 11،12.

[2] _ القانون 09/04، مصدر سابق.

[3] _أحسن بوسقيعة، **الوجيز في القانون الجزائي العام**، دار هومة الجزائر، ط 10، 2011، ص 27

[4] _أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط2، 2006، ص 78

ويتميز هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره تفسيرا ضيقا بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل لم يرد نص بتجريمه على فعل ورد نص بتجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني للتشابه بين الفعلين. [1]

إن ظهور شبكة الانترنت أدى إلى تطور ظاهرة الإجرام بشكل خطير في تفشي الجريمة الالكترونية وازداد هذا الوضع خطورة خاصة حين أصدر المجلس الأوروبي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص عقابية خاصة بجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

وقد اختلفت في اختيار التقنية التشريعية المناسبة، فمنها من قام بإجماع النصوص العقابية المتعلقة بالإجرام المعلوماتي في قانون العقوبات التقليدي، ومنها من قام بوضع قانون جنائي مستقل للمعلوماتية يدخل في القانون الجنائي التقني.

تستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة المعلوماتية فقد بذلت هيئة الأمم المتحدة جهودا كبيرة إضافة إلى جهود المجلس الأوروبي الإقناع الدول بوضع تشريعات لتصدي ومواجهة ومكافحة الجرائم المعلوماتية وتعزيز التعاون الدولي في هذا المجال.

وكمثال على ذلك التوصية رقم (89) المتعلقة بالجرائم المرتبطة بالحاسب الآلي.

المطلب الثاني: الركن المعنوي

إن الركن المعنوي في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتخذ صورة القصد الجنائي.

[1] _ مولود ديدان، **قانون العقوبات قانون رقم 09-01** المؤرخ في 25 فبراير 2009، د ط، دار بلقيس للنشر والتوزيع، الجزائر، 2009، ص 04

الفرع الأول: الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات

إن الركن المعنوي لجريمة الدخول والبقاء غير المشروعين، لأنه أكثر إنتشارا يتخذ صورة القصد الجنائي من علم وإرادة باعتبارها من الجرائم العمدية، وقد عبر نص المادة 394 مكرر عن القصد الجنائي العام بتطلبه أن يكون الدخول أو البقاء عن طريق الغش، فاستخدام هذه العبارة يعنى أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع، وهو نفس ما عبر عنه المشرع الفرنسي في نص المادة 323[1]

يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وبناء أركانها، واستكمال عناصرها، وخاصة الركن المادي منها، وأول هذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج، باعتباره محل الحق الذي يحميه المشرع، فإذا اعتقد الفاعل بناء على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، دون أن يتجه علمه إلى أنه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فإن قصد الدخول أو البقاء لا يتوفر فيه.[2]

كذلك يتعين أن يعلم بخطورة الفعل الذي يقوم به، فإذا كان ذلك ينتفي القصد الجنائي، ويتطلب القصد الجنائي أيضا أن يتوقع الجاني النتيجة الإجرامية التي ستترتب عن القيام بفعله، فتوقع النتيجة هو أساس النفي الذي تقوم عليه إرادتها، فحيث لا يكون التوقع لا نتصور الإرادة، والنتيجة التي يجب أن يتجه إليها توقع الفاعل هي النتيجة التي يحددها القانون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

[1] – المادة 394 مكرر من قانون العقوبات ، مصدر سابق.

[2] _ مولود ديدان، المرجع السابق، ص 04

ولا يشترط أن يتوقع الضرر الذي سوف يلحق النظام أو صاحبه من جراء هذا الدخول[1]، فإذا توقع الفاعل أنه بصدد الدخول إلى نظام معين، ثم ترتب على فعله الدخول إلى نظام آخر، فإن القصد الجنائي يظل متوافرا لديه.

وهناك وقائع يسأل فيها الجاني عن الجريمة دون أن يتطلب القانون علمه بها، فحين يقرر القانون لبعض الجرائم عقابا معينا إذا أحدث الفعل نتيجة ذات جسامة معنية، وإذا ازدادت جسامة هذه النتيجة فأفضت إلى نتيجة أشد جسامة، شدد القانون العقاب، ويتطلب المشرع انصراف القصد الجنائي إلى النتيجة الأقل جسامة، ولكنه لا يتطلب انصرافه إلى النتيجة الأشد جسامة، بحيث يسأل الجاني عنها بالرغم من عدم توقعها لها . [2]

وهذا ما ينطبق على الفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات حيث يعاقب الجاني على النتيجة الأشد بمجرد ترتبها عن الدخول أو البقاء غير المشروع الذي قصده.

ويجب أن يعلم مرتكب جريمة الدخول أو البقاء غير المشروعين داخل نظم المعالجة الآلية للمعطيات، أن دخوله إلى هذا النظام غير مشروع أو غير مصرح به، فلا يتوافر القصد الجنائي إذا وقع الجاني في خطأ، كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول أو البقاء.[3]

أما بالنسبة لإرادة الجاني فيجب أن تتجه إلى الدخول أو البقاء غير المشروعين داخل النظام، أي أن تتجه إرادته لتحقيق هذه النتيجة، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول أو البقاء سواء كان هذا الباعث هو الفضول، أو إثبات القدرة على المهارة والانتصار على النظام،

---

[1] _ نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي**، منشورات الحلبي الحقوقية ،2005، ص 365.

[2] _ المرجع نفسه، ص 366.

[3] _ مولود ديدان، المرجع السابق ، ص 04

حتى وإن كانت الغاية نبيلة كمن يدخل إلى النظام غير المصرح له بالدخول رغبة في الكشف عن أوجه القصور التي تعتري النظام الذي تمكن من الدخول إليه، وذلك لتجنب هذا القصور مستقبلا.[1]

الفرع الثاني: الركن المعنوي للاعتداءات على سير نظام المعالجة الآلية للمعطيات والاعتداءات على المعطيات خارج وداخل النظام

إن الاعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التعطيل أو العرقلة وإفساد النظام، لا تكون إلا عمدية هذا ما يميزها عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء غير المشروعين داخل النظام. [2]

وهذه الاعتداءات تتطلب القصد الجنائي العام من علم وإرادة، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنه يقوم بإحدى هذه الأعمال التي أوردها النص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التعديل، ويعلم خطورة النشاط الإجرامي الذي يقوم به وما يترتب عنه من عقاب.

كما يجب أن تتجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التعديل، فلا يسأل من قام بذلك خطأ أو عن غير قصد، بل يسأل طبقا للمادة 394 مكرر 2/3 التي تتناول الصورة المشددة لجريمة الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات، كونها تعاقب الفاعل من الحذف والتغيير المترتب عن الدخول أو البقاء غير المشروعين حتى وإن كان خطأ، كون أن نص المادة 394 مكرر 1 من قانون العقوبات اشترط أن ترتكب هذه الأفعال بطريق الغش.

وهي العبارة المستعملة كذلك في نص المادة 323-3 من قانون العقوبات الفرنسي

---

[1] _ نائلة عادل محمد فريد قورة المرجع السابق، ص 368.

[2] _ أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، ط2، دار هومة، (الجزائر)،2007، ص 124

frauduleusement ، أي أن يعلم أنه ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته، ولا يتطلب نص المادة 394 مكرر 1 قصدا جنائيا خاصا، إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التشريعات المقارنة التي اشترطت قصدا خاصا إلى جانب القصد العام، يتمثل في اتجاه نية المتهم إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، وهو ما كان عليه النص الفرنسي القديم قبل تعديله، ويبرز ذلك في عبارة ارتكاب الفعل دون مراعاة حقوق الآخرين، وقد انتقدت هذه المادة قبل تعديلها بشدة لتطلبها القصد الجنائي الخاص، كون أن اشتراط هذا القصد الخاص سوف يؤدي إلى اللاعقاب في الحالات التي لا تتجه فيها نية الفاعل إلى تحقيق ربح على الرغم من أهمية المعلومات التي قد يتم إتلافها، مثل إتلاف معلومات علمية. [1]

أما بالنسبة للاعتداءات العمدية الماسة بالمعطيات الموجودة خارج النظام، فيجب القيام الركن المعنوي أن يتوافر القصد الجنائي العام، وهو ما عبرت عنه المادة 294 [2] مكرر 2 بعبارة كل من يقوم عمدا وعن طريق الغش.

وبالتالي يجب توافر العلم والإرادة لدى الجاني لقيام الركن المعنوي، فيجب أن يكون عالما أن المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك بتصميمه أو بحثه أو تجميعه أو توفير أو نشره أو الاتجار في هذه المعطيات، أي علمه بأن هذه المعطيات يمكن أن تكون وسيلة لارتكاب الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

[1] _ قارة أمال، مرجع سابق، ص 41.

[2] – المادة 294 مكرر 2 من قانون العقوبات ، مصدر سابق.

ويجب أن يعلم الجاني كذلك، أن إتيانه أحد الأفعال السابقة ينصب على معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، وكذلك أن يعلم بخطورة الفعل الذي يقوم به، وأن يتوقع النتيجة المترتبة عن القيام بأحد الأفعال السابقة.

المطلب الثالث: خصوصية الركن المادي

الركن المادي هو أحد الأركان الأساسية للجريمة، ويشير إلى الجانب الملموس أو الفعلي من السلوك الإجرامي. يُعبر عن الأفعال أو التصرفات التي تُرتكب من قبل الجاني، والتي يترتب عليها تحقيق النتيجة الجرمية المنصوص عليها في القانون.

