وزارة التعليم العالي والبحث العلمي
جامعة عبـــاس لغرور
- خنشلـــــة -

كليـــة الحقوق و العلوم السياسية

القسم:الحقوق

نيابة العمادة في الدراسات للتدرج

الجرائم الإلكترونية في التشريع الجزائري والتشريع الفلسطيني

(دراسة مقارنة)

مذكرة مكملة لنيل شهادة الماستر في الحقوق
تخصص: قانون جنائي و علوم جنائية

إعداد الطالب:

معاذ عبدالعال

تحت إشراف الدكتور:

عرشوش سفيان

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الأصلية	الصفة
شنّة محمد	أستاذ محاضر أ	جامعة خنشلة	رئيساً
عرشوش سفيان	أستاذ محاضر أ	جامعة خنشلة	مُشرفاً و مُقرراً
كواشي نجوى	أستاذ مساعد أ	جامعة خنشلة	عُضوا مُمتحناً

السنة الجامعية : 2018-2019


بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ
Quran-HD.com

" وماتـــوفـيـقـــي إلا بـالله عَليه تَوَكّلت وإليه أنيب "

الآية : 88 / هود"

شكر وتقدير

الشكر الأول والأخير لله الواحد القهار مكوّر الليل على النهار ، والصلاة والسلام على سيدنا محمد المختار ، فالحمد لله حمدا تتم به الصالحات على إتمام بحثي هذا والذي آمل أن أكون قد وفقت لتحقيق الغاية المرجوة منه .

وأتقدم بالشكر الجزيل إلى الدكتور المشرف " عرشوش سفيان " على قبوله الإشراف على هذه المذكرة وعلى كل ماأسداه لي من توجيهات قيمة ومأأمدني به من معلومات وعلى سعة صدره وسمة التواضع والتي كان لها الأثر البالغ في تتويج إنجاز هذا العمل .

ولاننسى في هذا المقام أعضاء لجنة المناقشة لقبولهم مناقشة هذا الموضوع

الدكتور " شنة محمد " ، و الأستاذة " كواشي نجوى "

كما وأتقدم بالشكر للدكتورة " أوشن حنان " لما أسدته لي من نصائح ومعلومات قيمة

ولابد ونحن نخطو خطواتنا الأخيرة في الحياة الجامعية من وقفة نعود إلى أعوام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل متميز ، وقبل أن نمضي نقدم أسمى آيات الشكر والإمتنان والتقدير والمحبة إلى الذين حملو أقدس رسالة في الحياة وإلى الذين مهدوا لنا طريق العلم والمعرفة إلى جميع الأساتذة الأفاضل كل حسب لقبه واسمه .

كل من ساهم بإنجاز هذا البحث بنصيحة أو توجيه أو ترجمة .

إهـــــداء

عانينا الكثير من الصعوبات وهانحن اليوم والحمد لله نطوي سهر الليالي وتعب الأيام وخلاصة مشوارنا بين دفتي هذا العمل المتواضع

إلى الذي أفنى عمره محترقا شامخا لكي يريني النور

لمن يبحث عن أفضل الطرق لإدخال السعادة على وجوهنا

إلى من سعى وشقي لأنعم بالراحة والهناء الذي لم يبخل بشيء من أجل دفعي في طريق النجاح الذي علمني أن أرتقي سلم الحياة بحكمة وصبر

إلى الذي رغم كل جراح الزمن لم ترتسم الدموع على عينيه

إلى ذلك الوجه المكابر إلى تلك الهمة العالية

إلى أبي الجبيب

إلى من حاكت سعادتي بخيوط منسوجة من قلبها

إلى القلب الدافئ واليد الحنونة والإبتسامة الخجولة

إلى من سهرت الليالي ... لأجمل من رأت عيني

إلى التي الجنة تحت أقدامها...إلى الملاك السماوي

إليك ياأمي

إلى من أشد بهم أزري وسندي في الدنيا وإلى من حبهم يجري في عروقي ويلهج بذكراهم فؤادي أخواني وأخواتي

إلى زميلة الدراسة الأستاذة كاميليا معاشي

إلى سعادة سفير سفارة دولة فلسطين في الجزائر السيد أمين مقبول

والأخ المستشار الأمني الدكتور رائد حاج أسعد

إلى الأستاذ أمين أبو عرقوب

إلى الغاليين على قلبي أبناء خالي وأبناء عمي ، وأخص بالذكر المهندس محمد عبدالمعز سرحان ، عماد سرحان

أحمد جمال عبدالعال،أدهم عبد العال،شعبان عبدالعال

إلى الأحبة الأعزاء : السيد سيف الدين مشاقي ، المهندس مالك عباس

إلى رمز البراءة والصدق مجد ، عمر ، زيد، آدم ، ميرال، رحمه، يمان، حمزة

وإلى كل العائلة والأحباء والأصدقاء رفقاء الدرب في هذه الحياة

إلى الأصدقاء اللذين أنجبتهم الغربة لي الدكتور صهيب شاهين ، الدكتور عدي خمايسة، الأستاذ أحمد الأقطش، الأستاذ فريد دلني، الأستاذ محمد عدوان، الأستاذ إبراهيم الغربية .

إلى من علمونا حروفا من ذهب وكلماتٍ من دُرر وعباراتٍ من أسمى وأجلى عبارات في العلم إلى من صاغوا لنا علمهم حروفاً ومن فكرهم منارةً تنير لنا سيرة العلم والنجاح

إلى جميع أساتذتي الكرام

ولن أنسى أن أهديه إلى من هو أعز من نفسي علي وطني الجريح فلسطين

وبلدي الثاني الجزائر

مـــقـــدمـــــة

تمهـــــيد :

تعد تقنية المعلومات الحديثة أو تكنولوجيا المعلومات والإتصالات ومانتج عنها من شبكات ووسائط إلكترونية، قفزة حضارية نوعية في حياة الأفراد والدول، إلا أن هذا الجانب الإيجابي المشرق لهذه التكنولوجيا لم ينف الإنعكاسات السلبية التي أفرزتها إساءة إستخدام هذا التطور وما صاحبه من ظهور أنماط مستحدثة من السلوكيات الجرمية، بواسطة توظيف تقنيات المعلومة الحديثة في إرتكاب الجرائم وبواسطة شبكة المعلومات (الإنترنت) أو الأجهزة الأخرى كالهواتف النقالة فقد تحول الإنسان إلى هدف من أهداف مجرمي التقنية الحديثة، بعد أن أتاحت الثورة الرقمية تحقيق أغلب صور الإعتداء على الأشخاص أو أسرارهم الخاصة وحتى أموالهم.

وظهرت جملة من الجرائم الإلكترونية التي قصرت التشريعات العقابية عن تجريمها لتعددها ولغياب نص التجريم، إضافة إلى تعقيدات التحقيق فيها وضبط أدلتها ومرتكبيها، كل ذلك يجعل دراستها ومواجهتها أمرا لاينفصل عن التعرف بشكل عام على مفهومها وتطورها وآثارها ودوافعها وإجراءات التحقيق والمحاكمة فيها والجهود الدولة والوطنية للحد منها والعقوبات المقررة لملاحقة مرتكبيها، لذا فإنه مع التطور التكنولوجي الهائل على شتى الأصعدة والطفرة المعلوماتية الرهيبة التي غزت القارات الخمس، لم يعد ثمة مكان يعيش بمنأى عن آثار العولمة الإلكترونية بشكل أو بآخر، ومن خضم هذه التطورات نتجت مجموعة من الجرائم ذات الطابع الإلكتروني ماعهدها الناس من قبل سميت بالجرائم الإلكترونية .

إن تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الإتصالات الحديثة وسائر صور الإتصال الإلكتروني عبر الأقمار الصناعية إستغله مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت

حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، إستعصى إدراجها ضمن الأوصتف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، ولعل التطور الهائل في مجال تكنولوجيا المعلومات ودخول وسائلها إلى شتى مجالات الحياة والذي أدى إلى تعاظم دورها بشكل غير محدود فقد باتت الحواسيب الآلية والتقنيات الإلكترونية وشبكة الإنترنت لغة العصر التي لايمكن الإستغناء عنها، ولاشك أن هذه الجرائم ماولدت إلا نتيجة إساءة إستخدام وسائل الإتصال الإلكترونية التي ظهرت على الساحة الدولية، ولم يكن لها وجود من قبل فقد تباينت الصور الإجرامية للظاهرة الإلكترونية وتشعبت أنواعها فمنها ما يتصل بالإعتداء على ذات النظام الإلكتروني ومنها مايتعلق بالإعتداء على المعلومات، ولهذا فإن الجريمة الإلكترونية عبارة عن مصطلح زئبقي صعب الإمساك به والإحاطة بتعريف شامل له حيث أن معظم التشريعات لم تعرف الجريمة الإلكترونية ولكن وضعت قوانين خاصة و أدرجت وأفردت بقوانين وحدها تجرمها وتعاقب على إرتكابها فمنهم من عرفها بأنها كل سلوك غير قانوني يتم بإستخدام الإجهزة الإلكترونية ينتج عنها حصول المجرم على فوائد مادية ومعنوية مع تحميل الضحية خسارة مقابلة وغالبا مايكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات.

وأن التطور الذي جاء في السنوات الأخيرة أن هذه التكنولوجيا كشفت النقاب عن تكنولوجيا متطورة لم تكشفها عقودا من الزمن سميت بالجرائم الإلكترونية التي تعتبر الإبن غير الشرعي نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، وقد تعددت ألفاظ ومفردات وصيغ ومصطلحات الجريمة الإلكترونية تعدداً يحمل صورة التنوع والثراء لا التنازع والتّضاد فأطلق على الجريمة الإلكترونية هذا المسمى وجرائم الكمبيوتر والإنترنت والسيبر، وأيضاً ومن حيث مايرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على إستيعاب هذه الظاهرة الإجرامية الجديدة سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل

تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة إحترام مبدأ شرعية الجرائم والعقوبات من ناحية ومبدأ الشرعة الإجرائية من ناحية أخرى وتتكامل فيه في الدور والهدف مع المعاهدات الدولية .

فالإنترنت كما شبهها البعض بأرض أمريكيا في القرن التاسع عشر بأنها أرض السيء والجيد فعالم الإنترنت والإتصالات والإلكترونيات له سحر مغوي ومقلق في آن واحد فقد أصبح فجأة فن جديد للحياة، فالكل يجد فيه رغباته دون مراعاة للعمر أو الثقافة، ولأنه ليس هناك لعبة في الواقع بدون قاعدة ولا أفق بلا حدود وكذلك مثل باقي النشاطات الفردية والإجتماعية لامجتمع بدون قاضي، وكان لزاما بسبب هذا التداخل الواسع في العالم الإفتراضي وعالمنا أن يندرج في إطار قانوني حتى لاتكون الإنترنت وباقي تكنولوجيات الإعلام والإتصال أدغالاً حيث وحدهم المفترسون يزدهرون، ولا أن تقيد الحريات فيها إلى حد أن تكون كحديقة فرنسية تُخنق فيها حيوية الحرية التي تعد المحرك الحقيقي لكل شيء رقمي والذي هو شعار التطور الذي تؤول إليه المجتمعات بعد إنتشار تكنولوجيات الإعلام والإتصال وإنشاء الحكومات الرقمية لجعل كل شيء رقمي .

أولا: أهمية الموضوع :

يكتسب موضوع البحث أهمية متزايدة بسبب إستغلال وسائل الإتصالات الحديثة وسائر صور الإتصال الإلكتروني عبر الأقمار الصناعية التي إستغلها مرتكبو الجرائم لتسهيل إرتكابهم لجرائمهم، فموضوع دراستنا هو جانب من القانون المتمثل في دراسة القواعد الموضوعية والإجرائية الخاصة بالجرائم الإلكترونية حيث يتناول الرؤى والصور المتعلقة بهذه الجوانب في محاولة لتقديم الحلول القانونية الممكنة لمكافحة هذه الجريمة في ظل النصوص التشريعية، والتعرف على الجرائم المرتكبة ضد الحاسوب وشبكة الإنترنت وإلقاء العبئ على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها، وأيضا تبرز أهميته من خلال إرتباطه الوثيق بظاهرة جديدة ظهرت مع التطور التكنولوجي وهي الجرائم الإلكترونية التي تعتبر من الجرائم التي

أثارت الكثير من المشاكل فالطبيعة القانونية والفنية والتقنية الناجمة عن هذه الجرائم نتج عنها نوع جديد من الأدلة في الإثبات الجنائي وهو الدليل الإلكتروني، كما وعالج هذا البحث واقع الجرائم الإلكترونية وملاحقتها في فلسطين، نظرا لحداثة الجريمة الإلكترونية في المجتمع الفلسطيني وأنه يعتبر حالة مختلفة عن واقع هذه الجرائم في مختلف الدول بسبب وقوعها تحت الإحتلال الإسرائيلي الذي يسيطر على سماء وفضاء فلسطين الإلكتروني سيطرة تامة مما يضفي لونا خاصا عند ملاحقة هذه الجرائم .

ثانيا: إشكالية البحث :

في ظل تزايد إنتشار هذه الجريمة في فلسطين والجزائر بشكل كبير، وملاحقتها والتعرف على التشريعات التي تنظم تجريم وملاحقة هذه الجرائم على المستويات الوطنية والدولية، وعدم تحقيق في حالة الردع لمرتكبيها وفي أحيان أخرى عجز المؤسسة القضائية عن الحكم على بعض الجرائم الإلكترونية بغياب النصوص القانونية التي تجرمها وفي ظل إنقسام وجهات النظر في مدى إمكانية الإستفادة في ملاحقة هذه الجرائم بناءا على قوانين العقوبات السارية والمعمول بها والإنضمام للإتفاقيات الدولية والإقليمية، وأن تفاقم الجرائم الإلكترونية يشكل تهديدا مباشرا لأكثر المرافق العامة والمصالح خاصة ويمثل عدوانا على حقوق الأفراد وأنها تحدث في أي مكان وكونها عابرة للقارات وغير ملموسة وهناك صعوبة في تتبعها كونها جرائم مستحدثة .

وللوقوف السليم على هذه المشكلة وأبعادها القانونية وحتى نكون في بر الأمان وللخروج من عنق الزجاجة وعدم البقاء في التقوقع فمن خلال ماسبق، ونظرا لأهمية الموضوع وتشعبه فإن محاولة دراسته تتطلب الخوض في الإشكالية الآتية :

الى أي مدى وفق المشرع الجزائري والفلسطيني في سنّ أحكام قانونية وإجرائية كضمان لدرء مخاطر وأضرار جرائم إلكترونية ؟

وللإجابة عن هذه الإشكالية يستلزم طرح بعض التساؤلات الفرعية والتي نوردها على النحو التالي :

1.مالمقصود بالجريمة الإلكترونية ؟

2.ماهي طرق إثبات الجريمة الإلكترونية وكيفية التحقيق في مثل تلك الجرائم ؟

3.مامدى نجاعة سلطة البحث والتحري في ملاحقة مرتكبي الجرائم الإلكترونية ؟

4.ماهي العقوبة التي حددها المشرع لمرتكبي الجرائم الإلكترونية ؟

5.ماهي الآليات الوطنية والدولية لمكافحة الجريمة الإلكترونية ؟

ثالثا: منهج الدراسة :

كون هذا الموضوع من الجرائم العصرية المستحدثة التي لاقت إهتماما كبير من رجال الفكر والقانون، وبخصوص المنهجية المتبعة في هذا البحث فقد إعتمدت على المناهج التالية التي أرى أنها تتماشى مع طبيعة الموضوع المطروح :

المنهج الوصفي التحليلي: لأن دراستنا تعتمد على تحليل النصوص القانونية المنظمة للجرائم الإلكترونية، وكذا وصف هذه الجرائم وفقا لما نص عليه المشرع الفلسطيني والجزائري، وكذلك تبيان إجراءات البحث والتحري والتحقيق في الجرائم الإلكترونية وذلك من خلال الرجوع للدراسات السابقة والأبحاث والرسائل والإتفاقيات الدولية ذات الصلة.

المنهج التاريخي: من خلال التطرق إلى نشأة وتطور الجريمة الإلكترونية والتطورات التي حصلت في القرن المنصرم، وهذا من شيوع إستخدام الكمبيوتر وصولا إلى يومنا هذا، وكذا من خلال التتبع لأهم القضايا الإلكترونية التي حصلت سابقا وماجرى في الألفية الثالثة .

المنهج المقارن: قمنا بالمقارنة مابين التشريعين الفلسطيني والجزائري فيما يخص بعص العناصر من تحديد سلطات الضبط القضائي، وطرق التحقيق والإثبات في الجرائم الإلكترونية،

وأيضا قارنا بين العقوبات التي أوقعها المشرعين على مرتكبي الجرائم الإلكترونية لنصل في النهاية إلى كيفية الوقاية والمكافحة لمثل هذه الجرائم، مع تبيان موقف المشرعين من الجريمة الإلكترونية من خلال توظيفها في التعاريف .

رابعا: أهداف الدراسة :

إستنادا لما سبق فإن بحثنا هذا يسعى إلى تحقيق جملة من الأهداف التي يسعى التي يمكن من خلالها الإحاطة بجوانب الموضوع المختلفة، فنظرا للتطورات التكنولوجية والمعلوماتية الحديثة وإنتشارها على نطاق واسع وغير محدود أصبحت الدول أمام مشاكل قانونية متعددة خصوصا فيما يتعلق بالإعتداءات الواقعة على الأنظمة الإلكترونية، فأصبحت مواجهة هذه الجرائم واقعا مفروضا على مختلف التشريعات وبالتالي فإننا نهدف إلى تبيان الآتي :

1. تقديم رؤية متكاملة حول الجرائم الإلكترونية وصورها وأركانها والإلمام بالإحكام الموضوعية والإجرائية للجريمة الإلكترونية .

2. تقديم دراسات قانونية وموضوعية تكشف الملامح والجوانب المختلفة لهذه الظاهرة.

3.التوصل للإختلافات (إن وجدت) والتي تتعلق بالنصوص القانونية للجرائم الإلكترونية .

4.معرفة سلطات الضبط القضائي في التحقيق في الجرائم الإلكترونية، وكذلك المحكمة المختصة بالنظر فيها .

5.بيان مدى فعالية نصوص التجريم للجرائم الإلكترونية في التشريع الفلسطيني مقارنة مع التشريع الجزائري .

خامسا: أسباب إختيار الموضوع :

إن إختيار موضوع الجريمة الإلكترونية يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها شخصي (ذاتي) والآخر علمي (موضوعي) .

فالأسباب الشخصية (الذاتية) : تكمن في إهتمامي بمجال الجريمة الإلكترونية ومايلقاها من جرائم وكذا من إجراءات خاصة، وأن إجراءات المتابعة فيها تختلف كل الإختلاف عن إجراءات المتابعة في الجرائم التقليدية، بالإضافة إلى انه موضوع جديد في فلسطين وسن له قانون خاص ينظمه وأن المشرع الفلسطيني مازال يبحث عن دراسات في الجريمة الإلكترونية وذلك لسد الفراغ التشريعي ومازال يفتقر إلى الدراسات في مجال الجريمة الإلكترونية، ومن باب إثراء الحقل العلمي من مثل تلك الدراسات لأنها تجمع بين الدراسة الفنية والتقنية والقانونية وأنه لم ينل حظه بعد من البحث والتمحيص، وأن معظم الدراسات التي تهتم بالجرائم الإلكترونية تركز فقط على الجانب الموضوعي مانتج عنه فراغ في الجانب الإجرائي لهذا الموضوع، وأيضا رغبتي الشديدة في الغوص في مجال إجراءاتها وكذا مكافحتها والوقوف على حقيقة التعامل مع الجريمة الإلكترونية من الناحية الإجرائية .

أما الأسباب العلمية (الموضوعية): فتكمن فيما يطرحه موضوع الجريمةالإلكترونية من إشكاليات قانونية التي لابد من الوقوف عليها نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وأيضا القواعد الإجرائية الحديثة التي جاء بها قانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في الجزائر، وقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في فلسطين، ونظرا لأهمية المكافحة في الجريمة الإلكترونية ومافرضته من تحديات خاصة في عصرنا الحالي، ونظرا للتزايد المستمر للجرائم الإلكترونية، وكذلك إستكمالاً للحصول على متطلبات شهادة الماستر في العلوم الجنائية والقانون الجنائي .

سادسا: الدراسات السابقة :

معظم الدراسات التي اطلعنا على محتواها ونحن بصدد إنجاز مذكرتنا هذه، جاءت بمعظم الأفكار التي يجي التطرق إليها في هذا الموضوع، فمثلاً :

1. يوسف خليل يوسف العفيفي ،الجرائم الإلكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة) رسالة ماجستير – تخصص القانون العام ، بإشراف الدكتور أيمن عبدالعال، الجامعة الإسلامية – كلية الشريعة والقانون، غزة – فلسطين، 2013 : حيث تناول فيها الباحث مضوع دراسته من خلال ثلاثة فصول متكاملة حيث الفصل الأول الجريمة الإلكترونية (تعريفها، صورها ، طبيعتها، خصائصها) أما الفصل الثاني فكان بعنوان القواعد الموضوعية للجرائم الإلكترونية متطرقا فيها إلى أركان الجريمة الإلكترونية وعلى الجزاء الجنائي للجريمة الإلكترونية مستعينا بالقانون الفلسطيني والأردني، أما الفصل الثالث فكان بعنوان القواعد الإجرائية للجرائم الإلكترونية مبينا من خلال ذلك المراحل الجزائية التي تمر بها الدعوى الجزائية في الجريمة الإلكترونية وإجراءاتها الكاملة بشكل مفصّل، وقد توصل الباحث إلى النتائج التالية : أن الجريمة الإلكترونية تتكزن من فعل أو إمتناع عن فعل بإستخدام إحدى الوسائل الإلكترونية، ونتيجة أخرى أن الجرائم الإلكترونية تتخذ نفس الإجراءات التي تتم في الجرائم التقليدية ، وأيضا أن سبب إنتشار الجرائم الإلكترونية الإنترنت التي جعل العالم كقرية صغيرة، كذلك أن قانون العقوبات الفلسطيني إعتبر الجرائم الإلكترونية من الجنح وهذا غير رادع ولايتناسب مع جسامة الخطر الناتج عن الجريمة الإلكترونية.

2. بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي ، أطروحة دكتوراه تخصص قانون عام، بإشراف البروفيسور البقيرات عبد القادر، جامعة الجزائر 1 – كلية الحقوق – بن يوسف بن خدة، بن عكنون الجزائر، 2018 : حيث تناول فيها الباحث موضوع دراسته من خلال بابين متطرقا في الباب الأول إلى مكافحة الجريمة على المستوى الدولي مقسما الباب الأول إلى فصلين الفصل الأول المكافحة الموضوعية والإجرائية للجريمة المعلوماتية، والفصل الثاني فتناول فيه الباحث الآليات الدولية لمكافحة هذه الجريمة، والباب الثاني بعنوان مكافحة الجريمة المعلوماتية على المستوى الداخلي كذلك قسمه الباحث لفصلين تناول في الفصل الأول المواجهة التشريعية للجريمة المعلوماتية والفصل الثاني المكافحة

الإجرائية للجريمة المعلوماتية على المستوى الداخلي، حست توصل الباحث إلى النتائج التالية نذكر بعضها : أن هذه الجرائم تهدد الإقتصاد العالمي نتيجة للخسائر الناتجة عنها ، وأن بعض الإتفاقيات الدولية مازالت تتخذ كمرجع لصياغة النصوص القانونية المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي، وأنه على المستوى الإقليمي فقد أصدر المجلس الأوروبي إتفاقية بودابست المتعلقة بمكافحة الإجرام المعلوماتي والتي تعتبر مرجعاً لايستهان به في ميدان محاربة الإجرام السيبري، وأنه على الصعيد العربي قد صدر القانون العربي الإسترشادي النموذجي، بينما في الجزائر هناك محاولات لتطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال إصدار تشريعات تواكب التطور الحاصل في المجال المعلوماتي .

سابعا: صعوبات الدراسة :

لحسن حظنا ونحن بصدد الدراسة والبحث في موضوع الجريمة الإلكترونية لم نواجه صعوبات كبيرة إلا أنه واجهنا قلة المراجع والدراسات في موضوع الجريمة الإلكترونية لأنه لايوجد دراسات سابقة كثيرة عن هذا الموضوع وخصوصا في فلسطين، أما بالنسبة للتشريع الجزائري فواجهتنا صعوبة في عرض صور الجرائم الإلكترونية بالتحديد وأيضا موضوع إثبات الجريمة الإلكترونية حيث أن المشرع الجزائري لم يولي له إهتماما كبيرا في الطرق الحديثة أو مايسمى بالدليل الإلكتروني، وأيصا بالنسبة للعقوبات المقررة لمرتكبي الجريمة الإلكترونية في فلسطين واجهنا صعوبة في حصرها كونه قانون جديد سنه المشرع الفلسطيني، وأيضا بالنسبة لموضوع التحقيق في الجريمة الإلكترونية كونها تفرض على المحقق قيود وضعها قانون الإجراءات الجزائية فوجدنا صعوبة بكيفية توظيفها في الموضوع .

ثامنا: خطة البحث :

لقد تناولنا موضوع الجريمة الإلكترونية في التشريع الجزائري والفلسطيني من خلال فصلين يحتوي كل فصل على مبحثين وكل مبحث على ثلاثة مطالب، وكل مطلب على فروع مقسمة

بشكل نظامي تتناسب وطبيعة البحث العلمي، وبدأنا في المقدمة على حسب أصول البحث العلمي المتناسق والصحيح، حيث تطرقنا في الفصل الأول إلى الأحكام الموضوعية للجريمة الإلكترونية، وذلك من خلال مبحثين الأول ماهية الجريمة الإلكترونية والثاني أركان الجريمة الإلكترونية، ومن ثم قمنا بالولوج إلى الفصل الثاني لنعالج الأحكام الإجرائية للجريمة الإلكترونية وأيضا من خلال مبحثين وفي ضوء هذا تناولنا في المبحث الأول المراحل الإجرائية للجريمة الإلكترونية وفصلنا ذلك في مطالب وفروع، وفي نهاية المطاف وفي المبحث الثاني أيضا تناولنا آليات المكافحة الإقليمية والدولية للجريمة الإلكترونية، وآليات الوقاية من الجريمة الإلكترونية وذلك في التشريعين الجزائري والفلسطيني وكيف ساهم كل من التشريعين في إخماد وإطفاء لهيب الجريمة الإلكترونية بل وإن صح التعبير في التخفيف من إستمراريتها يوما عن آخر بسبب تطور الوسائل التكنولوجية، ومن ثم وضعنا خاتمة حوصلنا فيها النتائج وبعض التوصيات المقترحة التي إستخلصناها وارتأينا إليها من خلال البحث في موضوع الجريمة الإلكترونية .

الفصل الأول : الاحكام الموضوعية للجريمة الالكترونية .

أدى الاستخدام المتزايد للمعلوماتية الى ظهور مايعرف بالاجرام المعلوماتي وذلك راجع إلى إستخدام الحاسب الالي في كافة مجالات الحياة اليومية والذي بواسطته تم جعل المعلومات في متناول الجميع من خلال شبكات الإنترنت وأن هذا المجال لايعرف الحواجز الجغرافية ولا المسافات بصورة يمكن معها القول بأن العالم صار أشبه بقرية صغيرة تترابط به الحاسبات وشبكات المعلومات.

ولكشف مايتعلق بهذا النوع من الاجرام تقتضي دراستنا أن نتاول في هذا الفصل مايلي وذلك بتقسيم هذا الفصل الى مبحثين :

المبحث الاول : ماهية الجريمة الالكترونية .

المبحث الثاني : أركان الجريمة الالكترونية .

المبحث الاول : ماهية الجريمة الالكترونية

إن التعرف على ماهية الجرائم المعلوماتية شرط أساسي للتوصل الى كيفية التحري والتحقيق فيها وتعتبر الجرائم المعلوماتية جرائم مستحدثة لإرتباطها بالتطور والتقدم التكنولوجي حيث كان هناك اتجاهات متعددة في تعريفها كما أنها تتميز عن الجرائم الأخرى بمجموعة من الخصائص وجاءت بنمط جديد يطلق عليهم بمصطلح مجرمي المعلوماتية[1].

وبتنامي معدلات الجريمة وتطور أشكالها وتهديدها المباشر قد دقّ ناقوس مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها الواسعة[2].

وعلى هذا الأساس سيتم تقسيم هذا المبحث إلى ثلاثة مطالب يتم من خلالها تحديد مفهوم الجريمة الالكترونية ونشأتها والتطور التاريخي لها في المطلب الأول ونخصص المطلب الثاني للخصائص التي يتميز بها هذا النوع من الجرائم أما المطلب الثالث يتضمن صور الجريمة الالكترونية .

المطلب الأول : مفهوم الجريمة الإلكترونية

سيتم في هذا المطلب تحديد المفاهيم الخاصة بالموضوع، وذلك من خلال التطرق إلى التعريف اللغوي وكذا الاصطلاحي لكل من : **الجريمة، الإلكترونية (المعلوماتية)،المجرم المعلوماتي، الحاسب الآلي،المعلومات.**

---

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع،ط2،عمان،2010، ص45

2. فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها** ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية، طرابلس ، 24-25 مارس 2017، ص2.

ومن ثم التطرق إلى تعريف الجريمة الإلكترونية – حسب إتجاهات الفقهاء ورجال القانون – من حيث :

1) وسيلة أو أداة إرتكاب الجريمة.
2) وفقا لمحل أو موضوع الجريمة.
3) وفقا لمعرفة الفاعل بتقنية الملومات.
4) وفقا لمعايير أخرى.

وذلك في الفرع الأول أما في الفرع الثاني سنتطرق إلى النشأة والتطور للجريمة الإلكترونية .

الفرع الأول : تعريف الجريمة الإلكترونية .

قبل الولوج في تعريف الجريمة الإلكترونية هناك مصطلحات لابد من توضيحها لتبيان معنى الجريمة الالكترونية وهي مفاهيم متعلقة بهذه الدراسة

أولا: تحديد معنى الجريمة :

سنحدد معنى الجريمة من خلال التعرف على المعنى اللغوي والإصطلاحي.

1. المعنى اللغوي للجريمة

الجريمة:من فعل جرم جرما وجريمة ويأتي بمعاني عديدة ومنها:

أ. الجرم:التعدي والذنب، والجمع إجرام وجروم، وهو الجريمة.

ب. والجرم: مصدر الجارم الذي يجرم نفسه وقومه شراً.[1]

[1] ابن منظور،**لسان العرب**،ط1، دار صادر،لبنان،م3،ص129–130 .[1]

جريمة: جمع جرائم وهي التي يعاقب عليها القانون،سواء كانت مخالفة أو جنحة أم جناية.

2. المعنى الاصطلاحي للجريمة:

(هي سلوك إرادي يحظره القانون ويقرر لفاعله جزاءا جنائيا) [1] .

لكي ترتب الجريمة اثارها الجنائية يجب أن يكون هناك قاعدة قاعد قانونية جنائية تحظرها وتقرر لها جزاءاً جنائياً أن تتوافر أركانها بحيث تتطابق مع نموذجها القانوني كما رسمته تلك القاعدة .

وبذلك فإن تعريف الجريمة هي: كل فعل أو امتناع صادرعن ارادة جنائية حرة وواعية،يحظره القانون ويقرر لها جزاءا جنائيا .

ثانيا: تحديد معنى الإلكترونية (المعلوماتية)

سنحدد معنى الإلكترونية(المعلوماتية) من خلال التعرف على المعنى اللغوي والاصطلاحي لها .

1.المعنى اللغوي للإلكترونية (المعلوماتية) .

يقصد بها المعالجة الالية للمعلومات وهي ترجمة للمصطلح الفرنسي informatique، وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر وقد استعمل مصطلح traitement automatise des données ويعني المعالجة الآلية للبيانات ومصطلح télématique أي اتصالات وهي تعادل مصطلح Telecom في اللغة الانجليزية وإن كان ليس لها أصل في القاموس الانجليزي ، مستمدة من اللغة الفرنسية[2].

[1] . علي عبد القادر القهوجي،**شرح قانون العقوبات(القسم العام)** دراسة مقارنة،منشورات الحلبي الحقوقية،لبنان،2002،ص44 .

[2] خالد ممدوح ابراهيم،**أمن الجريمة الإلكترونية**،دار الجامعية،الإسكندرية،2008،ص43 .

المعلومة: مشتقة من كلمة علم ودلالتها هي المعرفة التي يمكن نقلها واكتسابها.

العلم: نقيض الجهل وعلمت الشيء أعلمه علما : عرفته[1] .

وتحقيقه – اليقين والمعرفة – وهو نور يقذفه الله في قلب من يحب، فينتج به ماتسعد به الإنسانية.

ويطلق العلم على مجموعة من المسائل المتنوعة والأصول الكلية المتكون منها الهيكل العام لكل مادة أو فن[2] .

2.المعنى الاصطلاحي للالكترونية (المعلوماتية) .

أ. بقصد بها مثل ماعرفتها الأكاديمية الفرنسية في تعريفها التي صاغته في أفريل 1967: علم التعامل العقلاني على الأخص بواسط آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الانسانية وعمادا للاتصالات في ميادين التقنية والاقتصاد والاجتماع.

ب. كما تعرف أنها: علم المعالجة العقلية للمعلومات باستخدام الات تعمل ذاتيا [3].

ثالثا: تحديد معنى المجرم المعلوماتي :

- هو شخص يتمتع بالمهارة والمعرفة والذكاء وعند ارتكابه للجريمة يبررها بمبررات مختلفة لأنه يخاف من كشف جريمته، ومن الدوافع التي تدفع المجرم المعلوماتي لإرتكاب

---

[1] ابن منظور،**لسان العرب**،ط1،دار صادر،لبنان،م10،ص263 .

2. محمود المسعدي،**القاموس الجديد للطلاب:معجم مدرسي الفبائي**،ط7،المؤسسة الوطنية للكتاب،الجزائر،1991،ص696

[3] أحمد خليفة الملط،**الجرائم المعلوماتية**،ط2،دار الفكر الجامعي،مصر،2006،ص79.

الجريمة الرغبة في التعلم وقهر النظام المعلوماتي وإثبات الذات والرغبة في الإنتقام والمتعة والتحدي وهناك دوافع مادية مثل الربح [1] .

رابعا: تحديد معنى الحاسب الآلي :

هو عبارة عن جهاز الكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وادارة المعلومات بطريقة ما وذلك بتنفيذ ثلاث عمليات أساسية :هي استقبال البيانات المدخلة ومن ثم معالجة البيانات الى معلومات وأخيرا اظهار المعلومات المخرجة[2].

- مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات المدخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة.

خامسا:تحديد معنى المعلومات

- إقترح الأستاذ catala تعريف المعلومات: بأنها رسالة ما يعبر عنها في شكل يجعلها قابلة للنقل أو الابلاغ للغير[3].
- ومن القوانين العربية التي عرفت المعلومات القانون الأردني للمعاملات الالكترونية رقم 85 لسنة 2001، حيث المادة الثانية من هذا القانون بأنها (البيانات أو النصوص أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات التي انشأت أو أرسلت أو استلمت أو خزنت بوسائل إلكترونية) [4].

---

1. نهلا عبدالقادر المومني،**الجرائم المعلوماتية**،ط1،دار الثقافة للنشر والتوزيع،2008،ص20.
2. **نفس المرجع**،ص20.
3. سامي علي حامد عياد،**الجريمة المعلوماتية وجرائم الانترنت**،دار الفكر الجامعي،الإسكندرية،2008،ص24.
4. خالد ممدوح ابراهيم،**المرجع السابق**،ص26.

- والمعلومات حسبما يعرفها البعض بأنها: أحد عناصر المعرفة التي يتصل بها الغير من خلال وسيلة مناسبة لنقلها أو تسجيلها أو معالجتها، وتأخذ شكل رسالة يمكن نقلها للغير[1].

بعدما أوضحنا المفاهيم الأساسية المتعلقة بالجريمة الالكترونية سنتطرق الان الى تعريف الجريمة الالكترونية بالتفصيل بمعناها الضيق والواسع وحسبما عرفها الفقهاء ورجال القانون حسب تقسيم تعريفها.

سادسا : تعريف الجريمة الالكترونية (المعلوماتية) :

إن لتعريف الجريمة أثر كبير في تحديد أركانها، وكل ذلك بدوره له أهمية خاصة بالنسبة للمحققين ورجال جمع الأدلة الجنائية اللذين يبغون دوماً إثبات أركان وعناصر الجريمة حسبما يحددها المشرع، وقد أبانت التجربة أنه في كثير من الدول يعاني المحققون ورجال الشرطة من الكثير من المصاعب في التصدي للجرائم المعلوماتية بسبب عدم وضع تعريف محدد لهذه الجرائم وعدم تحديد الأفعال الجرمية التي تشكل هذه الجرائم بشكل واضح [2].

فالجرائم المعلوماتية أو كما يسميها البعض بالجرائم الإلكترونية أو جرائم الكمبيوتر والإنترنت أو جرائم الغش المعلوماتي أو الجرائم السايبرية أو جرائم التقنية العالمية، وغيرها من المصطلحات [3]. بذل الفقهاء جهوداً حثيثة في محاولتهم لوضع تعريف جامع ومانع لها، ولكن

---

1. محمد حماد مرهج الهيتي،**التكنولوجيا الحديثة والقانون الجنائي**،ط1،دار الثقافة للنشر والتوزيع،الأردن،2004،ص182

2. .رشاد خالد عمر،**المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية**،المكتب الجامعي الحديث،الإسكندرية،2013،ص18 .

3.إخترنا **مصطلح الجريمة الإلكترونية** بإعتباره المصطلح الأكثر شمولا من غيره من المصطلحات لأغلب صور هذه الجرائم التي لايمكن حصرها.فمصطلحا الجرائم المعلوماتية وجرائم السيبر يشملان فقط الجرائم الواقعة عبر شبكات الإنترنت فيما أن مصطلح جرائم الكمبيوتر قاصر عن شمول الجرائم المعلوماتية التي تقع عبر أجهزة الهاتف النقال أو المحمول(الموبايل)،فيما يقصر مصطلح جرائم الغش المعلوماتي عن شمول جرائم الإتلاف المعلوماتي والتجسس المعلوماتي وصور أخرى كثيرة لهذه الجرائم.

من دون أن يثمر ذلك عن الوصول الى تلك النتيجة المرجوة،وذلك بالنظر لإختلافاتهم إلى عدة إتجاهات حول المعيار الواجب الإعتماد عليه في تعريف هذه الجرائم .