الفرع الأول: تعريف الركن المادي وعناصره

الركن المادي الذي يتمثل في الأفعال أو التصرفات التي يرتكبها الجاني وتؤدي إلى النتيجة الجرمية المنصوص عليها قانونا.

أولا: تعريف الركن المادي

عرفه الفقهاء على أنه كل فعل ينتج عنه توقيف نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي، وبالرغم من الجهد الفقهي الذي صاحب مفهوم النظام المعلوماتي، حول شموله جل عناصره من عدمه، إلا أن غالبية الفقه ترى بضرورة عدم اشتراط أن يقع فعل التفضيل أو الإضرار للنظام جملة، بل يكفي أن يؤثر على أحد عناصره فقط، كجهاز الحاسوب نفسه أو تمتد إلى شبكات الاتصال أو البرامج والمعطيات.

وعليه تكون أمام الركن المادي للجريمة المعلوماتية إذا تم الاعتداء على نظام المعالجة الآلية للمعلومات أو سلامته، كما تكون في حالة الدخول والبقاء غير المشروع في هذا النظام أو الحذف

أو التغيير أو في المعطيات، كما يمكن اعتبار التخريب أو أي إتلاف في نظام الاشتغال اعتداءات مادية المادة 394 مكرر ق. ع. ج). [1]

كل تلك الصور تضمنها المشرع الجزائري من خلال قانون العقوبات المعدل لسنة 2004 أضاف العديد من الصور المادية الكافية لقيام الركن المادي للجريمة المعلوماتية كإدخال معلومات في نظام المعالجة الآلية أو إزالتها المادة 394(مكرر). [2]

– حيث يتحقق الركن المادي بإحدى الصور أولهما اختراق الأجهزة الرئيسية بطريقة الغش إلى نظام المعالجة الآلية للمعطيات وثانيهما البقاء أو المكوث بطريقة الغش في نظام المعالجة الآلية للمعطيات [3]، حيث نصت المادة 394 مكرر من قانون العقوبات[4] على أن الدخول أو الدخول والبقاء غير المشروع في نظام المعالجة الآتية للمعطيات يشكل فعلا إجراميا.

ولعل جريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعلومات من أهم جرائم المعطيات والجرائم المعلوماتية عموما، ذلك أن أغلب جرائم المعلومات لا يمكن ارتكابها إلا بعد الدخول إلى النظام. [5]

ويتمثل النشاط الإجرامي في الأفعال التالية:

---

[1] _ المادة 394 مكرر من القانون رقم 04-14، مصدر سابق.

[2] _ المادة 394 مكرر من قانون العقوبات.

[3] _ عزيزة رابحي، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة دكتوراه في القانون كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد تلمسان الجزائر، 2018، ص 108

[4] _ المادة 394 مكرر من القانون رقم 04-14 ، مصدر سابق.

[5] _ محمد قسيمة، حمزة حضري، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في القانون الجزائري، **مجلة صوت القانون**، جامعة خميس مليانة الجزائر، المجلد 07 العدد 02 نوفمبر 2020، ص ص 126-155 ص .131

-1-1- فعل الدخول: تتسع هذه العبارات على إطلاقها لتشمل كافة فنيات الدخول الاحتياطي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك مفتاح الدخول في منظومة [1]

وفعل الدخول الذي شكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل التقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الالكتروني. [2]

يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات ، ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأي وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر شرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ.[3]

- ويمكن الإشارة أيضا إلى أنه جريمة الدخول إلى النظام المعلوماتي في جريمة شكلية أي أنها لا تتحقق بمجرد الدخول إلى النظام للمعلوماتي ولا يشترط لاكتمال الركن المادية فيها أن يتم الوصول إلى المعطيات التي يحويها النظام أو إحداث ضرر بصاحب هذه المعطيات. [4]

---

[1] _ أحسن بوسقيعة، **الوجيز في القانون الجزائري الخاص** الجزء الأول، الطبعة الحادية عشر، دار هومة، الجزائر 2019، ص 148.

[2] _ نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط 01، دار الثقافة، الأردن، 2010، ص 148

[3] _ جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، **المجلة النقدية**، جامعة مولود معمري، تيزي وزو 127 الجزائر المجلد 11، العدد 02 نوفمبر 2016، ص ص 124-155

[4] _ نسمة بطيحي،جريمة الدخول والبقاء غير المشروع إلى النظام المعلوماتي، **مجلة الفكر القانوني والسياسي**، جامعة تليجي عمار الأغواط الجزائر، المجلد 01، العدد 01، جوان 2019، ص78.

لذلك لا تتوفر الجريمة إذا تم الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعلومات، كالدخول إلى برنامج منعزل عن غيره من العناصر، أو أن يقتصر الشخص على مجرد قراءة الشاشة.

-2-1- فعل البقاء: يتسع ليشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أداء إتاوة، ويمكن تعريف البقاء الاحتيالي في نظام المعلوماتية بأنه كل تواجه غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول والنظر فيه أي في المعطيات التي يتضمنها، وغيرها من التصرفات غير المسموح بها التي تشكل بدورها بقاء احتيالي ويكون البقاء معاقبا عليه استقلالا حتى يكون الدخول إلى النظام مشروعا.[1]

[1] - جمال براهيمي، مرجع سابق، ص ص 124-155

خلاصة الفصل الأول :

إن مفهوم الجريمة المعلوماتية في الفقه هي كل فعل إجرامي غير مشروع يكون العلم بتكنولوجيا الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى.

أيضا انصبت على أنها كل فعل غير مشروع يستهدف تغيير بيانات أو معلومات كيفما كان هذا التعريف، والتغيير سواء كان بواسطة جهاز الحاسوب كما يمكن أن يكون بواسطة استخدام جهاز تكنولوجي اخر .

أما تعريفها من الناحية القانونية فالمشرع الجزائري أغفل تنظيم مجال الجريمة المعلوماتية قانونا وذلك ما جاء به القانون 15/04/المتضمن تعديل قانون العقوبات، ثم جاء القانون 04/09الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة والمتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

فقد حددت المادة 02 من أن الجريمة المعلوماتية "يقصد بها جرائم متصلة بتكنولوجيا الإعلام والاتصال ومنظومة معلوماتية ومعطيات معلوماتية".

ومن بين خصائصها أنها تتميز بجملة من الخصائص لا تتوافر في الجرائم العادية من بينها أنها جريمة.

عابرة للحدود :اي لا يعتد بالحدود الجغرافية للدول ولا بين القارات.

صعبة الاثبات :اي أنها تتميز بالخفاء وعدم وجود آثار مادية يمكن متابعتها وهي خطيرة وصعبة الاكتشاف .

ومن بين انواع هذه الجرائم :

1. الجرائم الواقعة بواسطة النظام المعلوماتي هناك جرائم واقعة على الأشخاص أي انتهاك حرمة الحياة الخاصة للأفراد والجرائم الواقعة على الأموال من بينها قرصنة ارقام البطاقات الممغنطة.

2. جرائم واقعة على النظام المعلوماتي

منها ما يعرف بالجرائم الواقعة على المكونات المادية للنظام المعلوماتي، وهي الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله، ومنها ايضا ما يعرف بالجرائم الواقعة على المعلومات المدرجة في بالنظام المعلوماتي، تتم بواسطة الاحتيال وإدخال معطيات في نظم المعالجة وايضا جرائم واقعة على برامج المعلوماتية عن طريق تحديد البرنامج اولا ثم التلاعب به وتعديله.

أما أركان الجريمة المعلوماتية

الركن الشرعي الذي يظهر في حالة توافر الشرط الافتراضي والأساسي للجريمة المعلوماتية الا وهو نظام المعالجة الآلية للمعطيات.

أما الركن المادي فقد عرفه الفقهاء على أنه كل فعل ينتج عن توقيف نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي، ويتوافر هذا الشرط والركن إذا تم الاعتداء على نظام المعالجة الآلية للمعطيات أو سلامته.

والركن المعنوي يقوم بقيام المسؤولية الجنائية ولأجل التأكد من وجود هذا الركن من عدمه فقد صرح بعض الفقه إمكانية فصل القصد الجنائي الخاص عند العام لهذه الجرائم.

الفصل الثاني:

إجراءات ووسائل التحري في الجرائم المعلوماتية

الفصل الثاني: إجراءات ووسائل التحري في الجرائم المعلوماتية

مع تزايد الجرائم المعلوماتية نتيجة التطور التكنولوجي، أصبحت إجراءات التحري ضرورية لكشف الجناة وجمع الأدلة الرقمية. تعتمد هذه الإجراءات على تقنيات متخصصة في التحليل الجنائي الرقمي وتتبع الأنشطة المعلوماتية ، لضمان حماية البيانات وتحقيق العدالة.

المبحث الأول: إجراءات التحقيق بالوسائل الحديثة

إجراءات التحري في الجرائم المعلوماتية تعتمد على تقنيات حديثة لجمع الأدلة وتتبع الجناة، بهدف حماية البيانات وتحقيق العدالة من بينها:

المطلب الاول: المراقبة والترصد المعلوماتي

سيتم تقسيم هذا المطلب إلى فرعين، حيث تم تخصيص الفرع الأول إلى المراقبة والترصد المعلوماتي ، أما الفرع فهو مخ الثاني فخصص إلى أسباب المراقبة المعلوماتية.

الفرع الأول: تعريف المراقبة المعلوماتية

هي السلطة التي تطبق وتمارس بمقتضى الشرع والنظام وذلك لتحقيق الأهداف ومراعاة المصالح العامة من خلال استخدام تقنيات معلوماتية تمكن السلطات من تنفيذ النظام.

وقد عرف بعض المعاصرين المراقبة المعلوماتية بأنها : استخدام الوسائط المعلوماتية للتأكد من وجود الخاضع لها خلال فترة محددة في المكان والزمان السابق الإتفاق عليها بين الشخص الخاضع لها.[1]

[1] ديابلو محمد نجيب، الجريمة الالكترونية وجهة الدليل الرقمي في الاثبات الجنائي، ط 01 المركز التجاري الشرق أدنى للدراسات الاستراتيجية المملكة المتحدة بريطانيا، 2024، ص 16

إضافة الى تعريف آخر مفاده: "هي تسليط الأجهزة المعلوماتية على شخص بحيث يتم مراقبته عن طريق الاجهزة الصوتية أو البصرية فتحدد أماكن تواجد الشخص أو أقواله أو أفعاله كتحركاته وكتابته سواء كان بعلمه أو بلا علمه."[1]

الفرع الثاني : اسباب المراقبة المعلوماتية

المراقبة الالكترونية للأشخاص إذا تحققت أسبابها ودواعيها وتمت على النحو الصحيح فأنها تثمر النتيجة المطلوبة منها والتي هي جلب النفع للفرد المراقب لنفسه وعن المجتمع ككل.

ولكون الاصل في الانسان الحرية وعدم المراقبة فلابد من حصر الاسباب التي يتوجب الانتقال عن هذا الاصل وهي على النحو التالي:

أ- **السبب الأول:** المراقبة المعلوماتية قد تكون بسبب اجراء وقائي للفرد المراقب كأن يغلب على ظن السلطة أن المتهم أو المشتبه به يخفي دليلا مهما في القضية، أو يخطط لارتكاب جريمة فإن السلطة تعمل عددا من الإجراءات التي من اولها المراقبة والمتابعة.

ب- **السبب الثاني:** أن المراقبة المعلوماتية قد تكون بسبب إجراء وقائي للمجتمع، كمراقبة أفراد المجتمع أو بعضهم عن طريق تطبيقات الحجر الصحي لمنع انتشار وباء وما شابه.

ت- **السبب الثالث:** أن المراقبة المعلوماتية قد تكون عشرية على الشخص المستحق لذلك، أو جزل امن مشويه بحت بكل هده سعيه، وهو خارج السجن لا سيما إذا كان مستمر ما بالإجراءات القضائية والنظامية، ويرى السلطة السماح له بالخروج لما يتمتع به من ومن السلوك داخل السجن والندم على ما سبق، والعزم على عدم التكرار، أو بسبب صغر سنه او كبره.

ث- **السبب الرابع** : تطبيق المراقبة المعلوماتية في حق السجناء الذين تقتضي ظروفهم الإفراج عنهم على نحو مؤقت، لن يتم إخراجه من السجن مؤقتا، لحضور مناسبة أسرية لابد منها ، أو لظروف

[1] – منيرة بنت محمود المطلق، **المراقبة الالكترونية، مجلة كلية الشريعة والقانون**، العدد 25 ، 2022، ص 17 - 23

صحية، وهو ما يطلق عليه " الافراج الصحي ". وتتوقف المراقبة المعلوماتية عندما ينقضي سبب الافراج الشرطي.[1]

ج- **السبب الخامس:** انها قد تكون اجراء وقائي، ترى السلطة ضرورته بحق المريض فتعرفه على الشخص المريض بمرض معد، بحيث يمنع من الخروج من مكان إقامته، وذلك منعا لانتشار العدوى .[2]

الفرع الثالث: حالات اللجوء إلى المراقبة المعلوماتية

يمكن القيام بعمليات المراقبة المنصوص عليها في هذه الحالات التالية:

- للوقاية من الافعال الموصوفة بجرائم الإرهاب أو التخريب او الجرائم الماسة بأمن الدولة.

- في حالة توفر معلومات من احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة او الاقتصاد الوطني.

- المقتضيات التحريات والتحقيقات القضائية عند ما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة المعلوماتية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عملية المراقبة في الحالات المذكورة أعلاه الا بإذن مكتوب من السلطة القضائية المختصة.

[1] - منيرة بنت محمود المطلق، مرجع سابق، ص ص 17 – 23.

[2] - المرجع نفسه، ص ص 17 – 23.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" المادة، يختص النائب العام الذى مجلس قضاء الجزائر يمنح ضباط الشرطة القضائية المنتمين للهيئة إذن المدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير بين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها .[1]

الفرع الرابع: انواع المراقبة المعلوماتية

أنواع المراقبة المعلوماتية متعددة ومتطورة على نحو سريع السرعة تطور التقنية المعلوماتية المعاصرة، وفي هذا المطلب اذكر أهم انواع المراقبة المعلوماتية المستقلة في الوقت الحاضر فمنها:

– **المراقبة بواسطة الكاميرات:** ويستخدم هذا النوع المراقبة سير السيارات في الطرف العامة ومراقبة الموطنين فى أعمالهم، ومراقبة الأشخاص في المراكز التجارية والفنادق...

– **المراقبة بواسطة الهاتف:** ويستخدم هذا النوع المراقبة المكالمات المانعة وتتبع مواقع الهواتف ورصد بياناتها، وقد تم كشف الكثير من الجرائم وتحديد مواقع المجرمين عبر مراقبة وتتبع المواقع وشبكات الهاتف من خلال الاشارات التي يبثها ويستقبلها ذلك الجهاز.

– **المراقبة بواسطة الأساور المعلوماتية:** وهذا النوع يستخدم لمراقبة السجناء بين إطلاق سراحهم المشروط، والمراقبة سير الحجاج والمعتمرين عبر الأساور الإلكترونية، والمراقبة المستشفيات للمواليد الجدد.

– **المراقبة بواسطة الشرائح المعلوماتية:** ويتم زراعة تلك الشرائح في الجسم، كأن يتم زراعتها في أجسام البهائم لمراقبتها أو تتبع أصحابها وقد يتم وضعها في السيارات أو الممتلكات، لتتبع سيرها وتحديد موقعها.

[1] _ **القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق ل5 أوت سنة 2005، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، ج ر،ع47، المؤرخ في 5 أوت 2005.

– **المراقبة بواسطة التطبيقات المعلوماتية:** ويستخدم هذا النوع المراقبة الاشخاص حاملي الأجهزة التي تحتوي على تلك التطبيقات ولتحديد أمكنتهم ومدى التزامهم بالتوجيهات، ويتم ذلك عن طريق الأقمار الصناعية ومن أمثال ذلك تطبيق " تباعد" و"توكلنا.[1]

الفرع الخامس: ضوابط المراقبة والترصد المعلوماتي

لا بد من وجود ضوابط لنظام المراقبة والترصد المعلوماتي تنفذ عن طريق السلطة. على نحو صحيح من بينها:

– **الضابط الأول:** أن تكون المراقبة بإذن الحاكم وأن تنفذ عن طريق السلطة، وفي حال رأت السلطة ما يستدعي مراقبة شخص ما لوقوعه في محل تهمة، فإنه يتم مراقبته عن طريق النيابة العامة أو غيرها من الجهات.

– **الضابط الثاني:** إنتفاء القدر من المراقبة المعلوماتية فيشترط أن لا تسبب أجهزة المراقبة ضرراً صحيا على المراقب، فلا بد من التأكد من عدم خطورة استعمال السوار الإلكتروني، أو الشريحة مثلا.

ومن القدر أيضا أن يترتب على المراقبة مثلا كشف عورة الإنسان المراقب او تصميم المراقبة عليه لتتجاوز المراقبة أسرته من غير مصلحة، أو التشهير به أنه تتم مراقبته إلا أن كان هناك مصلحة في ذلك ، كما لا يكون فيها إهانة لكرامة الجاني.

– **الضابط الثالث:** أن تكون المراقبة المعلوماتية ملائمة لحال الشخص وذلك بمراعاة حال الإنسان المراقب من حيث حسن سلوكه بعد فعل الجناية وهل هو من أهل الصلاح والشرف، ومن حيث اجابته تمرض لا يرجى شفاؤه ، بحيث يخرج ليكمل عقوبته في بيته أو من حيث الحمو لحوق التهمة

[1] _منيرة بنت حمود المطلق، مرجع سابق، ص26.

به بحيث يستدعي مراقبته حتى تثبت إدانته أو براءته، ومن حيث عدد سوابق المتهم وكونها التهمة الأولى، ونحو ذلك مما يجعل الشخص المراقب مستحقا لها.[1]

– **الضابط الرابع**: أن تكون المراقبة ملائمة لحال الشخص وذلك بأن تكون المراقبة المعلوماتية ملائمة لحال البناية من حيث اسبابها، من حيث عظيم الجنابة وخفتها و تأثيرها وخطورتها على المجتمع ماذا كانت الجنابة عظيمة لم سمح له بالخروج لظهور صلاح الجانى وتوبته، فتستمر المراقبة المعلوماتية عليه حتى لا تسول له نفسه تكرارها، وفي المقابل قد تكون الجناية بسيرة لا تستدعي المراقبة بعد معاقبة الجاني والإفراج عنه.