قدم الفقهاء ودارسي القانون عددا ليس بالقليل من التعريفات ،لكنها تتمايز وتتباين تبعا لموضوع الدراسة ذاته، لذا سيتم تقسيم هذه التعريفات حسب ما إذا كانت مرتبطة بوسيلة ارتكابها أو محل أوموضوع الجريمة أو لمعرفة الفاعل بتقنية المعلومات.

الإتجاه الأول: ويرى أصحابه بضرورة الاعتماد على معيار **أداة أو وسيلة ارتكاب الجريمة** في تعريف هذه الجرائم،باعتبار ان هذه الجرائم انما هي تلك التي يستخدم فيها الكمبيوتر كوسيلة لإرتكابها [1]. ومن أنصار هذا الاتجاه الفقيه الألماني **تاديمان** (Tiedemann) الذي عرف هذه الجرائم بأنها : "كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب " . والفقيه الإنجليزي **ليزلي بول** (Leslie Ball) الذي عرفها بأنها:" فعل اجرامي يستخدم الحاسب في إرتكابه كأداة رئيسية"، وكذلك الفقيه **فان دير ميروي** (Van der merwe) والذي عرفها بأنها:" الفعل غير المشروع الذي يكون الحاسب داخلا في إرتكابه.[2]

وكذلك الحال بالنسبة للفقيهين الإنجليزيين ريتشارد توتي وأنثوني هاردكاسل (Richard Totty & Anthony Hardcastle) اللذين عرفاها بأنها:" تلك الجرائم التي يكون فد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسب، وبعباة أحرى تلك الجرائم التي يكون دور الجاسب فيها ايجابيا أكثر منه سلبيا" [3].

---

1. أيمن عبدالله فكري،**جرائم نظم المعلومات**،دار الجامعة الجديدة،الإسكندرية،2007،ص83

2. هشام محمد فريد رستم،**الجرائم المعلوماتية**،بحث مقدم لمؤتمر الكمبيوتر والإنترنت في جامعة الامارات العربية المتحدة،ط3، 2004،ص405-406.

3. أيمن عبدالله فكري،**المرجع السابق**،ص83-84.

ولكن يؤخذ على هذا الاتجاه ان الأخذ به وحده ،سيجعل التعريف قاصرا،وشاملا فقط للجرلئم المرتكبة بواسطة الكمبيوتردون الجرائم الواقعة على الكمبيوتر هذا من جهة، زمن جهة أخرى فإن المشرع عندما يجرّم سلوكاً ما فإنه لاينظر إلى الوسيلة أو الأداة المستخدمة في إرتكاب الجريمة وإنما بنظر إلى مدى خطورة السلوك [1] .

الاتجاه الثاني: يستند هذا الاتجاه في تعريفها الى وجوب أن يكون **الحاسب الآلي هو محل الجريمة**،فيشترط الإعتداء على الحاسب الآلي أو على نظامه، ويمثل هذا الاتجاه روزنبلات (Rosenblatt) الذي عرفها بأنها:" نشاط غير مشروع موجه لنسخ أوالوصول الى المعلومات المخزنة داخل الحاسوب أتغيرها أو حذفها أو الوصول أو التي تحول عن طريقه [2] ". وتعرض هذا التعريف للانتقاد جيث اعتبر بداية أن جرائم الحاسب الآلي من الجرائم المحصورة ضمن نشاط معين يتفق مع مبدأ الشرعية الجنائية، إلا أنه توسع في النشاط غير المشروع المتعلق بالمعلومات عبر الحاسب وترك مجالاً واسعاً للإجتهاد والتفسير وهذا يتعارض مع مبدأ المشروعية في تحديد السلوك الإجرامي، بالإضافة إلى تبني معيار موضوعي أدلى إلى ظهور مفاهيم عامة لاتحدد الأفعال المرتبطة بجرائم الحاسوب بشكل دقيق. كما وعرفتها هدى قشقوش بأنها:" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقلها " وعرفها خبراء منظمة التعاون الإقتصادي والتنمية بأنها:" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" [3]. فهذه الجرائم تقع على

---

1. محمد بن حميد المزمومي،**جريمة الاعتداء على الأموال عن طريق الحاسب الآلي** ،رسالة ماجستير،قانون اقتصادي،كلية الاقتصاد والادارة،جامعة الملك عبدالعزيز ،جدة،2007،ص19.

2. يونس عرب،**دليل أمن المعلومات والخصوصية**،ط1،ج1،إتحاد المصارف العربية،2002،ص213.

3. هدى حامد قشقوش،**جرائم الحاسب الإلكتروني في التشريع المقارن**،دار النهضة العربية،1992،ص5.

الحاسب الآلي وبرامجه ومكوناته .من وصف هذين التعريفين بالعمومية والشمولية والمرونة إلا أنه يوسع نطاق التجريم إلى الأفعال الأخلاقية التي تخرج عن التجريم وفقا للقوانين الجنائية، وتبنى هذا المفهوم الألماني (Ulrich Sieber) الذي يعتمد على وصف السلوك وإتصاله بالمعالجة الآلية للبيانات أو نقلها.

الإتجاه الثالث: تم وضع عدد من التعريفات في هذا الإتجاه فمنها الضيق ومنها الواسع بخصوص تعريف الجريمة الإلكترونية **وفقا لمعرفة الفاعل بتقنية المعلومات** .

وبعتمد أصحابه على **معيار معرفة الجاني بالتقنية المعلوماتية** كمعيار لتعريف الجرائم المعلوماتية، وبمقتضى هذا الإتجاه تكون الجريمة معلوماتية فيما إذا توافرت لدى مرتكبها المعرفة والدراية الفنية بتكنولوجيا المعلومات. ومن الفقهاء اللذين أخذوا بهذا الإتجاه الفقيه البلجيكي ستين ستشيولبيرج(Stein schiollberg) الذي عرفها بأنها:" الجرائم التي تتطلب إلماما خاصا بتقنيان الحاسب ونظم المعلومات، لإرتكابها أو التحقيق فيها ومقاضاة فاعليها"[1]. والفقيه ديفيد ثومبسون (David Thompson) الذي عرفها بأنها:" أي جريمة يكزن متطلبا لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب" [2]. وقد تبنى معهد ستانفورد في الولايات المتحدة الأمريكية في إحدى دراساته هذا الإتجاه ، حيث عرفت الدراسة هذه الجرائم بأنها:" أية

---

1 . Stein Schiollberg, **computer and penal legislation**,A study of the legal politics of a new technology,Oslo,Universitets for lagest, 1983, p.40 89 (نقلا عن: أيمن عبدالله فكري،المرجع السابق،ص89

2. David Thompson, **Current trends, in computer control crime, computer quarterly,** vol 9, no 12, 1991. P.2

(نقلا عن عبد الفتاح بيومي حجازي،**مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، دار الكتب القانونية،مصر،2007،ص25)

جريمة لفاعلها معرفة فنية بتقنية الحاسبات تُمكّنه من إرتكابها" [1]. ومن ثم تبنت وزارة العدل الأمريكية التعريف السابق بمقتضى دليلها الصادر عام 1979. وقد إنتقد الفقه هذا الإتجاه بإعتبار أن الأخذ به يؤدي بنا إلى البحث في الظروف الخاصة بالجاني للوصول إلى حقيقة وجود مثل هذه المعرفة من عدمها، وهذه مما لايتناسب مع القانون الجنائي الذي هو قانون موضوعي ولايعتد بالظروف الشخصية إلا على سبيل الإستثناء كما وأنه يؤدي الى إفلات بعض الجناة من العقاب ،مثلا كمن يقوم بإتلاف بيانات مخزنة داخل الكمبيوتر من دون أن تكون لديه أية معرفة فنية بتكنولوجيا المعلومات بالرغم من أن هذا الفعل مجرم ومعاقب علبه في بعض القوانين حتى ولو لم تتوفر لدى الجاني أية معرفة فنية من هذا القبيل، كما ويؤخذ على هذه الإتجاه أغفل عن التطورات الحاصلة في مجال الأجهزة التقنية كالكمبيوتر والموبايل التي أدت إلى تسهيل إستخدام هذه الأجهزة حتى من قبل من هو أميّ [2] .

أما بالنسبة للفقه المصري فقد عرفها بأنها:" تنشأ عن الإستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الإعتداء على الأموال والأشياء المعنوية .

وإن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات وأَوكَلو مهمة ذلك إلى الفقه والقضاء، إلا أن بعضهم إتجه إلى وضع تعاريف لنظام المعلومات وليس لنظام المعالجة الآلية للمعطيات ومن بين التشريعات التي عرفت النظام المعلوماتي نذكر:

---

1. محمد عبيد الكعبي،**الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت**،ط2،دار النهضة العربية،القاهرة،2007،ص35.

2. رشاد خالد عمر ،**المرجع السابق**،ص19-20 .

1. قانون اليونسترال النموذجي بخصوص التجارة الإلكترونية لسنة 1996 حيث عرف هذا القانون من خلال نص المادة 2 نظام المعلومات على أنه :" النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو إستلامها أو تحزينها لتجهيزها على أي وجه آخر "[1].
2. قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 حيث عرف هذا القانون بدوره من خلال نص المادة 2 الفقرة 10 أيضا نظام معالجة المعلومات على أنه:" النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه آخر " [2] .
3. قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكتروني رقم 02 لسنة 2002 حيث عرف هذا القانون من خلال نص المادة 2 الفقرة 6 على أنه:" نظام إلكتروني لإنشاء أو إستخراج أو إرسال أو إستلام أو تخزين أو عرض أومعالجة المعلومات أو الرسائل إلكترونيا" [3].

والملاحظ على التعريفات الثلاثة السابقة أنها تنطبق على نظام المعالجة الآلية للمعطيات أكثر من على نظام المعلومات ككل ، كذلك أنها إنصبت في مجرى واحد معتمد في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها أو ينجزها هذا النظام والتي تمثل طرق المعالجة المعلوماتية.

1.نشناش منية،**مداخلة حول الركن المفترض في الجريمة المعلوماتية**،جامعة بسكرة–الجزائر ،2015–2016،ص3.

2. قانون رقم 85 لسنة2001،**الجريدة الرسمية للمملكة الأردنية الهاشمية** ، رقم4524 الصادرة بتاريخ 12/31/ 2001

3. قانون إمارة دبي رقم02 لسنة 2002**متعلق بالمعاملات والتجارة الإلكترونية**،صادر بتاريخ2002/2/12

الإتجاه الرابع: وفقا لمعايير أخرى

يبنى هذا الإتجاه نعريفات متعددة على أكثر من معيار ومنها تعريف منظمة التعاون الإقتصادي والتنمية(OCDE) خول الغش المعلوماتي عام 1982، حيث تم تعريف الجريمة الإلكترونية(المعلوماتية) بأنها:" كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية،يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية [1].

نرى أن هذا التعريف واسع وشامل وأن الفقه المصري أيّد هذا التعريف لأستبعاده أشكال التجريم التي يكون دور الحاسب الآلي فيها ثانويا أو عارضا. وانتقد هذا التعريف لإدراجه الأموال المادية كونها بمكن حمايتها بموجب القوانين التقليدية.

وعرفها الفرنسي ماس (Mass) بأنها:" الإعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلومات التقنية بغرض تحقيق ربح"

وبتعريف الخبير الأمريكي **دون باركر**(Don Barker) أنها:" أي فعل إجرامي أيا كانت صلته بتقنية المعلومات ،يلحق بالمجني عليه خسارة أو ربحا يحققه الفاعل [2].

والان وبعد أن أوردنا التعريفات السابقة نرى بأنه من الضروري أن نحاول بدورنا وضع تعريف للجرائم المعلوماتية، وفي هذا الإطار فإننا نرى بأنه عند وضع أي تعريف للجريمة عموما وللجرائم المعلوماتية خصوصا فإنه ينبغي الإعتماد على ما يمكن من خلاله تحديد أركان الجريمة أي أن يتضمن التعريف جميع أركان الجريمة (الخاصة والعامة) ولما كانت الجريمة التقليدية عموما تعرف بأنها:" كل سلوك خارجي إيجابيا كان أم سلبيا جرّمه القانون وقرر له

---

1. سامي محمد الشوا،**ثورة المعلومات وانعكاساتها على قانون العقوبات**،ط2،دار النهضة العربية،القاهرة،1994،ص32.

2.نهلا عبد القادر المومني،**المرجع السابق**،ص48.

عقابا إذا صدر عن إنسان مسؤول [1] . فقياسا على ذلك ولمّا كانت الجرائم المعلوماتية لاتختلف عن الجرائم التقليدية إلا من حيث أن محلها هو دوماً المعلومات والبيانات الإلكترونية التي قد تكون متعلقة بالمال أو بالحياة الخاصة أو بالمصالح العامة وغيرها وسواء كانت موجودة بداخل الحاسوب أو بأي جهاز تقني آخر أو كانت موجودة بالفضاء الإلكتروني على شبكة الإنترنت فيمكننا بناءا على ذلك تعريف الجرائم الإلكترونية (المعلوماتية) بأنها:" **كل سلوك متعمد بواسطة الحاسب الآلي أو الشبكة المعلوماتية يشكل إعتداءا على المعلومات أو البيانات الإلكترونية ضمن بيئة إلكترونية يجرمه المشرع ويقرر له عقابا اذا صدر عن شخص مسؤول.**"

ولو قمنا بتحليل تعريفنا هذا نلاحظ فيه مايلي:

1. أنه من حيث الركن المادي للجريمة يشمل جميع صور السلوك الإيجابية (فعل) والسلبية (إمتناع)
2. أنه من حيث الركن المعنوي للجريمة يتعلق بالسلوك الصادر عن شخص مسؤول يتوفر لديه القصد الجنائي بشقيه (العلم والإرادة) وهذا الشخص يستوي أن يكون شخصا طبيعيا أو معنويا .
3. أنه من حيث الركن الشرعي يشمل جميع صور السلوك الذي يجرمه المشرع في الحاضر والمستقبل ويفرض له عقابا فمهما كان السلوك غير أخلاقي أو غير إنساني فإنه لايعتبر جريمة مالم يجرمه المشرع.
4. أنه من حيث الركن الخاص بالجرائم المعلوماتية، يشمل جميع صور الإعتداء الحالية والمستقبلية على المعلومات أو البيانات الإلكترونية ضمن بيئة إلكترونية ,وبناءً على

1.علي حسين الخلف وسلطان عبدالقادر الشاوي،**المبادئ العامة في قانون العقوبات**، مطابع الرسالة،الكويت،1982،ص134.

ذلك نستبعد من نطاق هذه الجرائم جميع صور السلوك التي تتعلق بالمعلومات أو البيانات في صورتها المادية ،لأنها تخضع للنصوص التقليدية الخاصة بالجرائم التقليدية من دون أن تثير أية مشكلة .[1]

كماأنه يجب التفرقة بين الجرائم المعلوماتية بالمعنى الفني عن بقية الجرائم الإخرى التي يستخدم فيها الحاسب الآلي عموما والإنترنت خصوصاً، فجرائم الإنترنت وشبكات المعلومات يقصد بها الدخول غير المشروع إلى الشبكات الخاصة كالبنوك والمؤسسات وكذا الأفراد، والقيام بالعبث في البيانات الرقمية، التي تحتويها شبكة المعلومات مثل تغيير البيانات أو إتلافها أو محوها، وكذلك بالنسبة للبرامج والأجهزة التي تحتويها، بينما الجرائم التقليدية مثل غسيل الأموال والإرهاب والدعارة ، تجارة المخدرات ، إستخدام غير المشروع لبطاقات الإئتمان فيعتبر الإنترنت أداة لإرتكابها وليست ضمن جرائم الإنترنت بالمعنى الفني وإن كان يطلق عليها الجرائم المعلوماتية [2] .

- **بالنسبة للمشرع الفلسطيني في تعريفه للجريمة الإلكترونية (المعلوماتية) :**

لم يضع المشرع الفلسطيني تعريفاً جامعاً للجريمة الإلكترونية ولكنه من خلال المواد والنصوص القانونية عاقب عليها وذلك من خلال ماجاء به القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، إذ أصبح هذا القانون حاجة أساسية وضرورية للمجتمع الفلسطيني في ظل التغيرات التكنولوجية وتطورها وخاصة بعد انضمامها إلى الإتفاقيات الدولية والإقليمية حول الجرائم المعلوماتية التي حثّت الدول الأعضاء على إتخاذ تدابير تشريعية لإصدار قانون الجرائم الإلكترونية إلا أن ملاحقة مرتكبي مثل هذه الجرائم سابقاً

1. رشاد خالد عمر،**المرجع السابق**،ص25-26.

2.عرشوش سفيان ، **جرائم المساس بأنظمة الكمبيوتر** ، مذكرة ليسانس ، بإشراف الدكتور سعيد فكرة ،معهد العلوم القانونية،المركز الجامعي خنشلة ،2006،ص10 .

قبل صدور هذا القرار كانت تتابع وتطبق القوانين السارية المفعول في الضفة الغربية وقطاع غزة فكان يطبق قانون العقوبات الأردني رقم (16) لسنة 1960على الجرائم الإلكترونية، والقانون رقم (3) لسنة 1996 بشأن الإتصالات السلكية واللاسلكية بالإضافة إلى القرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الإتصالات[1] . وقانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته، وإن تعطل المجلس التشريعي والإنقسام السياسي حال دون إصدار قرار بشأن الجرائم الإلكترونية وتأخر صدوره، مادفع برئيس دولة فلسطين بموجب صلاحياته الدستورية وفق أحكام المادة **(43)** من القانون الأساسي الفلسطيني لسنة 2005 وتعديلاته إلى إصدار قرار بشأن الجرائم الإلكترونية لسنة 2017 لمواجهة هذه الجريمة في المجتمع الفلسطيني وليردع مرتكبيها، متماشيا مع الإلتزامات المترتبة على دولة فلسطين نتيجة التوقيع والانضمام للمعاهدات الدولية والاقليمية الخاصة بذلك ومنها :

1. إتفاقية بودابست لعام 2001.
2. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات وصادقت عليها فلسطين بتاريخ 2013/05/21.

- **بالنسبة للمشرع الجزائري في تعريفه للجريمة الإلكترونية (المعلوماتية)** كما قلنا سابقاً أن الجريمة الإلكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلاً، كونها تستخدم اللأجهزة التقنية الحديثة في الوصول إلى المبتغى المقصود، وبهذا فإن الفقه الجزائري تبنى تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة الإلكترونية (المعلوماتية) :" جريمة يمكن إرتكابها

1.محمد الشلالدة،عبدالفتاح أمين،**الجرائم الإلكترونية في دولة فلسطين**،بحث مقدم لكلية القانون جامعة جرش حول الجرائم المعلوماتية،5-2015/5/7،ص8.

بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من وتتمثل من ناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية.

وتبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبراً أن النظام المعلوماتي بحد ذاته ومايحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الإعتداء على هذا النظام فإن ثبت تخلف هذا الشرط فلا يكون هناك مجال لهذا البحث.[1]

حيث أنه عرف من خلال نص المادة (2) الفقرة (ب) من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها . مسمياً إياه" المنظومة المعلوماتية": وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضعا البعض أو مترابطة،يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين" .

حيث جرّم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم (04-15) المؤرخ في 2004/11/10 المتمم للأمر رقم (66-156) المتضمن قانون العقوبات واالذي تضمن 08 مواد من **المادة 394 مكرر وحتى المادة 394 مكرر 7**[2] ووفق المشرع الجزائري كغيرهِ من

---

1. قانون رقم(09-04) المؤرخ في 14 شعبان 1430 لسنة 2009 **يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها** ح ر ع 47 صادر بتاريخ 2009/08/16، ص5.

2. عائشة بن قارة،**حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن**،دار الجامعة الجديدة،الاسكندرية،2006،ص27.

التشريعات في تعريفه لنظام المعالجة الآلية للمعطيات واشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها،وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال. ، ونجد أن المشرع تطرّق لتعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 2 من قانون رقم 04/09 وجرّم الأفعال في مواده من 394-394 مكرر 7 من قانون العقوبات الجزائري .

الفرع الثاني: نشـــأة الجريمة الإلكترونية (المعلوماتية) .

إن التتبع التاريخي لمسار فرع قانوني أو موضوع قانوني يفيد كثيراً، بل هو لازم، حين يكون الغرض التوصل إلى محددات عامة تؤطر المسائل الجزئية ذات الإتصال بالفرع مدار البحث، والحقيقة إن تتبع المسيرة التاريخية لعلاقة القانون بالكمبيوتر والإتصالات أو النقل بتكنولوجيا المعلومات ليس المقصود منه التوثيق لأحداث تاريخية بل قراءة المفاصل التي هي في حقيقتها ولادة الفروع والجزئيات .

وفي السياق التاريخي وحتى الان، أثّرت تقنية أو تكنولوجيا المعلومات على مختلف فروع القانون التقليدية، فأظهرت الحاجة إلى الإعتراف بمصالح جديدة، وأوجبت إعادة تقييم القواعد القانونية والإجرائية في العديد من فروع القانون القائمة لجهة التعامل من أنماط السلوك والعلاقات القانونية المستجدة في بيئة تقنية المعلومات . [1]

فلذلك إن تاريخ ظهور الجرائم المعلوماتية حديث نسبيا،فهذه الجرائم ترتبط في وجودها التاريخي بتاريخ ظهور الكمبيوتر ،ومن الوجهة التاريخية، طرح أول كمبيوتر للشراء عام 1954 بالولايات المتحدة الأمريكية ولم تمضي فترة طويلة على ذلك حتى سجّل وقوع أول جريمة إلكترونية(معلوماتية) في نفس البلد عام 1958،ومنذ ذلك الحين زادت نسبة هذه الجرائم يوماً

1. أمير فرج يوسف،**الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت**،ط1،مكتبة الوفاء القانونية،الإسكندرية،2011،ص39.

بعد يوم وتنوعت أساليب إرتكابها وتعددت إتجاهاتها،كما وزاد حجم الخسائر الناجمة عنها وأخطارها حتى غدت اليوم واحدة من أكثر و أخطر الأنشطة الإجرامية إنتشارا في العالم، ففي عقد الستينيات من القرن المنصرم توسعت دائرة هذه الجرائم حيث بدأت الصحف ولأول مرة تنشر المقالات بصددها، ومن ثم زادت حدة هذه الجرائم في فترة السبعينيات بحيث بدأت ملامح ظاهرة الإجرام الإلكتروني تلوح في الأفق، وبدأت الأبحاث المعتمدة على الأسس العلمية ببحث هذه الجرائم في منتصف هذه الفترة، وقد كان الإضرار بأجهزة الكمبيوتر وتخريب شبكات الهاتف من الصور الشائعة لهذه الجرائم في تلك الفترة، في حين أن فترة الثمانينات والتسعينيات، سجلت قفزة في حجم هذه الجرائم من حيث الكم والنوع بحيث تحدد مفهوم وماهية هذه الجرائم وتبلور مفهوم ظاهرة الإجرام الإلكتروني(المعلوماتي) بصورة واضحة تماما .[1]

وذلك بعد أن زاد نطاقها بشكل هائل بفعل ظهور الشبكة العنكبوتية "الإنترنت" وإستخدامها من قبل عدد هائل من المستخدمين،مما أدى إلى ظهور أنماط وصور جديدة من هذه الجرائم. ففي الثمانينات أظهرت دراسة قام بها **معهد كولفيلد للتكنولوجيا** في أستراليا عام 1985 ، بأن مايتزيد عن 900 جريمة معلوماتية سنويا تقع في أستراليا،وفي اليابان كشفا الشرطة المركزية بالعاصمة طوكيو عام 1988 عن وقوع 1136 جريمة معلوماتية في اليابان خلال ذلك العام وحده، وفي التسعينات سجلت الشرطة الألمانية وقوع 5004 جريمة معلوماتية في ألمانيا خلال عام 1991 وحده.[2]

1. رشاد خالد عمر،**المرجع السابق**،ص15-16.

2. نائلة قورة،**جرائم الحاسب الآلي الإقتصادية**،ط1،منشورات الحلبي الحقوقية،بيروت،2005،ص80.

وأما الألفية الجديدة فإنها شهدت تزايدا لامثيل لها في حجم هذه الجرائم فبحسب الإحصاءات التي قام بها مركز **(IC3)**[1] لتلقي الشكاوي عن الجرائم المعلوماتية عبر الإنترنت، حيث بلغ عدد الشكاوى النى تلقاها المركز في عام 2001 مامجموعه(336655) شكوى.[2]

وهذا يعني بأن نسبة هذه الجرائم في تزايد مستمر مع الأخذ بنظر الإعتبار أن النسب المذكورة تمثل فقط عدد الجرائم المعلوماتية التي تم إكتشافها والإبلاغ عنها للمركز المذكور وليس العدد الكلي لها في العالم، حيث أنه وبمقتضى دراسة المركز الأمريكي للإستراتيجيات والدراسات العالمية، فإن الحجم الحقيقي لهذه الجرائم في العالم يبلغ مايقارب 10 مليارات سنويا.[3] وبعد الإندماج مابين الحوسبة و الإتصالات ظهرت الأنشطة التي تستهدف المعطيات عن بعد كاختراق شبكات الحاسوب للتوصل غير المصرح به مع أنظمة الإتصال البعدي .

وأيضاً في ثمانينيات القرن المنصرم طفا على السطح مفهوم جديد ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وأنشطة نشر وزراعة الفيروسات الإلكترونية، التي تقوم بعمليات تدميرية للملفات أو البرامج وقد شاع اصطلاح **(الهاكرز)** المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لإرتكاب هذه الأفعال ظل في غالب الأحيان محصورا بالحديث عن رغبة المخترقين في تجاوز أجراءات أمن المعلومات وفي إظهار تفوقهم التقني، وانحصر الحديث عن مرتكبي هذه الأفعال حول صغار السن من المتفوقين الراغبين في التحدي والمغامرة، ولكن الحقيقة أن

---

1. **مركز(آي سي 3):** هو مركز مؤسس بشراكة مابين كل من مكتب التحقيقات الفيدرالي(ق.بي.اي) والمركز الوطني الأمريكي لمكافحة جرائم الياقات البيضاء(ان دبليو 3 سي) لتكون بمثابة وسيلة لتلقي الشكاوى عبر شبكة الإنترنت عن الجرائم المعلوماتبة في العالم.

2. The internet crime complaint center(I C3,) IFCC 2001 Internet Fraud Repon ,The national white collar crime center, 2002. P 3

3. أيمن عبدالله فكري،**المرجع السابق**،ص103.

مغامري الأمس أصبحوا أداة إجرام فيما بعد، إلى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم، وظهر المجرم المعلوماتي لبمتفوق لبمدفوع بأغراض إجرامية خطرة،القادر على إرتكاب أفعال تستهدف الإستيلاء على المال أو تستهدف التجسس او الإستيلاء على البيانات السريّة الإقتصاديّة و الإجتماعيّة والسياسيّة والعسكريّة.[1]

ولقد كان أول ظهور لأول جريمة إلكترونية في جرائم التقنية العالية في نهاية الثمانينيات من القرن المنصرم، حين أفاق العالم على جريمة العدوان الفيروس **(دودة موريس)** المؤرخة واقعتها في 1988، وتعد هذه الحادثة أول الهجمات الكبيرة والخطرة في بيئة الشبكات، حبث تمكن طالب يبلغ من العمر 23 عاما يدعى **(Rober Morris)** من إطلاق فيروس عرف بإسم (دودة موريس) عبر الإنترنت أدى إلى إصابة 6000 جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها أجهزة العديد من الدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار بالإضافة إلى مبالغ أكثر من ذلك تمثل الحسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة وقد حكم على موريس بالسجن لمدة 3 سنوات وبغرامة مالية 10000$.[2]

---

1. بن مكي نجاة،**السياسة الجنائية لمكافحة الجرائم المعلوماتية**،مذكرة مقدمة لنيل شهادة الماجستير،تخصص القانون الدولي الجنائي، إشراف البروفيسور زواقري الطاهر،كابة الحقوق،جامعة خنشلة،2009،ص16-17.

2. **الإنترنت: هو شبكة عالمية تربط عدة الاف من الشبكات وملايين أجهزة الكمبيوتر المختلفة الأنواع والأحجام في العالم وتكمن فائدة الإنترنت في كونها وسيلة يستحدمها الأفراد والمؤسسات للتواصل وتبادل المعلومات ،وبدأ العمل في الإنترنت الأمريكية، ثم تطور الأمر إلى أن تخلت تلك الوزارة عنها فأصبحت ذات طابع دولي يتاح لجميع الأفراد في العالم في التعامل من خلالها وذلك بإبرام الصفقات المختلفة وتبادل المعلومات والمراسلات الخاصة وهذا ماسهل على الأفراد التواصل فيما بينهم،فأصبح الإنترنت منتج غير مستهدف في صراع طال بين الشرق والغرب وأصبحت شبكات الثرن الواحد والعشرين هي محرك الحضارة الجديدة التي تقوم على فكرة الإتصال لا الإنتقال .**

ومن أشهر القضايا الإلكترونية أيضا **قضية الجحيم العالمي**، حيث تعامل مكتب التحقيقات الفيدرالية مع قضية أطلق عليها اسم **مجموعة الجحيم العالمي (GLOBAL HELL)**، فقد تمكنت هذه المجموعة من إختراق موقع البيت الأبيض والشركة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية في الولايات المتحدة، وقد أُدينَ إثنين من هذه المجموعة جراءَ تحقيقات الجهات الداخلية في الولايات المتحدة وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الإختراق أكثر من التدمير أو إلتقاط المعلومات الحساسة وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبرَ الشبكة وتتبع آثار أنشطتها، وقد كلّف التحقيق مبالغ طائلة لما تَطلبه من وسائل معقدة في المتابعة.[1]

وهناك أيضاً العديد من الجرائم الإلكترونية والقضايا الإلكترونية التي قامت بتدمير عدد من المواقع والوصول إلى المعلومات الحساسة وقد كلّفت المبالغ الطائلة في ملاحقتها ومتابعة مرتكبي هذه الجرائم نكتفي بذكرها فقط وهي :

1. **فايروس ميلسا.**

2. **حادثة المواقع الإستراتيجية.**

3. **حادثة الأصدقاء الأعداء(الهاكرز الإسرائليين).**

4. **حادثة شركة أوميجا.**[2]

وبما أنها هذه الجرائم مستحدثة تتّنوع وتتضاعَف كل يوم فالمُستَجد هو الكيانات المعنوية ذات القيمة المالية ولولا هذه الطبيعة لما كنا أمام ظاهرة مستجدة برمتها، وبالتالي فإننا نلاحظ أن تطوّر الجريمة الإلكترونية مرّ في ثلاثة مراحل نلخصها كما يلي :

1.يوسف حسن يوسف،**الجرائم الدولية للإنترنت**،ط1،المركز القومي للإصدارات القانونية،2011،ص51.

2.انظر: يوسف حسن يوسف،**المرجع نفسه** ،ص51-55.

1. **المرحلة الأولى:** من شيوع إستخدام الحواسيب من الستينيات إلى السبعينيات من القرن الماضي إقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أم ظاهرة مستحدثة .وأن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة الحوسبة.

2. **المرحلة الثانية:** في بداية الثمانينات من القرن الماضي تاكد مفهوم جديد لجرائم الكمبيوتر والإنترنت حيث إرتبطت هذه الأخيرة بعمليات إقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج وشاع إصطلاح **(الهاكرز)** المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي .

3. **المرحلة الثالثة:** حيث شهدت فترة التسعينيات تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيلات لعمليات دخول الأنظمة وأقتحام شبكة المعلومات حيث ظهرت أنماط حطيرة في ذات الوقت بحيث نَمت الإنترنت بشكل مذهل خلال هذه الفترة بعدما كانت مجرد شبكة أكاديمية صغيرة وتحوّلت إلى بيئة متكاملة للإستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي البداية لم يكن ثمة إهتمام بمسائل الأمن بقدر ماكان الإهتمام ببناء الشبكة وتوسيع نشاطها دون مراعاة تحديات أمن المعلومات، فالإهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة وهذه الثغرة التي شجّعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة، وهو ماأدّى إلى لفت الأنظار إلى حاجة شبكة الإنترنت إلى توفيير معايير من الأمن وبدأ التفكير مَليّاً في الثغرات ونقاط الضعف وعليه قد يكون الكمبيوتر هدفاً للجريمة وغايته المعلومات المخزنة والسيطرة على النظام دون التصريح والسرقة والإعتداء على الملكبة الفكرية، كما قد يكون الكمبيوتر محلاً للجريمة كحالة إستغلال الكمبيوتر للإستيلاء على أموال

الغير بإجراء تحويلات غير شرعية، كما أنه قد يعد أداة للجريمة كحالة تخزين البرامج المنسوخة أو في حالة إستخدامه لنشر مواد غير قانونية.[1]

- أما بالنسبة للجرائم الإلكترونية في فلسطين حيث سجلت وحدة الجرائم الإلكترونية [2]، مابين (2013–2017) مايقارب (3525) شكوى وهذه الشكاوى المبلغ عنها فقط والتي وصلت هذه الوحدة ،حيث بلغ عددها (174) في العام 2013،وفي العام 2014 بلغ عددها (361) شكوى أي بزيادة مقدارها51,1% وارتفع في العام 2015 إلى (502) شكوى بنسبة زيادة 65,3%، في حين وصلت في العام 2016 إلى (1327) شكوى بزيادة 86,9%، ومذ بداية العام 2017 حتى شهر أوت سجلت (1161) شكوى مقدمة لوحدة الجرائم الإلكترونية.[3]

وقد تنوّعت الشكاوى الواردة إلى وحدة الجرائم الإلكترونية مابين شكاوى النصب والإحتيال،السّب والشّتم، التّهديد، التّشهير، وإنتحال الشّخصية، والقرصَنة الإلكترونية وسرقة الحسابات، وإفساد الرابطة الزوجية، والإبتزاز وجرائم مختلفة. ويتضح لنا من خلال تلك الأعداد والنسب أن الجرائم الإلكترونية في تزايد مستمر كلما تقدمنا بالتطور والتقدم التكنولوجي كلما أصبح الأمر أكثر تعقيداً وخطورة، وأنها تزيد بين الفَينة والأخرى وعلى

---

1. فضيلة عاقلي،**المرجع السابق**،ص8–9.

2. **وحدة الجرائم الإلكترونية: هي إحدى الوحدات الحديثة في جهاز الشرطة الفلسطينية حيث أنشئت بقرار من مدير عام الشرطة الفلسطسنية في النصف الثاني من العام 2013**،**وتتبع للمباحث الدنائية العامة، وتتكون من قسم متابعة شكاوى الإنترنت ومختبر الأدلة الإلكترونية وقسم متابعة جرائم الإتصالات بالإضافة إلى قسم التوعية والإرشاد والدائرة القانونية**،**وعدد العاملين فيها لايتجاوز 12 شخص وعدد من الضباط موزعين على كافة المحافظات فالعاملين في هذه الوحدة معظمهم من خريجي البرمجة والهندسة الإلكترونية ومن الضباط الحقوقيين أوتتنوع مؤهلاتهم العلمية وفق احتياجات جهاز الشرطة الفلسطينية .**

3. نبيل أبو الرب،**الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين**،رسالة ماجستير،تخصص قانون جنائي،إشراف الدكتور أنور جانم،كلية الحقوق،جامعة النجاح – فلسطين ، 2017،ص63.

الجهات المسؤولة بذل أقصى الجهد للحد والتقليل من هذه الجرائم من خلال تعزيز التنسيق والتعاون بين المؤسسات القانونية الإقليمية والدولية والعمل على نشر الثقافة والوعي بمخاطر الجرائم الإلكترونية .

المطلب الثاني: خصـــائـــص الجـــرائـــم الإلكـــترونـــيـــة :

(خصائص الجرائم المعلوماتي و المجرم المعلوماتي)

تتميز الجرائم الإلكترونية بخصائص تختلف إلى حد ما عن الجريمةالعادية نذكرها مع التوضيح كما يلي:

1.**جرائم عابرة للدول:** يطلق تعبير "جرائم عابرة للدول" أو جرائم عبر وطنية على تلك الجرائم التي تقع بين أكثر من دولة بمعنى أنها لاتعترف بالحدود الجغرافية للدول كجرائم تبييض الأموال وغيرها.

وفي عصر الحاسب الآلي ومع إنتشار شبكة الإتصالات العالمية، أُمكن ربط أعداد هائلة لاحصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والإتصال فيما بينها أمراً سهلاً، طالما جدد عنوان المرسل إليه أو أمكن معرفة كلمة السر(Password)، وسواء تم ذلك بطرق مشروعة أو غير مشروعة.

في هذه البيئة يمكن أن توصف الجرائم الإلكترونية بأنها جرائم عابرة للدول، إذ غالبا مايكون الجاني في بلد والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر الجرائم الإلكترونية شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القاريّة، وهذا مايثير عدة تحديات في مجال الإختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش، وهذا مايُظهر الحاجة إلى التعاون الدولي في مجال مكافحة هذه الجرائم، وتجدر الإشارة هنا إلى جهود الإنتربول في هذا

المجال، من خلال الضباط المنتشرين في كافة الدول في العالم والمُكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تُشكّل نقطة الإنطلاق والمكافحة والتصدي لهذه الجرائم.[1]

2. جرائم صعبة الإكتشاف والإثبات: تتميز هذه الجرائم بصعوبة إثباتها وإكتشافها نتيجة لعدم تركها أي أثر خارجي التي تمكن الجاني من إرتكابها في دول مختلفة، وقدرة الجاني على تدمير الدليل وإخفاءه بسهولة في أقل من ثانية، كمسح البرامج أو وضع رموز وكلمات سرية لتشفير المعلومات والبيانات، مما يصعب على أجهزة التحقيق والملاحقة في الوصول إلى الدليل الرقمي لإدانة المجرم المعلوماتي.[2] وإن صعوبة إكتشافها يرجع إلى الصدفة البَحِتَة، والدليل على ذلك أنه لم يكتشف إلا نسبة 1% فقط منها، وأن 15% منها تم الإبلاغ عنها، وأن 5/1 من النسبة الأخيرة هي التي يصدر فيها أحكام بإدانة مرتكبيها.[3]

3.جرائم مغرية للمجرمين: تعتبر الجرائم المعلوماتية جرائم مغرية للمجرمينلسرعة تنفيذها ومع إمكانية تنفيذها عن بعد دون الحاجة للتواجد في مسرح الجريمة، ولضخامة المكاسب المادية والمعنوية التي قد يحققها الجاني من إرتكابه لهذه الجرائم،وترجع أسباب ذلك نتيجة لإستغلا التقدم التكنولوجي الحديث، وغياب النصوص العقابية القانونية الرادعة مما أدى إلى ظهور أشكال وأنماط جديدة لهذه الجرائم.[4]

4.جرائم ناعمة (جرائم سهلة الإرتكاب Soft Crime) : إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي من نوع ما كجرائم القتل، السرقة، الإغتصاب، فإن جرائم الحاسب الآلي على العكس لاتحتاج إلى أدنى مجهود عضلي ،بل تعتمد على الدراية

---

1. أسامة المناعسة وآخرون،**جرائم الحاسب الآلي والإنترنت**،ط1،دار وائل للنشر،الأردن،2001،ص105-106.