– **الضابط الخامس**: أن تكون المراقبة المعلوماتية متوافقة مع مصالح المجتمع عنا تكون المراقبة المعلوماتية مراعبة لمصلحة المجتمع، فيراقب من فيه خطر على المجتمع. وتراعي مصلحة المجتمع من حيث تخفيف أو تشديد العقوبة كما يراعي أن لا يترتب على العقوبة ضرر بالمجتمع او يهدد صحة أفراده. [2]

المطلب الثاني: الشهادة المعلوماتية والتفتيش

الفرع الاول: الشهادة المعلوماتية

كان ولا يزال سماع الشهود مصدرا اساسيا وغالبا من مصادر الادلة الجنائية حيث أنه في محمل القضايا لا يمكن ان تكون هناك قضية بدون شهود فشاهد حين يدلي لمعلوماته لا يكون له إرتباط بدعوة بأي إرتباط اذ هو ليس من اطرافها وان يقدم معونة ضرورية لتحقيق الحقيقة وشاهد ملتزم بتقديم الشهادة بصفته في المجتمع كفرد في جماعة و الإلتزام المفروض عليه بعرضه للمسألة القانونية وفرض غرامة مالية وايضا احضاره للمحكمة واذا نكل عن الشهادة او زور مضمونها ولا

[1] – منيرة بنت حمود المطلق . مرجع سابق ، ص ص 27-26.

[2] – المرجع نفسه ، ص ص 27-26.

تقتصر الشهادة على التحقيق الابتدائي بل لازمة ايضا مع التحقيق النهائي، ولا تكون فقط في التحقيق القضائي ، الرجال البحث وتحوي يمكنهم ان يقوموا بتحقيق اولى يسمعون فيه الى الاقوال.

في معظم القضايا خاصة التي تحيطها ظروف غامضة، فإن الشهود يتوفرون سواء اشار إليهم المشتكي في بلاغة او قام بتوثيقهم المحتوى من خلال إفادة المشتكي، لذا يجب ان يتوافر في الشهود شروط مهمة:

- أن يكون ذا أهلية.
- أن يكون يتمتع بالجلسة التي تمكنه من إدراك المعلومة التي سوف يشهد عليها كافة تفاصيلها.
- أن يكون عاقلا.[1]

وهناك اثنين من عوامل تؤثر في الشهادة قد يرغب الشاهد قول الحقيقة لكنه لا يستطيع ذلك لسبب او لآخر قد يكون ضعيف الادراك او صغر او كبر سنه او ضعف بصره الى اخره وقلة الخبرة التي يتمتع بها الشاهد ولوجود الاختلافات بين الناس في درجة استيعابهم وادراك تفاصيل الحدث الذي يجري امامهم حتى الاحداث اليومية التي تحدث معهم ناهيك عن الاحداث المثيرة.

والشهادة في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة العالية في الحاسب الالي وصاحب التخصص الذي لديه العلم والدراية عن ماذا سوف يدلي بوقائعه شهادته والذي يكون لديه معلومات جوهرية هامة او اللازمة للدخول الى نظام المعالج الالية للبيانات اذا كانت مصلحة التحقيق تقتضي ذلك للتنقيب عن ادلة الجريمة المعلوماتية ويمكن ان يكون شاهد احدى الطوائف التالية:

- **مشغلوا الحاسب**: وهم الخبراء الذين لديهم الخبرة والدراية العالية بالتشغيل الحاسوب الالي ومعرفة التطبيقات وقواعد البيانات والاجهزة والملحقات الواصلة بالحاسوب.

[1] _عبد العزيز زينب ، **الترصد الإلكتروني وحماية الحرية الشخصية في قانون الفساد**، رسالة ماجستير منشورة جامعة قاصدي مرباح ، الجزائر ،2017/05/21، ص 36.

- **المحللون:** هو المحلل الذي يحلل الخطوات ويقوم بالتجميع بيانات نظام معين وتحليلها الى وحدة منفصلة واستنتاج العلاقات الوظيفية منها كما يعمل على تتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات.
- **المبرمجون:** وهم الاشخاص المختصين في كتابة اوامر البرنامج كصناعة برنامج الفيسبوك او فيروس لنشره على الشبكة العنكبوتية.
- **مهندسوا الصيانة والاتصالات:** هم الاشخاص المختصين في صيانة الشبكة العنكبوتية وتقنيات الحاسوب بكافة مكوناتها.
- **مديروا النظام:** وهم الذي يوكل إليهم اعمال الإدارة في النظم المعلوماتية.

وعلى صاحب الصلاحية من الشرطة او النيابة العامة والقاضي عند اخذ افادة الشهود ان ينصب عينيه عن امرين مهمين هما:

– ان تغطي الشهادة جميع الوقائع او تغطي الجزء المهم في محور القضية الذي يدلي الشاهد بأقواله عنه.

– ان يتأكد بان الشاهد لا يكذب ويقول الحقيقة وهذه تأتي من خلال شهادته على محضر الافادة او تحقيق بأن لا يأتي بأقوال غير منطقية أو بعيدة كل البعد عن مسرح الجريمة.[1]

الفرع الثاني: التفتيش الالكتروني

أولا: تعريف التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش وبقدر ما اعتبره اجراء من اجراءات التحقيق واحاطة بضوابط صارمة نظرا لأهميته في كشف الادلة وخطورته فيما قد يترتب عنه من مساس بحرية الاشخاص وبكرامتهم ومما يؤكد ذلك اهتمام الدستور الجزائري بهذه النقطة اذ نص في

[1]– مصطفى محمود محمد، **الاثبات في المواد الجنائيه في القانون المقارن**، ط 1، القاهرة ،1987 ص 214.

المادة 40 منه بالقول فلا تفتيش الا بمقتضى القانون وفي اطار احترامه ولا تفتيش الا بأمر مكتوب صادر عن السلطة القضائية المختتمة. [1]

وكما هو الشأن في مختلف التشريعات العربية فان التعريفات تجمع على ان التفتيش هو اجراء من اجراءات التحقيق يباشر موظف مختص بهدف البحث عن ادله ماديه لجناية أو جنحه ونسبتها الى المتهم تحقق وقوعها في محل يتمتع بجرمه وذلك وفقا للضمانات والقيود القانونية المقررة ويعرف كذلك التفتيش بانه اجراء من اجراءات التحقيق غريته ضبط ادلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شانها [2]

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في اطار قانون الاجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد نقطة يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث او بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات لإنجاز مهمتها. [3]

---

[1] – المادة 12 من **الاعلان العالمي لحقوق الانسان**، مصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 1948/12/10.

[2] – رشيده بوكر، **جرائم الاعتداء على نظم المعالجه الآليه وفي التشريع الجزائري المقارن**، ط1، منشورات الحلبي الحقوقيه بيروت لبنان، 2012، ص 3.

[3] – المادة 05 من القانون رقم 04/09، مصدر سابق.

ثانيا: شروط تفتيش المنظومة المعلوماتية

يمكن تقسيم شروط التفتيش الكتروني الى نوعين موضوعيه وشكليه:

1- الشروط الموضوعية للتفتيش الالكتروني

- وقوع جريمة المعلوماتية: والجريمة المعلوماتية هي كل فعل غير مشروع باستخدام الحاسب الالي لتحقيق اغراض غير مشروعه [1]، وحتى يكون التفتيش صحيحا متفقا عليه قانونيا فإننا لابد وان يكون بصدد جريمة معلوماتية مما يعتبر القانون جناية او جنحة [2].

- تورد شخص او اشخاص معينين في ارتكاب الجريمة المعلوماتية او الاشتراك فيها: ينبغي ان تتوافر في حق الشخص المراد تفتيشه دلائل كافيه تدعو الى الاعتقاد بانه قد ساهم في ارتكاب الجريمة الإلكترونية سواء وصفه فاعلا لها او شريكا فيها وفي مجال الحسب الالي.

- توافر امارات قوية او ادلة تفيد في الكشف عن الجريمة المعلوماتية: لا يوجد تفتيش الا اذا توافرت لدى المحقق اسباب كافية على انه يوجد في مكان او لدى الشخص المراد تفتيشه ادوات استخدمت في جريمة إلكترونية واشياء متحصل منها.

- محل تفتيش الخاص بالنظام الحاسبي الالكتروني: وهي كل مكونات الحاسب سواء كانت ماديه او معنويه او شبكات الاتصال الخاصة بها بالإضافة الى الاشخاص الذين يستخدمون الحاسب الالكتروني محل التفتيش[3].

---

[1] _هشام محمد فريد رستم، **قانون العقوبات ومخاطر تقنيه المعلومات**، مكتبه أسيوط، 1992 ص30.

[2] _خالد ممدوح إبراهيم، **الفن التحقيقي الجنائي في الجرائم الالكترونية**، ط 1، دار الفكر الجامعي للنشر، الاسكندريه، 2009، ص 210.

[3] _علي عدنان الفيل، **اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمه المعلوماتية دراسه مقارنة** مكتب الجامعي للنشر كليه الحقوق جامعه المفصل، 2011، ص 50.

2- الشروط الشكلية للتفتيش الالكتروني

يستخلص من نص المادة 5 من القانون 09/ 04 المشار إليه سابقا بان التفتيش في مجال الجرائم المعلوماتية والذي يختلف كليا عن التفتيش العادي يتوقف اساسا على طبيعة المكان الذي يحتوي اجهزه الكمبيوتر ومكوناتها وفيما إذا كان خاصا ام عاما هذا فضلا عن تحديد الاقليم فيما إذا كان وطنيا أو أجنبيا.[1]

ويمكن تحديد اهم عناصر التفتيش فيما يلي من خلال القواعد العامة للقانون الاجراءات الجزائرية كالتالي: وفقا للأحكام المادة 44 من قانون الإجراءات الجزائية، لا سيما بعد التعديل وهي:

- وجود اذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.

- الاستظهار بالإذن قبل الدخول للمنزل المراد تفتيشه.

- ان يتضمن الاذن وصف الجريمة البحث عن الدليل بشأنها وعنوان الاماكن المقصودة بالتفتيش.

- حضور الشخص المعني بالتفتيش لمسكنه أو من ينوب عنه.

- في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين لسلطته.[2]

اما التفتيش في الاماكن العامة وهي التي يرتدوها العامة في كل وقت ولا يتمتع لجرمة المنزل فيمكن دخولها خلاف الاماكن الخاصة وتفتيشها إذا ما تم غلقها انتهاء فطرة العمل وانصراف العامة[3].

---

[1] _**القانون رقم 02/15 المؤرخ في 20 سبتمبر 2006، المتعلق بالإجراءات الجزائية**،ج ر، معدل ومتمم بالقانون رقم 06/24 المؤرخ في 28 أفريل 2024.

[2] _ الماده 44، المصدر نفسه.

[3] _ علي عدنان الفيل، مرجع سابق، ص54.

ثالثا: التفتيش الالكتروني عن بعد

اجاز القانون الجزائري 09/ 04 المشار له سابقا القيام بتفتيش المنظومة المعلوماتية عن بعد ويقتضي ذلك الدخول اليها دون اذن صاحبها والولوج الى الكيان المنطقي للحاسوب، فالتفتيش يستهدف اشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات ولان هذه قد تكون وسيلة لارتكاب الجريمة.

– فقد اجاز المشرع الجزائري من افراغ او نسخ تلك المعلومات المشكوك فيها والتي من شانها الافادة في الكشف عن الجريمة او مرتكبيها او حجز المعطيات وضبطها كدليل اثبات ضد المتهم يقدم أمام المحكمة.

– الا انه برنامج الحاسوب وقاعدة البيانات تتمتع بالحماية القانونية في القانون الداخلي وفي اتفاقية الدولية كما هو الشأن في التشريع الجزائري اذا اعتبر برنامج الحاسوب وقاعدة البيانات مصنفات محمية بموجب قانون 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة[1].

المطلب الثالث: الصعوبات التي يواجهها المحققون في الجريمة المعلوماتية

عملية البحث والتحري عن الجريمة المعلوماتية هي من الاجراءات المهمة، ومن خلالها يمكن الكشف عن الجريمة إذا قام المحقق بإتمام العمل وفقا للإجراءات القانونية السليمة، الا أنه يمكن أن يواجه المحقق وخلال إجراءات البحث والتحري صعوبات وتحديات وتقود هذه الصعوبات لمشاكل يواجهها المحقق نفسه، أو بفعل الجاني، أو الأسباب وعوامل أخرى، وهذا ما يمكن ايجازه وفقا للتالي:

أولا : تكتم المجني عليهم وإحجامهم عن الابلاغ عن الجرائم المعلوماتية ويعود ذلك إلى عدة أسباب خوف الجهات المتضررة من الابلاغ عن الجريمة خشية من عمليات التفتيش التي تقوم بها جهات التحقيق وكشف أسرارهم أو الاطلاع على معلومات وبيانات يتكتمون عن الإفصاح عنها، أو اذا

[1] _ محمد يحياوي منير بودشيش خليل، مرجع سابق، ص58.

قاموا بالإبلاغ عنها ستؤدى إلى ضرب المؤسسة خشية على سمعتها لنقص ثقتهم في نظام الحماية الخاص بتلك المؤسسات.

وأيضا جعل المجني عليهم بأن هذه الهجمات هي هجمات إجرامية معلوماتية تؤدي الى اتلاف او دمار نظام المؤسسة

ثانيا: اهتمام الشركات والمؤسسات بالجانب الترويجي والتسويقي لمنتجاتها لتحقيق الارباح واهمالها للجانب الأمني للحصول على كم هائل من الأرباح، من خلال بلاغ عنها خوفا على سمعتها.[1]

ثالثا: عدم إدراك خطورة للجرائم المعلوماتية من قبل المجني عليه كما أسلفنا سابقا، اما لعدم علمه الكافي بأن حاسوبه الآلي يتعرف عليه بنوع من البصمات المعلوماتية ، أو يعلم بذلك لكن لا ينظر إلى ما يتعرض له.

رابعا: نقص الخبرة من جهات البحث والتحري والتحقيق في الجرائم المعلوماتية ، حيث أن عمل وهان البحث والتحري من أهم الأعمال التي من خلالها تؤدي إلى كشف الحقيقة والنقص الخبرة في هذا المجال يؤدي الى العروف بالمقدرة عن البحث والتحري، ويشترط على من لتعامل بعده الطبيعة الخاصة للجد القران يكون مؤهلاً على التعامل بها.[2]

خامسا: قلة خبرة القائمين بالتحقيق في الجرائم وذلك لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارات في علنية استخدام جهاز الحاسوب والانترنت وعدم توافر المعرفة بأساليب تدابير جرائم الحاسوب والأنترنت وقلة المعرفة واللغات الأجنبية لاسيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة، أصبحت تشكل الطابع المميز للمحادثات وأساليب التفاهم

[1] – محمد منير يحياوي، بودشيش خليل، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات الماستر المهني، تخصص إدارة التحقيقات الإدارية والمالية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة 2018-2019، ص72.

[2] – المرجع نفسه، ص72.

بينهم . وليس هذا فحسب. بل احترام العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لديهم تعرف بلغة المختصرات .

سادسا: الصعوبات التقنية لاستخدام بروتوكول TCP/IP في الإثبات

هناك تحديات عند استخدام المحقق بروتوكول TCP/IP كدليل الكتروني وهي:

بروتوكول IP : وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الاشخاص، لذلك فمن الصعب إثبات أن شخصاً محدد أحدث الفعل الغير مشروع، ومع ذلك يمكن أن يستخدم كقرينة فضائية ضد مالك الجهاز على أن يثبت ذلك العكس.

الجاني يعمد الى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة، لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان وبعد مرور فترة زمنية لقوم بغلق الاتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الاجرامي غالبا موزعاً على عدة عناوين.

تكون المعلومات المحلية لمصدر عنوان IP غير حقيقية او زائفة وهذا ممكن باستخدام مصدر زائف له بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر.

سابعا: ارتفاع تكاليف جمع الأدلة

ان التحقيق في هذه الجرائم يحتاج الى خبراء مختصين وهؤلاء يحتاجون إلى دورات متزامنة مع تطور التقنية المعلوماتية ، وهذا الأمر مرتبط بالتكاليف الباهظة، كذلك التحقيق في الأدلة يحتاج إلى فحص آلاف الصفحات خصوصاً عندما لا تثبت تلك الصفحات ذلك. [1]

[1] – عدلى رحمان ، سعد الدين تامر البشير، **التحقيق الحناني في الجرائم الالكترونية**، مذكرة من متطلبات نيل شهادة الماجيستر في حقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة زيان كلية الحقوق، جامعة زيان عاشور 2020 /2021، ص 25، 26.

المبحث الثاني: اجراءات التحقيق بالوسائل التقنية

يحتوي القانون 09/04، ستة فصول تناولت على التوالي احكام عامة، مراقبة الاتصالات المعلوماتية ، القواعد الاجرائية، التزامات مقدمي الخدمات والهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وبذلك قد يكون القانون 09 /04 تضمن مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع الجرائم الالكترونية، او الكشف عنها وعن مرتكبيها في وقت مبكر ومن بينها تعاون مزودي الخدمة في جهات التحقيق.

المطلب الاول: تعاون مزودي الخدمة مع جهاز التحقيق

فرض القانون 09/04 على مقدمي الخدمات مجموعة من الالتزامات تساهم بدورها في الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل أهم هذه الالتزامات.[1]

الفرع الاول: تقديم المساعدة للسلطات

حيث يجب على مقدمي الخدمات تقديم المساعدة اللازمة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات وبوضع المعطيات التي يتعين حفظها تحت تصرف السلطات المكلفة بتحريات القضائية، كما يتعين على مقدمي الخدمات بإطار هذه المساعدة كتمان وسرية المعلومات، والعمليات التي ينجزونها بطلب من المحققين وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

الفرع الثاني: حفظ المعطيات المتعلقة بحركة السير

يلتزم مقدمو الخدمات بحفظ ما يلي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة

[1] - القانون 09/04، مصدر سابق.

- المعطيات المتعلقة بالتجهيزات المستعملة للاتصال.

- معطيات المتعلقة بالخدمات التكميلية المطلوبة والمستعملة ومقدميها

- المعطيات التي تسمح بالتعرف على المرسل اليه او المرسل إليهم بالاتصال وكذا عناوين المواقع المطلع عليها.[1]

إضافة إلى ما سبق نص المشرع الجزائري مقدمي خدمة الإنترنت بالتزامات المعينة، تدفق كذلك الى الوقاية من الجرائم الالكترونية ومكافحتها وتتمثل هذه الالتزامات في:

_ التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل للدخول اليها غير ممكن.[2]

وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحوي معلومات مخالفة للنظام العام او الآداب العامة او اخبار المشتركين لديهم بوجودها.