2.جميل عبد الباقي الصغير،**الجرائم الناشئة عن استخدام الحاسب الآلي**،ط1،دار النهضة العربية،1992،ص17.

3.بن مكي نجاة،**المرجع السابق**،ص19.

4.خالد ممدوح ابراهيم،**الجرائم المعلوماتية**،ط1،دار الفكر الجامعي،الإسكندرية،2009،ص78

الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات الحاسب الآلي، ولذا كان الشرط الأساسي في المجرم توافر العلم الكافي بكيفية عمل الحاسب الآلي وآلية تشغيله، بالإضافة إلى الإحاطة ببعض البرامج التشغيلية.

5.الحاسب الآلي هو أداة إرتكاب هذه الجرائم: وتعتبر من أهم الخصائص التي تميز جرائم الإنترنت عن غيرها من الجرائم الأخرى لاسيما التقليدية، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها **بالحاسب الآلي**[1] هو أمر لامفر منه باعتباره النافذة التي تطل بها على الشبكة على العالم الخارجي.[2]

6.مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الحوسبة: تتطلب جرائم الإنترنت على غرار الجرائم التقليدية تقنية فنية عالية سواء عند إرتكابها أو عند العمل على عدم إكتشافها من الشخص الذي يرتكبها، أي يجب أن يكون ذلك الشخص خبيراً بالقدر اللازم والكافي بأمور الحوسبة والإنترنت، ولذلك نجد أن معظم من يرتكبون الجرائم الإلكترونية هم من الخبراء في مجال الحاسب الآلي، وأن الشرطة أول ماتبحث عن خبراء الكمبيوتر عند إرتكاب هذا النوع من الجرائم. [3]

7.جرائم ترتكب عبر شبكة الإنترنت: تعدّ شبكة الإنترنت هي حلَقة الوَصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف التي ماتكون غالباً

1.الحاسب الآلي:"كل جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال أو إحراج معلومات وإجراء عمليات حسابية أو منطقية وهو يقوم بالكتابة على أجهزة الإحراج أو التخزين والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات إدخال أ, إسترجاعها من وحدة المعالجة المركزية وبعد معالجة البيانات تتم كتابتها على أجهزة الإحراج وهو يتكون من كيانين مادي ومعنوي". انظر: هلالي عبدالله أحمد،نظم الحاسب الآلي ص16-17.

2.نبيلة هبة هروال،**الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات**،دار الفكر الجامعي،الإسكندرية،2013،ص35.

3.نبيلة هبة هروال،**المرجع نفسه**،ص37-38.

الضحية لتلك الجرائم وهو مادعا معظم تلك الأهداف إلى اللجوء إلى نُظم الأمن الإلكترونية في محاولة منها لتحمي نفسها من تلك الجرائم أو على الأقل لتحدّ من خسائرها عند وقوعها ضحية لتلك الجرائم.[1]

8. جرائم ترتكب عادة بتعاون أكثر من شخص: من يقوم بإخراج الجريمة من حيّز الوجود الخارجي غالبا أشخاص متخصصون فنياً في مجال تقنية المعلومات لتشكيل النشاط الجرمي، وبالتعاون مع شخص آخر لتغطية وإخفاء عمليات التلاعب والتحويل.[2]

9. جرائم مكلفة للضحايا: فإذا كانت هذه الجرائم مُربحة للجناة فإنها في ذات الوقت مُكلفة للضحايا حيث أنها تسبب عموماً في إلحاق أضرار مالية باهظة بضحاياها مقارنة مع مايمكن أن تتسبب به الجرائم التقليدية، وبالتالي فإن لها الخطورة الكبيرة على إقتصاديات الدول.

10.قليلة المخاطرة: فنسبة مُخاطرة الجاني قليلة نسبياً بالمقارنة مع تلك التقليدية، فهو غير مُعرض لخطر المواجهة المباشرة مع المجني عليه أو غيره ولا لِخطر المُواجَهة المُسلحة مع الشرطة.

11.خفيّة عن الأنظار: حيث أنها ترتكب بخفّة و خِفية شديدة من دون أن يرى طرفا الجريمة بعضهُما البعض **(المجرم المعلوماتي و الضحية المعلوماتية)** وأن أغلَب ضحاياها ليس لديهم الخبرة الكافية بحماية أنظمتهم المعلوماتية، وبالتالي يَسهل على الجاني إختراق جدران الحِماية الأمنية لتلك المعلومات .[3]

1.منير و محمد الجنبيهي،**جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**،دار الفكر الجامعي،الإسكندرية،2005،ص14.

2.سامي الشوا،**ثورة المعلومات وانعكاساتها على قانون العقوبات**،دار النهضة العربية،القاهرة،1994،ص46.

3.رشاد خالد عمر،**المرجع السابق**،ص29.

كما رأينا أن خصائص الجريمة الإلكترونية متعددة، ويتبين لنا أن العلاقة طرديّة مع المعرفة التقنية فكلما زادت المعرفة التقنية لدى الأشخاص كلما زادت إحتمالية توظيف هذه المعرفة بشكل غير مشروع، وأن عولمة هذه الجرائم أدت إلى تشتيت جهود التّحري والتّنسيق الدولي لتعقّبِها بسبب عَولمة هذا النوع من الجرائم، وبالتالي صعوبة تحديد مَن هو المسؤول جنائياً عن تلك الأفعال كما وأن نسبة إكتشاف المجرم المعلوماتي هي 1 من 22000 حالة نتيجة صعوبة تتبع أثره، وهذا ماجَلب إهتمام المُجتمع الدولي قَصد مُكافحتها والحد من إنتشارها وتزايُد مخاطِرها ووضعها على أجندة إهتمام المُجتمع الدولي كونَه يصعُب على الدولة الواحدة مكافحة من يرتكب مثل هذه الجرائم.

المطلب الثالث: صور الجرائم الإلكترونية:

لِلجرائم الإلكترونية (المعلوماتية) صور متعددة لايمكن حصرها، كونهامتجددة ومتزايدة بإستمرار وبصورة مطّردة مع التطور التكنولوجي من جهة، ومع تزايد استعمال الكمبيوتر والإنترنت وغيرها من الأجهزة التقنية في مجالات الحياة المختلفة من جهة أخرى بالإضافة إلى أنّ صور الجرائم الإلكترونية تختلف من بلد لآخر، ولقد اختلف الفقه في تصنيفها إلى عدة مسميات ولم تراعي أغلب التقسيمات خصائص الجرائم الإلكترونية وموضوعها، وإنّ أهم مايميز الجرائم الإلكترونية عن غيرها هو أن هذه الجرائم تستهدف الكيانات المعنوية للحاسب الآلي، وتُرتكب بواسطة جهاز إلكتروني، حيث أن الجرائم الإلكترونية لاحصر لها ولايُمكننا أن نُجمِلها بكلّ أصنافها وأشكالها فهي متغيرة ومتجددة فكلّما ظهرت وَسيلة جديدة لإستخدام الحاسب الآلي والإنترنت ظهرت معهُ جريمة جديدة وعليه سَنحاول إيراد بعض من هذه الصور ضمن أهم تلك التصنيفات، وكالآتي:

الفرع الأول : التصنيفات الفقهية للجرائم الإلكترونية :

أولا: تصنيف الفقيه مارتن فاسك (Martin Vasik): وهو يصنف هذه الجرائم إلى ثلاثة طوائف، تتضمن كل طائفة منها مجموعة من الجرائم، وكما يلي:

الطائفة الأولى: الدخول والإستعمال غير المصرح بهما للنظام المعلوماتي وتشمل جرائم (الدخول غير المصرح به إلى النظام المعلوماتي بحد ذاته، الدخول غير المصرح به إلى النظام المعلوماتي بقصد إرتكاب جريمة معلوماتية أخرى، الإستعمال غير المصرح به للمعلوماتية، الإعتراض غير المشروع للمعلوماتية، الأفعال غير المشروعة المتصلة بالمعلومات الشخصيةالمعاجة آليّا) .

الطائفة الثانية: الإحتيال المعلوماتي وسرقة المعلومات، وتتضمن جرائم (التلاعب بالمعلومات المعالجة آليا بهدف الحصول من ورائه على ربح مادي غير مشروع، تزوير المعلومات المعالجة آليا بنيّة إستخدامها فيما بعد في أغراض غير مشروعة، القرصنة الواقعة على البرامج المعلوماتية).

الطائفة الثالثة: الجرائم الوقعة من خلال الكمبيوتر والأفعال المساعدة على إرتكاب الجريمة المعلوماتية وتشمل جرائم (أفعال التخريب والإتلاف الواقعة على المكونات المادية أو المعنوبة للحاسب الآلي، الإبتزاز والتهديد بتدمير المكونات المادية أو المعنوية للحاسب الآلي، صناعة وبيع المعدّات والأدوات المساعدة على إرتكاب جرائم الكمبيوتر مِثل إعداد البرامج الخبيثة أي الفيروسات التي تساعد على إرتكاب جرائم إتلاف المكونات المادية أو المعنوية للحاسب الآلي، الإفشاء غير المشروع للمعلومات التي يؤتمن الجاني عليها بحكم وظيفته، إستعمال أنظمة الكمبيوتر في جرائم الإعتداء على أمن وسلامة الأفراد) . [1]

1.أيمن عبدالله فكري،المرجع **السابق**،ص123.

ويؤخذ على هذا التصنيف أنه يعتبر الجرائم الواقعة على المكونات المادية للكمبيوتر، جرائم معلوماتية وأننا أكدنا سابقا على أنها جرائم تقليدية وليست معلوماتية، كما ويُعاب على هذا التصنيف محاولة حَصر وتحديد الأفعال المساعدة على إرتكاب الجرائم الإلكترونية في ظلّ التطورات السريعة والمستمرة للتكنولوجيا واستخداماتها المُتشعبة.

ثانيا: تصنيف الفقيه أولرتش سيبر (Ulrich Sieber) : وهو يصنفها إلى الطوائف التالية[1]:

الطائفة الأولى: جرائم الكمبيوتر المتصلة بإنتهاك حرمة الحياة الخاصة ويتضمن جرائم (إستخدام بيانات شخصية غير صحيحة سواء عن طريق تغييرها أو محوها من قبل أشخاص غير مرخّص لهم بذلك أو عن طريق جمعها أو نشرها أو معالجتها من قِبل أشخاص مصرّح لهم بذلك سواء عن طريق العمد أو الإهمال، جمع وتخزين بيانات صحيحة على نحو غير مشروع وذلك إما لإستعمال أساليب غير مشروعة في الحصول عليها أو لِوقوعها من قبل أشخاص غير مصرّح لهم بذلك أي لِوقوعها بصورة مخالفة للقواعدالشكلية المحددة لذلك القانون)

الطائفة الثانية: جرائم الكمبيوتر الإقتصادية وتشمل جرائم (الإحتيال المعلوماتي بقصد الحصول وبغير حق على أموال أو أصول أو خدمات، التّجسس المعلوماتي في نِطاق قِطاع الأَعمال، القرصنة على برامج الحاسب الآلي، الإتلاف المعلوماتي من خلال الإعتداء على مكونات الكمبيوتر المادية أو غير المادية، أفعال الدخول غير المصرح به للنظام المعلوماتي، الجرائم التقليدية الواقعة في نطاق الأعمال بمساعدة النظام المعلوماتي) .

الطائفة الثالثة: الجرائم التي تهدد المصالح القومية للدولة و السلامة الشخصية للأفراد وهي تتضمن مايلي (الجرائم المعلوماتية التي تشكل الإعتداء على أنظمة الدفاع في الدولة، الجرائم التي تشكل الإعتداء على أنظمة الطيران، والتحكم الإلكتروني بما يهدد السلامة البدنية للأفراد)

1. See: Ulrich Sieber. Op. eit. P. 27.39 and 58.

ويُؤخذ على هذا التصنيف نفس النقد الذي وجهناه لتصنيف مارتِن فاسك لأنه يعد الجرائم الواقعة على المكونات المادية للكمبيوتر جرائم معلوماتية .

ثالثا: تصنيف منظمة التعاون الإقتصادي و التنمية (OECD) الصادر عام 1986ضمن تقرير المنظمة عن جرائم الحاسب الآلي: وبمقتضاه تصنف الجرائم المعلوماتية إلى الطوائف الخمس التالية [1] :

1. إدخال معلومات إلى نظام الكمبيوتر أو تعديل أو محو معلومات موجودة بالفعل في الحاسب الآلي، اذا ماتم ذلك على نحو غير مشروع بنيّة تحويل الأموال أو الممتلكات التي تمثلها تِلك المعلومات.

2.إدخال معلومات إلى نظام الكمبيوتر أو تَعديل أو مَحو معلومات موجودة فيه بالفعل، وإعتراض نظام الحاسب الآلي، إذا ماتمّ ذلك بنيّة إعاقة الحَاسِب عن أداء وظيفته.

3. إستغلال برامج الكمبيوتر تجارياً وطرحها في الأسواق، في حال وقوع ذلك بالإنتهاك لحقوق مَالِك تِلك البرامج أو وقوعِه بطريق الحصول غير المشروع على المعلومات.

4. الدخول أو الإعتراض غير المصرح به لنظام الكمبيوتر متى ماتمّ ذلك عن عمد، سواء كان الدخول أو الإعتراض مجرداً أم أنه حصل بنيّة إرتكاب جريمة معلوماتية أُخرى.

5. الإستعمال غير المصرّح به لنظام الحاسب الآلي.

يُعاب على هذا التصنيف من قبل المنظمة أنه ليس تصنيفاً بالحقيقة إنما هو سَرد لِصُوَر الجرائم المعلوماتية فقط .

1. نائلة قورة،**المرجع السابق**،ص248-249.

الفرع الثاني : التصنيفات التشريعية للجرائم الإلكترونية :

أولا: تصنيف وزارة العدل الأمريكية: وهي تصنف الجرائم إلى ثلاثة طوائف [1] :

الطائفة الأولى: الجرائم التي يكون الكمبيوتر فيها جسماً للجريمة، مثلاً كجرائم (الدخول غير المصرّح به للمعلومات المخزنة في الكمبيوتر أو الشّبكة الضحيّة، والإتلاف غير المصرّح بهِ لتلك المعلومات، سرقة الهويّة الإلكترونيّة) .

الطائفة الثانية: الجرائم التي يكون الكمبيوتر فيها **موضوعاً** للجريمة، مثلا (بث أو نشر أو إرسال الفيروسات والقنابل المنطقية وأحصنة طروادة [2]، والقرصنة المعلوماتية) .

الطائفة الثالثة: الجرائم التي يكون الكمبيوتر فيها **أداة** لإرتكاب جرائم تقليديّة ، مثلا كَجرائم (سرقة بيانات البطاقة الإئتمانية، نشر الصور الإباحية) .

رَأينا أن هذا التصنيف أفضل من التصنيفات السابقة كَونه لم يَعتبر الجرائم الواقعة على المكونات المادية للكمبيوتر جرائم معلوماتبة ولكنّه يُؤخذ عليه رَبطه للجرائم الإلكترونية بالكمبيوتر .

ثانيا : صور الجرائم الإلكترونية في التشريع الفلسطيني:

- **مشروع قانون العقوبات الفلسطيني لسنة 2010:** لم يرَ مشروع قانون العقوبات الفلسطيني النور بعد، فما زال بين المداولات والمناقشات في أروقَة المجلس التشريعي، وقد

---

1. رشاد خالد عمر ، **المرجع السابق**،ص35.

2. أحصنة طروادة : وهو من البرامج الخطرة على الإطلاق التي تستخدم في عملبات إختراق أجهزة الحاسبات الآلية نظرا لتمتعه بعدة مميزات تجعل منه الأقدر على عملية الإختراق دون القدرة على كشفه وتتبعه والقضاء عليه لذلك فقد اكتسب هذا البرنامج شهرة كبيرة في مجال إختراق أجهزة الحاسبات الآلية. أنظر :منير و ممدوح الجنبيهي،جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها،ص55-56.

تضمّن هذا المشروع بَاباً خاصا وهو الباب السابع لِيُعالج مَسألة الجرائم الإلكترونية، ولكن هل تضمن هذا الباب كافة أشكال الجرائم الإلكترونية ؟

أ. جرائم التنصت والإعتراض: تحدّث المشرع عن جريمة التّنصت والإعتراض الغير المشروع فَتُعتبر هذه الجريمة من جرائم الإعتداء على حُرمة الحياة الخاصة، ومثالُها تَسجيل المكالمات الهاتفية أو المحادثات الإلكترونية، فكل ما مِن شَأنه التنصت على الآخرين فهو عَمل غير مشروع ويُجرّمه القانون وكان هَدف المُشرّع من ذلك هو حماية الحقّ في حرية الإتصال وإحترام نقل البيانات دون تدخل من أحد. [1]

ب. جرائم أنظمة المعلومات ونشر الفيروسات وإستخدام الأجهزة:

يعرف الفيروس بأنه: هو عبارة عن مجموعة من التعليمات التي تَتكاثر بِمُعدّل سريع جداً وتُصيب النظام المعلوماتي بِشلل النظام .[2]

نصّ المشرع الفلسطيني في المواد (382،383) على الجرائم التي تستهدف أنظمة المعلومات والبرامج ونظم التشغيل من حيث إقتحام النظم وتعطيلها أو محو أو تخريب أو حجب أو إتلاف البيانات وكذلك نشر الفيروسات أو إساءة إستخدام الأجهزة الإلكترونية بشكل عام.[3]

1.**نصت المادة 381 من مشروع قانون العقوبات الفلسطيني لسنة 2010 على أنه** : كل من تنصت أو إعترض بدون حق بإستعمال سبل تقنية على أية معلومات غير معروضة للعموم من وإلى أو داخل نظام الحاسوب بما في ذلك الإصدارات الإلكترومغناطيسية لنظام حاسوب يحتوي على معلومات محوسبة يعاقب بالحبس لمدة لاتزيد عن 6 أشهر وبغرامة لاتتدتوز 200 دينار أردني أو بإحدى هاتين العقوبتين.

2. محمد علي العريان،**الجرائم المعلوماتية**،دار الجامعة الجديدة،2011،الإسكندرية،ص 102

3.**نصت المادة 380 من مشروع قانون العقوبات الفلسطيني 2010 على أنه** : 1-كل من إقتحم نظاما نظاما لمعلومات حاسوب خاص بالغير أو بقي فيه دون وجه مشروع يعاقب بالحبس مدة لاتزيد عن سنة وبغرامة لاتتجاوز ألف دينار أردني أو بإحدى هاتين العقوبتين،2 – واذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها تكون العقوبة الحبس وبغرامة لاتتجاوز ثلاثة الاف دينار اردني أو بإحدى هاتين العقوبتين.

ج. **التزوير المعلوماتي** :المواد رقم (385،386،387،388) ، فنصت على جرائم التزوير المعلوماتية ، وإستغلال الحاسب الآلي في عملية التزوير المعلوماتي، أو تزوير أي نظام إلكتروني بشكل غير مشروع.

ويُعرف التّزوير المعلوماتي على أنه: " تغيير الحقيقة بقصد الغشّ في مُحرّر تغييراً واقعياً على شيء، مما عدّ هذا المُحرر لإثباته ومن شأنه أن يسبّب ضرر". ويتمثل الركن المادي لهذه الجريمة من خلال النشاط الذي يمارسه الجاني لتغيير الحقيقة، ويَستخدم وسائل إلكترونية في ذلك محدثاً ضرراً يُلحق بالغير، أما الركن المعنوي فيتكون من القصد العام بِعلم الجاني بالأفعال التي إرتكبها واتجاه إرادته لإرتكابها أما القصد الخاص فهو أن يتم تغيير الحقيقة بقصد التزوير، والذي دفع فقهاء القانون الجنائي إعتبار التزوير المعلوماتي جريمة نظراً لِزيادة التّلاعب في الحواسيب العائدة للبنوك والمؤسسات المالية والتي يَنتج عنها خسائر مالية كبيرة.[1]

وأيضاً من صور الجرائم الإلكترونية في قانون العقوبات الفلسطيني **الجرائم الجنسيّة** التي يَستخدم فيها الجاني أساليب الإبتزاز الجنسي عن طريق تهديد الفتيات بنشر صُور لهنّ عَبر الإنترنت وأخطر الجرائم الجنسية هي الإستغلال الجنسي للأطفال وقد نصت المادة 389 من نفس القانون على هذه الجرائم .

والصورة الأخرى هي **الجرائم المالية**، من نفس القانون من حيث الإعتداء على الحسابات البنكية أو المصرفية أو الحصول على أرقام بطاقات الإئتمان وكل جريمة إلكترونية تهدف إلى

ونصت المادة 382 من نفس القانون على أنه : كل من قام بتخريب أو محو أو فساد أو تغيير أو حجب معلومات حاسب آلأي خاص بالغير مما أدى إلى إلحاق ضرر جسيم بهم يعاقب بالحبس وبغرامة لاتتجاوز ثلاثة الف دينار اردني أو بإحدى هاتين العقوبتين .

1.يوسف العفيفي، **الجرائم الإلكترونية في التشريع الفلسطيني**،رسالة ماجستير،تخصص قانون عام(جنائي)،إشراف الدكتور أيمن عبدالعال،الجامعة الإسلامية – غزة ، 2013،ص37.

عائد مادي أو إقتصادي للجاني ، وكذلك **جرائم سرقة البيانات والمعلومات والحقوق الفكرية والإلكترونية** حيث نص المشرع الفلسطيني عليها في المواد (390) ، مثل الكتابات والأعمال الفنية سواء الصوتية أو المرئية وسرقة البيانات والمعلومات التي تتعلق بالآخرين سواء تم سرقتها أثناء تسجيلها أو ارسالها أو تخزينها، **وفي آخر المواد** (395) نص المشرع الفلسطيني على الجرائم التي تضرّ بالآخرين سواء في أجهزتهم أو سمعتهم أو شرفهم وهي **جرائم الإتلاف والتعدي على الأشخاص** ومن أمثلتها: إتلاف الأجهزة أو اختراقها أو نشر صور فاضحة لأشخاص بهدف الإساءة لِسُمعَتِهم، ومن الجرائم التي تستهدف الأشخاص أيضاً **جَرائم التّشهير** ويتمثّل الركن المادي فيها بنشاط الجاني المتمثل في فِعل التشهير وأما الركن المعنوي فهو عِلم الجاني بالسلوك الذي إقترفَه وإتجاه إرادته نَحو إرتكاب هذا الفِعل .[1]

إن الجرائم المذكوره أعلاه هي من الجرائم الإلكترونية التي نص عليها المشرع الفلسطيني في مشروع قانون العقوبات لسنة 2010، وأَجملت أَغلب صُور الجرائم الإلكترونية التي ظهرت على الساحة الفلسطينية، وهناك جرائم موجودة بالدُّول المجاورة لم يذكرها المشرع الفلسطيني أو لم تظهر بعد وهي ليست ببعيدة وكان على المشرع أن يتفادى الفراغ التشريعي الذي من الممكن أن يحدث في المستقبل فمن هذه الجرائم: المواقع الإلكترونية التي تروّج لِلمُخدّرات أو لِلعبْ القمار أو التي تتعلق بالإتّجار بالجِنس البشري، وهذا مادَفع بالمشرع الفلسطيني إلى نص قانون خاص لِمُكافحة الجرائم الإلكترونية سنة 2018.

المبحث الثاني: أركـــان الجـــريـــمـــة الإلـــكـــتـــرونـــيـــة :

لاتختلف جريمة الإنترنت عن أي جريمة أخرى، إذ أنها تتطلب لِتحقّقها الأركان المُتفق على ضرورة توفّرها في أي جريمة لِكي تتواجد على أرض الواقع، فبالإضافة إلى ضرورة تواجُد الشّرط المبدئي في كل جريمة أي النّص الشرعي المُجرّم أو الصّفة غير المشروعة فإنه لابدّ

1.يوسف العفيفي،**المرجع السابق**،38-39.

من وجود الركنين اللّذين تتألّف منهما كل جريمة وهما: الرّكن المادي والرّكن المَعنوي ، وبالتالي سَنعرض لأركان الجريمة الإلكترونية بالتّفصيل مع العلم أنّ الركنين المادي والمعنوي هما عمودا الجريمة الإلكترونية وبِدونهما تكون الجريمة مُستحيلة الحدوث.

المطلب الأول : الركن الشرعي في الجريمة الإلكترونية :

الفرع الأول : التعريف بالركن الشرعي للجريمة الإلكترونية :

النص الشرعي هو نص والتجريم الذي يضفي على الفعل أو المتناع الصفة غير المشروعة وقد اختلف الفقه ولازال حول طبيعته،فهناك من يعتبره ركنا من أركان الجريمة[1]. إلى جانب الركن المادي والمعنوي، وهناك من يعتبره صفة غير مشروعة تقترن بالسلوك فتجعله مجرما ومعاقب عليه [2]، ويتجسد هذا النص من خلال مبدأ شهير وهو "لاجَريمة ولاعُقوبة ولا تَدابير أمن إلا بِقانون" أي مايعرف بمبدأ شرعية الجرائم والعقوبات، وهو مبدأ ذو طابع عالمي إلا أنّ

1.ويستندون ذلك الوجود إلى المبررات التالية: 1. تبدو دراسة عدم مشروعية الفعل أو نص التجريم كركن للجريمة أمر يستجيب لإعتبارات الوضوح والاتساق النظري. 2. اذا كان نص التجريم هو خالق للجريمة فانه ليس من المنطقي اعتبار الخالق شقا من المخلوق فربما كان هذا القول مقبولا بصدد تحليل فكرة الجريمة في ذاتها، بيد ان فكرة الجريمة ليست غاية منهجية في ذاتها. 3. ان فكرة عدم مشروعية الفعل أو نص التجريم لاتستعصي على التحليل بوصفها ركنا شرعيا للجريمة شأنها شأن الركنيين المادي والمعنوي فلهذا الركن عناصره وشروطه وضوابطه. للمزيد أنظر: سليمان عبد المنعم ومحمد أبو عامر ،القسم العام من قانون العقوبات،دار الجامعة الجديدة،الإسكندرية،2002،ص.141

2. ويستند في عدم التسليم للركن الشرعي الى: أن نص التجريم ينشأ الجريمة فكيف يمكن لنا اعتبار المنشأ ركنا فيما أنشأ

وأيضا لو كان نص التجريم ركنا في الجريمة لترتب علىه إلغاء المقنن له أن تزول الجريمة بدورها بصفتها كائنا قانونيا، ولو اعتبر أن نص التجريم ركنا في الجريمة لترتب على هذا الشرط إحاطة علم الجاني بهذا النص قي الجرائم العمدية وهذا مايتناقض مع مبدأ افتراض العلم بالنص الجنائي ،للمزيد أنظر: عبد الفتاح الصيفي، الاحكام العامة للنظام الجنائي في الشريعة والقانون ،دار النهضة العربية،القاهرة،2004، ص63.

الدُّول اعتادَت على الإعتراف بِه في النّطاق المحلّي لاغير، والإشكال المطروح هنا مامحلّ الجريمة الإلكترونية من مبدأ شرعية الجرائم والعقوبات ؟ [1]

لقد أثار الفقه المعاصر موضوعاً على جانب كثير من الأهمية يتعلّق بتفاعُل نُظم التقنية الحديثة مع القانون الجنائي وتأثير ذلك على مبدأ الشرعية لاسِيّما حال إنعدام وجود نصوص قانونية تحكُم مظاهر التّعامل مع ذلك التقنية .

وتُعتبر الجرائم الإلكترونية التي أفرزتها تقنية الإنترنت، أحد التحديات الكبرى التي تقف أمام تطبيقات القانون الجنائي والذي يكون في كثير من الأحيان محلاً لِقُصور بَيّن في تنظيم تلك الجرائم المستحدثة، وهذا مايسهّل للكثير من المجرمين إرتكابها والإفلات من العقاب، ولعلّ القوانين الأمريكية والفرنسية والإنجليزية أحسن مثال على ذلك فَكم من الإنتهاكات حدثت عبر جرائم الإنترنت ونتيجة لِعدم وجود نصوص تجرّم وتعاقب، أَفلت الجُناة من العقاب ولكن هذا لايعني أن مبدأ شرعية الجرائم والعقوبات لاوجود له فيما يخص جرائم الانترنت، فلو قلنا ذلك فإننا نَنفي وجود تلك الجرائم في حد ذاتها، اذ وبالرّغم من حداثتها وإعتمادها على التقنية ولاسيّما في إطار تهديدها للألفية الثالثة فإن التشريعات المقارنة قد تصدي لهذه الأخيرة بتجريمِه لصور الإعتداء الناجمة عن المعالجة الآلية للبيانات والتي تنطبق بِلا شَك على صُور الإعتداء على شبكة الانترنت حيث أصدر نصوصا قانونية عدة تكفَل الحماية الجنائية للحاسب الآلي وشبكاته وخصوصاً الإنترنت فعلى سبيل المثال: نجد أن المشرع الفرنسي قد جرّم في المادة 323-1 الى المادة 323-7 من قانون العقوبات الجديد لسنة 2003 صور الإعتداء الناجمة عن المعالجة الآلية للبيانات مما يَسمح بإنطباقه على الأفعال التي تقع على الإنترنت (كمحل للإعتداء) أو بواسطته (كوسيلة للإعتداء).

1. نبيلة هروال،**المرجع السابق**،ص41-42.

وفي نفس السياق نجد أن المشرع الأمريكي قد أصدر العديد من القواعد القانونية لمواجهة الجرائم المرتكبة عبر الإنترنت ومنها : قانون آداب الإتصالات عام 1996، والذي جرّم من خلاله أفعال القذف والسبّ عبر شبكة الإنترنت وكذا أفعال التعرض للأخلاق والآداب العامة عبر تلك الشبكة كما كفل الحماية الجنائية للأطفال ضدّ الإستغلال الجنسي لهم بقانون عام 1998 المعروف ب: "قانون حماية الأطفال على الخط" وفي إطار حماية حُرمة الحياة الخاصة من الإعتداء عليها، وأصدر المشرع الأمريكي "قانون الخصوصية عام 1974"، وقانون "خصوصية االإتصالات الإلكترونية عام 1998"، كما قام بإصدار " قانون منع القرصنة الإلكترونية عام 1997". وقد سار المشرع الإنجليزي على نفس المِنوال، فَبادر إلى مواجهة المشكلات القانونية الناجمة عن تطور التقنيات المعلوماتية، وذلك بإفراده حماية خاصّة للأطفال من الإستغلال الجنسي بقانون " حماية الطّفل لعام 1978".

أما على مستوى الدول العربية فإنه لم تقم أغلبية الدول العربية بسنّ قوانين خاصة بجرائم الإنترنت ماعدا البعض منها مثل مصر والجزائر، كمصر مثلاً والتي تناولتها في قانون الإتصالات لعام 2003 وكذا من خلال " قوانين الملكية الفكرية " لسنة 2002 .[1]

الفرع الثاني :الركن الشرعي للجريمة الإلكترونية بالنسبة للمشرع الجزائري : فإنه أورد قسماً خاصّاً للمساس بأنظمة المعالجة الآلية للمعطيات فيه وهو **القسم السابع مكرر بمحتوى المادة 394 مكرر الى 394 مكرر 7** ، بمقتضى القانون 04-15 المؤرخ في 2004/11/10، ولم يكتفي المشرع الجزائري بذلك بل فَرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23/06 المؤرخ في 2006/12/20 والذي مسّ المادة 303 وإقراره بالمادة 303 مكرر الى 303 مكرر 03، وهذا تصدياً للإستخدام السيءْ لوسائل التّكنولوجيا الحَديثة .

1.نبيلة هروال ، **المرجع السابق** ، ص44-45.

الفرع الثالث : الركن الشرعي بالنسبة للمشرع الفلسطيني : فإنه قد وضع قانون خاص بالجرائم الإلكترونية وهو **قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية**، وقد إحتوى على **52 مادة** يجرم المشرع الفلسطيني من خلال بعضها ويعاقب مرتكبي الجرائم الإلكترونية، إلى أن وَضع المشرع وسنّ قانون جديد وهو **قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته**[1]، والذي يحتوي على **57 مادة**، وبالتالي فإن معالجة هذه القضايا الإلكترونية نجد أن المشرع وضع نصوصاً خاصة لتجريمها لأن العقاب على الجريمة الإلكترونية لابدّ من وجود نص تشريعي بذلك **طبقاً للمادة الأولى من مشروع قانون العقوبات الفلسطيني لعام 2010 والتي تنص على: " لاجريمة ولاعقوبة إلا بنص في القانون، ولاعقاب إلا على الأفعال اللاحقة لنفاذ القانون الذي ينص عليها** " ، والمشرع الفلسطيني خَطى خُطوات التشريعات الأخرى في مكافحة هذه الجريمة وملاحقة مرتكبيها، حيث أنه يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكمبيوتر والإنترنت عن طريق إسقاط نُصوص قوانين العقوبات السارية في فلسطين مثل: نُصوص الإبتزاز والنّصب والإتلاف والتزييف والسّرقة وتقليد الأختام والتزوير وخيانة الأمانة والسّب والقَذف والتشهير وإفشاء الأسرار والحضّ على الفُجور، بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكمبيوتر أو شبكة الإنترنت إلا أن المُجرم أحياناً يَفلُت من العقاب لعدم وجود نص تشريعي مناسب للتجريم وبالتالي تدقّ الحاجة الى التّجريم الإلكتروني الخاص بهذه الجرائم، ومن الأمثلة التي نص عليها المشرع الفلسطيني ووضع لها تنظيم خاص ويعاقب علبها عند إتيان هذا الفعل الجرمي: **قانون الإتصالات السلكية واللاسلكية الفلسطيني رقم 3 لسنة 1996**، وعالجها وسنّها من خلال عرض الجرائم والعقوبات المقررة لها في المواد من (86-100) ومن ضمنها المواد (93-3، 92-2، 91- أ- ب ،90-أ) علما أن هذا القانون يعتبر من القوانين الحديثة نسبياً في مجال

1. معظم التعديلات جاءت بتخفيض العقوبات المالية والحبس بما ينسجم مع الواقع الفلسطيني ، كما جرى تعديل واعادة صياغة أخرى اما بالحذف أو الإضافة .

تكنولوجيا الإتصالات كونه يتعلق بمعالجة الجوانب الفنية لعملية الإتصالات ذاتها وكذلك معالجة الإطار الرّقابي وضبط المخالفات والجرائم التي ترتكب في إطار الإساءة لتقنية الإتصالات، وأيضا **مشروع قانون العقوبات الفلسطيني** الذي يتعرَض وبشكل مباشر لجرائم الحاسوب والإنترنت في الباب الخامس منه في المواد (379-396) وجاءت هذه النُّصوص لتلبّي الحد الأدنى من مُتطلبات التجريم في مُواجهة الجرائم الإلكترونية ذلك أن الأمر لايَخلو من النّقد على عدم إشتماله على بعض صور الجرائم الإلكترونية، مثل الإطلاع غير المشروع على المعلومات وكذلك جَسامة العقوبات وإيرادها على سبيل التخيير بين الحبس والغرامة والذي يوسّع حدود السلطة التقديرية للقاضي، وكذلك من مُحاولات المشرع الفلسطيني لمواجهة الجرائم الإلكترونية **مشروع قانون الإنترنت والمعلوماتية لسنة 2002** والذي يتكون من تسعة فصول ويضم **35 مادة** وأنه استكمالاً لما بدأه المشرع في قانون الإتصالات السلكية واللّاسلكية لعام 1996. وبهذا نرى أن المشرع الفلسطيني قد أقرّ في نصوصه الجرائم الإلكترونية [1] .

ولسدّ المُعضلة القانونية والفَراغ القانوني الذي كان في السابق نتيجة عدم وجود قانون خاص ينظم الجريمة الإلكترونية، رغم أن هذا القانون **– قانون الجرائم الإلكترونية لسنة 2017 –** الذي حُضّر بعيداً عن وسائل الإعلام والمؤسسات الحقوقية ومؤسسات المجتمع المدني إلا أنه سُرّب بعد أيام من المصادقة عليه وأكد الخبراء في قانون الإعلام الإلكتروني وحقوقيون أن القانون بشكلِه الحالي مسّ خَطير بِحرية الرأي وحرية الإعلام وحقّ الحُصول على المعلومات وأن هذا القانون يتضمن مواد عدّة تَنال من حرية الرأي والتعبير والحق في الخصوصية وضم مصطلحات فضفاضة مثل: **المواد (16،20،51)** – والتي أُلغيت فيما بعد – من القانون نفسه وماحصل فإنه يخالف التشريع وفقاً للقواعد والإجراءات المنصوص عليها في القانون الأساسي الفلسطيني وفي إجراء المجلس التشريعي، فيجب إعلاء الصوت

1. عبد اللطيف ربايعة، **الجرائم الإلكترونية** ، بحث مقدم الى المؤتمر الأول للجرائم الإلكترونية في فلسطين والمنعقد في جامعة النجاح الوطنية – نابلس ، 2016 .

للاحتجاج على مشروع، القانون إعادة النقاش فيه بحيث تنسجم مع القواعد والمبادىء الدستورية واحترام الإلتزامات التي قطعتها السلطة الفلسطينية عند توقيعها على بعض المواثيق الدولية كإتفاقية العهد الدولي لحقوق الإنسان، حتى لايبقى هذا القانون مِقْصَلَةٌ يقع تَحتها الفلسطينيّون[1].

المطلب الثاني : الركن المادي للجريمة الإلكترونية : –

الفرع الأول : الركن المادي للجريمة الإلكترونية :

يعد السلوك هو القاسم المشترك بين جميع الجرائم، وهو العُنصر الأول من عناصر الركن المادي للجريمة ويجب أن يكون الموضوع الذي يقع عليه السلوك محل حماية من قبل المشرع وأن يكون مجرّم بنص مِن القانون .

وذلك أن مفهوم أو مَناط التجريم ينصبّ على نظام إلكتروني يُساء إستعمالَهُ أو يتم إقتحامهُ على نحو غير مشروع، بما يكون لذلك الإستعمال أو الإقتحام من أثر مادي ملموس يظهر إما في صورة تَدمير للمعلومات وهو مايُثير امكانية الإتلاف العمدي لِلمَنقولات أو السّرقة وذلك عن طريق إساءة إستعمال بطاقات الإئتمانْ أو يُثير شُبهة التزوير عن طريق التّلاعب في بيانات الحاسب الآلي [2] . **إذاً فالركن المادي " فهو يتمثل في سلوك إرادي تترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية، ففيما يتمثل هذا الركن المادي في الجرائم الإلكترونية "** .

من خلال استقرائنا للتعريف السابق يتبيّن لنا أن الركن المادي يتكون من **سلوك مادي إرادي، ونتيجة إجرامية ، ورابطة سببية .**

---

1 العربي الجديد **AL araby. Co. Uk** ، تاريخ الإطلاع على الموقع : 2019/4/27.

2. عبدالله دغش العجمي،**المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة)**،رسالة ماجستير– تخصص قانون عام،إشراف الدكتور أحمد اللوزي، جامعة الشرق الأوسط – الكويت، 2014،ص26–27.

1 . السلوك الإجرامي: يعتبر السلوك المادي عبر الإنترنت محلاً لجُملة من التساؤلات، لاسيّما فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، وهو يختلف عما هو الحال في العالم المادي ذلك لأن ارتكاب الجريمة عبر الانترنت تحتاج بالضرورة إلى منطق تقني، أي أنها تتم عبر الإنترنت أو بإستخدام المعالجة الآلية للبيانات، كما أنها تحتاج إلى ممارسة نشاط تقني (أي توافر القدر اللازم العلم والإدراك لإستخدام الإنترنت والحاسوب) . ومن أمثلة السلوك المادي في الجريمة عبر الإنترنت: المصرفي الذي يَنوي سرقة مبالغ مالية من المصرف الذي يعمل فيه بإستحدام الإنترنت وذلك بممارسة نشاط التعامل مع الحاسوب والولوج إلى الإنترنت ثم الدخول على شبكة المصرف عبر مزوّدات مجهولة يمكن الإستعانة من خلالها ببرمجيات إختراق موضوعة على مواقع هَكرة يتم تجديدها بإستمرار، ففي هذا المثال فإن المصرفي يُمارس النشاط المادي للإختلاس عن طريق الحاسوب أو الإنترنت .

2. النتيجة الإجرامية: يُعد هذا العنصر أحد عناصر الركن المادي وتُثير مَسألة النتيجة الإجرامية مشاكل عدّة أهمُّها تحديد هل جريمة الإنترنت هي جريمة مرتكبة سلوكاً ونتيجةً ؟

3. علاقة السببية: أيضاً هي عنصر من عناصر الركن المادي في الجريمة ويجب لقيام الجريمة الإلكترونية أن تكون هناك رابطة مادية مابين السلوك المادي والنتيجة الإجرامية، فمثلا: يجب لتحقق انتهاك الحق في الخصوصية عبر الإنترنت أن يكون هناك دخول على الإنترنت باستخدام الحاسوب واختراق الخوادم في مسارها، ثم التعدي على خصوصية موقع ما. [1]

1.نبيلة هروال ، **المرجع السابق** ، ص 46-47-48.

الفرع الثاني : الركن المادي وتطبيقاته على الجريمة الإلكترونية في التشريع الجزائري في قانون العقوبات الجزائري فهي كما يلي :

إن الركن المادي للجريمة الإلكترونية يقوم على صورتين أساسيتين: الصورة الأولى متمثلة في الإعتداء على نظام المعالجة الآلية للمعطيات وهذه الأخيرة تحتوي على نوعين من الإعتداء **والنوع الأول** : هو الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وتنطوي تحت هذا النوع ثلاثة أفعال: فعل الدخول والبقاء والعرقلة أو التعطيل والإفساد، **أما النوع الثاني:** متمثل في الإعتداء العمدي على المعطيات وتندرج تحت هذا النوع كذلك ثلاثة أفعال وهي فعل الإدخال والمحو والتعديل، أما الصورة الثانية متمثلة في الإعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي[1]. وبالتالي سيتم دراسة هذا الركن المادي في التشريع الجزائري حسب ماذكر أعلاه .

أولا : الإعتداءات على أنظمة المعالجة الآلية للمعطيات : (عمدية في الدخول والبقاء)

سنبدأ بدراسة الدخول والبقاء غير المشروع في نظام المعالجة غير الآلية ثم نتطرق إلى الإعتداء العمدي على نظام المعالجة الآلية .

1. النوع الأول: الدخول أوالبقاء غير المشروع في نظام المعالجة الآلية للمعطيات : نصت المادة 394 مكرر من قانون العقوبات الجزائري على أنه : " يعاقب بالحبس من ثلاث أشهر إلى سنة، وبغرامة مالية من 50000 **إلى** 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك .

1. علي عبد القادر القهوجي،**الحماية الجنائية لبرامج الحاسب الآلي** ، دار الجامعية للطباعة والنشر،بيروت،1999،ص35.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 دج إلى 150000دج " .

نصت المادة 1/323 من قانون العقوبا ت الفرنسي على أنه " فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه، يعاقب بالحبس لمدة سنة وبغرامة مالية 60000 يورو " فاذا نتج عن الدخول أو البقاء سواء محو أو تغيير في النظام فإن العقوبة تصبح الحبس لمدة سنتين والغرامة تصل إلى 120000 يورو" . [1]

* ونستخلص من النصين السابقين وجود صورتين لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات **الصورة الأولى** تتمثل: في الصورة العادية: وهي مجرد الدخول أو البقاء غير المشروعين في النظام ، **والصورة الثانية** تتمثل في: هي الصورة المشددة تتحقق بتوافر ظروف مشددة وهي:

1) حذف أو تغيير نظام المنظومة بعد الدخول أو البقاء غير المشروعين .

2) تخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين.

1. الصورة العادية: يتمثل النشاط الإجرامي في هذه الصورة في الأفعال الآتية :

أ. فعل الدخول: يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المحزنة داخل النظام ودون علم ورضاء صاحبها، لأن هذا النظام لايسمح للدخول فيه إلا لأشخاص معيّنين أو يسمح الدخول لكن مقابل نَفقات . أما بالنسبة للتشريعات المختلفة فقد تَباين موقفها تُجاه تَحديد محل الركن المادي في جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات وبذلك يمكن أن نميز بين ثلاث صور وهي: الصورة الأولى تتمثل في المعلومات ذاتها والثانية

1.المادة 1/323 قانون رقم 97 – 1159 المؤرخ في 19 ديسمبر 1997 والمتضمن قانون العقوبات الفرنسي .

في أنظمة المعالجة الآلية للمعطيات التي تتداخل فيما بينها من خلال شبكة الإتصال، والثالثة شبكات المعلومات، فهذا التباين والإختلاف حول محل الركن المادي لهذه الجريمة أورد ثلاث إتجاهات هي :

الإتجاه الأول (الموسع): يجمع بين الصور الثلاث ويتخذها جميعها محل للجريمة وهي المعلومات الواسعة للمعالجة الآلية للمعطيات وشبكات المعلومات وتبنى هذا الإتجاه المشرع الفرنسي والجزائري .

الإتجاه الثاني: استبعد شبكات المعلومات من نطاق التجريم، ويتبنى هذا الإتجاه المشرع الإنجليزي .

الإتجاه الثالث: جرّم فعل الدخول عبر الإنترنت، وتبّناه المُشرع السّويسْري .

إن جريمة الدخول غير المصرح إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لاتشترط تحقق الجريمة [1]، ويرتكب فعل الدخول بأي وسيلة كانت لأن المشرع الجزائري لم يحددها، ويستوي أن يتم الدخول بطريق مباشر حيث يستطيع الجاني الوصول إلى المعلومات المخزنة لدى الأنظمة المعالجة الآلية بإستخدام الشاشو والإطلاع على ماهو مكتوب عليه وبإستخدام آلة الطابعة يستخرج البرامج الموجود داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالإلتقاط المعلوماتي.

ب. فعل البـقاء : معنى البقاء : هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من لهُ الحق في السيطرة على هذا النظام، ويتحقق هذا البقاء غير المشروع عند دخول شخص في نظام بتصريح ولكن تجاوز المدة المسموح له بها (بالبقاء داخل النظام)، أو أن يقوم

1. نائلة قورة، **جرائم الحاسب الآلي الإقتصادية**،ط1،منشورات الحلبي الحقوقية،2005 ،ص323.

بطباعة نسخة من المعلومات في حين سمح له بالرؤية فقط فهنا تقوم جريمة البقاء غير المشروع في نظام المعالجة الآلأية للمعطيات .

يجتمع فعل البقاء مع الدخول غير المشروع للنظام مثل أن لايكون للجاني حق الدخول ويدخل عن طريق الغش المعلوماتي، حيث نصت المادة 394 مكرر من قانون العقوبات الجزائري على فعل البقاء غير المشروع، على غِرار المُشرع الفرنسي في المادة 1/323 من قانون العقوبات الفرنسي جيث يصعب تطبيق النص في قرائته الأولى لأنه فقط ينصّ على الدُّخول، غير مُرفق الجزء الخاص بالبقاء غير المشروع.[1]

جرّمتْ محكمة الإستئناف في باريس في حكمها في 1994/4/5 البقاء غير المشروع سواء تم بطريقة الخطأ أو بطريقة مشروعة داخل نظام المعالجة الآلية للمعطيات إلا أنه إكتسب بعدَ ذلك صفة عدم المشروعية [2].

2. الصورة المشددة : نصت المادة 394 مكرر فقرة 2،3 من قانون العقوبات الجزائري على طروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل للمعطيات التي يحتويها النظام وإما عدم صلاجية النظام لأداء وظائف النتيجة، وإن ظرف التشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية لكي نقول أن الشرط متوافر. وفي المادة 394 مكرر من الفقرة الأخيرة شدد المشرع عقوبة المحو وتعديل المعطيات كل واحد على حدى تخريب نظام اشتغال المنظمة من جهة أخرى، وعقوبة هذه الأخيرة أشد لأن عقوبة المَحو أو التَّغير هي ضِعف عقوبة الدخول والبقاء غير المشروعين

1. آمال قارة،**الحماية الجزائية المعلوماتية في التشريع الجزائري**،ط2، دار هومة،،الجزائر،2007،ص110.

2. نائلة قورة، **المرجع السابق**،ص347.

أما بالنسبة للمشرع الفرنسي فجمع بين الطرفين في فقرة واحدة وفي عقوبة واحدة في المادة 1/323 من قانون العقوبات الفرنسي .

2. الإعتداءات العمدية على نظام المعالجة الآلية، (الإعتداء على نظام المعالجة ولكن عمدية):

نصت على هذه الصورة المادتان (5 ، 8) من الإتفاقية الدولية للإجرام المعلوماتي .

أما بالنسبة للمشرع الجزائري لم يُورد نصّاً خاصاً بالإعتداءْ العَمدي على سَير النِّظام واكْتفى بالنص على الإعتداء العمدي على المعطيات الموجودة داخل النظام ،وهذا راجع إلى تفسير أن الإعتداء على المعطيات قد يُؤثر على صَلاحية النظام ووظائفه. [1]

1. التعطيل أو العرقلة: إن المشرع لم يشترط الوسيلة التي يتم بها فعل التعطيل قد تكون وسيلة مادية أو معنوية سواء إقترنت الوسيلة المادية بعنف أم لا كَكَسرْ الأجهزة المادية للنظام أو تَحطيم الإسطوانة وتكون مَعنوية إذا وقعت على الكيانات المَنطقية للنظام مثل البَرامج والمعطيات: كإدخال برنامج فيروسي .

2. الإفساد: يقصد بفعل الإفساد وهو كل فعل يؤدي إلى جعل نظام المعلجة الآلية للمعطيات غير صالح للإستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها [2].

1.آمال قارة،**المرجع السابق**،ص190.

2. بعرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري**،مذكرة مكملة لنيل شهادة الماستر – تخصص قانون جنائي،اشراف الأستاذ بنشوري الصالح،جامعة محمد خيضر – بسكرة،2016،ص55.

ثانيا : الإعتداءات العمدية على المعطيات :نصت على الإعتداءات العمدية على المعلومات المواد (3،4،8) من الإتفاقية الدولية للإجرام المعلوماتي[1].

ونصت المادة 394 مكرر2 من قانون العقوبات الجزائري على الإعتداءات العمدية بنصها " يعاقب بالحبس من شهرين الى 3 سنوات وبغرامة من 1000000 إلى 5000000 دج كل من يقوم عمدا أو عن طريق الغش المعلوماتي بما يأتي:

1. تَصميم أو بَحث أو تَجميع أو تَوفير أو نَشر أو الإتّجار في مُعطيات مخزّنة أو مُعالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

2.حِيازة أو إنشاء أو نشر أو إستعمال لأي غرض كان المعطيات المُتحصّل عليها من إحدى الجرائم المنصوص عليها في هذا القسم " .

النشاط الإجرامي يتجسد في صورتين :

الصورة الأولى: الإعتداءات العمدية على المعطيات الموجودة :

وتتجسد هذه المعطيات في ثلاثة أفعال: الإدخال ، المحو ، التعديل .

ولتوافر الركن المادي في هذه الجريمة لابد من توافر الأفعال الثلاثة، ولايشترط إجتماعها، يكفي إتيان واحد منها وهي: **أ. الإدخـــال** : يقصد به: هو إضافة معطيات جديدة على الدَّعامة الخاصة سواء كانت خيالية، أم كانت يوجد عليها مُعطيات من قبل ونكون أمام فعل الإدخال

1.آمال قارة،**المرجع السابق**،ص120.

في حالة الإستحدام التعسفي لبطاقات السحب و الإئتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير.[1]

ب. فعل المحو: هو إزالة جزء من المعطيات المسجلة داخل النظام وتحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات في ذاكرة مختلفة .

ج. فعل التعديل: هو تغيير المعطيات الموجودة داخل النظام وإستبدالها بمعطيات أخرى ويتحقق ذلك عن طريق برامج تتلاعب بالمعطيات سواء بالمحو الكلي أو جزئي وهي برامج الفيروسات وهي مختلفة الأنواع والأشكال [2] .

الصورة الثانية: المساس العمدي بالمعطيات خارج النظام :

نصّ المشرع الجزائري على صورتين لِلمساس العمدي بالمُعطيات خارج النظام :

الصورة الأولى: تتعلق بحماية المعطيات من إستعمالها في الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات .

الصورة الثانية: تتعلق بحماية المعطيات المتحصل عليها من هذه الإعتداءات .

وذلك في نص المادة 394 مكرر 2 من قانون العقوبات الجزائري، المشار إليه سابقا .

حيث يتبين لنا من خلال هذا النص أن هناك فرق بين الصورتين المنصوص عليهما في المادة السابقة،(394 مكرر 2)، حيث أن الصورة الأولى تكون فيها المعطيات وسيلة لإرتكاب هذه الإعتداءات .

1. آمال قارة،**المرجع السابق**،ص121.

2. بعرة سعيدة،**المرجع السابق**،ص57.

أما الصورة الثانية فتكون المعطيات هي المحصلة أو نتيجة لإرتكاب الإعتداءات الماسة بالأنظمة والحماية التشريعية في هذه الصورة تهدف إلى الوقاية من إرتكاب جريمة أخرى تتمثل في حيازة أو إفشاء أو نشر أو إستعمال هذه المعطيات المُتحصل عليها من هذه الإعتداءات[1].

ثالثا: الإعتداءات على منتوجات الإعلام الآلي (التزوير المعلوماتي) :

إن الإعتداءعلى منتوجات الإعلام الآلي هو الفعل الثني لتحقق الركن المادي للجريمة الإلكترونية، فيعد هذا الفعل من أخطر صور الغش المعلوماتي نظراً لما يتمتع به الحَاسبْ الآلي من خطورة [2] .

وتجدر الإشارة إلى أن المشرع الجزائري إقتدى بالمشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير ولكن الفرق يكمُن في أن نصوص قانون العقوبات الجزائري الخاصة بالتزوير الذي يَرد على محرّر لذلك لايمكن الإقتِداء بالمشرع الفرنسي الذي يجعل موضوع التزوير دعامة مادية، ولهذا الإختلاف لابد من تعديل نصوص التزوير التقليدية في قانون العقوبات الجزائري الخاصة بالتزوير في المواد من (214- 229) .

- **مدى خضوع منتوجات الإعلام الآلي لنصوص التزوير :**

هل يمكن تطبيق نصوص التزوير في قانون العقوبات الجزائري على الإعتداءات الماسة بمنتوجات الإعلام الآلي ؟ وللإجابة على هذا الإشكال لابد للتطرق إلى مايلي :

- مدى إنطباق وصف المحرر على منتوجات الإعلام الآلي :

أن مفهوم المحرر في نصوصه التقليدية يختلف عن مفهومه في مجال المعالجة الآلية للمعطيات لأنه يشترط أن يكون شكلا كتابيا وأن يكون منسوباً لشخص معين، وأن يحدث

1. بعرة سعيدة ، **المرجع السابق** ،ص57.

2.آمال قارة ،**المرجع السابق**،ص133.

المحرر آثاراً قانونية فلذلِك لايُمكن إسقاط معنى المحرر التقليدي على المُعالجة الآلية للمعطيات وذلك لعدم توفر شرط الكتابة فجريمة التزوير عُنصر قيامها الكتابة وأي تغيير في الوعاء المعلوماتي لايعتبر تزوير لإستيفاء هذا الشرط [1].

ومن بين التشريعات التي واجهت القصور في النصوص التقليدية إلى إستحداث نصوص تجريمية جديدة أو إدخال تعديلات من أجل المعاقبة على جريمة التزوير هو القانون الفرنسي الذي إستحدث نصّاً خاصّاً بالتّزوير المَعلوماتي من قانون العقوبات، وذلك بموجب تعديل عام 1988، غير أنه تراجَع عن ذلك بموجب تعديل عام 1994، وألغى النص الخاص بالتزوير المعلوماتي وأخضعه للنصوص التقليدية[2] .

- **مدى خضوع منتوجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير :**

تقوم جريمة التزوير على فعل التغيير الحقيقة القانونية السببية وليست الحقيقة الواقعية المطلقة، بمعنى إستبدالها بما يخالفها وإذا إنتفى هذا التغيير إنتفى هذا التزوير معه، ويقع فعل التغيير الحقيقة من خلال طرق التزوير المادية والمعنوية .

ونَستخلص أن المشرع الجزائري رَغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام الإلكتروني وذلك بتجريم الإعتداءات الواردة على منتوجات الإعلام الآلي، وبالتالي لم يتبنى الإتجاه الذي تبنته التشريعات التي عملت على توسيع المحرر ليشمل كافة صور التزوير الحديث.

1. آمال قارة،**المرجع نفسه**،ص136-137.

2. بعرة سعيدة ،**المرجع السابق**،ص59.

الفرع الثالث : الركن المادي وتطبيقاته على الجريمة الإلكترونية في التشريع الفلسطيني في قانون العقوبات الفلسطيني :

سنعرض التعريفات الخاصة بذلك ثم نستعين بالأمثلة على الجرائم الإلكترونية مبينين الركن المادي فيها.

نص المشرع الفلسطيني في الجزء الثاني من المادة الأولى من قانون العقوبات الفلسطيني على أن " ... ولا عقاب إلا على الأفعال اللاحقة لنفاذ القانون " . ويجب أن يترتب على هذا السلوك نتيجة إجرامية وهو العنصر الثاني للركن المادي، للجريمة وهو الأثر الذي يتركه السلوك الإجرامي سواء كان فعلاً أم تركاً في العالم الخارجي وذلك طبقاً للإتجاه المادي، أما الإتجاه القانوني فهو الضّرر الذي يُصيب المصلحة التي يحميها الشارع، أما العنصر الثالث فهو علاقة السببية بين السّلوك سواء كان فعل أم امتناع وبين النتيجة الإجرامية، وبمعنى آخر لولا السلوك فعلاً أم إمتناعاً ماكانت لتحدث النتيجة الإجرامية. أما المشرع الفلسطيني فقد إكتفى بالسلوك أو النشاط الإجرامي فقط ليتحقق الركن المادي للجريمة دون النظر إلى النتيجة الإجرامية وعلاقة السببية فيكفي أن يباشر المُجرم سلوكه الإجرامي للقول بأن الركن المادي للجريمة إكتمل .

السلوك المادي (تشريع فلسطيني) :

من أهم مايميز الجرائم الإلكترونية بشكل عام هو وجود حاسب آلي، فبدون الحاسب الآلي لايمكننا تصور جريمة إلكترونية وأن استخدام الحاسوب والإنترنت كأصل عام مشروع، ولكن الخلاف يثور حين تستخدم هذه الوسائل الحديثة لغايات غير مشروعة فالسلوك هنا يتطلب وجود بيئة رقمية من حيث الجهاز الإلكتروني للجرائم الإلكترونية بشكل عام والإنترنت لجرائم الإنترنت بشكل خاص، ويتخذ السلوك هنا صورتين: الأولى وهي السلوك الإيجابي والذي يتطلب مجهود بدني يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف

الإعتداء على المصلحة ومثال ذلك في الجرائم الإلكترونية: كل الأفعال التي يرتكبها الحاني في التلاعب ببرامج وبيانات الحاسب الآلي بهدف إتلاف البيانات أو سرقتها أو نسخها، أما الصورة الثانية وهي: السلوك السلبي وهو الإمتناع عن إتيان أمر يوجبه المشرع أي الإمتناع عن قاعدة فرضها المشرع ومثال ذلك: إمتناع موظف أمن عن حِماية بيانات ومعلومات الشركة التي يعمل بها، أو عدم الإبلاغ عن جريمة للحفاظ على حقوق الغير.

النتيجة الإجرامية (تشريع فلسطيني) :

وهو عبارة عن الضرر الذي نتج هن السلوك الإجرامي سواء كان فعلاً أم تركاً، وهو الأثر الخارجي الذي يتولّد عن السلوك ويحدث تغييراً يعتد به القانون ومثال ذلك: الطبيب المعالج الذي يدخل إلى قاعدة بيانات المستشفى عن طريق الإنترنت من منزله أو مكان آخر ثم يقوم بتغيير معدّل دواء لأحد المرضى بهدف قَتله فإذا ماتَ المريض تحقّقت النتيجة الإجرامية لسلوكْ الطَّبيب والذي يكون لديهِ العلم الكافي لإرتكابه الفعل الإجرامي .

علاقة السببية (تشريع فلسطيني) :

يقصد بعلاقة السببية أن السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية ، ولولا هذا السلوك ماكانت لتحدث النتيجة الإجرامية، وتبرز أهميتها من حيث أنها من العناصر الأساسية للركن المادي وتحققها شرطاً جوهرياً من شروط المسؤولية الجزائية ولكي تكتمل هذه العلاقة السببية في جريمة التعدي على الحق في الخصوصية، يجب أن يكون هناك إتصال بالإنترنت من خلال جهاز إلكتروني ومن ثم إختراق جهاز ما أو موقع ما للوصول إلى بياناته الخاصة وبعدها يتم نشر هذه البيانات [1] .

1. يوسف العفيفي ،**المرجع السابق** ، ص51-52-53 .

تطبيق من بعض المواد في قانون العقوبات الفلسطيني للركن المادي :

1. جريمة الدخول غير المشروع : من أمثلة جرائم الإختراق التي تتعلق بأنظمة المعلومات والسبكات جرائم تدمير المواقع واختراق المواقع الرسمية واختراق الأجهزة الشخصية، واختراق البريد الإلكتروني للآخرين أو الإستيلاء عليه، وجميع هذه الجرائم تبدأ بإنتهاك خصوصية الشخص وهذا سببا كافيا لتجريمها فضلا عن إلحاق الضرر المادي والمعنوي بالمجني عليه، ونص مشروع قانون العقوبات الفلسطيني لعام 2010 على جريمة الدخول غير المشروع إلى نظام إلكتروني أو البقاء فيه بوجه غير مشروع وعاقب عليها بالحبس مدة سنة والغرامة 1000 دينار أردني، وأيضا إذا ترتب على هذا الدّخول التّدمير والإتلاف فتكون العُقوبة مشدّدة بالحَبس وغرامة لاتتجاوز 3000 دينار أردني، ويتمثل الركن المادي هنا بفعل الدخول الذي يطلق عليه الدخول المَنطقي، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناته المنطقية كما ويجب أن يكون الموقع الذي تم إختراقه غير مُتاح للجمهور ولايمكن الدخول إلا لأشخاص معينين .

نرى أن المشرع الفلسطيني عاقب على جريمة الدخول غير المشروع العمدي في المادة 2-1/380، ووضع لها ظرف تشديد وعقوبة مُغلّظة وسار مِثلما سَار عليه المشرع الجزائري في العقاب على فعل الدخول والإتلاف أو الإفساد والتعديل عند الدخول غير المصرح للنظام في المادة (382)، وأيضا عاقب على جريمة البقاء بوجه غير مشروع وحدد لها عقوبة لاتزيد عن سنة وغرامة لاتتجاوز 1000 دينار أردني وعاقب أيضا على جريمة التّنصت والإعتراضْ ويتمثل الركن المادي فيها بقيام الجاني بإستراقْ السمع أو إعتراض المعلومات بإستعمال أي من الأجهزة المخصصة لذلك، وكذلك جريمة إساءة إستخدام الأجهزة ونصت عليها المادة 384 من نفس القانون، المواد (380،381،382،383) من مشروع فانون العقوبات الفلسطيني لعام 2010، كما أن قانون رقم 10 لسنة 2018 عالج الدخول غير المشروع في المادة (4) منه .

2. جرائم التزوير بإستحدام أجهزة الحاسوب :

ليست المعلومات الورقية وحدها تقبل التزوير فكذلك البيانات والمعلومات الإلكترونية تقبل التزوير حيث نص المشرع في المواد (385،386،387) من مشروع قانون العقوبات الفلسطيني على جريمة التزوير بواسطة الحاسوب، حيث " أنه كل من قام بإدخال أو تغيير أو مَحو أو حَجب معلومات حاسوب مما يؤدي إلى نُشوء معلومات غير موثوق فيها....يعاقب بالحبس مدة لاتزيد عن سنة وغرامة لاتتجاوز 2000 دينار أردني أو بإحدى هاتين العقوبتين" وأيضا " كل من زوّر وثائق حاسوب ..... يعاقب بالحبس وغرامة لاتتجاوز 3000 دينار أردني أو بإحدى هاتين العقوبتين"، وأيضا " كل من عرقل أو أفسد عمدا نظام حاسوب....يعاقب بالحبس وبغرامة لاتتجاوز 3000 دينار أردني "، كما وعاقب المشرع الفلسطيني على جرائم أنظمة المعلومات التي تقع على المكونات المادية للحاسب الآلي من بيانات ومعلومات، كما ونص على جريمة التزوير في المادة 11 والمادة 12 فقرة 2، 3 من القرار بقانون رقم 10 لسنة 2018 .

وبهذا نرى كيف عاقب المشرغ الفلسطيني أيضا على جرائم التزوير بواسطة الحاسوب بالحبس أو بالغرامة أو بكليهما مثل المشرع الجزائري .

3. جرائم الإعتداء على الحياة الخاصة والجرائم الإباحية :

ويظهر الركن المادي في هذه الجريمة من خلال سلوك الجاني بِتمام وُلوجه إلى النظام الإلكتروني وينتهي بتمام فعله، ويتمثل الكن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صَفحات تحمل في طَيّاتها مواد مخلة للآداب العامة، ويقوم بنشرها عبر الإنترنت ونص المشرع الفلسطيني على الجرائم التي تمس الحياة الخاصة ومنها: جرائم التنصت على الآخرين كتسجيل صوت أو فيديو أو رسالة أو صورة، أو إذا قام بنشر أو ترويج دون

عِلم و رِضا صَاحِب الأمر والشأن ونصّ عليها المُشرع الفلسطيني في المادة 16 من قانون رقم 10 لسنة 2018 .

والكثير من الجرائم التي يظهر فيها الركن المادي للجريمة الإلكترونية والتي وضع لها المشرع الفلسطيني العقوبات، والتي نكتفي بذكر منها مثل :

1. **جرائم الإحتيال والسرقة الإلكترونية .**
2. **جرائم الإعتداء على الملكية الفكرية وسرقة البيانات الإلكترونية .**
3. **جرائم تتعلق بالإنترنت .**

ونص على الجرائم الواقعة على الأشخاص في المادة **(15)** من القرار بقانون رقم 10 لسنة 2018، وكذلك على الجرائم المخلة في الآداب العامة في المادة **(16)** من نفس القانون، والجرائم المتعلقة بأنظمة البيانات والإعتداء عليها في المادة **(4)** من نفس القانون، وعلى الحضّ على جرائم ضد الإنسانية في المادة **(25)** من نفس القانون وأيضا نص على التعطيل والعرقلة والإيقاف للنظام المعلوماتي في المادتين **(5 ، 6)** وأيضا نص على الإعتراض والتنصت في المادة**(7)** وعلى فك البيانات المشفرة في المادة **(8)** كما ونص على الإنتفاع بغير وجه حق بخدمات الإتصال في المادة **(9)** .

وبهذا نكون قد استعرضنا الركن المادي للجريمة الإلكترونية مع تطبيقاته في قانون العقوبات لدى المشرعين الجزائري والفلسطيني، مبينين أن الركن المادي في هذه الجريمة لقيامه لابد من وجود جهاز إلكتروني وهو الحاسب الآلي حتى تتحقق النتيجة الإجرامية وتكتمل العلاقة السببية بين السلوك الإجرامي والنتيجة وكما لاحظنا سابقا أن أكثر الجرائم الإلكترونية التي تحدث بواسط الحاسب الآلي ألا وهي القذف والذم، وسرقة البرامج الإلكترونية لإستعمالها، وجريمة الولوج والبقاء في نظام المعالجة الآلية للمعطيات باسنخدام الحاسب الآلي الذي يؤدي إلى إنتهاك نظام الحماية الأمنية .

ولكن تبقى الإشكالية في النتيجة الإجرامية في الجرائم الإلكترونية في مكان تحديد زمان ومكان تحقق نتيجة الجريمة ؟ ، وإشكالية أيضا ماهو القانون الواجب التطبيق في حالة وجود البعد الدولي ؟

المطلب الثالث : الركن المعنوي في الجريمة الإلكترونية : –

الفرع الأول : التعريف بالركن الشرعي للجريمة الإلكترونية :

سنتكلم بشكل عام عن الركن المعنوي ومن ثم سنتطرق للركن المعنوي للجريمة الإلكترونية .

يعد الركن المعنوي عنصر أساسي لقيام المسؤولية الجزائية، وبدونه لاتقوم الجريمة إذ ولايُسأل الشخص عن جريمة مالم تقم عَلاقة بين ماديّاتها ونفسيّة الجاني وسَيطرة الإرادة الجُرمية للجاني على ماديات الجريمة وبالتالي تّتحدّد صورة القصد الجرمي للجريمة مقصودة، أم تأخذ صورة الخطا الذي تكون به الجريمة غير مقصودة ؟

فالركن المعنوي للجريمة هو الوجه الباطني النفسي للسلوك الذي قام به الجاني، والنص القانوني هو الذي يحدد الوجه الباطني النفسي ونوعه، لكن في بعض الأحيان يتعدى السلوك الإجرامي نفسية صاحبه أو مرتكب الجريمة لأسباب خارجة عن إرادته ضغطت عليه ودفعته لإرتكاب الجريمة كأن يُكره شخص على التوقيع بإمضاء سَند مزوّر وفي هذه الحالة فإن الجاني لايُسأل جزائيا عن السلوك الذي قام به لذلك فإن الركن المعنوي للجريمة يفترض وجود معيارين الأول: وجود العلاقة النفسية، والثاني: هو تقييم القانون لهذه العلاقة وحكمه عليها [1] .

1.لورنس سعيد الحوامدة ، **الجرائم المعلوماتية أركانها وآلية مكافحتها**، مجلة الميزان للدراسات الإسلامية والقانونية، صادرة عن عمادة البحث العلمي في جامعة العلوم الإسلامية – الأردن ، 2017،ص23 .

الفرع الثاني : القصد الإجرامي للجرائم الإلكترونية :

فالقصد الجنائي هو إرادة إتجهت على نحو معين وسيطرت على ماديات الجريمة، وهي تعبر عن خطورة الجاني والنتيجة مؤكدة على الإدانة له أمام المحكمة متى تبيّن للمحكمة صدق هذه الإرادة .

أما الركن المعنوي للجرائم الإلكترونية فيعد كغيره من أهم الأركان وبدونه لاتتحقق المسؤولية الجزائية للجرائم الإلكترونية، لذلك سنبحث هنا عن القصد العام والقصد الخاص للجرائم الإلكترونية، وهل الجرائم الإلكترونية يتطلب فيها وجود قصد خاص أم لا ؟

تعد الجرائم الإلكترونية كغيرها من الجرائم والتي تفترض بالأساس وحود القصد العام (العلم ، الإرادة) لتحديد المسؤولية الجنائية ولايمكن تصور قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص بالجريمة الإلكترونية فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من جراء القيام بعمل غير مشروع أو إرتكاب الجريمة، فكل جريمة إلكترونية تختلف عن الأخرى من حيث أركانها وماهيتها وطبيعتها .

ويرى إتجاه من الفقه أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب بإستخدام الإنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاماً أو خاصاً .

وأن القصد الخاص يتوافر في بعض الجرائم الإلكترونية، سيّما وأن معظم الجرائم الإلكترونية تقوم بتوافر القصد العام وهو علم الجاني بمضمون الفعل الذي قام به أو سَيقوم به بأن هذا الفعل غير مشروع، وكذلك إرتباط هذه العلم بالإرادة، وهي حَالة نفسية مُرتبطة بماديّات الجَريمة، فمثلا في جريمة سرقة المعلومات وهي من الجرائم الإلكترونية يجب أن ينصبّ علم الجاني على أن فعل سرقة المعلومات من الحاسب الآلي أو البريد الإلكتروني يعدّ فعل غير مشروع، ويجب أن يَرتبط هذا العلم بالإرادة وهي الحالة النفسية التي تَعكس قيام الجاني بالسلوك،

ويترافق مع القصد العام في جريمة سرقة المعلومات (نيّة التملك)، للمعلومة التي تم سرقتها والتي تعكس (القصد الخاص)، في مثل هذه النوع من الجرائم .

ويرى إتجاه من الفقه أن نيّة التملك في جريمة سرقة المعلومات تبدأ بقيام الجاني بالدخول على أدوات الحاسب الآلي من وحدات الإدخال والإخراج والتخزين والمعالجة أو البرامج والبيانات والمعلومات والنظم المخزنة داخل ملفات الحاسب الآلي أو في ذاكرته، كل هذا من أجل الإستيلاء على المعلومات الموجودة لقصد نيّة التملك والإضرار بالمجني عليه [1]، ومن خلال عرضنا فيما بعد لبعض الجرائم سَنرى ذلك في جريمة الدخول غير المشروع للمواقع الإلكترونية وجريمة التعدي على الحاسب الآلي .

الفرع الثالث : الخطأ غير المقصود في الجرائم الإلكترونية :

ويقصد به التّصرف الذي لايتفق مع الحِيطة التي تتطلبها الحياة الإجتماعية فَقد يقع بِفعل سَلبي أو إيجابي.

وله عنصرين : 1. الإخلال بواجبات الحيطة والحذر، 2. العالقة النفسية بين الإرادة والنتيجة.

الخطأ هو أحد صور الركن المعنوي وهو يمثل الركن المعنوي في الجرائم الغير مقصودة، وأن المشرع الفلسطيني نص على صورة الخطأ غير المقصود، ووضع لها شروط وأحوال معينة وافترض المشرع ضمنياً حُسن نيّةُ مُرتكب السلوك بأنه لم يتوقع حدوث النتيجة التي أفضى سُلوكَه إليها، ولذلك لايتحمل الجاني أي مسؤولية جزائية عن الخطأ الذي إرتكبه، فالمشرع الفلسطيني لايقرر المسؤولية الجزائية عن الخطأ إلا بنص خاص وأن يكون الجاني مُتمتعاً بكامل قواه العقلية فالجاني هنا أراد السلوك ولكنه لم يُرْجُ ولم يتوقع النتيجة، فالخطأ والجهل

1. لورنس سعيد الحوامدة ، **المرجع السابق** ، ص24-25.

من المتصور وقوعه في الجرائم الإلكترونية، وهذا يمكننا إستنباطه، من خلال النصوص العقابية للجرائم الإلكترونية [1].

فعلى سبيل المثال ذكر المشرع الفلسطيني جريمة الدخول غير المشروع فإنه يمكن الإحتجاج بالخطأ أو الجهل فربما يكون الجاني من المستخدمين الجُدد للحاسب الآلي وقد دخل نظام وهو لايعلم بأن الدخول للنظام أو البقاء فيه مَحظور أو كان يَعتقد بأن الدخول مُباح .[2]

وجريمة الذّم من الجرائم العَمَدِيّة التي يكفي لإثباتها القصد العام ويتخذ فيها الركن المعنوي صورة القصد الجنائي، بعنصريهِ العلم والإرادة فيكفي لإثبات ذلك أن يكون الجاني يَعلم بالألفاظ التي خرجت منه وأن القانون يعاقب عليها، وإرادته هي من وَجهت هذه الأقوال، ويُترجَم ذلك من خلال إخراج هذه الأقوال على أي شكل كانت كتابيّة أو سمعيّة أو غيرها عن طريق أي وسيلة من الوسائل الإلكترونية .

وجريمة الإتلاف الإلكتروني من الجرائم القصدية والتي يعتبر الركن المعنوي فيها هو القصد الجنائي، فالقثد الجنائي في جريمة الإتلاف الإلكتروني يتكون من عنصرين العلم والإرادة، فلو قام شخص بإتلاف برامج أو معلومات بشكل عمدي، وإتجهت إرادته لهذا الفعل وكان يعلم بأن عمله غير مشروع توافر في حقه القصد الجنائي، على خلاف إذا ماقام بإتلاف برامج أو معلومات كان مُطالباً منه ومن الواجب عليه إتلافها فلا نكن هنا بصدد جريمة الإتلاف الإلكتروني .

1. يوسف العفيفي ، **المرجع السابق**، ص61-62.

2. **المرجع نفسه**، ص60-61.

ويتوافر الركن المعنوي أيضا فيمن يقوك بتزوير بطاقة الإئتمان ، ذلك لأنه يقوم بتغيير الحقيقة في البطاقة المُمَغنطة وهو يعلم بجميع أركان التزوير ويترتب على هذا الفعل ضرراً يلحق بالفرد أو المُجتمع كَكُل .

وبهذا نرى أن المشرع الفلسطيني قد وظّف صور الركن المعنوي في الجريمة الإلكترونية من خلال قانون العقوبات الفلسطيني .