بموجب المادة 10 من قانون 04/ 09 الزمت مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش كما الزمتهم ايضا بكتمان السر، بخصوص العمليات التي ينجزونها بطلب المحققين وما تحصل عن ذلك من المعلومات وذلك تحت طائلة العقوبات التي يقررها القانون في حاله إفشاء أسرار تحقيق ويطلقوا على مقدمي الخدمات في مجال الإنترنت تسمية الوسائط في خدمة الإنترنت ويكمن دورهم في تمكين مستخدمي الانترنت من الدخول الى الشبكة والاطلاع عليها ،قد عرفت المادة الأولى الفقرة الثالثة من الاتفاقية الأوروبية لمكافحة جرائم الالكترونية التي تم إقرارها في بودباست سنة 2001:" عرفت مزودي الخدمات بأنه كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الاتصالات بين أجهزة الكمبيوتر

---

[1] – مهداوي حنان " التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، **مجلة الفكر القانوني والسياسي** مجلة 06، العد02، كلية الحقوق والعلوم السياسية، جامعة سطيف 2، 2022، ص ص 1070-1071.

[2] – المرجع نفسه، ص ص 1070-1071.

وكذلك كل ما تولى معالجة المعطيات المخزنة نيابة عن المزود الخدمة على هذه أهم إجراءات البحث والتحري في إجراءات البحث والتحري في الجرائم الالكترونية.[1]

في اطار تعديل من القانون إجراءات الجزائية الجزائري بالقانون 06/ 22 مؤرخ في 20 ديسمبر 2006، الذي جاء فيه إجراءات مستحدثة للكشف عن الجرائم الماسة بأنظمة المعالجة للمعطيات.

المطلب الثاني: تسجيل واعتراض المراسلات.

الإذن المكتوب المسلّم لضبّاط الشرطة القضائية المنتدب الذي مكنّه المشرع الجزائري من صلاحية إعتراض المراسلات، وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية وهي إجراءات تباشر بشكل خفي على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة، و إلتقاط صور يكون بالتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة أما تسجيل الاصوات فيكون عن طريق وضع الرقابة على الهواتف وتسجيل الأحاديث التي عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة وقد يتم أيضا عن طريق إلتقاط إشارات لاسلكية او إذاعية.

إنما يهم هو مثل هذه الإجراءات يمكن له المساس بالحرية الشخصية خصوصا إذا علمنا أنه سرية المراسلات هي حق دستوري فقد جاء في المادة 3 من القانون رقم 04 /09 المؤرخين في 5/اوت 2009 [2]

---

[1] – بن محمد الأمين " **وسائل أساليب التحري في مجال مكافحة الجرائم الالكترونية**، مذكرة نهاية الدراسة لنيل شهدة الماستر، تخصص قانون قضائي كلية الحقوق، جامعة عبد الحميد بن باديس، مستغانم 2020، ص ص 78 – 79.

[2] – المادة 03 من القانون رقم 04 /09، مرجع سابق.

يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال مكافحتها انه:" مع مراعاة الاحكام القانونية التي تخص السرية المراسلات والاتصالات "يمكن لمقتضيات حماية النظام العام او مستلزمات التحريات او التحقيقات القضائية الجارية وفقا لقواعد النصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات انتقالية لمراقبة الاتصالات المعلوماتية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية. [1]

بالإضافة إلى أنه كل متهم بريء حتى تثبت إدانته، لذلك يجوز إثبات أو نفي الإتهام على المشتبه فيه باللجوء الى وسيلة التسجيل الصوتي و إعتراض المراسلات والتقاط الصور في الأماكن العامة والخاصة وخصوصا أن مثل هذه الإجراءات أو الوسائل قد لا تمس بشخص المتهم فقط، إنما كذلك بمن يحيطون به من اقاربه ومعارفه.

يفرق الفقه بين مصطلح إعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن ويخضع لتقدير الهيئة القضائية وعند تسخير مصالح البريد والمواصلات في المادة 65 مكرر بموجب قانون الإجراءات الجزائية تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع، بمعنى أنه إجراء التحري والتحقيق لهذا نجد المشرع الجزائري حاول أن يوفق بين هذه المتعارضات بأن أجاز هذه الأساليب ولكن بضوابط، وهي: مباشرة

التحري بإذن من وكيل الجمهورية المختص والتزام أعوان وضباط الشرطة القضائية القائمين بإجراء السر المهني.

[1] – عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الدور الثاني، تخصص ادارة التحقيقات الاقتصادية والماليه، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة، 2019، 2018، ص ص 53-57.

الفرع الأول: مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء إعتراض المراسلات وتسجيل الأصوات و إلتقاط الصور بقصد التحرير والتحقيق عن جرائم المساس بأنظمة معالجة الآلية للمعطيات إلا بإذن من وكيل الجمهورية المختص وتباشر هذه العمليات تحت مراقبته وهذا ما قررته المادة 4 من قانون 09/04 التي جاء فيها انه:" لا يجوز إجراء عملية المراقبة في الحالات المذكورة الا بإذن مكتوب من السلطة القضائية المختصة ويجب أن يتطلب الإذن كل عناصر التي تسمح بالتعرف على الاتصالات المطلوب بالتقاطها والأماكن المقصودة سواء كانت سكنية أو غير سكنية.[1]

وعند مباشرة التحريات والتحقيقات يحرر ضابط الشرطة القضائية المأذون له من طرف القاضي المختص محضر عن كل عملية إعتراض للمراسلات وتسجيل الاصوات و إلتقاط الصور وحتى عن عملية وضع الترتيبات التقنية وعملية الالتقاط والتسجيل الصوتي سمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات و الإنتهاء منها، بحيث يشتمل المحضر على كل بياناته المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة ويجب أن يشتمل المحضر على توقيع محرره في نهايته، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له المراسلات والصور أو المحادثات المسجلة في إظهار الحقيقة في محضر، يوضع بملف المتهم وتنسخه و تترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء.

الفرع الثاني: الالتزام بالسر المهني

تكون اجراء التحقيق والتحري بسرية ومن ثم فإن بحثها ضمن الضمانات الممنوحة للمتهم والسرية، تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم بالمحافظة على السر المهني، فقد نص المشرع الجزائري صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به، فالضابط المأذون له باعتراض مراسلات وتسجيل الأصوات و إلتقاط صور

[1] – عمار حشمان، مرجع سابق، ص ص 53 –55.

ملزم قانونا بكتمان السر المهني، ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام ذلك السر فقد نص على ذلك قانون الإجراءات الجزائية وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات، وتحت طائلة العقوبات المنصوصة عليها فيمنع منعا باتا ان يخبر المشتبه فيه بهذه التحريات أو أي شخص اخر كذلك يمنعه على ضابط الشرطة المأذون له أن يفصح عن مضمون محضر التحريات مع أي شخص تحت طائلة الجزاء الجنائي، بتهمة إفشاء السر المهني.[1]

المطلب الثالث: الخبراء المعلوماتيين

سيتم التطرق في هذا المطلب إلى فرعين، الفرع الأول تم التطرق فيه إلى تعريف الخبير التقني المعلوماتي، أما الفرع الثاني فتم تخصيصه لشروط الحصول على صفة الخبير القانوني.

الفرع الاول: تعريف الخبير التقني المعلوماتي

هو شخص ذو دراية عالية له إلمام بموضوع فني أو علم أو عمل يستعين به القضاء في امور تدخل في الاختصاص ولا يجوز له ان يجاوز المهمة المعهودة له بها، ويشترط فيها يكون انسانيا واجتماعيا وعرف كذلك بأنه كل شخص له دراية خاصة عالية بمسألة من المسائل، وله كفاية فنية وعلمية خاصة أما في مجال الجرائم المعلوماتية يطلق عليه مصطلح الخبير المعلوماتي او الخبير الرقمي أو التقني. والذي يعرف بأنه الشخص الذي تعمق في دراسة الأعمال المعلوماتية تخصص في إدارة تخصص في أداة لفترة زمنية طويلة مما أكسبه خبرة عملية، بحيث أصبح ملما بتفصيلاته مما جعله متفوقا على الشخص العادي وجعله قادرا على ابداء الرأي المعلوماتي الرقمي في الامور المتصلة.[2]

---

[1] – عمار حشمان، مرجع سابق، ص ص 56 -57.

[2] – نبيهة قنفود، الخبرة التقنية في مجال إثبات الجريمة الإلكترونية، **مجلة جامعة الامير عبد القادر الاسلامية**، قسنطينة الجزائر، العدد 2، مجلد 30، 2022، ص ص 411، 412.