أما بالنسبة للمشرع الجزائري ونوظيفه للركن المعنوي في الجرائم الإلكترونية ، فإننا نجد أن الركن المعنوي للجرائم المعلوماتية يختلف بإختلاف أشكالها وعليه إرتأينا التعرض للركن المعنوي لكل جريمة على حده:

1. جريمة الد خول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات :

إن جرائم الدخول والبقاء غير المشروع هي جرائم عمدية تتطلب قصداً خاصاً وذلك بنص المادة 394 مكرر من قانون العقوبات الجزائري التي عبرت عن القصد الجنائي بنصها " كل من يدخل أو يبقى عن طريق الغش "، وتعني هذه العبارة أن الفاعل له كامل العلم بأن الدخول والبقاء غير مشروع، ولتوافر القصد الجنائي لابد أن يكون الجاني محيطا علما بكافة العناصر الجريمة وله علم بأن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج كما ذكرنا سابقا .

بمعنى آخر أن إتجاه إرادة الجاني إتجهت إلى فعل الدخول أو فعل البقاء وأن الجاني يعلم بأن ليس له الحق في الدخول إلى النظام والبقاء فيه، ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله وبقاؤه داخل النظام مسموح به أي مشروع أو كان الجاني يجهل بوجود حظر الدخول أو البقاء [1] .

1.آمال قارة، **المرجع السابق**، ص124.

أما بالنسبة لنية الغش تبدو من خلال الغشّ الذي تم به الدخول من خرق الجهاز الرّقابي الذي يحمي النظام، بالنسبة للبقاء فيُستنتج من العمليات التي تمّت داخل النظام وفي الحقيقة أن الدخول و البقاء بالغش لايتضمن معنى خرق الجهاز الرقابي للنظام وإنما يظهر من خلال الولوج دونَ وَجه حق إلى النظام وأن الدخول للنظام غير مرخص به [1] .

2. جريمة الإعتداءات على سير نظام المعالجة الآلية للمعطيات :

إن جريمة الإعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا مايميزه عن الإعتداء غير العمدي لسير النظام الذي يعتبر ظرفا مشدّداً لجريمة الدخول والبقاء غير المشروع داخل النظام وعليه فالقصد الجنائي المفترض ينتج م نطبيعة الأفعال المجرمة.

3. الإعتداءات العمدية على المعطيات :

هي جريمة عمدية يتخذ فيها القصد الجنائي بعُنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال والمحو والتعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضاً أنه ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، ويشترط لتوافر الركن المعنوي بالإضافة للقصد الجنائي العام نيّة الغش لكن هذا لايعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق رُكنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك وإتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشلط الإجرامي، إلا أنه ليس عنصرا في الجريمة [2] .

---

1. آمال قارة، **المرجع السابق** ،ص125.

2.**المرجع نفسه**،ص125-126.

4.إستخدام المعطيات كوسيلة في إرتكاب الجرائم الماسة بالأنظمة المعلوماتية :

إن هذا الإستخدام يكون عمديا وذلك الإستخدام متمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، ويكون هذا الإستحدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نيّة الغش[1] .

هناك ركن آخر في الجريمة الألكترونية غير موجود في كل الجرائم يسمى بالركن المفترض للجريمة الإلكترونية :

الركن المفترض في الجرائم الإلكترونية :

يذهب الفقه الإيطالي إلى تعريف الشرط المفترض للجريمة بأنه عنصر أو ظرف إيجابي أو سلبي يسبق لاضرورة وجود الجريمة أو الواقعة، أو هو عنصر أو مركز يسبق في وجوده قيام الجريمة – منطقيا وقانونيا – ويعد بمثابة الوسط الضروري لتوافر السلوك غير المشروع، أما الفقه الفرنسي إعتمد على أفكار (**قوان**)، الذي يُعد أول من إستخدم هذا الشرط وقد عرف هذا الفقيه الشرزط المفترضة بقوله بأنها: العناصر التي تحدد المجال الذي يمكن للجريمة أن ترتكب فيه، وهي مراكز قانونية أو واقعية سابقة على النشاط الإجرامي من دون أن ينفكّ عنه أو هي مراكز محايدة في ذاتها تمثل نقطة البدء لإرتكاب بعض الجرائم وتكون لازمة لوقوع الجريمة[2] .

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة ومستحدثة تتسع قوالبها لتشمل الجرائم الإلكترونية، فالجريمة الإلكترونية تحتاج إلى ركن مفنرض كغيرها من الجرائم التقليدية،

1.آمال قارة ، **المرجع السابق** ، ص126.

2. المرجع الإلكتروني للمعلوماتية .**AL merja. Net** ، تاريخ الإطلاع على الموقع : 2019/4/30.

فالجريمة الإلكترونية دون وجود الحاسب الآلي والشبكة المعلوماتية ووجود معلومات معالجة آليا لامجال لوقوع هذه الجريمة .

فالركن المفترض: هو الشرط الذي يفترض القانون تواجده وقت مباشرة الجاني لفعله وبدونه لايتصِف هذا النشاط بأي جريمة، وعليه يُعتبر القاسم المشترك بين الجرائم الإلكترونية هو وجود الشبكة المعلوماتية وجهاز الحاسب الآلي ووجود نظام معالجة آلي للبيانات، ولابد من التعريج على ماهية بيانات وبرامج الحاسب الآلي حتى يتسنى فهم الركن الإفتراضي بسكل سلس، حيث تعد البرامج والبيانات رُوح الحاسب الآلي ودون وجودها يعتبر لاقيمة له والبرامج هي مجموعة متسلسلة من التعليمات التي ترشد الحاسب الآلي، لإتمام العمليات المنطقية بغرض الوصول إلى نتيجة معينة، كما وعرف المشرع الفلسطيني معالجة البيانات على أنها: " إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات سواء تعلقت بأفراد أو خلافه، بما في ذلك جميع تلك البيانات أو إستلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو إسترجاعها أو محوها أو نشرها أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو الغاؤُه أو تعديل محتوياتِه " .

يمثل نظام المعالجة الآلية للمعطيات الركن المفترض في الجرائم الإلكترونية كافة حسب التشريع الفرنسي، ودون هذا النظام لايكون هناك مجال للبحث عن أي ركن من أركان الجريمة، وهذا شرط يعتبر لازماً لتوافر أي جريمة من الجرائم الإلكترونية، وإن نظام المعالجة الآلية للمعطيات هو مفهوم تقني فني لابد من وجود أشخاص فنيين مُتخصصين حتى يتسنى لِرجل القانون فَهْمُه، وبناءا عليه نلاحظ أن للجريمة الإلكترونية طبيعة خاصة حيث أن وسيلة إرتكابها

تُعتبر جُزءاً لايتجزأ من الرُّكن المفترض (الشَّرط المُفترض) الذي يعتبر عنصر أساسي لقيام الجريمة الإلكترونية [1] .

خـــلاصـــة الـــفـــصـــل الأول :

على ضوء ماتقدم فإننا في معرض تحديد الأحكام الموضوعية للجريمة الإلكترونية، يَجدر بنا القول أن الجريمة الإلكترونية هي من الجرائم المستحدثة وهي جريمة وليدة التطور العلمي والتكنولوجي الكبير الذي وصل إليه العالم، فَرغم الوجه المشرق الذي تقدمه إلا أن لها جانب آخر سلبي عندما يستعمل في غير الغرض الذي وجد من أجله، وهذا النوع من الجرائم مرتكب من صنف من الأشخاص يطلق عليهم تسمية المجرمين المعلوماتيين وهو يتمتعون بالذكاء والفطنة في التعامل مع برامج الحاسب الآلي من خلال مايحدثونه من تخريب أو تدمير أو إتلاف للمنظومة الإلكترونية وذلك نتيجة دوافع خاصة قصد تحقيق الربح، وكما رأينا أن الجريمة الإلكترونية مرت بتطور تاريخي من تبعا لتطور التقنية وذلك من أواخر الخمسينيات إلى أن ظهرت أول معالجات لما يسمى بالجريمة المعلوماتية وبدأ الحديث عنها كظاهرة إجرامية، كما عرضنا أيضا للخصائص التي تتميز بها الجريمة الإلكترونية ووجدنا أنها عابرة للحدود ويصعب إكتشافها و إثباتها بسهولة كما أنها تتم بأسلوب لايتمتع بالعنف وتتم عادة بتعاون أكثر من شخص ومن ثم تناولنا صور الجرائم الإلكترونية كما بينها ووضحها المشرعين الجزائري والفلسطيني ومن ثم بيّنا الأركان التي تقوم عليها الجريمة الإلكترونية وحتى يتم الوقوف الصحيح على الأركان ولنكون في بر الأمان قمنا بتطبيقها على التشريعين من خلال عرض المواد القانونية في الركنين المادي والمعنوي ورأينا كيف عاقب وجرّم المشرعين على

1. نداء المصري، **خصوصية الجرائم المعلوماتية**، رسالة ماجستير – تخصص قانون عام ، إشراف الدكتور فادي شديد ،كلية الدراسات العليا، جامعة النجاح الوطنية،نابلس فلسطين،2017،ص9-12.

جرائم الدخول غير المصرح به وذلك بالولوج إلى أنظمة المعالجة الآلية للمعطيات والإطلاع على المعلومات وغيرها، وتطرقنا إلى الركن المفترض الذي لاتقوم الجريمة الإلكترونية إلا به، وأيضا قمنا في ثنايا الفصل ألأول في التعرف على موقف المشرعين والمواجهة الجنائية لتلك الجرائم مبينين المواد القانونية التي سن المشرع من خلالها على الجرائم الإلكترونية وكما ظهر لنا أيضا من خلال التعريف أنه لايوجد تعريف متفق عليه للجريمة الإلكترونية رغم إبرام العديد من المؤتمرات والإتفاقيات الدولية والإقليمية وأيضا كذلك الشأن بالنسة لتسميتها وأن المحل الجريمة المعوماتية هو المعطيات وأن الحاسب الآلي يلعب الدور الكبير في هذا النوع من الجرائم ، وأن أهم القوانين المعمول بها في التجريم على هذاالنوع هو القانون رقم 15/04 لعام 2004 تحت عنوان المعالجة الآلية للمعطيات وهذا في قانون العقوبات الجزائري ، أما المشرع الفلسطيني فقد نص عليها تحت عنون قرار بقانون رقم 10 لسنة 2018 والذي يعد أهم القوانين الحديثة التي تعاقب على هذه الجريمة وكيف تصدّت هذه القوانين للجريمة العصرية التي إستحدثتها الوسائل الإلكترونية عبر القارات ورأينا أنه هناك قوانين وضعها المشرع يمكن من خلالها مكافحة هذه الجريمة، وأن هذا التطور الكبير ألقى على عاتق المشرع الجنائي مسؤولية كبيرة لمواجهة الجرائم الإلكترونية .

وبما أنها جريمة مستحدثة في محتواها ومخاطرها وأشكالها ومشكلاتها وطبيعة مرتكبيها هذا يدفعنا إلى التساؤل التالي :

ماهي إجراءات البحث والتحري في الجريمة الإلكترونية ؟ وماهي الآليات المتبعة في مكافحة هذا النوع من الجرائم على المستوى الوطني والدولي ؟ كون أن هذه الجرائم من أهم القضايا التي تقلق رجال الفكر القانوني في الوقت الحاضر.

الفصل الثاني : الأحكام الإجرائية للجريمة الإلكترونية :

إن التطور المذهل والمتسارع والمتلاحق في تكنولوجيا المعلوماتية وشبكات المعلومات أدى إلى ظهور نمط جديد وهو الجريمة الإلكترونية، وتكمن خطورة هذه الجريمة في كونها تنصب على بيانات رقمية لاتخلّف أثراً مادياً يكشف عنها أو يُستدل به من خلالها على فاعلها، وأن التحقيق والبحث والتحري ليس أسئلة تلقى ولاإجابات تدوّن لكن فنٌ و دِراسة خِبرة وفراسَة، وأن شبكات الإتصال المتعددة ساهمت في عولمة الجريمة الإلكترونية، وتنوعت الأنشطة الإجرامية فيها مما حتّم تنوعاً في ملاحقتها ومتابعتها إبتداءاً من تجريمها وبيان إجراءات ملاحقتها، وكذا الأجهزة المختصة في الوقاية منها، فأُبرمت الإتفاقيات وعُقدت النّدوات والمؤتمرات وتزايدت خُطط مكافحة هذه الجرائم وإنصبّت الجُهود على دراستها المتعمقة وخلق آليات قانونية للحماية من أخطارها، وأن طبيعة هذه الجرائم بعناصرها ووسائل إرتكابها قد تدفع المشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرائية وخاصة فيما يتعلق بمسألة الإثبات في هذا النوع من الجرائم، بالإضافة إلى الدور البارز الذي تلعبه المنظمات الدولية والإقليمية الخاصة بالكشف عن الجرائم ومحاولة القبض على المجرمين .

وعلى هذا الأساس سيتم تقسيم هذا الفصل إلى مبحثين :

المبحث الأول : المراحل الإجرائية للجريمة الإلكترونية .

المبحث الثاني : آليات مكـــافحة الجريمة الإلكترونية .

المبحث الأول : المراحل الإجرائية للجريمة الإلكترونية .

لم تكتفِ التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الإعتداء عليها أي حماية موضوعية، وإنما نظراً لخطورة الإجرام الإلكتروني في حد ذاته لكون محل الجريمة مجموعة معطيات هي عبارة في الحقيقة عن ذَبذبات إلكترونية يَسهل على الجاني القيام بعمل إجرامي عليها دون تَرك آثار ودون أن يَستغرق هذا العمل وقتاً طويلاً وهو ماجعلها صعبة الكتشاف والإثبات، وبما أنها جرائم حديثة لايمكن تطبيق النصوص التقليدية عليها من جهة وعدم القدرة الكافية والفنيّة لرجال القانون من جهة أخرى لإكتسابها . ولذلك وُضعت مجموعة من الإجراءات منها مايعتبر قاسماً مشتركاً بين الجرائم التقليدية والجرائم الماسّة بالمعطيات ومنها لايطبّق إلا على الجريمة الإلكترونية خاصة في مرحلة جمع الإستدلالات والتحري والتحقيق، وأن المراحل الإجرائية: هي عبارة عن الخطوات الواجب توافرها منذ لحظة وقوع الجريمة حتى تنفيذ الحُكم ولهذا تمرّ الإجراءات الجنائية بعدة مراحل وهذا يدفعنا إلى طرح التساؤل الآتي :

فيما تتمثل إجراءات البحث والتحري والتحقيق في الجريمة الإلكترونية ؟ وماهي طرق إثبات الجريمة الإلكترونية ؟

ومن هذا المنطلق سنقسم هذا المبحث إلى ثلاثة مطالب وسَنُعالج في المطلب الأول مرحلة جمع الإستدلالات التي قُمنا بتقسيمها إلى فِرعين كما هو موضح .

المطلب الأول : مرحلة جمع الإستدلالات .

الفرع الأول : إجراءات التحري الخاصة في مجال مكافحة الجريمة الإلكترونية .

الفرع الثاني : آليات الإثبات في مجال مكافحة الجريمة الإلكترونية .

ومن ثم سنعرض في المطلب الثاني **مرحلة التحقيق والمحاكمة**، وسنتطرق في المطلب الثالث إلى **العقوبات المقررة التي وضعها المشرعين الجزائري والفلسطيني لمرتكبي الجرائم الإلكترونية .**

المـــطلب الأول : مرحـــلة جـــمع الإســـتـــدلالات .

كما عرفنا أن مرحلة جمع الإستدلالات هي من المراحل الإجرائية التي تمر بها الجريمة والتي تنحصر مهمتها في البحث عن الجرائم ومرتكبيها وجمع عناصر التحقيق، وأنها مرحلة عادةً تسبق مرحلة الدعوى الجنائية وهي تعتبر ممهدة له وهذه المرحلة تبدأ بالتتبع وتجميع العناصر والأدلة المادية التي تُثبت وقوع الفعل الإجرامي بالإضافة إلى عمل التّحريات الضرورية واللازمة كي تستطيع النيابة العامة توجيه تحقيقها بالشكل الذي يصل بها إلى الحقيقة المنشودة [1] .

الفرع الأول : إجراءات البحث والتحري الخاصة في مجال مكافحة الجريمة الإلكترونية .

لإرتباط الجريمة الإلكترونية بأنماطْ ودرجاتْ مُختلفة من تكنولوجيات الإعلام والإتصال، ولتباعد المسافات بين الفعل والنتيجة فإنه لكي يُفضي التحري للوصول إلى الجاني يَنبغي وجود أجهزة ضَبط قضائي متخصصة شُرع لها اختصاص إقليمي موسع، وبالتالي فإننا سنتعرض في هذا الفرع من هي السُّلطة المُختصة أو الجهاز المُختص في البحث والتحري ومن ثم سنحدد الإختصاص الإقليمي لهذا الجهاز لمتابعة هذا النوع من الجرائم .

أولا : تحديد الأجهزة المختصة بمهمة البحث والتحري عن الجرائم الإلكترونية .

إن إجراءات جمع الإستدلالات من الإجراءات التي تسبق التحقيق ورفع الدعوى الجزائية، والتي يختص بها مأموري الضبط القضائي والتي يكون النائب العام مُشرف ومسؤول أعمالهم، حيث يحق للنائب العام الإشراف على أعمال الضبطية القضائية ويحق له مسائلتهم إن حدث تقصير

---

1. **Blogs, Najah, edu** / تاريخ الإطلاع على الموقع : 2019/5/1 .

منهم [1] ، وإجراءات جمع الإستدلالات ينطوي فيها عملية البحث والتحري والتحري حول الجريمة والتمهيد للتحقيق فيها، دون التّوغل في عملية التحقيق التي تَختص بها النيابة العامة دون غيرها [2] .

لم تَسلم أجهزة الضبط القضائي من ضرورات التطور التقني والتكنولوجي لما تَطرح الجريمةالإلكترونية من تحديات، ونتيجة لذلك قامت الدول بإستحداث أجهزة ضبط متخصصة، تختلف عن الأجهزة التقليدية من حيث تكوينها، وعلى هَديْ ذلك سَنقف عند تشكيل الضبطية القضائية المُختصة بالبحث والتحري عن الجريمة الإلكترونية في التشريعين الجزائري والفلسطيني .

1. تشكيل سلطة البحث والتحري في التشريع الجزائري :

لقد نهج المشرع الجزائري نهج التمييز بين الإختصاص العام والإختصاص الخاص طبقاً للمادة 15 من قانون الإجراءات الجزائية الجزائري، فَيتولّى الضُّباط المحددون في البنود من 1-6 من المادة 15 من قانون الإجراءات الجزائية الإختصاص العام بالبحث والتحري في جميع الجرائم دون التقيد بأي نوع منها، يُساعدهم في ذلك الأعوان طبقا للمادتين 19،20 من نفس القانون، أما الإختصاص الخاص فَيتولاّه الضباط المُحددون بالبَند رقم 7 من قانون الإجراءات الجزائية وهي فئة لاتقوم بوظيفة الضبطية القضائية إلا في نطاق محدود مَقصور على الجرائم التي تقع في دوائر إختصاصهم وتكون معلقة بأعمال وظائفهم [3]

1.راجع **المادة (19،20) من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001** .

2. عبد القادر جرادة ، **موسوعة الإجراءات الجزائية في التشريع الفلسطيني**،مكتبة آفاق،غزة-فلسطين،2009،ص277.

3.لهوة رابح،**البحث والتحري في الجريمة المعلوماتية**،رسالة ماجستير-تخصص علوم جنائية،بإشراف الدكتورة ميموني فايزة ، كلية الحقوق والعلوم السياسية ، جامعة خنشلة ، 2014،ص41.

ومانخلص إليه بالإطلاع على المواد السابقة من قانون الإجراءات الجزائية الجزائري، أن فئة الضباط ذات الإختصاص العام هي من لها الحق في سلطة البحث والتحري في الجرائم الإلكترونية ولايجوز لغيرها من الفئات، وأن المشرع الجزائري لم ينص على الأصل المُترتب على مخالفتها ولكن من الفقه رتّب عليها البطلان وهو بطلان متعلق بالنظام العام لأنه يمس قواعد الإختصاص في المواد الجنائية وهي قواعد يترتب على مخالفتها بطلان متعلق بالنظام العام .

ونجد المادة **1/12** من قانون الإجراءات الجزائية الجزائري تنص على: " يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون المبينون في هذا الفصل ".

وتنص المادة **14** : " يتمثل الضبط القضائي:

1.ضباط الشرطة القضائية .

2.أعوان الضبط القضائي .

3. الموظفون والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي " .

واعتنت المواد **(15 ، 19، 20، 21 ، 27 ، 28)** من قانون الإجراءات الجائية الجزائري بتعداد فئات الموظفين و الأعوان اللذين تثبت لهم صفة الضبطية القضائية المحددة بالمادة 14 من نفس القانون أو اللذين يمكن اضفاؤها عليهم وفقا لقواعد محددة سلفا، فجاءت المادة 15 من محددة لمن تثبت لهم صفة ضابط شرطة قضائية، وجاءت المادتان 19 ، 20 محددتين لطائفة الأعوان وحددت المادتين 21 ، 28 طوائف الموظفين المَوكُول إليهم بعض مهام الضبط القضائي، وأحالت المادة 27 على القوانين الخاصة التي تخوّل الموظفين والأعوان مباشرة بعض سلطات الضبط القضائي، وهنا المشرع الجزائري مَنح سلطة البحث والتحري

لأعوان الضبط القضائي في التحقيق الأولي تحت رقابة ضابط الشرطة القضائية بموجب المادة 63 منه [1] .

2. تشكيل سلطة البحث والتحري في التشريع الفلسطيني :

نص المشرع الفلسطيني على من يخول لهم صفة الضبطية القضائية حيث نص في المادة **21** من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 على أنه: " يكون من مأموري الضبط القضائي :

1. مدير الشرطة ونوابه ومساعدوه ومدير شرطة المحافظات والإدارات العامة .

2.ضباط وضباط صف الشرطة ، كل في دائرة إختصاصه.

3.رؤشاء المراكب البحرية والجوية .

4.الموظفون الذين خوّلوا صلاحيات الضبط القضائي بموجب القانون " .

فَبِمُقتضى هذه المرحلة تجمع الدلائل التي تفيد في كشف الحقيقة، والتي قد تَصلُح أساساً للمحاكمة في الجنح والمخالفات، أو أساساً للتحقيق الإبتدائي في الجنايات والجنح .

نلاحظ هنا أن المشرعين الجزائري والفلسطيني قد أبْقَوا على أجهزة الضبطية القضائية [2] ، التقليدية في مواجهة هذا النوع من الإجرام وفقاً لتنظيمهم المحدد في قانون الإجراءات الجزائية لكليهما، فالجزائر إكتفت بالنّص على التّدابير الإجرائية لمكافحة الإجرام الإلكتروني دون أن تؤَهّل أجهزتها على الوَجه اللازم لِخَوض تلك المواجهة فَالإجراءات الجنائية لمكافحة هذه

---

1. لهوة رابح ، **المرجع السابق** ، ص 42-43 .

2.**الضبطية القضائية عرفها الفقه بأنها** : الجهة التي أناط بها المشرع صلاحية تعقب الجريمة بعد وقوعها بالحث عن فاعليها، وجمع الإستدلالات اللازمة لإثبات التهمة عليهم . للمزيد الإطلاع على :إبراهيم طنطاوي ، سلطات مأموري الضبط القضائي،دراسة مقارنة،رسالة دكتوراه،دار النهضة العربية،القاهرة،1993،ص71.

الجريمة لاتعتمد على التدريبات البدنية أو الفيسيولوجية التي يتلقاها مأموري الضبط القضائي وإنما تعتمد على البناء العلمي والتكنولوجي لضباط الشرطة القضائية حنى تتولى مهمة جمع الإستدلالات في العالم الإفتراضي من أجل كشف النقاب عن هذا النوع من الإجرام، أما فلسطين بالإضافة للمهام الموكلة لمأموري الضبط القضائي فإنها أنشأت وحدة متخصصة لمتابعة وملاحقة مرتكبي الجرائم الإلكترونية في عام 2013 وتتبع للمباحث العامة الجنائية، أما من ناحية التدريب والتأهيل وتوزيع الضباط على المحافظات فهي غير متطورة وليست في المستوى المطلوب وليست بالقَدر الكافي من العامِلين، وكذلك العامِلين في الإدارة العامة من تلك الوحدة تختلف مُؤهلاتهم عن تلك العاملين في المحافظات فَمُعظمهم من خريجي القانون والعلوم الشُّرطية وهندسة الكُمبيوتر والهندسة الإلكترونية، وهذا مايجعل المجرم المعلوماتي يشعر بأن جهاز الضبط القضائي غير قادر عى إكتشاف أمره وأن دَهائه وخِبرته الفنية تجعلُه بِمنأى عن المسائلة الجزائية بما يَمنحه ثقة أكبر في إرتكاب جرائم إلكترونية أكثر فداحة وأشد ضرراً، وجهات الضبط القضائي تُعاني عموماً ضعف الثقافة القانونية اللازمة للتعرف على الجرائم الإلكترونية وتقدير خطورتها عند المشرعين الجزائري والفلسطيني، لذا لابد من وجود شخص متخصص يُكلف بجمع الأدلة الرقمية وهو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها .

فتنص المادة 17 من قانون الإجراءات الجزائية الجزائري على :" يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 ، 13 ويتلقون الشكاوي والبلاغات ويقومون بجمع الإستدلالات وإجراء التحقيقات الإبتدائية" وتنص المادة 22/ 1 من قانون الإجراءات الجزائية الفلسطيني على أنه : " وفقا لأحكام القانون على مأموري الضبط القضائي بما يلي :

1. قبول البلاغات والشكاوي التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة .

3.هناك هيئات أخرى لمساعدة سلطة البحث والتحري على المستوى الوطني (الجزائر) وعلى المستوى الدولي وعلى المستوى العالمي :

على المستوى الوطني (الجزائر) :

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، فقد نصت الإتفاقية الأوروبية للجريمة المعلوماتية على وجوب إنشاء شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة بموجب نص المادة 35 منها وقد تجسد ذلك في التشريع الجزائري من خلال هذه الهيئة [1] .

2. مقدمي الخدمات: يشمل إرتكاب الجريمة المعلوماتية تلقائياً عددا من الأشخاص حتى وإن كان الجاني يتصرف بمفرده وذلك بسبب هيكلة الإنترنت، فإرسال بريد إلكتروني يتطلب خدمة عدد من مزودي الخدمات، كخدمة البريد الإلكتروني وخدمة النفاذ وخدمة التسيير، وهكذا ظل مقدموا الخدمات دائما محوراً للتحقيقات الجنائية، وهؤلاء يقدمون خدمتهم للجمهور بوجه عام في مجال الإتصالات الإلكترونية وهم على ثلاثة أصناف : أ- مقدمي خدمة التوصيل ، ب- مقدمي خدمة الإستضافة، ج- مقدمو المضمون أو الناشرون [2] ، كما ويوجد في فلسطين مثل هذا النوع ممن يقدّمون الخدمات وذلك مانصت عليه المادة 31 من قانون رقم 10 لسنة 20018 بشأن الجرائم الإلكترونية وذلك بتزويد الجهات المختصة بمعلومات المشترك وهذا يعد من الهيئات المساعدة لسلطة البحث والتحري في فلسطين .

1.لهوة رابح ، **المرجع السابق** ، ص74.

2.**المرجع نفسه** ، ص81.

على المستوى الدولي :

أولا : هيئات التعاون الدولي على المستوى الأوروبي .

1. الأوربول أو مركز الشرطة الأوروبية: هو أخد الأجهزة المتواجدة على المستوى الأوروبي والتي تتخذ من لاهاي بهولندا مقرا لها وقد تم انشاؤه بموجب إتفاقية 26 جويلية 1995 وهي مكلفة بمكافحة الإجرام عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على المستوى الأوروبي ودعم وتشديع سلطات التحقيقمن أجل مكافحة هذا النوع من الإجرام [1] ,

2. المركز الأوروبي للجريمة الإلكترونية : إلى جانب مركز الشرطة الأوروبية، سعت الدول الأوروبية إلى تعزيز النعاون الشرطي بينها وذلك من خلال آلية مختصة بمكافحة هذه الجريمة التي لايمكن بحال معرفة حدودها إلى جانب قدرة مُنفذيها على التواري إلى إِستجابة مرنة وكافية لذا تم تصميم هذا المركز ليكون بَوتقَة تَنصهر فيها الجُهود ومركزاً للدعم الإستخباراتي والتشغيلي والقضائي يقوم بالرد على الجرائم الإلكترونية [2] .

3. الأورجِست : وهو جهاز تابع للإتحاد الأوروبي وهو يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة ومكلّف بتحسين فعالية السُلطات المختصة للدول الأعضاء في مكافحتهم للجريمة المُنطمة العابِرة للحدود كالجريمة الإلكترونية. وقد تم إنشاؤه بموجب القرار الصادر عن مجلس الإتحاد الأوروبي بتاريخ 28 فيفري 2002 [3] .

---

1. لهوة رابح ، **المرجع السابق** ، ص94.

2.**المرجع نفسه**، ص95.

3.**المرجع نفسه**،ص96.

على المستوى العالمي :

توجد على المستوى العالمي **الأنتربول أو المنطمة الدولية للشرطة الجنائية،** وقد أنشئت سنة 1929 وهي تسعى إلى توطيد التعاون البوليسي في العالم بفضل مكاتب مركزية ووطنية في 186 بلد عضو، وذلك لتسهيل تبادل المعلومات من أجل مكافحة فعالة لجميع أنواع الجريمة حيث يملك نظام إتصال معلوماتي مشترك بين جميع الدول الأعضاء تعمل على مدار السنة ومجموعة قاعدة بيانات لمعلومات الشرطة ومصالح مختصة في تحليل المعلومات حول الجريمة الإلكترونية وبطاقة الدفع، ولايمكن لأعضاء هذا الجهاز التدخل إلا بطلب مساعدة من الدولة المعنية وفقاً للإجراءات القانونية حيث يقوم الإنْتَربول بإطلاع مَصالح البَحث والتحري الوطنية عبر المكاتب المركزية الوطنية على بعض المعلومات المتعلقة بالجرائم الإلكترونية والمجرمين والضحايا، وفي هذا الصدد تتم المباشرة في إعداد بيانات وَصفية دولية تتعلق خاصة بأشخاص متابعين بغرض تسليمهم [1] .

ثانيا : نطاق إختصاص سلطة البحث والتحري في الجريمة الإلكترونية على الصعيد الوطني (الجزائر وفلسطين) ، وعلى المستوى الدولي :

1 . نطاق إختصاص سلطة البحث والتحري على المستوى الوطني (في الجزائر) :

إذا كان الإختصاص الإقليمي للضبطية القضائية فيما يتعلق بالجرائم التقليدية يتحدد كأصل عام بنطاق العمل الوظيفي العادي طبقا للمادة 16 فقرة 1 من قانون الإجراءات الجزائية الجزائري التي تنص على: "يمارس ضُباط الشرطة القضائية إختصاصهم المحلي في الحدود التي يُباشرون فيها وظائفهم العادية ". إلا أن هذا الإختصاص لهُ ذاتية خاصة في مجال محاربة الجريمة الإلكترونية.

1. لهوة رابح ،**المرجع السابق** ، ص97-98.

فَالوَاضح أن المشرع الجزائري تَدارك النَّقص وَسَدَّ الفراغ القائم بشأن إختصاصات الضبطية القضائية إثَ التطور الذي عرفتهُ الجريمة سيّما بأشكالها الحديثة كما هو الحال في الجريمة الإلكترونية، لذا جاءت تعديلات قانون الإجراءات الجزائية مُتعاقبة سيّما التَّعديل الذي جاء به القانون 06-22 المؤرخ في 2006/12/20 والذي مدَّدَ صَلاحيات الضَّبطية القضائية ووسَّع دائرة إختصاصها [1] .

فتنص المادة 16 الفقرة 7 من قانون الإجراءات الجزائية على:"غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الوطنيةوالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال، ....، يمتد إختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

ويتميز هذا الإختصاص المكاني الوطني – على عكس الجرائم التقليدية – بأنه إختصاص عام يشمل جميع ضباط الشرطة القضائية وأعوانهم المُكَونيين لِسُلطة البحث والتحري في الجريمة الإلكترونية مهما كانت صِفة إنتمائهم الأصلية الدَّرك أو الشُّرطة أو الأمن العَسكري، ويكون عملهم تحت رقابة النائب العام لدى المجلس القضائي المختص إقليمياً ويُعلم وكيل الجمهورية بذلك في جميع الحالات طِبقا لمقتضيات الفقرة الأخيرة من المادة 16 من قانون الإجراءات الجزائية الجزائري [2] .

2. نطاق إختصاص سلطة البحث والتحري على المستوى الوطني (فلسطين) .

إذا كان الإختصاص الإقليمي للضبطية القضائية فيما يتعلق بالجرائم التقليدية يتحدد كأصل عام في نطاق العمل العادي، وذلك طبقا للمواد 19 ، 20 من قانون الإجراءات الجزائية الفلسطيني حيث يشرف النائب العام على مأموري الضبط القضائي ويخضعون لمراقبته فيما يتعلق بأعمال وظيفتهم وذلك حسب نص المادة 1/20 من نفس القانون، كذلك نص المادة 1/168 :" تختص

1.زيبحة زيدان ، **الجريمة المعلوماتية في التشريع الجزائري والدولي**،دار الهدى ،الجزائر،2011،ص115.

2.لهوة رابح ، المرجع السابق،ص71-72.

محاكم البداية لنظر جميع الجنايات وجرائم الجنح المتلازمة معها والمحالة إليها بموجب قرار الإتهام " .

وبالتالي فإن المشرع الفلسطيني الفلسطيني لسد الثغرة والفراغ القانوني أيضا قام بإنشاء وحدة متخصصة لِملاحقة ومُتابعة مرتكبي الجرائم الإلكترونية حيث نصت المادة 3 الفقرة 1 من القانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية على إنشاء هذه الوحدة بقولها : " تُنشأ وحدة متخصصة في جهاز الشرطة وَقُوى الأمن من مأموري الضبط القضائي تسمى وِحدة الجَرائم الإلكترونيّة، وتتولى النيابة العامة الإشراف القضائي عليها كل في دائرة إختصاصه ".

وبهذا نرى أن المشرع الفلسطيني قد اهتم بهذا النوع من الجرائم مع العلم أن نطاق الإختصاص يتحدد بما للسلطة الوطنية الفلسطينية من سلطة وسيطرة ذاتية على الأراضي التي بحوزتها أو التي تفرض أحكامها عليها أو التي تمارس مَهامها القضائية فوق أراضيها وضمن صلاحياتها، وذلك نتيجة للوضع السياسي القائم بها وأنها تحت سيطرة الإحتلال الإسرائيلي لبعض أراضيها والتي لاسلطة للقانون الفلسطيني عليها .

3 . نطاق إختصاص سلطة البحث والتحري على المستوى الدولي :

يمكن إرتكاب الجريمة الإلكترونية من أقصى بقاع الأرض بنفس سهولة إرتكابها من أقرب مكان ما يجعلها في أغلب صورها جرائم عبر وطنية نظراً لعنصر الإنترنت الذي أزال الحدود الجغرافية بين الدول، وأتاح للمجرم إتيان إجرامه دون أن يكون في مسرح الجريمة، ورجوعاً إلى أحكام الإتفاقية الأوروبية حول الجريمة المعلوماتية فقد اشارت المادة 22 منها إلى المبادئ التي يجب على الدول الأطراف إعتمادها لتحديد الإختصاص فيما يتعلق بالجرائم المنصوص عليها في هذه الإتفاقية وهذه المبادئ سنكتفي بذكرها فقط وهي:

1. مبدأ الإقليمية ، 2. مبدأ نسبية الإختصاص المكاني (الإقليم الإعتباري) ، 3. مبدأ الجنسية .

ولكنه من المناسب إعتماد مبدأ الإختصاص العالمي بشأن بعض صور الجرائم المعلوماتية التي يمتد ضررها ليُسيئ للإنسانية أجمع من الجرائم الأخلاقية، وأنه يجب الحذر من التوسُّع المُبالغ فيه في الإختصاص لأن ذلك يفضي إلى تنازع الإختصاص كنشر الإباحية على الإنترنت أو نشر الفيروسات وغيرها، مما يجعل جميع الدول مختصة بملاحقة فاعلها لمبدأ الوجود في كل مكان بما يثير تنازعا قد تستغرق إجراءات الوصول إلى حل بشأنه فترة كَفيلة بإفلات المجرم وهي مُجازفة بِفقدان الأدلة بإعتبار أن السرعة هي إحدى المَفاتيح الرئيسة لمكافحة الجريمة الإلكترونية أو يَنجر عنه تباطؤ في إجراءات المساعدة الدولية بين الدول المختصة بتمسُّك كل دولة في حقها بالملاحقة الجنائية [1] .

ثالثا : الإجراءات التقليدية (الكلاسيكية) والحديثة للكشف عن الجريمة الإلكترونية :

1. الإجراءات التقليدية للكشف عن الجريمة الإلكترونية :

في مجال المكافحة الإجرائية للجريمة المعلوماتية يتعين الإشارة إلى الدور الذي تلعبه الشرطة القضائية كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفة عامة ومن الجريمة الإلكترونية بصفة خاصة [2]، وبما أنها تتسم بالخفاء وتفتقد لأي أثر تقليدي لوقوعها في مسرح أفتراضي مما يعقد مهمة كشفها من قبل الضبطية القضائية التي إعتادت على تلقي الشكاوي والبلاغت والمراقبة المادية .

أ . تلقي الشكاوي والبلاغات :

الواقع أن الجريمة عادة تظل مَستترة ما لم يتم التبليغ عنها إلى السلطات المختصة إلا أن المَعضلة التي تواجه أجهزة الأمن هي أن هذه الجرائم لاتصل إلى عِلم السلطات المعنية

1.لهوة رابح ، المرجع السابق ، ص 66

2.أمحمدي بوزينة آمنه ، إجراءات التحري الخاصة في الجريمة المعلوماتية ، أعمال الملتقى الوطني لآليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر،29 مارس 2017 ، ص57 .

بالصورة العادية [1]، حيث إن أول مايُحرك الضبطية القضائية هو وجود بَلاغ أو شَكوى من شخص أو جهة معينة تفيد بوقوع جريمة إلكترونية، أو أن هُناك جريمة على وَشَكْ الوقوع وبعد أن يتلقى مأموري الضبط القضائي بلاغ أو شكوى حول وقوع جريمة إلكترونية يبدأ بالتحري والإستقصاء لمعرفة ملابسات الجريمة [2]، وتعد إحدى الوسائل التي تتحقق بها الضبطية القضائية من وقوع الجريمة، وهي من الواجبات المفروضة عليها في المادة 17 من قانون الإجراءات الجزائية الجزائري. ويعرف البلاغ بأنه :" إخطار بالجريمة يقدمه أي شخص " [3]، وتعرف الشكوى بأنها : " إجراء يباشره المجني عليه في جرائم محددة يعبر فيها عن إرادته الصريحة في تحريك الدعوى الجزائية لإثبات المسؤولية الجزائية وتوقيع العقوبة القانونية بالنسبة للمشكو منه"[4]، ويمكن أن تكون شفاهة أو كتابة وفور وصول البلاغ أو الشكوى يتعين على رجال الضبطية البحث عن الركن الشرعي أي معرفة إذا كان الفعل المرتكب يشكل جريمة أم لا وكذلك البحث عن المشتبه بهم وسماع أقوالهم، وندب الخبراء وسماع أقوال المتواجدين وكل ذلك يتم على وجه السرعة لأن عنصر السرعة يعد في غالب الأحيان العنصر الجوهري في البحث والتنقيب عن الجريمة الإلكترونية، لأن أي تأخير سيؤدي إلى ضياع الأدلة وتغيير في مسرح الجريمة كما أن التبليغ عن الجرائم من قبل الأفراد قد يكون إلزامي في بعض الأحيان لكل من وصل إليه العلم بوقوع جريمة، وكل ذلك تقوم به الأجهزة المختصة والمؤهلة لمكافحة هذا النوع من الإجرام [5] .

1.لهوة رابح ، المرجع السابق،ص109.

2.يوسف العفيفي ، الجرائم الإلكترونية في التشريع الفلسطيني (دراسة مقارنة) ،رسالة ماجستير – تخصص قانون عام جنائي ،بإشراف الدكتور أيمن عبد العال ، كلية اشريعة والقانون ،الجامعة الإسلامية ، غزة – فلسطين ،2013،ص99.

3.محمود نجيب حسني ،شرح قانون الإجراءات الجنائية ،دار النهضة العربية ، القاهرة،2013.ص435.

4.سماتي الطيب،حماية حقوق الضحية في الدعوى الجزائية في التشريع الجزائري ، ط1، البديع للنشر والخدمات الإجتماعية ، الجزائر ، 2008 ، ص42 .

5.يوسف العفيفي ، المرجع السابق، ص99 .

ب. المراقبة المادية :

ويقصد بها متابعة ورصد حركات وتنقلات و أقوال شخص أو أشخاص حكم بها أو شخاص مشبوهين تقتضي متطلبات الأمن مراقبتهم دون أن يشعروا بذلك، والمراقبة هي الأسلوب الأمثل للرؤية الفعلية والملاحظة البصرية لدى رجل هيئة الشرطة في الإستمرار بجمع المعلومات للوصول بها إلى الإستدلالات المؤدية لكشف الجريمة، وتنصبّ هذه المراقبة على الأشخاص والأموال وهكذا نجد أن إتفاقية الأمم المتحدة لمكافحة الجريمة المنطمة العابرة للحدود الوطنية المعتمدة من طرف الجمعية العامة يوم 2000/11/15 المصادق عليها بتحفظ بموجب المرسوم الرئاسي رقم 55/02 المؤرخ في 2002/02/05 وتضمنت في مادتها 1/20 هذه المراقبة بمناسبة التطرق لموضوع المراقبة الإلكترونية بإضافة عبارة (أو غيرها من أشكال المراقبة) .[1]

2 : الإجراءات الحديثة للكشف عن الجريمة الإلكترونية :

إن الإجراءات التقليدية لاتسمح بالكشف عن غموض الجريمة الإلكترونية لذا كان من اللازم تطوير أساليب كشف الجريمة الإكترونية وإستحداث وسائل جديدة، لأن الإجراءات التقليدية عجزت عن كشف التعقيد التقني الذي تَمتاز به الجريمة الإلكترونية .

أ. مراقبة الإتصالات الإلكترونية :

إن حَقّ الخصوصية هو من أهم الحُقوق التي أكدت عليه جميع المواثيق والدساتير، حيث تنص المادة 1/46 من الدستور الجزائري على : " لايجوز إنتهاك حرمة المواطن الخاصة وحرمة شرفه ويحميها القانون ، سرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة "، لذا فإن الإعتداء على حُرمة الحياة الخاصة من الجرائم التي يعاقب عليها القانون فلايَجوز لأي شخص أن يقوم بالمراقبة إلا إذا كان مُخوّلاً له من جهة مختصة، وفي إطار ذلك فقد أجاز المشرع الفلسطيني للنائب العام أو أحد مساعديه أن يقوم بمُراقبة المحادثات الشخصية وأن يسجلها ولكن

1.مجراب الذاودي ، أساليب البحث والتحري على ضوء القانون 22/06 المتضمن تعديل قانون الإجراءات الجزائية ، رسالة ماجستير ، كلية الحقوق ، بن عكنون ، جامعة الجزائر 1 ، 2012 ، ص14.

ذلك ضمن شروط وذلك من المادة 51 من قانون الإجراءات الجزائية الفلسطيني، كما ونصت المادة 34 فقرة (1، 2) من قانون الجرائم الإلكترونية بفلسطين رقم 10 لسنة 2018 على المراقبة الإلكترونية للبحث عن الدليل وذلك بإذن من قاضي الصلح أو النائب العام أو أحد مساعديه، وللرسالة حُرمة من لَحظة إرسالها إلى لَحظة وصولها للمرسل إليه، ففي المراسلات أو المكالمات الهاتفية أدق أسرار الناس وخباياهم، ومن هذا المنطلق نجد أن المشرع الجزائري كرّس حماية جزائية للمراسلات وعاقب لأول مرة إعتراض الإتصالات السلكية واللاسلكية دون إذن وذلك بموجب المادة 303 مكرر من قانون العقوبات، حيث أن هذه المراقبة تتم من خلال أجهزة وتقنيات خاصة ومعدة خصيصا لتعقب وإلتقاط مثل هذه الإتصالات والتنصت عليها من دون أن يشعر طرفا أو أطراف المحادثة بخضوع إتصالهم للمراقبة، حيث يتم وضع الخادم المعلوماتي لمزود الخدمات تحث المراقبة بإستخدام تقنيات وبرامج متطورة، وفي حال إذا ما أفضت المراقبة إلى إكتشاف جريمة معينة تم التحفظ السريع على مضمون البيانات المخزنة، وبهذا تخضع المراقبة الإلكترونية لرقابة القضاء فلا مجال لترك هذه العملية بين أيدي ضباط الشرطة القضائية تنفيذا وإشرافا، مع إحترام مدة المراقبة الإلكترونية والتي حددها المشرع الجزائري بأربعة أشهر قابلة للتجديد وذلك بالمادة 65 مكرر 7 الفقرة 2 من قانون الإجراءات الجزائية الجزائري، مع إحترام السر المهني لهذه العملية .

ب. التسرب الإلكتروني :

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الإلكترونية، وقد كانت إتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية سَبّاقة إلى إحتواء هذا الإجراء بنصها في المادة 20 على أساليب التحري الخاصة بما فيها التسرب الذي عبّرت عنه **بالأعمال المستترة**، أما المشرع الجزائري فقد تبنى بدوره هذا الإجراء **مباشرة** عُقب تصديق الدولة الجزائرية على إتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم (05/02) المؤرخ في 2002/02/02 بتحفظ وإتفاقية مكافحة

الفساد لسنة 2003 بتاريخ 2004/04/19. وقد ورد هذا النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون رقم (01/06) المتعلق بالوقاية من الفساد ومكافحته في عام 2006، الذي نص في المادة 56 من على أنه: " من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللُّجوء إلى التسليم المراقب و إتباع أساليب تحري خاصة كالترصُّد الإلكتروني والإختراق على النحو المناسب وبإذن من السلطة القضائية المختصة " . وبقي هذا الإجراء جامد إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون رقم (22/06) المؤرخ في 2006/12/20 أين تم تحديد معالم إجراء التسرب من خلال تعريفه وتحديد ضوابطه والآثار المترتبة عنه [1] .

1 . المقصود بالتسرب : تعرف المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري التسرب على أنه " **قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف** " .

يتبين لنا أن عملية التسرب عملية مُعقدة جدا تتطلب أحياناً من العون أو ضابط الشرطة القضائية المُساهمة المباشرة في نشاط الخَليّة الإجرامية التي تم التسرب إليها وإرتكاب أفعال محظورة قصد الوصول إلى المُبتغى ليس هذا فحسب بل أحاط المشرع الجزائري المسرّب بضمانات من أجل حمايته وحماية أسرنه أثناء عملية التسرب وبعد إنقضاؤها منها ماورد في المادة 65 مكرر 16 / 17 من قانون الإجراءات الجزائية الجزائري ، وبهذا لايجوز اللجوء إلى عملية التسرب إلا في الجرائم الخطيرة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65 مكرر [2] .

1.براهيمي جمال ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة دكتوراه – تخصص القانون ، بإشراف الأستاذ الدكتور إقلولي محمد ، كلية الحقوق والعلوم السياسية، جامعة مولود معمري ، تيزي وزو– الجزائر، 2018 ، ص 82-83

2. المرجع نفسه ، ص 84-85 .

وتبرز أهمية عملية التسرب الإلكتروني في كونه يرسي بنيان جنائي للنعلوماتية يحاصر النشاط الجرمي، إذ يستخدم هذا الإجراء من قبل العديد من مؤسسات الضبطية حول العالم ، حيث ترفع بعتاصرها وتجندهم مع الغير للدخول إلى المجالات الرقمية عبر حلقات النقاش وقاعات البحث والإتصال المباشر بإستخدام أسماء وصفات مستعارة ووهمية قصد البجث عن الجرائم ومرتكبيها وتقديمهم إلى المحكمة [1] .

2. الضوابط التي تحكم عملية التسرب في الجرائم الإلكترونية (الشروط الشكلية والموضوعية) :

إن إضفاء صفة المشروعية على إجراء معين مهما كان ماسّاً بحق الخصوصية لايتأتّى من خلال إباحة هذا الإجراء فقط وإنما تقتضي المشروعية إحاطة الإجراء بالضمانات اللازمة لصيانة هذا الحق في الخصوصية ليس فقط بالإستناد إلى قواعد القانون بل أيضا بالإستناد على قواعد مصدرها الأخلاق .

2 – 1 . الضوابط الإجرائية: تتلخص الضوابط العجرائية للتسرب الإلكتروني في الإذن القضائي وكل مايجب أن يتضمنه من أحكام إذ لايجوز للضابط أو عون الشرطة القضائية الخوص في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القصائية المختصة، وذلك حسب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري والمتمثلة في وكيل الجمهورية قبل إفتتاح التحقيق أو قاضي التحقيق بعد إفتتاحه، على أن تتم هذه العملية تحت رقابة الجهة الصادرة للإذن وذلك لتلافي تجاوزات وتعسف في إستعمال هذا الحق، ويجب أن يكون الإذن مكتوباً وإلا كان الإجراء باطلاً وذلك حسب المادة 65 مكرر 15 من نفس القانون، كما يجب أن يتضمن الإذن جملة من البيانات منها ذكر نوع

1. بن شهرة شول ، الحماية الجنائية للتجارة الإلكترونية ، أطروحة دكتوراه ، كلية الحقوق والعلوم السياسية،جامعة محمد خيضر ، بسكرة – الجزائر ، 2011 ، ص 216.

الجريمة محل عملية التسرب، تحديد المدة المطلوبة لها والتي لاتتجاوز أربعة اِشهر قابلة للتجديد حسب مقتضيات التحقيق[1]. ويجب أن يكون في هذه العملية السرية التامة وإلا يكون مصيرها الفشل إذا لم يتحقق هذا الشرط وهذا مانصت عليه المادة 65 مكرر16، هذا إلى جانب إحترام مبدأ نزاهة الأدلة في هذه العملية .

2 – 2 . الضوابط الموضوعية : وتحتوي هذه الضوابط على عنصرين وهما التسبيب والثاني يتعلق بتحديد نوع الجريمة .

العنصر الأول : التسبيب، وقد تضمنته المادة 65 مكرر 15 ويتمثل في المبررات والحجج التي أقنعت الجهات المختصة لِمنح الإذن بإجراء التسرب وكذلك الدوافع والأسباب التي جعلت ضابط الشرطة القضائية اللجوء إلى هذه العملية المتمثلة عادة في صرورة التحقيق .

العنصر الثاني: تحديد نوع الجريمة التي يتصب عليها الإذن بالتسرب، والتي لايجب أن تخرج عن نطاق الجرائم الخطيرة التي حددها المُشرع في المادة 65 مكرر 5، وذلك لسرعة إنتشارها وإمتداد آثارها خارج الحدود الوطنية وقائمة على التخطيط ومُجرميها أذكياء ويَمحون آثار الجريمة ويَطمسون معالمها مما يجعل الإستعانة بعملية التسرب مبررا لها [2] .

رابعا : الإجراءات التقليدية والحديثة لجمع الإستدلالات في الجريمة الإلكترونية :

1. الإجراءات التقليدية لجمع الإستدلالات في الجريمة الإلكترونية :

من المعلوم أن القواعد الإجرائية سنت لتواجه سلوكا ماديا قابلا للإدراك والمشاهدة، على خِلاف الجرائم الإلكترونية التي يَغيب فيها الدّليل المادي الممكن بالقراءة فهمه ويَحل محله نَبضات إلكترونية وبيانات رقَمية مُسجلة بكثافة بالِغة على دعائم أو وسائط تخزين مُمَغنطة سريعة الزوال.

1.براهيمي جمال ، **المرجع السابق** ، ص 85-86 .

2.**المرجع نفسه**، ص87 .

أ. سماع الأقوال : لضباط الشرطة القضائية في نطاق جمع الإستدلالات أن يَسمعوا أقوال من لَديهم معلومات عن الجريمة ومرتكبيها .

أ.1. أقوال المشتبه به المعلوماتي: إذا وقعت جريمة معلوماتية وإتصل بها علم الشرطة القضائية كان على هذه الأخيرة أن تمارس سلطاتها في الوجه المبين في القانون، بسماع أقوال من تحوم حولهم الشُّبهات بإرتكاب الجريمة الإلكترونية وهذا الإجراء له ذاتية في مجال التنقيب عن الجريمة الإلكترونية من حيث أحكام سماع أقوال المشتبه به المعلوماتي ومدى جواز جبره على الإدلاء بأقواله، فهذه الأقوال مصدر هام للمعلومات التي تقوم أعمال الإستدلال بجمعها وقد يكون من بين من تسمع أقوالهم على هذا النحو من تحيط به شبهات الجريمة حيث يشترط القانون أن تكون الأسئلة الموجهة إلى المشتبه به في نطاق جمع المعلومات مع تجنب الأسئلة النفصيلية التي تدخل في نطاق الإستجواب، كما أنه ليس للضبطية إكراه أحد على الحضور أمامه ولايستطيع إصدار أمر بإحضاره وأن إمتناعه لايشكل جريمة [1] .

أ.2. سماع أقوال الشاهد المعلوماتي : ينصرف هذا المصطلح إلى أؤلئك المتحصصون في المعلوماتية من فئة أصحاب الخبرة والتخصص في مجال نظم المعلوماتية، وهو يملكون في الغالب معلومات فيّمة حول الجريمة الإلكترونية الواقعة مثل متعهد الوصول، ومزود الخدمة، وناقل المعلومات، وكذلك القائمون على تشغيل الحاسبات الآلية و المحللون و مهندسي الصيانة والمبرمجون، ومديرو النظم وغيرهم، فالشاهد المعلوماتي تنحصر شهادته على الإدلاء بما يعلمه بشأن كيفية النفاذ إلى الأنظمة الإلكترونية محل الإشتباه وكيفية فك التشفير وغيرها، والمشرع الجزائري لم يجبر الشاهد المعلوماتي على الإدلاء بشهادته ماعدا إلزام مزودي الخدمات بالتعاون لجمع وتسجيل المعطيات المتعلقة بمحتو الإتصالت في حينها [2]. كما أن المشرع الفلسطيني

---

1. محمود نجيب حسني ، المرجع السابق ، ص 439 .

2. لهوة رابح ، المرجع السابق ، ص 157 .

خوّل لمأموري الضبط القضائي [1] أن يستمعوا لأقوال الشهود والمشتبه بهم ونص على عدم تحليف الشاهد اليمين وذلك طبقا للمادة 22 / 2 من قانون الإجراءات الجزائية الفلسطيني .

ب. المعاينة: يقصد بمعاينة مسرح الجريمة هو فحص مسرح الجريمة وكل مايرتبط بمرتكبيها وإثباته على حالته، ولاتتمتع معاينة مسرح الجريمة الإلكتروني بالأهمية التي تتمتع بها مسارح الجرائم التقليدية وذلك لأن الجرائم الإلكترونية لاتترك آثاراً مادية قي العالم الخارجي مثل التي تتركها الجرائم التقليدية، ومع ذلك فهناك خطوات على مأموري الضبط القضائي إتخاذها في معاينة مسرح الجريمة الإلكتروني، مثل تصوير الحاسوب والأجهزة المتصلة به في أوضاعها، مع تصوير الأجزاء الخلفية للحاسب الآلي وإثبات الأسلاك المتصلة بالجهاز وتسجيل تاريخ كل عملية تصوير، وإذا كان الحاسب الآلي قيد التشغيل يجل منع أي شخص من إستخدامه، وعدم العبث من قبل طاقم المعاينة في البيانات والمعلومات المخزنة عليه مثل سجل المحادثات وسلة المحذووفات، والتحفظ على المستندات الورقية الموجودة في مسرح الجريمة [2]. ونص المشرع الفلسطيني في المادة **22 / 2** من قانون الإجراءات الجزائية الفلسطيني على أنه : "وفقا لأحكام القانون على مأموري الضبط القضائي القيام بما يلي : " .... 2. إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق .... ". ، أما المشرع الجزائري فقد أوجب بموجب نص المادة **42** من قانون الإجراءات الجزائية الجزائري على ضابط الشرطة القضائية بعد تسلمه بلاغاً عن وقوع الجريمة أن يُبادر بالإنتقال إلى مكان وقوعها حتى يتسنى له معاينة الآثار المادية ويسهر على المحافظة عليها متى كانت في حالة تلبس (بالمعنى).

---

1. **مأموري الضبط القضائي** : أشخاص منحهم القانون صفة تعقب الجريمة بعد وقوعها بالبحث عن فاعليها ، والتي بموجبها يكون لهم حقوق ويفرض عليهم واجبات تتعلق بالدعوى الجزائية . للمزيد الإطلاع على : حسن صادق المرصفاوي ، أصول الإجراءات الجنائية ، منشأة المعارف ،الإسكندرية ، 2000 ، ص291 .

2. أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الإنترنت ،دار المطبوعات الجامعية ، الإسكندرية ، 2008،ص230-231 .

ويُحظر على أي شخص أن يقوم بالمعاينة اذا لم يكن من إختصاصه وهذا بنص المادة 43 من قانون الإجراءات الجزائية الجزائري، كما ويعاقب كل شخص يؤدي إلى تغيير أو إحداث شيء في مسرح الجريمة، والمعاينة في الجرائم الإلكترونية قد تتطلب معاينة العالم الإفتراضي ويستطيع عُضو سلطة التحقيق أو مأمور لضبط القضائي الإنتقال إلى العالم الإفتراضي من خلال حاسوبه الشخصي أو أحد مقاهي الإنترنت، أو من خلال جهاز الخبي، أو عن طريق اللجوء إلى مقر مزود الخدمة والذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة وهناك خطوات يجب إتباعها في معاينة العالم الإفتراضي وهي تصوير شاشة الحاسب الآلي، وعدم نقل أي مواد معلوماتية من مسرح الجريمة قبل التأكد من عدم إختراق الجهاز الذي قد يتسبب في محو البيانات المسجلة، ويجب تعطيل حركة الإتصالات والتحفظ على سلة المهملات وفي النهاية يجب الإستعانة بأهل الخبرة متى دعت الحاجة لذلك [1] .

والعقبة في ذلك أن الضبطية القضائية تتعامل مع بيئة مليئة بالنبضات الإلكترومغناطيسية والبيانات المخزنة داخل نظام شديد الحساسية ولاتتعامل مع أوراق أو أسلحة أو أشياء قابلة للتحريز وهذا مايؤكد أن القواعد الإجرائية التقليدية سنّت لتواجه سلوكا ماديا يرتكب بواسطة آلات وأدوات قابلة للربط والتحريز .

2 : الإجراءات الحديثة لجمع الإستدلالات في الجريمة الإلكترونية :

إن كانت الإجراءات التقليدية تتمتع بالشرعية وإحترام حقوق الأفراد إلا أنها تفتقد إلى الفعالية اللازمة لأداء المطلوب في البحث والتحري وهذا مادفع بالتشريعات الإجرائية الجنائية إلى إيجاد آليات تشابه تلك التي ارتكبت بها هذه الجريمة .

1. نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، 2013، ص218 .

أ. التفتيش في مجال الجريمة الإلكترونية .

يُعتبر التفتيش من أهم الأمور التي منحت للمحقق وذلك لمساسها بالحريات التي تكفلها الدّساتير عادة، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته والأحوال التي تجوز فبها مباشرته وشروط إتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن .

ويعرف التفتيش بأنه: إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة الشخص أو المسكن وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محددة، ولايجوز أن يقوم به إلا من خَوّله القانون صِفَة الضّبطية القضائية .

وهدف التفتيش هو البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الإستدلالات عنها أو حصول التحقيق بشأنها [1]، لذا فهو بحث عن الحقيقة في مستودع السر. وأن مفهوم التفتيش الذي يرد على الماديات هو مفهوم عام يمكن أن يستوعب التفتيش في العالم الإفتراضي نظراً لإتفاقه من حيث الهدف مع التفتيش التقليدي [2]، ونص المشرع الجزائري على الحالات التي يتم بها التفتيش وهي التلبس بالجريمة طبقا لنص المادة 44 ومايليها، حالة الإنابة القضائية طبقاً للمادة 138، ورضا صاحب المنزل طبقا للمادة 64 من قانون الإجراءات الجزائية الجزائري كما نص في المادة 64 من نفس القانون على: " لايجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضاء صريح .... " كما ويقرر وجوب إحترام الضمانات القانونية المقررة في

---

1. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، ط1، دارالفكر الجامعي ، الإسكندرية ، 2009،ص182-183.

2. مانع سلمى ، التفتيش كإجراء للتحقيق في الجرائم الإلكترونية ، مجلة العلوم الإنسانية ، جامعة محمد خيضر –بسكرة ، العدد 22 ، 2011، ص229.

المواد من 44 إلى 47 منه على أوضاع التفتيش [1]، ولذلك أصبحت التشريعات الحديثة تجيز التفتيش للأجهزة الإلكترونية لضبط المعلومات المتواجدة فيها والتي تفيد في كشف الحقيقة طبقا للمادة 1/19 من اتفاقية بودابست تلتزم الدول الأطراف بتخويل السلطات المختصة صلاحية التفتيش والولوج إلى البيانات النعلوماتية التي تم إحتواؤها .... " [2]، ونظرا لكون التفتيش يتضمن قيدا للحرية الفردية ويمثل إعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لِصحّته وهي ضوابط موضوعية وأخرى شكلية، ومنها سبب التفتيش وهو أن نكون بصدد جناية أو جنحة، ومحل التفتيش وهو الشيء الذي يقع عليه التفتيش للحصول على أدلة في الجرائم المعلوماتية، وكذلك إحترام السر المهني (ضوابط موضوعية) ، وهناك ضوابط شكلية ومنها صدور الإذن بالتفتيش من الجهة المختصة وذلك حسب المادة 44 من قانون الإجرات الجزائية الجزائري، والحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش مثل المتهم والقائم بإجراء التفتيش وشاهدين من أهل المتهم وشاهدين تنيبهم النيابة العامة، وتحريرمحضرالتفتيش، وكذلك مراعاة الميعاد القانوني لإجراء التفتيش، وأيضا نص المادة 5 من القانون 04 / 09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الذي نصت على التفتيش للمنظزمة المعلوماتية .

كما ونص المشرع الفلسطيني على التفتيش وإجراءاته وحدد الضوابط الموضوعية والشكلية له وذلك في الفصل الرابع في المواد من (39 إلى المادة 52) من قانون الإجراءات الجزائية الفلسطيني، وحدد الجهة المختصة التي تصدر إذن التفتيش وهي مذكرة التفتيش من قبل النيابة العامة حسب المادة 39 من قانون الإجراءات الجزائية الفلسطيني، وتوقيع مذكرات التفتيش طبقا للمادة 40، والميعاد القانوني لها طبقا للمادة 41، والإستعانة بالقوة العسكرية أو الشرطة أثناء

---

1. شنّة محمد ، محاضرات ألقيت على طلبة السنة الأولى ماستر في إجراءات البحث والتحري – تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية ، جامعة خنشلة ، 2017–2018، ص26 .

2. لهوة رابح ، المرجع السابق ، ص170 .

إجراء التفتيش إن لزم الأمر طبقا للمادة 49 وأن التفتيش لايتم إلا عن الأشياء الخاصة بالجريمة طبقا للمادة 51 وكذلك يترتب على عدم مراعاة الأحكام الخاصة بالتفتيش البطلان طبقا للمادة 52 من نفس القانون، وأيضا نص المادة 32 من قانون الجرائم الإلكترونية الفلسطيني لعلم 2018 الذي نص على التفتيش الخاص بالجرائم المعلوماتية وإجراءاتها .

ب. ضبط المعطيات المعلوماتية: يعتبر الضبط الأثر المباشر للتفتيش، وأن الضبط بحسب الأصل لايرد إلا على أشياء مادية فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر، كرفع البصمات مثلا عنها، وكذلك لاصعوبة في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه غير المشروع أو إتلافه بوسائل تقليدية كالكسر أو الحرق، ولكن تكمُن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وفي ضبط بيانات الكمبيوتر لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات [1] .

والمشرع الجزائري لسد ماتبقى من فراغ تشريعي في المنظومة التشريعية فإنه قام بموجب رقم 04/09 المؤرخ في 14 شعبان 1430الموافق 2009/8/5 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث نص في المادة **6** من على أنه: " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ....".

وبهذا نرى أن ضبط المعلومات في مجال الجرائم هي حَتميّة ولُزوميّة، حيث أن المشرع الجزائري

1.خالد ممدوح إبراهيم ، المرجع السابق ، ص274 .

غطّى مايتعلق بالضبط بموجب نص المادة السابقة مع مراعاة مواد الإجراءات الجزائية مثل مشتملات الضبط .

أما المشرع الفلسطيني فإنه نص على التصرف في الأشياء المضبوطة وكيفية تخزينها ومن يُصدر أمر الضبط وكيفية حِفظها في المواد من (72-76) من قانون الإجراءات الجزائية الفلسطيني، وأيضا نص المادتين(33،35)، من قانون رقم 10 لسنة 2018 [1] بشأن الجرائم الإلكترونية، حيث نص على كيفية الضبط والتحفظ للمعلومات وعلى الإحتياطات الضرورية للحفاظ على المضبوط مع تحرير قائمة بذلك وتبيان جهته المصدرة، وهي النيابة العامة ويتم ذلك الضبط على كامل نظام المعلومات، وإتخاذ الإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية وخصوصيتها محل التحفظ إلى حين صدور قرار من الجهان القضائية المتخصصة بشأنها .

وهناك إجراءات أخرى نكتفي بذكرها فقط وهي الإستعانة أو ندب الخبراء أو الخبرة التقنية في الجريمة الإلكترونية، وتجميع معطيات المرور في وقتها الفعلي، إنتاج المعطيات المعلوماتية، الحفظ والإفشاء العاجلان للمعطيات الإلكترونية وهذا الأخير تمت الإشارة إليه في لائحة الجمعية العامة لمنظمة الأمم المتحدة رقم (65-66) المؤرخة في 2001/1/22،المتعلقة بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية [2] .

الفرع الثاني : آليـــات الإثـــبات في مجـــال مكـــافحة الجـــريمة الإلكـــترونيـــة :

إن أهم الأهداف التي يسعى القضاء لتحقيقها هو إقامة العدل بين الناس وذلك عن طريق إعطاء كل ذي حق حقه، وإنصاف المظلوم فالقاضي هو الذي أنيطت به هذه المهمة حيث أنه يتحرى

1.قرار رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية والمعمول به والمطبق في دولة فلسطين والمنشور في الجريدة الرسمية الفلسطينية ممتاز عدد 16 بتاريخ 2018/5/3 .

2. براهيمي جمال ، المرجع السابق ، ص 67،99،108،112 .

وجه الحق في الدعوى من البيانات المعروضة عليه ويدريها ويُمحّصَها وإختيارالأقرب منها للحقيقة ولهذا السبب إعتُبر الإثبات من أهم المواضيع في القانون الجنائي .

أولا : تعريف الإثبات الجنائي: هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية مُتنازع عليها بين الخصوم [1]. وهو كل مايؤدي لإظهار الحقيقة ولأجل الحكم على المتهم في المسائل الجنائية ثبوت وقوع الجريمة في ذاتها [2] .

1. الإثبات الإلكتروني: فيقصد به إستخدام الوسائل المستخرجة من تقنيات الإتصالات الحديثة في إثبات التصرفات التي تُبرم بين الأفراد عن بعد من خلال الإنترنت أو غيره من الوسائل الحديثة [3] .

ثانيا : صور أدلة الإثبات الجنائي :

إن الجناة في سَعي دائم للتخلص من الوسائل والأساليب القديمة التي أوضحت قُصورها وعدم نَجاعَتِها في الكشف عن مرتكبيها وفي المقابل فقد أصبحت التعددية في تقنيات الكشف عن الجريمة بطرق مستحدثة، فقد استفادت وسائل التحقيق من التطور التكنولوجي خاصة من ناحية وجود أدلة مادية في مسرح الجريمة وأن الوسائل التقنية هي الأخرى لم تسلم من الإجرام مما ألزم السلطات المختصة إلى اللجوء لوسائل حديثة وأساليب علمية ليتم الكشف عن الدليل المعنوي في هذه الجرائم والتي يكون الحاسب الآلي أداة ارتكابها .

1.أحمد عزمي الحروب ، السندات الرسمية الإلكترونية ، ط1، دار الثقافة للنشر والتوزيع،عمان ،2010،ص25 .

2. نصر الدين مبروك ، محاضرات في الإثبات الجنائي ، دار هومة للطباعة والنشر والتوزيع ، الجزائر ، 2003،ص167 .

3. أحمد عزمي الحروب ، المرجع السابق ،ص46 .

1. البصمة الورائية: وتعرف بأنها الهوية الوراثية الأصلية الثابتة لكل إنسان التي تتعين بطريق التحليل الوراثي وتسمح بالتعريف على الأفراد بيقين شبه تام [1]. وللبصمة الوراثية خصائص تميزها لعل أهما هو مايعرف ب (DNA) [2]، حيث يتميز هذا الحمض النووي بقوة إثبات عالية في الظروف المختلفة للجريمة والتي عن طريقه يتم معرفة الجاني وفق طرق معينة، وأن نسبة النوافق بين البصمات لشخصين حسب دراسة بريطانية تكاد تكون معدومة وهناك بصمات الأصابع، وبصمات الأسنان، وبصمة الشفاه، وبصمة الأذن، وبصمة الصوت وغيرها التي تستخدم في الإثبات، وأن البصمة الوراثية ساعدت في تنوير العدالة في الكثير من الحقائق، فقد إعتبرت القاعدة الأساسية التي من خلالها يتم الفصل في مختلف الجرائم كجريمة السرقة والإغتصاب والقتل وذلك عن طريق كل ماتخلّف عن المجرم في مسرح الجريمة وساعدت أيضا في الكشف عن العديد من الجرائم التي نُسبت لِمجهولين حيث قامت العديد من المحاكم بإعادة فتح التحقيقات وتبرئة المئات وإدانة آخرون، حيث تعد من أدق الأدلة في قضايا النسب والإرث والأبوة، وأن الولايات المتحدة الأمريكية تقوم بتصنيف هذا الحمض لجميع المواليد مما يسهل عليها عملية تعيين الهوية للأشخاص في المستقبل البعيد ،وبهذا فإن البصمة الورائية تعد من الأساسيات في عملية إثبات الجرائم [3] .

1.عبد الرحمن أحمد الرفاعي ،البصمة الوراثية وأحكامها في الفقه الإسلامي والقانون الوضعي – دراسة مقارنة ، منشورات الحلبي الحقوقية ، لبنان ، 2013 ، ص47 .

2. **الحمض النووي:** هي إختصار للكلمة (Deoxyribo Nucleic Acid) أي الحامض النووي الريبي المنزوع الأوكسجين وهو عبارة عن مركب كيميائي معقد ذو وزن جزئي عالي لايمكن للكائن الحي الإستغناء عنه ، للمزيد أنظر : خليفة علي الكعبي ، البصمة الوراثية وأثرها على الأحكام الفقهية، ط1،دار النفائس للنشر والتوزيع ،الأردن ، 2003، ص21 .

3.إلهام بوالطمين ، الإثبات الجنائي في مجال الجرائم الإلكترونية ، مذكرة ماستر – تخصص جنائي أعمال ، بإشراف الأستاذ اليزيد بومعراف،كلية الحقوق والعلوم السياسية،جامعة العربي بن مهيدي– أم البواقي ، الجزائر، 2018،ص29–30.

2. الدليل الإلكتروني:

إن الجرائم الإلكترونية ذات طبيعة خاصة فإن الكشف عن هذا النوع من الجرائم يحتاج إلى أدلة تعيش في العالم الإفتراضي، حيث تستخدم فيها الطبيعة التقنية وتتمثل في الدليل الإلكتروني ويعد الوسيلة الوحيدة للإثبات في هذه الجرائم لذلك ستكون محور دراستنا في هذا الفرع حول **تعريف الدليل الإلكتروني ، خصائصه، أنواعه ، عناصره ، الإجراءات الحديثة والتقليدية في كيفية البحث والتحري عن الدليل الإلكتروني بإعتباره الأساس في عملية الإثبات في الجرائم الإلكترونية ، مراحله ، مشروعيته ، حجيته أمام القاضي الجزائي .**

2 . أ . تعريف الدليل الإلكتروني: عرف الدليل الإلكتروني بأنه : الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة، فهو الجزء المؤسس على الإستعانة بتقنية المعالجة التقنية للمعلومات والذي يؤدي إلى إقتناع قاضي الموضوع بثبوت إرتكاب شخص ما لجريمة عبر الإنترنت [1] .

كما **عرف كذلك:** معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عيها بإجراءات علمية وقانونية بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الإتصال، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة [2] .

1.فتحي محمد أنور عزت ، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية ،دار الفكر والقانون ، مصر ، 2010 ، ص235 .

2.خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت ، ط1،دار الثقافة للنشر والتوزيع،عمان، 2011، ص230 .

كما عرف : بأنه كل البيانات التي يمكن اعدادها أو تخزينها في شكل رقمي بحيث تمكن الكمبيوتر من إنجاز مهمة لها [1] .

ويعود **سبب تسميته بهذا الإسم** كون أن البيانات الموجودة داخل نظام الحاسب الآلي سواء أكانت كتابات أو صور أو رسومات أو نصوص فإنها تكون في شكل أرقام المتمثلة في الرقمين (1،0) ليقوم هذا النظام بتحويل ومعالجة هذه الأرقام اتظهر عند معالجتها في شكل مستند أو صورة كما يمكن الحصول عليه عن طريق مخرجات الطابعة على الورق كالتقارير والرسومات[2] .

من خلال التعاريف السابقة يتضح لنا أن هناك من ألحق تعريف الدليل الإلكتروني بتعريف برامج الحاسب الآلي رغم الإختلاف بينهما والذي يكمن في الوظيفة التي يؤديها كل واحد منها فاللدليل الإلكتروني دور أساسي في معرفة كيفية وقوع جرائم الإعتداء على النظم المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبيها أما برامج الحاسوب فتتجلى أهميتها بوضوح في العمليات التي تقوم بها داخل نظام الكمبوتر كتشغيله وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة فبدونها يصبح الكمبيوتر مجرد آلة صماء كغيره من الآلات [3] .

2 . ب . خصائص الدليل الإلكتروني: يتميز الدليل الإلكتروني عن غيره من الأدلة الجنائية بعدد من الخصائص:

1 . تتكون الأدلة الرقمية من بيانات ومعلومات إلكترونية غير مرئية وغير ملموسة بحيث يتطلب لإدراكها أجهزة ومعدات الحاسب الآلي واستعمال نظم برمجيات الكمبيوتر.

---

1. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية ، دار الجامعة العربية ، مصر 2015 ، ص123 .

2. إلهام بوالطمين ، المرجع السابق ، ص31 .

3. أشرف عبد القادر قنديل ، المرجع السابق ، ص124-125 .

2. يعد الدليل الرقمي دليل علمي، بحيث يتطلب منه توافر مجال تقني للتعامل معه فكل ماينطبق على الدليل العلمي ينطبق على الدليل الرقمي، وهذا مايؤكد مقولة في القانون المقارن، إن القانون مسعاه العدالة أم العلم فمسعاه الحقيقة .

3. يعد الدليل الرقمي من طبيعة تقنية وهذا مايميزه عن الدليل التقليدي، من حيث أن التقنية لاتنتج سِكّينا يتم من خلاله معرفة القاتل أو اعترافا مكتوبا أو مالا قدم كرشوة أو بصمة الإصبع، بل تنتج التقنية نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه .

4. صعوبة التخلص من الدليل الرقمي وهذا أهم مايميز هذا الدليل مقارنة مع الأدلة الأخرى .

5. إمكانية توظيف نشاط الجاني لمحو أو إزالة الدليل من الحاسب الآلي كدليل إدانة ضده لأن فعل الجاني بمحو الدليل يتم تسجيله في الحاسوب والذي يمكن الحصول عليه لاحقا كدليل للإدانة.

6. تمتاز بعض الأدلة الرقمية بسعة تخزين عالية بحيث يمكن لقرص صغير تخزين مكتبة كاملة كما يمكن لآلة تصوير تخزين آلاف الصور .

7. يمكّن الدليل الرقمي من تسجيل المعلومات عن الجاني ورصدها وتحليلها في الوقت نفسه، لأن الدليل الرقمي يمكن أن يقوم بتسديل تحركات الأفراد، فالبحث الجنائي يكون بسهولة من خلال الدليل الرقمي مقارنة بالأدلة المادية .

8. الدليل الرقمي مفهوم يحتوي التطور والتنوع لأن هذا المصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقمياً بحيث يكون بين هذه البيانات والجريمة رابطة أو علاقة من نوع ما تلك التي تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة [1] .

1.معمش زهية ، غانم نسيمة ، الإثبات الجنائي في الجرائم المعلوماتية ، مذكرة ماستر – تخصص قانون خاص ، بإشراف الأستاذ بن فردية محمد ، كاية الحقوق والعلوم السياسة – جامعة عبد الرحمن ميرة – بجاية ، 2013 ،ص48 .