الفرع الثاني: شروط الحصول على صفة الخبير المعلوماتي

لا يكفي حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العلمية لأنها هي التي تحدد الكفاءة الفنية، ولذلك لا وجود لخبير لديه معارف متعمقة في وسائل في سائر انواع الحاسبات والبرمجة برمجيتها وشبكاتها او لديه القدرة على التعامل مع كل انواع الجرائم المعلوماتية مما تستوجب هذه الجرائم توافر شروط خاصة في الخبير التقني هي الالمام بتركيب الحاسوب وصناعته ونظم تشغيله الرئيسية، والفرعية، و المعالجة الالية وتحديد اماكن التخزين وسائل المستخدمة في ذلك كما يتطلب أيضا قدراته على الحفاظ على الأدلة المتحصل عليها دون تعرضها للتدمير او الاتلاف بالإضافة إلى قدرته على نقل أدلة الإثبات المرئية وتحويلها الى أدلة مقروءة. [1]

الفرع الثالث: انواع الخبراء

الطائفة الاولى: هم الخبراء من ضباط الشرطة القضائية الذين يعملون في مجال العمل الجنائي والادلة الجنائية، يقتضي تخصصهم تلقينهم و تدريبهم تدريبا خاصا ودراسة بعض العلوم كالكيمياء والطبيعة والهندسة والتصوير، و لمعاونتهم في التحليل العلمي، في مجال تخصصهم، وهذه الطائفة تتخصص في مجال فحص الأسلحة النارية، وللكشف عن التزوير.

الطائفة الثانية: وهم الخبراء من خارج الكليات العلمية كالطب، والهندسة والعلوم، ويتم تدريب هؤلاء وتلقينهم بعض المواد القانونية والشرطية.

الفرع الرابع: أحكام الخبرة في الجريمة المعلوماتية

تخضع الخبرة الفنية في أغلب التشريعات إلى نفس أحكام الخبرة القضائية من حيث القواعد القانونية، التي تحكم عمل الخبير وإجراءاته، أما التشريع البلجيكي الذي نظم الخبرة التقنية، في مجال الجريمة المعلوماتية من خلال القانون الصادر في 23 ديسمبر 2000، حيث نصت المادة 88 منه

[1] – نبيهة قنفود، المرجع السابق، ص ص 411، 412.

يجوز لأي قاضي التحقيق وللشرطة القضائية أن يستعين بخبير ليقدم وبطريقة مفهومة المعلومات اللازم عن كيفية تسجيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزونة، أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أي تطلب من الخبير تشغيل نظامه والبحث فيه هو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحمولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق وقد تناول المشرع الجزائري أحكام الخبرة في القسم التاسع من الباب الثالث في المواد 143 الى 155 من قانون اجراءات الجزائية. [1]

[1] – نبيهة قنفود، المرجع السابق، ص 413.

خلاصة الفصل الثاني

اجراءات التحقيق المتبعة في كافة الجرائم تأخذ بجميع عناصر التحقيق الجنائي المتكامل، وتمر بذات المراحل الفنية والشكلية، وتعد هذه الاجراءات في اي جريمة تماما كما هو الحال في الجرائم الاخرى او كانت الجريمة الكترونية، فالمحصل النهائي في التحقيق هو العثور على أدلة واضحة يمكن ان تستدل المحكمة فيها وتصدر العقوبة عليها.

يبدو جليا بأن عمل الاجهزة الشرطية والمخولين بذلك في البحث والتحقيق عن الجريمة، ما هو الا التوفيق بين مقتضيات كشف الحقيقة عند وقوع الجريمة، وبين حرية المتهم التي تصونها النظم القانونية باعتباره بريئا الى أن تثبت ادانته، وضرورة التحرك لجمع الادلة والاسراع بها دون تأخير.

ويعرف التحقيق انه مجموعة من الاجراءات التي تتبعها السلطات لاستظهار الحقيقة لجريمة معينة، والتثبت من كافة اركانها وكشف جوانبها تمهيدا للمسؤولية وايقاع العقوبة على المتسبب. وتعرف كذلك على انها علم متمم لقانون الجزاء واصول المحاكمات الجزائية، يرشد المحقق الى السير في التحقيق من البداية الى النهاية ويجمع الادلة المثبتة لوقوعها وكيفية ارتكابها والقبض على المتهم ومحاكمته.

ومن المسلم به ان الاجراءات السابقة لنشوء المحكمة للنظر في التحقيقات تنحصر في ثلاث اجراءات هي الاستدلال والاتهام، والتحقيق الابتدائي، وان مسألة البحث والتحقيق في جرائم الانترنت مسألة في غاية الاهمية بعض القوانين مثل مصر والامارات على اعطاء الحق لوزير العدل بالاتفاق مع الوزير المختص أو السلطة المختصة، بتحويل بعض الموظفين الى صفة مأموري الضبط القضائي بالنسبة الى الجرائم التي تقع في دائرة اختصاصهم.

وفي مجال التحقيق في الجرائم المعلوماتية ، تكمن صعوبة اكتشاف هذه الجرائم ومقاضاة المتهم في عدم وجود الخبرة الكافية والمعرفة الفنية لدى المحققين في استنتاج الادلة التي تم استخدامها في

ارتكاب الجريمة والذي يحتاجون الى المزيد من الخبرة العالية والكفاءة، وعدم وجود الخبرة الكافية والمعرفة الفنية في مجال الانترنت.

الخاتمة

الخاتمة

نستنتج من خلال هذه الدراسة أن الجرائم المعلوماتية. التي نتجت عن تعتبر من أخطر الجرائم التي تنجت عن الثورات المعلوماتية، وهو ما راجع إلى تطورها المستمر ومساسها بمختلف المجالات مما جعلها عقبة أمام جميع جوانب الحياة اليومية، ولكونها تتميز بخصائص مختلفة كثيرا عن الجريمة التقليدية في كونها جريمة عابرة للحدود الدولية والصعوبة في إثباتها وقلة الإبلاغ عليها، ومن أجل مواكبة التشريعات الرائدة في المجال المعلوماتي اقدم الشرع الجزائري على تعديل قانون الإجراءات الجزائية لسنة 2006 وكذا استحدث القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما عمل المشرع الجزائري على إتباع طرق حديثة تعمل على تسهيل عملية، التحري عن الجرائم الإلكترونية نظرا للخصوصية التي تتميز بها، حيث قام المشرع الجزائري وعلى سبيل الحصر بتحديد من يتمتع أو من أهم الأشخاص المكلفون بالتحري ، كما أعلى لهم بعض الصلاحيات الموسعة تحت إشراف وكيل الجمهورية وهذا لتسهيل مهامهم نسبيا، والدارس للقانون يلاحظ ظهور مفردات و مصطلحات حديثة ومختلفة من حيث المعاني والمباني وهذا ناتج عن الإنتشار الواسع للأنترنت الذي أدى في التأثير على سلوك الأفراد، حيث استعمل المشرع مصطلح التسليم المراقب في قانون الوقاية من الفساد ثم مصطلح المراقبة في قانون جرائم الانترنت، و استعمل كذلك مصطلح الاختراق في قانون الوقاية من الفساد ثم مصطلح التسرب في باقي الموائم الخاصة من بينها الجريمة المعلوماتية ، أي كان لابد عليه توحيد المصطلحات الإجرائية من خلال دراسة وإعادة صياغة المصطلحات بين القوانين الخاصة وقانون الإجراءات الجزائية.

1. وقد توصلنا من خلال دراستنا إلى مجموعة من النتائج والتي كانت إجابة عن الإشكالية التي طرحناها كالآتي:

2. عدم وجود تعريف أو مفهوم موحد وشامل للجريمة الإلكترونية وكذا صعوبة حصرها لتعدد وسائل ارتكابها وكذا المجالات الواقعة عليها.
3. الجريمة المعلوماتية ذات طابع دولي عابرة للحدود الوطنية فهي عالمية الوجود.
4. وجود عدة صعوبات تعيق عمل إجراءات مكافحة الجريمة المعلوماتية بالشكل الصحيح وأبرزها يتمثل في إختلاف القوانين من دولة لأخرى من حيث إجراءات التحري والاختصاص القضائي بين الدول.
5. نقص الخبرة لدى رجال الضبط القضائي وأجهزة العدالة أو الأجهزة الأمنية لصفة عامة فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال وهذا راجع إلى غياب أو نقص وسائل التكنولوجيا و البنية التحتية الحديثة التي تساعد في الكشف عن الجرائم المعلوماتية وملاحقة مرتكبيها.
6. أن المشرع الجزائري لم يتطرق إلى بعض الجرائم المعلوماتية وعلى رأسها الجرائم التقنية، ولذلك لا يمكن القياس عليها حسب نص المادة الأولى من قانون العقوبات.
7. وجود بعض النقائص فيما يخص الإجراءات الخاصة بمكافحة الجرائم المعلوماتية.

حيث أن المشرع لم يتطرق إلى ذكر الإذن والتسبيب في التسجيل الصوتي وهذا يعتبر مخالفا لما جاءت به المادة 46 من قانون الإجراءات الجزائية، وبناء على النتائج المتواصل إليها، يمكننا الإجابة على الإشكالية التي سبق طرحها بأن المشرع الجزائري قد وقف نسبيا في مجال التحري عن الجريمة المعلوماتية ، مع وجود بعض النقاط التي يتعين عليه تداركها.

وعلى هذا الاساس حاولنا وضع جملة من الاقتراحات التي من شأنها المساهمة في تدعيم الآليات القانونية المتعلقة بالتحري عن الجرائم الإلكترونية وهي كالاتي:

العمل على إيجاد مفهوم أو تعريف موحد للجريمة المعلوماتية من خلال وضع جملة من القوانين والعمل على تطورها وهذا ما يتطابق مع مبدأ الشرعية المذكور في نص المادة 01 من قانون العقوبات.

العمل على إثراء القانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المعلوماتية ببعض المواد القانونية لتجنب الوقوع في أي ثغرة قانونية من شأنها فتح المجال للمجرمين للإفلات من العقاب.