2 . ج. أنواع الدليل الإلكتروني : تتمثل أنواعه في التي أعدت لتكون وسيلة إثبات والثاني التي لم تعد لتكون وسيلة إثبات .

أ . الأدلة التي أعدت لتكون وسيلة إثبات : –

1. السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتتمثل هذه السجلات في مخرجات الحاسوب التي لم يكن للأفراد يد في انشاؤها وكأمثلة عن ذلك: الهواتف، البطاقات البنكية، الفواتي.

2. السجلات التي تم حفظ جزء منها والجزء الآخر تم إتشاؤه بواسطة الحاسب الآلي ومثال ذلك: غرف المحادثة المتبادلة عبر الإنترنت .

ب . الأدلة التي لم تعد لتكون وسيلة إثبات: وقد أنشأ هذا النوع من الأدلة دون إرادة الفرد فهي عبارة عن آثار يتركها الجاني في مسرح الجريمة دون رغبته في وجودها ويطلق عليها تسمية البصمة الوراثية ويمكن تسميتها أيضا بالآثار المعلوماتية والرقمية، حيث أن هذا النوع من الأدلة لم يعد للحفظ لكن الوسائل الفنية الخاصة تمكّنت من ضبط هذه الأدلة ختى وإن مرّت عليها فترة زمنية طويلة وأمثلة ذلك: الإتصالات التي تتم عبر الإنترنت والمراسلات التي صدرت من الجاني أو تلقاها [1] .

2 . د . الإجراءات الحديثة والتقليدية في إستخلاص الدليل الإلكترني :

نص المشرع الجزائري على إجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وببعض الجرائم الأخرى وتتمثل في **التسرب واعتراض المراسلات** وكذلك من خلال القانون 04/09، استحداث إجرائين هما **المراقبة الإلكترونية وحفظ المعطيات،** وكلها تحدثنا عنها في مرحلة البحث والتحري عن الجريمة الإلكترونية وبيّنا دور القائمين بهذه المهمة للوصول إلى الحقيقة، مع العلم أنه يوجد هناك الإجراءات التقليدية التي

1. خالد عياد الحلبي ، المرجع السابق ، ص234–235 .

لم نتحدث عن البعض منها سنذكرها بشرح مبسط هنا وهي **الإعتراف و الخبرة في مجال إثبات الجريمة الإلكترونية أم الشهادة فتحدثنا عنها فيما سبق .**

- **إثبات الجريمة الإلكترونية بالإعتراف:**

الإعتراف (الإقرار): هو الإقرار على النفس بحرية وإدراك بارتكاب الأفعال المكونة للجريمة أو بعضها، دون تأثير أو إكراه وان إقرار المدعي بارتكابه وقائع الجريمة كلها أو بعضها وأنه هو الذي قام بهذا الفعل بنفسه وهذا ماأقره الفقه والقضاء. والإعتراف بجوهره هو تقرير أو إعلان وأن موضوعه هو الواقعة سبب الدعوى ونسبة هذه الواقعة إلى المتهم. وله شكلان

أ . الإقرار الشفوي ، **ب** . الإقرار المكتوب . وأنواعه هي : **1**. الإقرار القضائي ، **2** . الإقرار غير القضائي .

- **إثبات الجريمة الإلكترونية بالخبرة:**

تعد عملية الحصول على الأدلة الرقمية أمراً صعب الوصول إليه لما تتطلبه من مهارة عالية وخبرة كبيرة في مجال الحاسب الآلي ويرجع ذلك لتعدد أشكال وصور الجريمة الإلكترونية، ويرى المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الإلكترونية التي تتم عبر الإنترنت تتم عبر ثلاثة مراحل وهي:

1. تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة ، حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة ايحاد أي أثر له.

2. وفي مرحلة المراقبة فهناك فرضية تقول بأن المجرم لابد وأن يعود أو يَحُوم حول مسرح جريمته وتتعدد طرق مراقبة هذه الحواسيب من إستخدام برامج مراقبة واستخدام كاميرات مراقبة أو زرع فيروس من نوع حصان طِروادة .

3. ضبط الأجهزة المشتبه فيها وفحصها فحصا فنيا وشرعيا حيث يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام المعلوماتي المشتبه فيه بمكوناته المادية والبرمجية سعيا لإشتقاق الدليل الرقمي لتقديمه لجهة التحقيق أو الحكم [1] .

2. هـ. حجية الدليل الرقمي أمام القاضي الجزائي:

من شروط قبول الدليل الرقمي في الجريمة الإلكترونية ما يلي: أ . شرط مشروعية الدليل الرقمي في الجريمة الإلكترونية، ب. شرط مناقشة الدليل الرقمي، ج . شرط بلوغ الإقتناع القضائي درجة اليقين.

انطلاقاً من الشرط الأخير حيث أن القاضي يتمتع بسلط واسعة في تقديره لأدلة الإثبات الجنائي حتى وإن كان دليل رقمي فبإمكانه أن يتحرى الحقيقة عن طريق جمع الأدلة دون إلزامه بتفضيل مسيق لدليل معين حتى وإن تم تحديد مسبق لنوع الأدلة التي لايجوز الإثبات بغيرها أو كان الدليل دليلا علميا كالدليل الرقمي.

يجب على القاضي أن يصدر الحكم عن إقتناع يقيني بالأدلة المتحصلة من الوسائل الإلكترونية فاليقين هو وجود حقيقة يستنتجها القاضي الجنائي بواسطة المعرفة الحسية بعيداً عن كل غموض أو إحتمال وهذا عن طريق معاينة القاضي لهذه الوسائل وفَحصِها بالمعرفة الذهنية وإستقراء النتائج ليتأكد من الحقيقة فَشَرط اليقين في أحكام الإدانة شرطٌ عام سواء كانت الأدلة تقليدية أم مُستحدثة كالدليل الرقمي، لذلك لابد أن يكون الدليل الرقمي غير قابل للشّك، اذ أن هذا الأخير يفسر لصالح المتهم بناءاً على قاعدة أن الأصل في الإنسان البراءة، وإذا كان القاضي يستطيع الوصول إلى اليقين بالمعرفة الحسيَّة فإن الجَزْم بوقوع الجريمة الإلكترونية ونسبتها الى المتهم تحتاج من القاضي نوع آخر من المعرفة وهي المعرفة العلمية بالأمور

1.لبيض عادل ، نزلي بشرى ، إثبات الجريمة الإلكترونية ، مذكرة ماستر – تخصص قانون جنائي ، بإشراف الأستاذ خويلدي السعيد ، كلية الحقوق والعلوم السياية – جامعة قاصدي مرباح ، ورقلة ، 2018 ، ص55 –56 .

المعلوماتية خصوصا أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات، ويؤدي الجهل بهذه الأمور إلى التشكيك في قيمة الدليل الرقمي وبالتالي يقضي للحكم بالبراءة ويستفيد من هذا الشّكْ المُتهم المعلوماتي مما يؤدي إلى إفلات المحرمين من العدالة والقانون، ومن ثم يترتب على ثبوت التهمة بلوغ الإقتناع بالإدانة درجة اليقين من القاضي الجنائي لأن الإقتناع ثمرة اليقين [1] .

2. و . مشروعية وجود الدليل الإلكتروني :

تقتضي مشروعية وجود الدليل الرقمي أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثيات الجنائي.

- **المقصود بمشروعية الوجود:** أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الإستناد إليه في تكوين عقيدته، والمعيار في قبول الدليل الرقمي يتمثل في نظام الإثبات السائد في الدولة، فالنظام القانوني في الجزائر يعتمد نظام الإثبات الحر (حسب المادة 212 من قانون الإجراءات الجزائية) والمشرع الجزائري لانجده قد أفرد نصوصا خاصة قد تحظر على القاضي مقدماً قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، وهو أمر منطقي طالما أن المشرع يستند إلى مبدأ حرية الإثبات، حيث لم يتضمن قانون 04/09 أية أوضاع خاصة وترك الأمر للقواعد العامة ومنها أن الاصل في الأدلة مشروعية وجودها، ومن ثم فإن الدليل الرقمي سيكون مشروعاً من حيث الوجود إصطحابا للأصل، ومن جهة أخرى وطبقاً لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولاً في عملية الإثبات إلا إذا كان مشروعا ذلك أن القاضي

1. عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن ، دار الجامعة الجديدة ، الأسكندرية ، 2010،ص278-279 .

لايقدر إلا الدليل المقبول ولايكون كذلك إلا إذا كان مشروعا بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة [1] .

- **المقصود بمشروعية الحصول على الدليل** : إنه من المقرر أن الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة وإحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية ولايكون مشروعاً إلا إذا أجرى التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون، فمتى تم الحصول على الدليل بغير الطرق القانونية فلا يعتَدّ به مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، والحقيقة أن مشروعية الدليل تعد قيدا وخطاً فاصلاً بين حق الدول في توقيع العقاب لضمان أمن وإستقرار المجتمع من جهة، وبين ضمان حقوق الأفراد وحرياتهم من جهة أخرى [2] .

2. ز. عناصر إثبات الجريمة الإلكترونية: يوجد عناصر مختلفة لإقبات الجريمة الإلكترونية وهي :

1. إظهار الركن المادي للجرائم الإلكترونية: النشاط أو السلوك المادي يتطلب وجود بيئة رقمية وإتصال بالإنترنت ويتطلب معرفة هذا النشاط والشروع فيه ونتيجته، لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية والحقيقة يصعب الفصل بين العمل التحضيري والنشاط الإجرامي في نطاق الجرائم الإلكترونية حتى وإن كان القانون لايعاقب على الأعمال التحضيرية، إلا أنه

---

1. سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير– تخصص علوم جنائية ، بإشراف الأستاذ الدكتور زرارة صالحي الواسعة ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لحضر ، باتنة ، 2013 ، ص208.

2 علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والإنترنت ، ط1، عالم الكتب الحديثة ،الأردن ،2004ص186.

في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء فشراء برامج إختراق، وبرامج فيروسات ومعدات لِفك الشيفرات وكلمات المرور فمثل هذه الأشياء تمثل جريمة بحد ذاتها.

2. إظهار الركن المعنوي للجرائم الإلكترونية: نجده هنا من خلال العلم والإرادة فالمجرم المعلوماتي تارةً يستخدم الإرادة والتخطيط وتارةً يستخدم العلم من أجل تنفيذ الجريمة الإلكترونية.

3.تحديد وقت ومكان إرتكاب الجريمة الإلكترونية: فلو قام أحد المجرمين بإرتكاب جريمة في أمريكيا اللاتينية بإختراق جهاز خادم أحد البنوك في الإمارات وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة ؟ وبالتالي فإن النتيجة الإجرامية تثير في جرائم الإنترنت مسائل عدة .

4. علانية التحقيق : إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة ولهذا فإن في العلانية إطمئنان للمتهم والجمهور أن الإجراءات تمشي في الطريق السليم، وهي تختلف في التحقيق الإبتدائي تعتبر نسبية قاصرة على الخصوم في الدعوى الجنائية، بينما في المحاكمة علانية مطلقة .

2.ح. مراحل الدليل الإلكتروني (الرقمي) في الإثبات الجنائي في الجريمة الإلكترونية : يمر في أربعة مراحل وهي :

1. مرحلة التحريز: يتم بهذه المرحلة التحريز والإحتفاظ بالأدلة الموجودة عن طريق إرسالها المختبر الجنائي بطريقة لاتمكنها من الكسر أو التلف، كما يتم إلتقاط الصور الفوتوغرافية بواسطة الفيديو لجميع آثار الجريمة كالحواسب وملحقاتها والبصمات وكل الأشياء التي تفيد بإظهار الحقيقة والتي عثر عليها بمسرح الجريمة، وعليه يتم الحفاظ على النظام الرقمي وكذلك نسخ جميع البيانات على الحاسب إلى الحاسب الخاص بالمختبر الجنائي الرقمي.

2.مرحلة التحليل : يتم في هذه المرحلة القيام بالفحص والتحليل لجميع الآثار المرتبطة والمستمدة من مسرح الجريمة ويشمل ذلك القيم الرقمية لتحديد نوع الدليل .

3.مرحلة التقديم والعرض: يتم فيها تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة .

4. مرحلة القبول: إن مرحلة قبول الأدلة الجنائية الرقمية المستخرجة من الوسائل الإلكترونية في المحاكم يعتمد على المبادئ القانونية التي تنظم عملية الإثبات أمام تلك المحاكم أي أن سلطة القاضي الجنائي في تقدير أدلة الإثبات تختلف من دولة لأخرى، حسبما تخضع له قواعد الإثبات في كل دولة وهناك نظامين هما نظام الإثبات المحدد، ونظام الأدلة الإقناعية، أي أن مرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوف إلى مدى توافر هذا الدليل في النصوص القانونية .

إن المشرع الفلسطيني أخذ بالدليل الإلكتروني كأحد أدلة الإثبات في الجرائم الإلكترونية وذلك مانصت عليه المادة **(37) من قانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية** بقولها :" **يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلوما ت أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات** " ، كما أن نص المادة **(38)** تتحدث عن الدليل المتحصل عليه في الدول الأخرى وفقا للتعاون الدولي بأنها من أدلة الإثبات وذلك لأنها جرائم عابرة للقارت بقولها: " **تعتبر الأدلة المتحصل عليها بمعرفة الجهات المختصة أو جهات التحقيق من دول أخرى ، من أدلة الإثبات ، طالما أن الحصول عليها قد تم وفقا للإجراءات القانونية والقضائية للتعاون الدولي**".

وبهذا نكون فد أستعرضنا لأهم المواضيع من هذا المطلب وهي إجراءات التحري الخاصة في مجال مكافحة الجريمة الإلكترونية وبيّنا ماهي الجهات المخولة بالضبط القضائي وماهي الإجراءات الحديثة والتقليدية التي إنتهَجها المُشرعين الفلسطيني وَالجزائري في مجال البحث

والتحري كما بينا أن الدليل الإلكتروني يعتبر أساس الإثبات في الجريمة الإلكترونية وتبين لنا أن الدليل الإلكتروني في ظل أنظمة الإثبات مقبول ويؤخذ به بإعتباره كدليل إثبات جنائي وله قوته الثبوتية .

المطلب الثاني : مرحلة التحقيق والمحاكمة في الجرائم الإلكترونية :

الفرع الأول: مرحلة التحقيق في الجريمة الإلكترونية: التحقيق الإبتدائي من المهام التي قصرها المشرع على النيابة العامة وحدها، وذلك حرصا منه على ضمان سير التحقيق على أكمل وجه وصولا لكشف الحقيقة [1]، ولأن إجراءات التحقيق الإبتدائي يترتب عليها آثار تمس بالمواطنين وخصوصياتهم، وقد تصل في بعض الأحيان إلى تقييد حريتهم، وللنيابة العامة أن تقوم في تفويض بعض إختصاصاتها لمأموري الضبط القضائي بهدف إستيعاب الكَمّ الكبير من القضايا النى يُفترض على النيابة العامة إنجازُها، وتكمن أهمية مرحلة التحقيق في أنها مرحلة تحضيرية للمحاكمة فيتم فيها جمع الأدلة وتمحيصها تمهيدا للمحاكمة [2]، وتعتبر هي المرحلة الثانية بعد جمع الإستدلالات .

أولا : الجهة المختصة بالتحقيق الإبتدائي :

النيابة العامة هي صاحبة الإختصاص الأصيل في تحريك الدعوى الجزائية [3]، فهي وحدها من تملك مباشرة التحقيق الإبتدائي حيث يملك النائب العام أو أحد مساعديه تحريك الدعوى

1.أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، ط8 ، دار النهضة العربية ،القاهرة،2012،ص690 .

2.محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ،ط2،دار النهضة العربية،القاهرة،1998،ص614.

3.أحمد فتحي سرور ، المرجع السابق،ص.613

4.ممدوح خليل البحر،مبادئ قانون أصول المحاكمات الجزائية ، دار الثقافة ، عمان،1998 ،ص229.

الجزائية ولايشمل ذلك باقي أعضاء النيابة العامة [1]، وذلك لأنها تملك الخبرة والقدرة على مباشرة التحقيق في الجنايات والجنح، وتعتير من أخطر المراحل في الدعوى كونها تأتي قبل مرحلة المحاكمة وأن المحكمة التي ستفصل في النزاع المعروص أمامها تبني أحكامها في الغالب على النتائج التي أسفر عنها التحقيق الإبتدائي [2].

كما أكد على ذلك المشرع الفلسطيني في المادة الأولى من قانون الإجراءات الجزائية الفلسطيني حيث نصت على: " تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية [3]، ومباشرتها ولاتُقام من غيرها إلا في الأحوال المبينة في القانون " وأيضاً المادة 55/ 1 من نفس القانون على أنه: " تختص النيابة العامة دون غيرها بالتحقيق في الجرائم والتصرف فيها .... " .

والمشرع الجزائري أيضا في نص المادة الأولى من قانون الإجراءات الجزائية :" الدعوى العمومية لتطبيق العقوبات يحركها ويباشرها رجال القضاء أو الموظفون المعهود إلبهم بها بمقتضى القانون"، وأيصا نص المادة 1/129 من نفس القانون: " تباشر النيابة العامة الدعوى العمومية باسم المجتمع وتطالب بتطبيق القانون.... " .

ثانيا : تعيين قاضي التحقيق : -

بموجب القانون 06/22 المؤرخ في 2006/12/20، يتعين قاضي التحقيق بموجب قرار من وزير العدل بعد إستشارة المجلس الأعلى للقضاء من بين قضاة الجمهورية، وهذا رُجوعاً إلى

1.عبدالقادر جرادة،موسوعة الإجراءات الجزائية في التشريع الفلسطيني،المجلد الثاني،مكتبة آفاق ،غزة-فلسطين،2009،ص.420

2.**الدعوى الجزائية** : هي الوسيلة القانونية التي تملكها النيابة العامة للمطالبة بتوقيع العقاب على مرتكب الجريمة أمام القضاء .

نص المادة 50 من القانون الأساسي للقضاة ، وتكون مدة التعيين ثلاث سنوات وتنتهي مهام قاضي التحقيق بنفس الشكل الذي يتعين فيه أي يقرار من وزير العدل .

ثالثا : إختصاص قاضي التحقيق :

أ . **الإختصاص الشخصي** : الأصل أن قاضي التحقيق يحقق مع جميع الإشخاص إلا أن القانون المشرع الجزائري إستثنى بعض الفئات كالأحداث،العسكريين، ضباط الشرطة القضائية، قضاة الحكم والتحقيق، ووكلاء الجمهورية ومساعديهم، وقضاة المجالس القضائية ورؤساء المحاكم، وقضاة المحكمة العليا، والنواب العامون، وأعضاء الحكومة، والولاة، وكذلك يختص بالتحقيق مع مع جميع جرائم القانون العام سواء كانت جناية أو جنحة أو مخالفة .

ب . الإختصاص النوعي: يختص قاضي التحقيق بالتحقيق في جميع الجرائم ويكون ذلك وجوبي في الجنايات وجوازي في الجنح إذل كان هناك نص واختياري في المخالفات طبقا لنص المادة 66 من قانون الإجراءات الجزائية الجزائري .

ج . الإختصاص المحلي: حسب المادة 40 من قانون الإجراءات الجزائية الجزائري فإن :" يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص .... " ، وكذلك نص المادة 40 مكرر 2 من نفس القانون .

رابعا : سلطات قاضي التحقيق وحدود الدعوى الجنائية أمامه : القيام بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وبالتحري عن أدلة الإتهام وأدلة النفي في المادة 68 من قانون الإجراءات الجزائية الجزائري، كما يجوز لقاضي التحقيق أن يأمر بإجراء الفحص الطبي طبقا للمادة 68، ويتشق القاضي المكلف بِسَيْر التحقيق سَير إجراءات التحقيق وله وَحده الصفة في مسائل الرقابة القضائية والحبس المؤقت وإتخاذ أوامر التصرف في القضية طبقا للمادة 70 من نفس القانون ، ويستطيع القاضي سماع أقوال كل من يشير إليهم في

الشكوى باعتبارهم شهودا طبقا للمادة 73 من قانون الإجراءات الجزائية الجزائري، ويستطيع قاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها طبقا للمادة 79 من نفس القانون، وإستدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أخد أعوان القوة العمومية طبقا للمادة 88، ويجوز للقاضي استدعاء مترجم طبقا للمادة 91، وأيضا إصدار أمر بإحضار المتهم أو بإيداعه بالسجن أو بإلقاء القبض عليه حسب نص المادة 109 من قانون الإجراءات الجزائية الجزائري، وأيضا القيام بالإجراءات الحديثة والتقليدية للكشف عن الجريمة من تفتيش المتهم وتفتيش مسكن غير مسكن المتهم ومراقبة المحادثات السلكية واللاسلكية وضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات لدى مكاتب البريد والبرق [1] .

خامسا : سمات التي يتميز بها قاضي التحقيق بالنسبة للجريمة الإلكترونية :

بما أن الجريمة الإلكترونية مختلفة عن الجرائم الأخرى لذا لابد أن يحقق فيها قاضي مختص يتميز بما يلي: كأن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، وأن يميل إلى تصميم البرامج أكثر من تشغيلها ويجب معرفة الجديد عن هذه البرامج ، وأن يستطيع تصميم وتحليل البرامج أو أنظمة التشغيل بسرعة وأن يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على إختراق الشبكة وكل هذه الأمور لاتتوفر إلا لمن كان لديه إمكانات عقلية تزيد عن متوسط العام المألوف [2] .

سادسا: كيفية إتصال قاضي التحقيق بملف الدعوى الخاص بالجريمة الإلكترونية :

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية أو عن طريق شكوى جزائية مقدمة من المضرور، وهذا ماأكدته المادة 3/38 من قانون الإجراءات الجزائية الجزائري

1.بعرة سعيدة ، **المرجع السابق** ، ص88-89 .

2.**المرجع نفسه**، ص89.

على : " .... يختص في بالتحقيق في الحادث بناءا على طلب من وكيل الحمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67،73 ".

1. الطلب الإفتتاحي لإجراء التحقيق: يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية أن يطلب فتح التحقيق مالم ينص القانون على وجوب التحقيق في بعض الجنح، ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا ظهرت وقائع جديدة طبقا للمادة 3/67 من قانون الإجراءات الجزائية الجزائري، ويتقيد قاضي التحقيق بالوقائع دون الأشخاص طبقا للمادة 4،3/67 من نفس القانون، ولقاضي التحقيق سلطة الإتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه [1] .

2. الشكوى المصحوبة بإدعاء مدني : تنص المادة 72 من قانون الإجراءات الجزائية على: " يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص ". ويلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وحرصا منه أن يكون الإشراف على ملف الدعوى من طرف قاضي التحقيق كما أنه يستفيد من تتبع مجريات الدعوى بنفسه إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء إستعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية الكاذبة إذا ماخَسر دعواه ولهذا عليه أن يتأكد من أن إتهامه كان مبنياً على دليل قوي في الدعوى [2].

سابعا : إستئناف أوامر قاضي التحقيق :

1. النيابة العامة: لوكيل الجمهورية أو أحد مساعديه إستئناف جميع أوامر قاضي التحقيق طبقا للمادة 170 من قانون الإجراءات الجزائية الجزائري [3]، ويجوز للنائب العام الطعن في

---

1. مولود ديدان ، **قانون الإجراءات الجزائية** ، دار بلقيس،الجزائر،2014،ص37.

2.عبد الرحمن خلفي ، **الإجراءات الجزائية في التشريع الجزائري والمقارن** ، دار بلقيس للنشر، الجزائر،ص231-233.

3.نفس المرجع ، ص295.

أوامر قاضي التحقيق في ظرف 20 يوماً على ألا يكون لهذا الطعن أثر مُوقِف في حالة إستئناف أمر الإفراج في ظرف 20 يوما ويفرج على المتهم رغم إستئناف النائب العام مالم يكن **وكيل الجمهورية** [1] قد إستأنفه بالطبع ويجب أن يبلغ النائب العام عند إستئنافه الخصوم في الدعوى، وذلك خلال العشرين يوماً التالية لِصُدور الأمر حتى يكونو على بينة من أمرهم ولايفاجؤوا بقرار من **غرفة الإتهام** [2] في غير صالحهم [3] طبقاً لنص المادة 71 من نفس القانون.

2. إستئناف المتهم: لايجوز للمتهم إستئناف جميع أوامر قاضي التحقيق ويرفع الإستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف 24 ساعة من تبليغ الأمر إلى المتهم طبقا للمادة 168 من نفس القانون.

3. إستئناف المدعي المدني: أجاز المشرع الجزائري للمدعي المدني ذلك فيما يتعلق بحقوقه المدنية وبمفهوم المخالفة لايجوز له إستئناف الأوامر المتعلقة بالجانب الإجرائي مثل : الحبس المؤقت والإفراج والرقابة القضائية [4].

1.**وكيل الجمهورية** : هو ممثل النائب العام على مستوى المحكمة أي أنه يمثل النائب العام على مستوى محاكم الدرجة الأولى وهو يتلقى المحاضر والشكاوى والبلاغات ويباشر بنفسه أو يأمر بإتخاذ جميع الإجراءات اللازمة ،ويبلّغ الجهات القضائية بالتحقيق أو المحاكمة لكي تنظر فيها، كما أنه يبدي أمام الجهات القضائية مايراه لازما من طلبات وذلك كطرف في الدعوى مدعيا بإسم الحق العام، ويطعن عند الإقتضاء في القرارات التي تصدرها بكافة طرق الطعن القانونية وذلك سواء أكانت أحكاما أو أوامر قضائية، كما ويعمل على تنفيذ قرارات التحقيق وجهات الحكم ، ويكون أقل درجة من النائب العام .

2. **غرفة الإتهام** : وهي نختصة في إستئناف أوامر قاضي التحقيق وتوجد على مستوى كل مجلس قضائي وتتشكل من رئيس ومستشارين وجلسات غرفة الإتهام تكون سرية إلا أنه يجوز للأطراف ومحاميهم طلب حضور الجلسات وتقديم ملاحظاتهم، حيث أنها تنظر في صحة الإجراءات المرفوعة إليها وتقضي ببطلانها عند الإقتضاء وهي جهة تحقيق عليا أي أن غرفة التحقيق كدرجة ثانية في الجنايات وتتميز في السرعة في إتخاذ الإجراءات .

3.مولود ديدان، **المرجع السابق** ، ص78.

4.عبد الرحمن خلفي، **المرجع السابق** ، ص298 .

ويرفع الإستئناف خلال 3 أيام من تاريخ تبليغ الأمر المراد إستئنافه إلى المدعي المدني، وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا للمادة 3/173 من قانون الإجراءات الجزائية الجزائري [1] .

- **الفرع الثاني : مـرحـلـة الـمـحـاكـمـة :**

السلطة القضائية هي السلطة الوحيدة التي خولها القانون صلاحية الفصل في المنازعات التي تنشأ بين الأفراد وقد منح القانون هذه السلطة الإستقلالية التامة [2]، فهي تصدرأحكامها في الوقائع التي تنظر فيها دون تدخل سلطة أخرى [3]. وتختلف مرحلة المحاكمة أو كما سماها البعض مرحلة التحقيق النهائي عن مرحلة التحقيق الإبتدائي، فالسلطة التي تختص في مرحلة التحقيق الإبتدائي هي النيابة العامة أما السلطة القائمة على المحاكمة فهم قضاة المحاكم وتختلف المرحلتان في أن التحقيق الإبتدائي يهدف للبحث عن الأدلة التي تدين المتهم أو تبرئته وإحالة الدعوى إلى المحكمة المختصة أما المحكمة فإن عملها يكمن في الفصل في الدعوى القائمة أمامها والفصل فيها إما بالإدانة أو البراءة أو أي قرار آخر يصدر عنها مثل الإسقاط أو عدم الإختصاص [4] .

أولا : إختصاص المحكمة :

أ . **الإختصاص المحلي في الجريمة الإلكترونية:** طبقا لنص المادة 37 من قانون الإجراءات الجزائية الجزائري يتحدد الإختصاص المحلي للجريمة في ثلاث ضوابط أما

---

1. مولود ديدان، **المرجع السابق** ، ص79.

2, **نصت المادة 98 من القانون الأساسي الفلسطيني** المعدل لسنة 2003 على أنه : " القضاة مستقلون لاسلطة عليهم في قضائهم لغير القانون ، ولايجوز لأي سلطة التدخل في القضاء أو في شؤون العدالة .

3. سالم أحمد الكرد ،**أصول الإجراءات الجزائية في التشريع الفلسطيني**،ط3، كلية الشرطة الفلسطينية ،فلسطين – غزة،2008،ص:5

4.يوسف العفيفي،**المرجع السابق**،ص129.

بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبة في مُساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى لو حصل هذا القبض لسبب آخر، وفي نطاق الجرائم الإلكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بثّ الفَيروس وتتحقق النتيجة بتدمير المعلومات في مكان آخر. فإن الإختصاص ينعقد إما في مكان السلوك أو في مكان تحقق النتيجة، وقد وسع المشرع الجزائري من إختصاص المحاكم الجزائية بالنظر في الجرائم الإلكترونية أو المُتصلة بتكنولوجيا المعلومات إذا إرتكبت خارج الإقليم الوطني أو إذا كان مُرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي[1].

ب. الإختصاص النوعي في الجريمة الإلكترونية: يتحدد الإختصاص النوعي للمحكمة الفصل في القضية المعروضة عليها تبعاً لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأعمال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الإتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الإستثناءات المعروضة عليها في قوانين خاصة حسب المادة 328 من نفس القانون، ولأن الطبيعة التقنية للجرائم الإلكترونية معقدة نوعاً ما فقد خصّها المشرع مع بعض أنواع الجرائم المتعلقة بالمُتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والجرائم المُتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذ جعل الإختصاص ينعقد إلى دائرة إختصاص أخرى وهذا مانصت عليه المواد 37،40،329 من قانون الإجراءات الجزائية الجزائري إثر التعديل الذي جاء به التعديل القانون رقم 14/04 المؤرخ في

1. المادة 15 قانون رقم 04/09 ، ص4 .

2004/11/10 ، وأيضا نص على انشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى بعض المحاكم .

أما بالنسبة للإختصاص القضائي في القانون الفلسطيني، حيث يعتبر الإختصاص القضائي هو سلطة القاضي في مباشرة ولايته القضائية في نطاق معين ونص المشرع الفلسطيني في المادة 163 من قانون الإجراءات الجزائية الفلسطيني على أن: " يتعين الإختصاص بالمكان الذي وقعت فيه الجريمة، أو الذي يقيم فيه المتهم أو الذي يقبض عليه فيه ". وبالتالي فهو خطى مثل المشرع الجزائري في تحديد الإختصاص وبناها على ثلاثة ضوابط فالأولى هي مكان وقوع الجريمة والثانية مكان إقامة المتهم والثالثة المكان الذي يقبض فيه على المتهم، وأيضاً نص المادة 2 من قانون الجرائم الإلكترونية رقم 10 لسنة 2018 والتي تنص على الإختصاص القضائي في هذا النوع من الجرائم داخل أو خارج فلسطين أو إمتد أثرها داخل فلسطين أو إذا ارتكبت ضد مواطن فلسطيني أو ضد مصالح فلسطينية أو إرتكبت من قبل أشخاص أو أطراف أجنبية مقيمة داخل فلسطين أو شخص عديم جنسية موجود داخل فلسطين، حيث تختص المحاكم النظامية في فلسطين بذلك على الحدود الداخلة تحت سيطرة السلطة الفلسطينية .

ثانيا : تشكيلة المحكمة :-

تختلف تشكيلة المحكمة الجزائية بحسب حيث قسم الجنح الخاص بالجريمة الإلكترونية على مستوى المحكمة يتشكل من فرد ويُساعده كاتب ضبط وبحضور وكيل الجمهورية ومساعديه، أما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فبها ثلاثية أي تتشكل من رئيس ومستشارين إثنين بالإضافة كاتب ضبط وبحضور النائب العام أو أحد مساعديه، أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب

ضبط والنيابة العامة أو من يمثلها [1]. **أما بالنسبة لتشكيل المحاكم في فلسطين** فإنه يوجد محاكم صلح وبداية ومحكمة جنايات كبرى وغيرها من المحاكم وتتكون محاكم الصلح من قاض منفرد ويتولى الإشراف الإداري فيها [2]، ومحاكم البداية من رئيس وعدد كافٍ من القضاة [3]، وأما محكمة الجنايات الكبرى تتشكل من عدد كافٍ من الهيئات وتَتَشكَّل كُل هيئة من ثلاثة قضاة لاتقل درجتُهم عن قاضي بداية وتكون الرئاسة لأَقدمِهم [4] .

ثالثا : إجراءات المحاكمة : –

تَستهلّ المحكمة جلستها بالإعلان أولاً عن إفتتاحها بالقول بإسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغِه بالتُهمة المنسوبة إليه والمادة القانونية المتابعة بها، وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة [5] كذلك الأمر في اجراءات المحاكمة في التشريع الفلسطيني وأيضا نص المادة 303 من قانون الإجراءات الجزائية الفلسطيني [6]، وفي هذه الحالة وطبقا للمادة 339 مكرر6 المستحدثة بموجب الأمر 02/15 المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية الجزائري تتخذ المحكمة الإجراءات التالية: 1.ترك

1.بعرة سعيدة، المرجع السابق ، ص : 95 .

2. المادة 9 من قانون تشكيل المحاكم النظامية الفلسطينية رقم 5 لسنة 2001 .

3. المادة 13 من قانون تشكيل المحاكم النظامية الفلسطينية رقم 5 لسنة 2001 .

4. المادة 3 من قانون رقم 9 لسنة 2018 بشأن محكمة الجنايات الكبرى .

5.عبد الرحمن خلفي ، **المرجع السابق** ، ص321.

6. المادة 303 من قانون الإجراءات الجزائية الفلسطيني تنص على " 1. عندما تودع لائحة الإتهام لدى قلم المحكمة ، تنظم مذكرات بالحضور وتبلغ إلى النيابة العامة والمتهم والمدعي بالحق المدني والمسؤول عن الحق المدني 2. تتضمن مذكرة الحضور اليوم والساعة المقرر فيهما نظر الدعوى " .

المتهم حرا. ، 2 .إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 من نفس القانون ، 3. وضع المتهم في الحبس المؤقت ، مع الإشارة وأن هذه التدابير لاتقبل الإستئناف.

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المُثول الفردي فإنه يُساق بواسطة القوة العمومية لِحُضور الجلسة ويُخطره رَئيس الجلسة بأن له الحق في إختيار محامِ الدفاع عنه فإن طلب ذلك أمهله القاضي مهلة لاتقل عن ثلاثة أيام لتحضير دفاعه، ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها بالتفصيل من طرف القاضي ويعدها يقوم القاضي بسماع الشهود، وبعد الإنتهاء من التحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم إلتماسها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم إلتماسها، ويكون بعدها للنيابة العامة والمدعي حق الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة للمتهم ومحاميه، ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق للنطق بالحكم [1].

رابعا : القاواعد العامة للمحاكمة : -

1. علانية الجلسة: جل التشريعات تقرر بمبدأ علانية الجلسة وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الإطمئنان والشعور بالعدالة وهذا على التحقيق الأولي الذي يقوم به ضباط الشرطة القضائية كذا التحقيق الإبتدائي التي تقوم به جهات التحقيق فكلاهم يتم في سرية إلا أن العلانيى ليست في جميع الجلسات بل للقاضي سلطة تقديرية في إخراج القصر من الجلسة، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على

1. بعرة سعيدة، **المرجع السابق**، ص96 .

النظام العام والآداب العامة، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية ، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري .

2. شفوية المرافعات: فلأطراف الخصومة الحق في مناقشة كل دليل يُعرض بالجلسة حتى يتمكّن الجميع من الدّفاع عن نَفسِه ولايتم الإكتفاء بالتحقيقات الأولية والإبتدائية التي سبقت المحاكمة [1] .

3. حضور أطراف الخصومة: لايجوز إجراء المحاكمة دون حُضور أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة للنيابة العامة فهي جزء من تشكيلة المحكمة [2] .

4. تدوين التحقيق النهائي: لايمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دوره يتجسد في تدوين كل مايدور بالجلسة [3] .

وبالتالي فإن الجريمة الإلكترونية لم يخصص لها إجراءات المتابعة خاصة بها في كلا التشريعين الجزائري والفلسطيني وإنما تَخضع لنفس الإجراءات التقليدية، ولكن هناك بعض الإشكاليات التي تواجه المحاكمة في الجرائم الإلكترونية مثل إقتناع القاضي بالدليل الإلكتروني ومدى حجية الأدلة المستخلصة من الوسائل الإلكترونية، والإشكالية الثانية هي مشكلة تسليم المجرمين في حال كانت الجريمة الإلكترونية وقعت في أكثر من دولة كونها جرائم عابرة للحدود كما ذكرنا في الفصل الأول .

---

1. عبد الرحمن خلفي،**المرجع السابق**، ص323.

2.**المرجع نفسه**، ص 324.

3.أسامة عبد الله قايد ، **شرح قانون الإجراءات الجنائية**،دار النهضة العربية،القاهرة،2007،ص608.

وهناك مشكلة أخرى تتعلق باللغة المستخدمة في المحاكمة لذلك لابدّ لِتجاوزصعوبة اللغة الخاصّة في تقنية المعلومات من إيجاد هيئات قضائية تتمتع بالحد الأدنى من المعرفة بالحاسب الآلي وتقنياته ونظريات الجريمة التي يدخل فيها، مع وجود فريق يضم الخبرة الفنية التي تكون مهمته هنا توضيح الأبعاد الفنية للسلوكيات المرتكبة وتحديد أُطرها، وتقديم الرأي في المسألة الفنية التي تشكل على هيئة المحكمة بالإضافة إلى مهمة فريق الخبراء في إيجاد أَرضيّة إتصال بين الشهود والمُشتبه بهم الذين لاتوجد لديهم معرفة بلغة الحاسب الآلي والقضاة [1] .

المطلب الثالث: العقوبات المقررة لمرتكبي الجرائم الإلكترونية : -

الفرع الأول: العقوبات المقررة للجرائم الإلكترونية في التشريع الجزائري :

لقد نصت المادة 13 من الإتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبات المقررة نتيجة إرتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية، كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناءاً على مبدأ له مسائلة الشخص المعنوي الواردة في المادة 12 من نفس الإتفاقية .

وبإستمرار نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري من المادة 394 مكرر إلى 394 مكرر 7 نجد أن المشرع الجزائري قد تبنى هذا المبدأ في تقريره للجزاءات الواجبة على هذا النوع من الجرائم فسنّ عقوبات تُطبّق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي وذلك كما يلي :

1.أسامة المناعسة وآخرون ، **جرائم الحاسب الآلي والإنترنت (دراسة مقارنة)** ، ط1، دار وائل للنشر ، الأردن،2001،ص297.