العمل على الاستفادة من خيرات وتجارب الأول الزائدة في مجال مكافحة الجريمة المعلوماتية من خلال فتح مجال التعاون الدولي بهذا الخصوص.

وضع آليات ردعية تتماشى مع التطورات الحاصلة من خلال فتح المجال لأصحاب الخبرات من خارج القطاع الأمني للمشاركة في مكافحة الجريمة المعلوماتية.

قائمة المراجع

– قائمة المصادر والمراجع:

أولا:المصادر.

الاتفاقيات:

1. الاعلان العالمي لحقوق الانسان، مصادر عن الجمعية العامة للأمم المتحدة، بتاريخ 1948/12/10

النصوص القانونية:

1. القانون رقم 04/15 المؤرخ في 01 فيفري 2015، المتعلق بالإجراءات الجزائية، ج ر ، ع 06 معدل ومتمم بالقانون رقم 06/24 المؤرخ في 28 أفريل 2024.
2. القانون رقم 04/09 المؤرخ في 5 أوت سنة 2005 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ج ر،ع47، المؤرخ في 5 أوت 2005 معدل ومتمم بالقانون 06/24 المؤرخ في 28 أفريل 2024.

الأوامر:

1. الأمر 66-155 المتضمن قانون العقوبات الجزائري، المعدل والمتمم بموجب القانون 24-06 المؤرخ في 28 أفريل 2024.

ثانيا: المراجع

– كتب:

1. أحسن بوسفيعة **الوجيز في القانون الجزائي العام**، دار هومة الجزائر، ط 10، 2011.
2. أحسن بوسقيعة، **الوجيز في القانون الجزائري الخاص** الجزء الأول، الطبعة الحادية عشر، دار هومة، الجزائر 148 2019.
3. أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط2، 2006.
4. أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، ط2، دار هومة، (الجزائر)،2007م.
5. ايمن عبد الله الفكري، **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية**، مكتبة القانون والاقتصاد، الرياض، 2014.

6. خالد ممدوح إبراهيم، **الفن التحقيقي الجنائي في الجرائم الالكترونية**، ط الاولى، دار الفكر الجامعي للنشر، الإسكندرية، 2009.
7. ديابلو محمد نجيب، **الجريمة الالكترونية وجهة الدليل الرقمي في الاثبات الجنائي**، ط 01 المركز التجاري الشرق أدنى للدراسات الاستراتيجية المملكة المتحدة بريطانيا، 2024.
8. رشيده بوكر، **جرائم الاعتداء على نظم المعالجة الآلية وفي التشريع الجزائري المقارن** ط1، منشورات الحلبي الحقوقية، بيروت لبنان 2012.
9. شريف حسين محمد، **القانون الواجب التطبيق على الجريمة الإلكترونية**، دار المصرية للنشر والتوزيع، مصر، 2025.
10. عدنان علي طياش، **الإنترنت في العصر الحديث وذكاء الاصطناعي والجريمة الالكترونية**، الكتاب 3، ط 1، 2022.
11. علي عدنان الفيل، **اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة** مكتب الجامعي للنشر كليه الحقوق جامعه المفصل، 2011.
12. مصطفى محمود محمد، **الاثبات في المواد الجنائية في القانون المقارن**، ط 1، القاهرة طبعة جامعة القاهرة 1987
13. نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط 01، دار الثقافة، الأردن، 2010.
14. هشام محمد فريد رستم، **قانون العقوبات ومخاطر تقنيه المعلومات**، مكتبه، أسيوط،1992.
15. نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي**، منشورات الحلبي الحقوقية 2005.

– أطروحات الدكتوراه:

1. عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد تلمسان، الجزائر، 2018.

– رسائل ومذكرات الماستر:

1. بن محمد الأمين، **وسائل أساليب التحري في مجال مكافحة الجرائم الالكترونية**، مذكرة لنيل شهدة الماستر، تخصص قانون قضائي كلية الحقوق، جامعة عبد الحميد بن باديس، مستغانم 2020.

2. شلاخ لطيفة، **انتشار الجريمة الالكترونية الماسة بالأشخاص في الهيئة الجزائرية**، دراسة ميدانية لبعض مستخدمي مقاهي النت بمدينة المسيلة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف – المسيلة ماي .2017

3. عبد العزيز زينب، **الترصد الإلكتروني وحماية الحرية الشخصية في قانون الفساد**، رسالة ماجستير منشورة، جامعة قاصدي مرباح، الجزائر ،2017.

4. عدلى رحمان، **سعد الدين تامر البشير، التحقيق الحناني في الجرائم الالكترونية**، مذكرة من متطلبات نيل شهادة الماجستير في حقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة زيا كلية الحقوق، جامعة زيان عاشور، 2020-2021.

5. عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الدور الثاني، تخصص ادارة التحقيقات الاقتصاديه والماليه، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة، 2019، 2018

6. كلتوم دهان، فاطمة دهان، **إجراءات البحث، والتحري في الجريمة المعلوماتية**، مذكرة مقدمة ضمن متطلبات بنك، شهادة ماستر أكاديمي، حقوق تخصص قانون جنائي وعلوم جنائية، جامعة غرداية 2022.

7.محمد منير يحياوي، بودشيش خليل، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة مقدمة لاستكمال متطلبات الماستر، تخصص إدارة التحقيقات الإدارية والمالية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرياح، ورقلة 2018-2019م.

المقالات العلمية:

1. بوضياف اسمهان "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر" **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، جامعة محمد بوضياف، مسيلة 2018 مارس 31 2018.
2. جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، **المجلة النقدية**، جامعة مولود معمري، تيزي وزو، الجزائر المجلد 11، العدد 02 نوفمبر 2016.
3. محمد قسيمة حمزة حضري، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في القانون الجزائري، **مجلة صوت القانون**، جامعة خميس مليانة، الجزائر، المجلد 07، العدد 02، نوفمبر 2020.
4. مهداوي حنان، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، **مجلة الفكر القانوني والسياسي**، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين – سطيف 2 – ، مجلد 06، العدد 02، 2022.
5. مهداوي حنان، التعليم القانوني للجريمة الالكترونية في التشريع الجزائري، **مجلة الفكر القانوني والسياسي**، كلية الحقوق والعلوم السياسية، جامعة محمد الامين دباغين سطيف 2، المجلد عدد 2، 2022.
6. نبيهة قنفود، الخبرة التقنية في مجال إثبات الجريمة الإلكترونية، **مجلة جامعة الامير عبد القادر الاسلامية**، قسنطينة الجزائر، العدد2، مجلد 30، 2022.
7. محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مراجعتها القانون الجنائي المعلوماتي، **مجلة دراسات وأبحاث**، كلية الحقوق ولأداء العلوم الاجتماعية، جامعة 8 ماي 1945، 2009.

الفهرس

شكر وعرفان 5

إهداء..... 6

الاهداء 7

مقدمة: ..... ب

الفصل الأول : الإطار الموضوعي للجريمة الالكترونية: 6

المبحث الاول: مفهوم الجريمة الإلكترونية : 7

المطلب الاول: تعريف الجريمة الإلكترونية 7

المطلب الثاني: خصائص الجريمة الإلكترونية:..... 14

المطلب الثالث : أنواع الجريمة الإلكترونية: 17

المبحث الثاني: خصوصية أركان الجريمة الإلكترونية 20

المطلب الأول: الركن الشرعي..... 22

المطلب الثاني: الركن المعنوي 27

المطلب الثالث: الركن المادي 27

الفصل الثاني: إجراءات ووسائل التحري في الجرائم الالكترونية..... 33

المبحث الأول: إجراءات التحقيق بالوسائل الحديثة 34

المطلب الاول: المراقبة والترصد الإلكتروني: 34

المطلب الثاني: الشهادة الإلكترونية والتفتيش:..... 39

المطلب الثالث: الصعوبات التي يواجهها المحققون في الجريمة الالكترونية:..... 45

المبحث الثاني :اجراءات التحقيق بالوسائل التقنية. 48

المطلب الاول: تعاون مزودي الخدمة مع جهاز التحقيق.....48

المطلب الثاني: تسجيل واعتراض المراسلات.....50

المطلب الثالث: الخبراء الالكترونيين. 53

الخاتمة 58

قائمة المراجع.....62

الملخص .....

ملخص:

أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، خاصة بعد اختراع الإنترنت، واستخلصنا اهم النتائج من هذا الموضوع والمتمثل في إجراءات البحث والتحري في الجريمة الإلكترونية أن عالم تقنية المعلومات الحديثة، عالم واسع لا يحده حد والوسائل المستعملة في ارتكاب الجريمة الإلكترونية متنوعة والتي تقوم بها جهات متخصصة في الكشف عن الجرائم، وهذا الأمر يتطلب وقفة من طرف المشرع والقضاء، لاتخاذ مجموعة من الإجراءات لمواجهة هذا النوع من الجرائم.

الكلمات المفتاحية:

جريمة إلكترونية- البحث والتحري- التشريع الجزائري.

Abstract:

Today, the world has come to live in Time of technological development what is known as the information revolution, especially after the invention of the internet We have extracted the most important results from this topic, that the world of modern information technology is a vast world without limits, and the means used in committing cybercrime are diverse and are carried out by entities specialized in detecting crimes. This matter requires a pause on the part of the legislator and the judiciary, to take a set of measures to confront this type of crime

Keywords: *cybercrime- research and investigation- Algerian legislation.*