أولا : العقوبات المطبقة على الشخص الطبيعي : -

1. العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات :

من خلال إستقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين أن وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يجدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات وسنجد سلم خطورة يتضمن ثلاث درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها جريمة الدخول والبقاء المشددة في الدرجة الثانية، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي للمعطيات [1] .

أ. جريمة الدخول والبقاء :

- **الدخول والبقاء بالغش: (الجريمة البسيطة)** العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50.0000 د.ج[2] إلى 100000د.ج غرامة (المادة (394 مكرر) .

- **الدخول والبقاء بالغش: (الجريمة المشددة)** تُضاعف العقوبة إذا ترتب على هذه الأفعال حذف أو تغيير للمعطيات فتكون العقوبة من 6 أشهر إلى سنتين وبغرامة من 50.000 إلى 150.000 د.ج إذا ترتب عن الدخول أو البقاء غير المشروع لنظام إشتغال المنطومة (المادة 394 مكرر/ 2،3) .

ب . جريمة التلاعب بالمعطيات: نصت عليها المادة 394 مكرر 1 من قانون العقوبات الجزائري بالحبس من 6 أشهر إلى 3 سنوات وعقوبة الغرامة من 500.000 إلى 2000.000 د.ج .

والملاحظ أن عقوبة التلاعب بالمعطيات تَفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لاتؤدي إلى أضرار تلحق بالمعطبات أو بنظام معالجتها وحتى في صورتها المشددة وإن أدت إلى نفس

1.آمال قارة ، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**،ط1،،دار هومة،2008،ص127.

2. د.ج : الدينار الجزائري وهي العملة المتداولة في الجمهورية الجزائرية الديمقراطية الشعبية .

النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي بينما لايتوافر هذا القصد لدى مرتكب جريمة الدخول والبقاء المشددة[1].

ج . جريمة التعامل في معطيات غير مشروعة : تعاقب المادة 394 مكرر 2 من قانون العقوبات الجزائري على جريمة التعامل فب معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبغرامة مالية من 1.000.000 د.ج إلى 5.000.000 د.ج، وبهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات – غير أن حدها الأدنى يقل عن تلك الجريمتين – وذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتيها (سنة أو سنتين) وتتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (3 سنوات) ، غير أن حدها الأدنى يقل عن الجريمتين معاً، لأن في جريمة الدخول أو البقاء البسيطة 3 أشهر في هذه الجريمة في صُورتها المشددة وفي جريمة التّلاعب هو 6 أشهر[2] .

ثانيا : العقوبات التكميلية : –

نصت المادة 394 مكرر 6 من قانون العقوبات الجزائري على العقوبات التكميلية، التييمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فبها مع الإحتفاظ بحقوق الغير حُسن النية بحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق الموافع التي تكون محلا لجريمة من الجرائم المعاقب علبها في هذا القسم، علاوة على إغلاق المحل أو مكان الإستعمال إذا كانت الجريمة فد إرتكبت بعلم مالكها ويستخلص من هذه المادة العقوبات التكميلية كالتالي :

1.نائلة قورة،**جرائم الحاسب الآلي الإقتصادية(دراسة نظرية وتطبيقية)**،منشورات الحلبي الحقوقية،بيروت،2005،ص228

2.محمد خليفة ، **الحماية الجنائية لمعطيات الحاسب الآلي في اقانون الجزائري والمقارن**، دار الجامعة الجديدة ، الإسكندرية،2008،ص219.

أ . مصادرة الأجهزة والوسائل والبرامج المستخدمة : مع الإحتفاظ بحقوق الغير حسن النية، وتجدر الإشارة هنا أن المُشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستتخدمة فقط، وأغفل مصادرة الوساءل الموجهة لإرتكاب الجريمة من المعطيات المُخزنة أو المعالجة أو المُرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 حيث أن عبارة " المستخدمة" الواردة في نص المادة 394 مكرر6 الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا مانصت عليه المادة 394 مكرر 6 من قانون العقوبات الجزائري التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجها للقيام بالجريمة [1] .

ب. إغلاق المواقع التي تكون محلا للجريمة من جرائم الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات[2]

ج. إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها وأضاف المشرع شرط علم المالك إذا كان على سبيل المثال الجاني مستأجرا للمحل المالك مؤجر له ، ويعلم خطورة الأفعال التي يقوم الجاني بها، كغلق نادي الإنترنت التي ترتكب فيه هذه الجرائم مع علم مالك أو مُسير النّادي بالأفعال الخطيرة التي يقوم بها زُبونَه، ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الإستغلال مما يطرح مشكلا في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل أو الأماكن كعقوبة تكميلية للشخص الطبيعي المسؤول جزائياً، ومن جهة

1.إبتسام موهوب،**جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري**،مذكرة ماستر – تخصص قانون جنائي للأعمال،تحت إشراف الأستاذة كوثر شريط، جامعة أم البواقي،2014،ص36.

2. أحسن بوسقيعة ، **الوجيز في القانون الجزائري الخاص**، الجزء الأول ، ط9، دار هومة ،الجزائر،2008،ص448.

أخرى لايمكننا الرجوع إلى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد مدى المدة، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي .

ثالثا : الظروف المشددة: نصت المادة 394 مكرر 2 –03 على ظرف التشديد في عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام إشتغال المنظومة.

- في الحالة الأولى تضاعفت العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر، وفي الحالة الثانية تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 د.ج إلى 150.000 د.ج

هذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع .

نصّت المادة 394 مكرر 3، على أن تضاعف العقوبات المقررة للجرائم الماسة بالمعالجة الآلية للمعطيات وذلك إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام .

رابعا : العقوبات المطبقة على الشخص المعنوي: يسأل الشحص المعنوي عن الجرائم الإلكترونية سواء بصفته فاعلا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد إرتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي علما أن نص المادة 18 مكرر من قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات المقررة له [1] .

1.فضيلة عاقلي،**المرجع السابق**،ص16.

خامسا: عقوبة جريمة الإتفاق الجنائي: تبنى المشرع الجزائري عقوبة الإتفاق الجنائي بنص المادة 394 مكرر 5، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية وعقوبة الإشتراك في الإتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد [1] .

سادسا: عقوبة الشُّروع: تبنى المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات الجزائري عقوبة الشروع فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحة ولاعقاب على الشروع في الجنح إلا بنص، ونصت المادة 394 مكرر7 من نفس القانون " يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها " .

الفرع الثاني : العقوبات المقررة للجرائم الإلكترونية في التشريع الفلسطيني :

لقد حاول المشرع الفلسطيني من خلال القوانين السابقة ملاحقة مرتكبي الجرائم الإلكترونية ومن الأمثلة عل ذلك نجد **قانون الإتصالات السلكية واللاسلكية رقم 3 لسنة 1996** والذي قام بالمعاقبة على الأفعال التي يأتيها مرتكب الجريمة الإلكترونية وذلك في المواد من (86 – 100) ، وأيضا هناك مشاريع قوانين ذات العلاقة بالجرائم الإلكترونية منها **مشروع قانون العقوبات الفسطيني لسنة 2010** والذي يتعرض وبشكل مباشر لهذه الجرائم كما ذكرناها سابقا في المواد من (379 – 396) لتلبي الحد الأدنى من متطلبات التجريم في مواجهة الجرائم الإلكترونية ، وأيصا **مشروع قانون الإنترنت والمعلوماتية لسنة 2002** والذي يضم 35 مادة ونص على المواد المتعلقة بالإنترنت في المواد (26 – 31)، ويمكن إعتباره إمتدادا وتكميلا لما بدأه المشرع في قانون الإتصالات السلكية واللاسلكية لعام 1996[2]، وأيضا **قانون**

---

1. فضيلة عاقلي، **المرجع السابق**، ،ص16.

2. عبد اللطيف ربايعة ، **الجرائم الإلكترونية** ،بحث مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين والمنعقد في جامعة النجاح الوطنية ،2016، ص13.

رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية في مواده من (44 – 46) والتي يبين فيها العقوبات ، إإلى أن جاء **قانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية** حيث وضع المشرع الفلسطيني قانونا خاصا يغطي الجريمة الإلكترونية من كافة نواحيها وقد نص هذا القانون على العقوبات المقررة للجريمة الإلكترونية كالتالي :

أولا : العقوبات الأصلية المطبقة على الشخص الطبيعي :

1. جريمة الدخول غير المشروع : عاقب المشرع الفلسطيني على هذه الجريمة في المادة 4 من قانون الجرائم الإلكترونية على كل من دخل دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاما أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المُصَرّحْ به ... " بالحبس وبغرامة لاتقل عن 200 دينار أردني ولاتزيد عن 1000 دينار أردني أو مايعادلها بالعملة المتداولة قانونا أو بكلتا العقوبتين، كما وشدد المشرع في حال إرتكب الفعل المذكور أعلاه على البيانات الحكومية حيث يعاقب بالحبس لمدة لاتقل عن 6 أشهر وبغرامة لاتقل عن 500 دينار أردني ولاتزيد عن 2000 دينار أردني أو مايعادلها بالعملة المتداولة أو بكلتا العقوبتين، وإذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة أ في النظام المعلوماتي أو حذفها أو إتلافها أو نقلها أو تغييرها ...، فإنه يعاقب بمدة لاتقل عن سنة وبغرامة لاتقل عن 1000 دينار أردني أ, مايعادلها بالعملة المتداولة أو بكلتا العقوبتين، واذا إرتكب الفعل السابق على البيانات الحكومية فإن المسرع شدد في ذلك فإنه يعاقب بالسجن مدة لاتزيد عن خمس سنوات وبغرامة لاتقل عن 3000 دينار أُردني أو مايعادلها بالعملة المتداولة قانونا.

2. جريمة التعطيل أو أعاقة الوصول والإعتراض والتنصت بغير حق : عاقب عليها المشرع الفلسطيني بالحبس أو بغرامة لاتقل عن 200 دينار أردني ولاتزيد عن 1000 دينار أردني وذلك حسب نص المادة 5 من قانون الجرائم الإلكترونية، وأما من عمل على إيقافها وتعطيلها

عن العمل وإتلاف البرامج وحذفها فإنه يعاقب بالسجن مدة لاتزيد عن 5 سنوات من 3000 – 5000 دينار أردني أو مايعادلها بالعملة المتداولة قانونا (المادة 6 من نفس القانون)، بينما التنصت والإعتراض يعاقب بالحبس مدة لاتقل عن سنة وبغرامة من 1000– 3000 دينار أردني (المادة 7 من نفس القانون) .

3.جريمة فك التشفير: يعاقب عليها بالحبس أو بغرامة من 200–1000 دينار أردني، ومن إستعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني يعاقب بالحبس مدة لاتقل عن سنة وبغرامة من 1000 – 3000 دينار أردني، (المادة 8 من نفس القانون).

4. جريمة الإنتفاع غير المشروع من خدمات الإتصال: يعاقب بالحبس مدة لاتقل عن 6 أشهر وبغرامة من 500 – 1000 دينار أردني، وإذا كان الإنتفاع قصد تحقيق الربح فشدد في ذلك بالحبس مدة لاتقل عن سنة وغرامة من 1000 – 3000 دينار أردني (المادة 9 من نفس القانون) .

5. جريمة عدم تقديم بيانات صحيحة للجهات المختصة عن هويته: يعاقب بالحبس وبغرامة من 200 إلى 1000 دينار أردني . (المادة 10 من نفس القانون) .

و. جربمة التزوير الإلكتروني: عاقب عليه المشرع بكل صوره وأشكاله سواء كان على المستندات أو التلاعب أو على التوقيع أو الوصول إلى أرقام أو بيانات أو زور بطاقة تعامل إلكترونية بالحبس أو بالسجن لمدة لاتقل عن 5 سنوات وذلك حسب التزوير وبغرامة تتاراوح مابين 200 – 5000 دينار أردني في جميع الحالات طبقا لنص المادة 11 ، 12 من نفس القانون .

6. جريمة السرقة الإلكترونية: عاقب عليها بالحبس مدة لاتقل عن سنة أو بالسجن وبغرامة من 1000 إلى 5000 دينار أردني (المادة 13،14 من نفس القانون) .

7. جريمة التهديد والإبتزاز عن طريق الشبكة الإلكترونية: يعاقب بالحبس مدة لاتقل عن سنة وبغرامة من 200 – 3000 دينارأردني (المادة 15 من نفس القانون) .

8. جريمة نشر وترويج للأعمال الإباحية والإستغلال الجنسي: عاقب المشرع عليها لمن فوق الثامنة عشر بالحبس لمدة لاتقل عن ثلاثة أشهر وبغرامة من 200 – 1000 دينار أردني، وشدد المشرع في ذلك إذا إرتكبت لمن لم يكتملو الثامنة عشر بالحبس مدة لاتقل عن سنتين وبغرامة من 1000 – 30000 دينار أردني وذلك طبقا للمادة 16 من نفس القانون .

9 . جريمة الإتجار بالبشر والأعضاء البشرية عبرالشبكة الإلكترونية: يعاقب بالسجن مدة لاتزيد عن 7 سنوات وبغرامة من 3000 – 5000 أو بالعملة المتداولة قانونا .

10. جريمة غسل الأموال وتمويل الإرهاب النافذ عبر الشبكة الإلكترونية: عاقب عليها بالحبس مدة لاتقل عن سنة وغرامة من 1000 إلى 3000 دينار أردني، أما تمويل الإرهاب بالسجن وبغرامة من 3000 – 5000 دينار أردني وذلك طبقا للمادة 18 من نفس القانون.

11. جريمة الإتجار وترويج المخدرات والمؤثرات العقلية عبر الشبكة الإلكترونية: عاقب عليها المشرع وشدّدَ في ذلك بالسجن مدة لاتقل عن 10 سنوات وبغرامة من 3000 – 5000 دينار أردني (المادة 19 من نفس القانون).

12.جريمة إنتهاك حقوق الملكية الفكرية عبر الشبكة الإلكترونية : بعاقب بالحبس مدة لاتزيد عن 6 أشهر وغرامة من 500 – 1000 (المادة 20 من نفس القانون) .

13. جريمة التدخل في الخصوصية والحياة الحاصة: يعاقب بالحبس مدة لاتقل عن سنة وبغرامة من 1000 إلى 3000 دينار أردني أو بالعملة المتداولة قانونا (المادة 22 من نفس االقانون).

14. جريمة إنشاء مواقع بقصد إدارة مشاريع مقامرة: يعاقب بالحبس مدة لاتقل عن 6 أشهر وبغرامة من 500 – 1000 دينار أردني (المادة 23 من نفس القانون) .

15. جريمة إثارة الكراهية العنصرية والدينية عبر الشبكة الإلكترونية: يعاقب بالحبس مدة لاتزيد عن سنة وبغرامة من 200 – 1000 دينار أردني (المادة 24 من نفس القانون) .

16. جريمة التشويه والتبرير لأعمال إبادة جماعية أو جرائم ضد الإنسانية عبر الشبكة الإلكترونية : يعاقب بالسجن مدة لاتقل عن 10 سنوات (المادة 25 من نفس القانون) .

ثانيا : العقوبات التكميلية: وضع المشرع الفلسطيني في قانون الجرائم الإلكترونية مثل المشرع الجزائري هذه العقوبات التكميلية وذلك بهدف المزيد من الردع من أجل أن يكسي العقوبة طبيعة مُزدوجة فهي عُقوبات وتَدابير بنفس الوقت، وذلك حسب نص المادة 50 من نفس القانون دون الإحلال بالعقوبات المنصوص عليها في هذا القانون وحقوق الغير حَسَنْ النية على المحكمة أن تُصدر قراراً يتضمن الآتي:

أ . مدة إغلاق المحل، وحجب الموقع الإلكتروني التي إرتكبت فيه، أو بواسطته تلك الجرائم حسب الأحوال.

ب. مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في إرتكاب أي من الجرائم المنصوص عليها ....).

ثالثا: الظروف المشددة: – لقد ضاعف المشرع الفلسطيني وشدد في بعض الجرائم الإلكترونية قصد الردع وذلك إذا قام الجاني بتكرار الجرائم المنصوص عليها في قانون الجرائم الإلكترونية سواء إرتكبت في فلسطين أو خارجها وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني وذلك حسب نص المادة 50، وأيضا ضاعف العقوبة إذا وقعت على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أوشيفرات أو صور يُدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها بما في ذلك الهيئات المحلية، أو إرتكابها من خلال

عصابة منظمة أو إستغلال من لم يكتمل الثامنة عشر، أو إذا وقعت الجريمة على نظام معلومات أو شبكة إلكترونية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التّقاصْ أو التّسوياتْ أو أي من الخدمات المصرفية من البنوك والشركات المالية وذلك حسب نص المادة 51 ، 52 م قانون الجرائم الإلكترونية .

وأيضا تضاعف العقوبة بمقدار الثلث إذا إرتكبت أي من الجرائم من قبل موظّف مستغلا صلاحياته أثناء تأدية عمله، كما وتضاعف العقوبة بمقدار الثلثين إذا إرتكبت من موظفي مزودي الخدمة أثناء تأدية عملهم أو بسببه أو سهل ذلك لغيره وذلك حسب المادة 27 من نفس القانون .

رابعا: العقوبات المطبقة على الشخص المعنوي: إذا إرتكب الشخص المعنوي بإسمه أو لحسابه إحدى الجرائم المنصوص عليها في هذا القرار يعاقب بغرامة من 5000 – 10.000 دينار أردني وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحلّه في حال الطبيعي التابع له ، وذلك حسب المادة 29 من نفس القانون .

خامسا: العقاب على جريمة الإتفاق والإشتراك والتحريض: عاقب عليها المشرع بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع سواء إشترك فيها أو تدخل أو حرّض على إرتكابها وذلك حسب المادة 45 من قانون الجرائم الإلكترونية وإذا ساعد فيها أو تدخل أو إتفق في إرتكاب جِناية أو جُنحة فيعاقب عليها بالعقوبات ذاتها المقررة للفاعل الأصلي وإن لم تقع الجريمة يعاقب بنصف العقوبة وذلك حسب المادة 48 من نفس القانون .

سادسا : العقاب على الشروع في الجريمة الإلكترونية : حسب نص المادة 49 من قانون الجرائم الإلكترونية فإنه "يعد مرتكبا جريمة الشروع كل من شرع في إرتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقرر لها " .

وبهذا نكون قد بيّنا إجراءات البحث والتحري عن الجريمة الإلكترونية وكيفية إثباتها ومرحلتي التحقيق الإبتدائي والنهائي بها والإجراءات التقليدية واالحديثة لها ، والعقوبات المقررة لمرتكبي الجرائم الإلكترونية في التشريعين الجزائري والفلسطيني .

*** إن العقوبات المقررة لمرتكبي الجرائم الإلكترونية في التشريع الفلسطيني قد أقرها القانون الخاص بالجرائم الإلكترونية رقم 10 لسنة 2018، وقمنا بتوظيفها بجهدنا الشخصي لأنه لايوجد لحد الآن دراسة سابقة عالجت هذه العقوبات، وأن هذا القانون قد سنّ في الآونة الأخيرة.**

المبحث الثاني : آليات مكافحة الجريمة الإلكترونية : -

إن مكافحة الجرائم الإلكترونية لن يكون له تأثير يذكر إلا إذا كان هناك تعاونا دوليا على أكبر قدر من التنسيق والتعاون، وأن مَجهودات الدول لن تأتي بأي نتيجة ملموسة للحد من هذا النوع من الجرائم، فتلك الجرائم لها طابع خاص تَتّسم بها لأنها جرائم عابرة للحدود فهي ترتكب داخل دولة وتمتد آثارها لعدة دول وعليه فإن الأساس الذي يرتكز عليه مجال مكافجة الجرائم الإلكترونية هو التعاون الدولي وتنسيق الجهود المبذولة بين كافة دول العالم لتكون هناك نتائج مهمة يمكن الإرتكاز عليها وتقويتها للحد من تلك الجرائم ذات النتائج البشعة على الدول [1]، وعليه فسوف يكون تناولنا لمكافحة الجرائم الإلكترونية من خلال التركيز على المواثيق والإتفاقيات الدولية وهذا في المطلب الأول، ومن ثم سنعرض الآليات الوطنية لمكافحة الجريمة الإلكترونية في الجزائر وفلسطين في المطلب الثاني، وأخيرا سنتطرق في المطلب الثالث إلى آليات وطرق الوقاية من الجريمة الإلكترونية وكيفية التصدي لها من خلال الجهود المبذولة .

1.منير الجنبيهي،محمد الجنبيهي، **جرائم الإنترنت والحاسب الآلي**، دار الفكر الجامعي ،الإسكندرية ،2005،ص 179.

المطلب الأول : الآليات الدولية لمكافحة الجريمة الإلكترونية : - (المواثيق والإتفاقيات الدولية) .

مع ظهور الإنترنت إزدادت الإعتداءات وأصبحت أكثر خطورة وإتساعا على ماكانت عليه في السابق، وهذا ماستدعى تدخل المشرع لوضع حد لهذا التنامي الخطير في ميدان الإجرام المعلوماتي وذلك عن طريق وضع نصوص قانونية موضوعية تجرم وتعاقب على الأفعال التي تشكل إعتداء أو تهديدا للأمن المعلوماتي، فمكافحة الجريمة المعلوماتية موضوعيا تعني دراسة القوانين التي صِيغت لسد الفراغ القانوني في مجال الإجرام المعلوماتي حتى لاتخرج الدول عن أهم مبدأ في قوانين العقوبات وهو مبدأ الشرعية [1]، وتظهر مكافحة الجريمة المعلوماتية في محتلف الإتفاقيات الدولية التي تم إبرامها في هذا المجال وعليه سوف نتطرق في هذا المطلب إلى الآليات الدولية والجهود الدولية والأمريكية والأوروبية والأمنية والتقنية والعربية المبذولة في مكافحة هذا النوع من الجرائم من خلال الإتفاقيات والمواثيق والمعاهدات الدولية والإقليمية المبرمة بين الدول .

أولا : الجهود الإقليمية والدولية لمكافحة الجريمة الإلكترونية :

1. الجهود الدولية للجريمة الإلكترونية :

إن الأمم المتحدة وأغلب المنظمات تُولي موضوع الجريمة المعلوماتية إهتماماً خاصاً، وهو الأمر الذي أفرز مجموعة من الإتفاقيات الدولية في هذا المجال، وهنا نشير إلى أهم الإتفاقيات التي تتناول هذا النوع من الجرائم :

1. إتفاقية برن ، 2 . معاهدة الويبو ، 3. إتفاقية تريبس .

1.بدري فيصل ، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي** ، أطروحة دكتوراه – تخصص قانون عام ،بإشراف البروفيسور البقيرات عبد القادر ، كلية الحقوق ، جامعة الجزائر 1 – بن يوسف بن خدة – ، 2018،ص12.

1. **إتفاقية برن** [1] : تعتبر إتفاقية برن التي تم التوقيع عليها في عام 1971في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الإتفاقية 120 دولة، وتعد المادة التاسعة من تلك الإتفاقية هي الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق إسْتئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان وتم تعديل هذه الإتفاقية في 1979 وإزداد عدد الدول فيها إلى 140 دولة في 1999 [2]، وبموجب إتفاقية برن الدولية تتمتع برامج الحاسب الآلي سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمالاً أدبية وفقاً لما جاء فيها، وأن إتفاقية برِن تقوم على مجموعة من المبادى التي تحدد نطاق الحماية الواجبة وأسلوب تطبيقها وهذه المبادئ لاتتغير مع التعديلات أو البروتوكولات التي قد تدخل على الإتفاقية وهي:

أ. مبدأ المعاملة الوطنية: وهو أن تتمتع كافة المصنفات الخاضعة لحماية الإتفاقية في إقليم دوبة عو بنفس الحماية التي تتمتع بها المصنفات الوطنية لهذه الأخيرة لدى الدولة الأخرى الطرف في الإتفاقية.

ب. الحد الأدنى للحماية: يعد هذا المبدأ محاولة من واضعي الإتفاقية لمواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة [3] .

---

1. المرسوم الرئاسي رقم 341/79 المؤرخ في 1997/09/13 المتضمن إنضمام الجزائر مع التحفظ إلى إتفاقية برن المؤرخة في 1869/09/09 والمتممة في باريس 1909/05/04 والمعدلة في 1997/09/28،ج.ر رقم 01 المؤرخة في 1997/09/14 ، وكذلك فلسطين إنضمت إليها في 1933 .

2.بن الأخضر محمد، **جرائم الكمبيوتر والإنترنت** ، مذكرة لنيل رتبة ضابط ،المدرسة العليا للشرطة ، بن عكنون،2008،ص48.

3.بدري فيصل ، **المرجع السابق**،ص15-16 .

وأن إتفاقية برن لم تعالج انشر الإلكتروني لأن آخر تعديل لها كان سنة 1971 وكان قبل حدوث ثورة الإتصالات والمعلومات وظهور الإنترنت، لذلك فهي قاصرة على تقديم حلول للمشكلات القانونية الناتجة عن المصنفات المنشورة على الإنترنت [1].

2 . معاهدات الويبو: إن معاهدات الويبو تنقسم إلى ثلاث معاهدات وهي :

أ. معاهدة الويبو بشأن حقوق المؤلف: تم التوقيع على تلك المعاهدة في 20 ديسمبر 1996 وتتكون من ثمانية عشر مادة، وتبدأ بالديباجة ثم تتناول علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق حماية حق المؤلف كحق التوزيع والتأجير ونقل المصنف إلى الجمهور والإلتزامات المتعلقة بالتدابير التكنولوجية والإلتزامات المتعلقة بالمعلومات الضرورية المتعلقة بالحقوق ومدة حماية المصنفات والإستثناءات والتقييدات على تلك الحقوق وكذلك الحقوق والإلتزامات المترتبة على المعاهدة ودخول المعاهدة حيز التنفيذ الفعلي وأخيرا تعرضت المعاهدة إلى للتحفظ عليها ونقضها سواء من أطرافها أو دول غير موقعة ولغاتها [2]

ب. معاهدة الويبو بشأن الأداء والتسجيل الصوتي : تم التوقيع عليها في 20 ديسمبر 1996 وتقع تلك المعاهدة في أربع فصول يتناول الفصل الأول منها الأحكام العامة وعلاقة تلك المعاهدة بالمعاهدات والإتفاقيات الدولية الإخرى والتعريف والمستفيدون من الحماية بناءا على تلك المعاهدة وكذلك المعاملة الوطنية، أما الفصل الثاني فيتناول حقوق فناني الأداء معنويا وماليا وحقوق الإستنساخ والتوزيع والتأجير وحق إتاحة الأداء المُثبت، أما الفصل الثالث فيتناول حقوق المنتجين كحق الإستنساخ والتوزيع والتأجير وحق إتاحة التسجيلات الصوتية، أما الفصل الرابع فيتناول الحق في مكافأة مقابل الإذاعة أو النقل إلى الجمهور والتقييدات والإستثناءات

1.بدري فيصل،**المرجع السابق**، ص17 .

2.منير وممدوح الجنبيهي ، **المرجع السابق** ، ص202 .

على هذا الحق ومدة الحماية والإلتزامات المتعلقة بالتدابير التكنولوجية والإلتزامات المتعلقة بالمعلومات الضرورية لإدارة الحقوق وأخيراً تم التعرض للإجراءات الشكلية [1] .

ج. معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة: وتبدأ تلك الإتفاقية بمقدمة ثم تتناول الطابع القانوني للمعاهدتين الجديدتين وعلاقتهما بالمعاهدات الدولية الأخرى، ثم تتناول اللإتفاقية دول الأعمال الرقمي والمعاهدات الجديدة ثم تتعرض الإتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديدتين و أخيراً أعمال المتابعة بعد المؤتمر الديبلوماسي [2] .

3. إتفاقية تريبس: هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع إنتشار عمليات السطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية، وتلك الإتفاقية تم التوقيع عليها عام 1994 وقد عالج موقعو الإتفاقية العامة للتعريفات والتجارة (الجات) حقوق الملكية الفكرية بتوقيع إتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية TRIPS، فربطوا بذلك بين المعايير الدولية والمعايير المحلية وتتضمن تلك الإتفاقية العديد من الإجراءات الفعالة لردع الإعتداءات على حقوق الملكية الفكرية [3] .

2. الجهود الإقليمية لمكافحة الجريمة الإلكترونية :

تبرز الجهود الإقليمية في مواجهة الجريمة الإلكترونية في المساعي التي قام بها المجلس الأوروبي، بالإضافة إلى الجهود التي تبذلها جامعة الدول العربية، وسنتناول في ذلك :

1.منير وممدوح الجنبيهي ، **المرجع السابق** ، ص204.

2.**المرجع نفسه** ، ص205.

3. **المرجع نفسه**،ص201.

أ. إتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام 2001 :

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات، وبعد التوقيع على تلك المعاهدة التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت والتي إنتقلت من مرحلة إبتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب والأعم من الحلات ودون أي غرض إجرامي إلة مرخلة جديدة يقوم بها محترفون على أعلى درجة من التخصص وتتمصل في الإحتيال والإختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات الكثيرين من روّاد شبكة الإنترنت للخطر، وبعد التوقيع على هذه الإتفاقية من المسؤولين في الدول الأوروبية إضافة إلى أمريكا وكندا واليابان وجنوب أفريقيا وهو نتاج مباحثات ومفاوضات إستغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيفة النهائية حتى يتم التوقيع عليها من جميع الأطراف [1]، وتكونت هذه الإتفاقية من 48 مادة وأكدت الغتفاقية على الحاجة إلى إتخاذ تدابير تشريعية لمكافحة جرائم الكمبوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء امكافحة الجريمة المعلوماتية واعتبرت مرجعا لايُستهان به في مجال محاربة الإجرام السيبري، ولقد ركزت الإتفاقية على ثلاثة عناصر أساساية:

1. يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية .

2. يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية أو النصوص الإجرائية .

---

1. منير ومحمد الجنبيهي،**المرجع السابق** ، ص182 .

3. يتمثل في أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم والإنطلاق مما أنجز من جهود دولية وإقليمية في هذا المجال . وكان ذلك مجسدا في مواد الإتفاقية المُوزّعة على أربعة فصول [1].

ب. القانون العربي النموذجي الإسترشادي لمكافحة الجريمة المعلوماتية [2] :

يعد القانون العربي النموذجي لمكافحة جرائم الكمبيوتر خطوة فعالة في مجال مكافحة الجريمة المعلوماتية ومسلك منطقي وضروري لابد من إتخاذه، لأن المحتمعات العربية ليست بمنأى عن هذه الجرائم الجديدة، وهو ثمرة عمل مُشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعا بخصوص مكافحة الجرائم المعلوماتية [3].

لقد إعتمدت جامعة الدول العربية ماسُمِيَ بقانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات ومافي حكمها نسبة إلى مقدم هذا المُقترح وهو دولة الإمارات العربية المتحدة[4]، وتم إعتماد هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 495- د19 2003/10/8 ، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 2004/21 .

1.بدري فيصل ، **المرجع السابق** ، ص29.

2. تم إعداد هذا القانون من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لوزراء الداخلية العرب ، حيث جرى إقراره بوصفه منهجا إسترشاديا للمشرع الوطني عند إعداد تشريع يتعلق بالجرائم المعلوماتية .

3.سعيداني نعيم ، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري** ، مذكرة ماجستير – تخصص علوم جنائية ، بإشراف الدكتور زرارة صالحي الواسعة ، جامعة باتنة ، 2013، ص86.

4.أمير يوسف فرج ، **الجريمة الإلكترونية والمعلوماتية والحهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت** ، مكتبة الوفاء القانونية ، الإسكندرية ، 2011،ص354.

يمنع قانون دولة الإمارات العربية المتحدة نسخ برامج الكمبيوتر بدون إذن وكل من يقبض عليه متلبسا بقرصنة البرامج سيخضع هو وشركته للمحاكمة بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب القانون غرامة مالية بالإضافة إلى مصادرة المُنتجات والحبس لمدة تصل إلى 3 سنوات [1].

كما نصت المادة 7 من القانون العربي النموذجي على معاقبة كل من زَوّر المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو على أسطوانة مُمَغنطة أو غيرها من الوسائل [2].

وهناك من الجرائم المدرجة ضمن **القانون العربي النموذجي** سنكتفي بذكرها فقط والتي عالجها وعاقب عليها هذا القانون وهي : **جريمة غسل الأموال عبر الوسائل الإلكترونية (المادة 19)، جريمة التزوير المعلوماتي (المادة 4)، جريمة إختراق النظم المعلوماتية (المادة)، جريمة السرقة المعلوماتية وعاقب عليها في (المادة 14) .**

ثانيا : التعاون الأمني الدولي في مكافحة الجريمة الإلكترونية :

نتيجة للتطور المذهل والملموس في الإتصالات وتكنولوجيا المعلومات وظهور الإنترنت والإنتشار الواسع والسريع لها أدى إلى ظهورأشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي من الجرائم الإلكترونية [3]، التي باتت تشكل خَطراً لا على سريّة النظم الحاسوبية فقط بل تعدت إلى أمن البُنى الأساسية الحَرِجَة ومع تَميزها بالعالميّة فإن

1.ممدوح ومنير الجنبيهي ، **المرجع السابق**، ص206 .

2.عبد الفتاح بيومي حجازي ، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي** ، دراسة متعمقة في القانون المعلوماتي ، دار الكتب القانونية ، مصر ، 2007، ص175.

3.الغافري حسين بن سعيد ، **الجهود الدولية في مجال جرائم الإنترنت** ، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي خلا إجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية الأول، المنعقد بالأمانة العامة بالرياض خلال الفترة 4-2004/4/5 ،ص3.

مكافحتها لاتتحقق إلا بوجود تعاون دولي على المستوى الإجرامي الجنائي بحيث يُسمح بالإتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها، ويُشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلال أجهزة الشرطة في الدول المحتلفة خاصة فيما يتعلف بتبادل المعلومات المتعلفة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفَارّين من وجه العدالة [1].

- **التعاون الأمني الدولي في مكافحة الجريمة الإلكترونية :**

1. جهود المنظمة الدولية للشرطة الجنائية (الإنتربول) في مكافحة الجريمة الإلكترونية:

إن البدايات الأولية للتعاون الدولي الشرطي ترجع إلى عام 1904 عندما تم إبرام الإتفاقية الدولية الخاصة بمكافحة الرّقيق الأبيض بتاريخ 1904/5/18، والتي نصت في مادتها الأولى على" تتعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة بإستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة " [2].

لم تمر سنة على هذه الإتفاقية إلا وكانت سبعة من الدول المتعافدة تنشئ مثل تلك الأجهزة وتتبادل من خلالها المعلومات والبيانات الخاصة بإستخدام النساء لغرض الدعارة في الخارج من أجل القضاء على هذه الجريمة في أقاليمها، وبعد ذلك أخذ التعاون الشرطي الدولي يأخذ صور المؤتمرات الدولية أولها وأسبقها تاريخياً كان مؤتمر موناكو (14-1914/4/18) والذي وضع رجال الشرطة والقضاء والقانون من 14 دولة وذلك لمناقشة ووضع أُسس التعاون

1.الغافري حسين بن سعيد ، **المرجع السابق** ، ص6.

2. **المرجع نفسه** ص6 .

الدولي في بعض المسائل الشُّرطية خاصة بما يتعلق بمدى إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية [1]، وبعد إنتهاء الحرب العالمية الأولى وتحديدا في 1919 حاول الكولونيل "**فان هوتين**" أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولي الشرطي وذلك بالدعوة لعقد مؤتمر دولي لمناقشة الموضوع غير أنه لم يوفق في مسعاه، وبنهاية 1923 تم عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في 1923/9/7 بحضور مندوبي 19 دولة وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (ICPC) (International Criminal Police Commission) ،وتعمل على التنشيث بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة [2] .

إلا أنه وبإندلاع الحرب العالمية الثانية توقفت اللُّجنة عن أعمالها، حتى وَضَعت الحرب أوزارها عام 1946 حيث عقد في بروكسل ببلجيكيا في 1946/6/9 مؤتمر دولي بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ بدعوة من المفتش العام للشرطة البلجيكية، وإنتهى الإجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية ونقل مقرها إلى باريس بفرنسا وغيّر إسمها ليصبح المُنظمة الدَّولية للشُّرطة الجِنائيّة (INTERPOL) [3]. وحتى الان فهي تضم 194 عضوا لغاية 2019 وإنضمت الجزائر إليها عام 1963 أثناء إنعقاد الجمعية العامة للإنتربول في العاصمة هلسنْكي، أما فلسطن انضمت للإنتربول عام 2017 خلال إجتماع الجمعية

1.الغافري حسين بن سعيد،**المرجع السابق** ، ص7 .

2.**المرجع نفسه**،ص8.

3.بدري فيصل،**المرجع السابق**،ص65

العامة المنعقد في العاصمة بكين [1]، وتهدف المنطمة الدولية للشرطة الجنائية طبقا للمادة 2 من القانون الأساسي إلى :

1. تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح للإعلان العالمي لحقوق الإنسان.

2. إنشاء وتنمي كافة المؤسسات القادرة على المساهمة الفعّالة في الوقاية من جرائم القانون العام ومكافحتها[2].

ومن بين الأمثلة على دور الإنتربول فيما يتعلق بالجرائم المعلوماتية ماحصل في الجمهورية اللُّبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللُّبناني بتهمة إرسال صور إباحية لقاصِرة دون العشرة أعوام من موقعه على شبكة الإنترنت وذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص [3] .

2. المساعدة القضائية والدولية في مكافحة الجريمة الإلكترونية :

تُعرف المساعدة القضائية دوليا بأنها "**كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم** "، وتتخذ المساعدة القضائية في المجال الدولي عدة صور منها:

أ. تبادل المعلومات: ويتم بواسطة تبادل البايانات والوثائق والمواد الإستدلالية التي تطلبها سلطة قضائية أجنبية بصدد النظر في جريمة ما، حُركت الدعوى ضد أحد رعاياها أو رعايا دولة أخرى مما يتضمن تبادل السوابق القضائية للمتابعين لمثل هذه الجرائم ونجد لهذه الصورة

---

1. **Ar.m.wikipedia.org** ، تاريخ الإطلاع على الموقع 2019/5/19 .

2. القانون الأساسي والنظام العام للشرطة الجنائية الدولية (الإنتربول) .من إتفاقية سنة 1956 .

3. بدري فيصل ، **المرجع السابق**،ص67.

تطبيقات عدة منها ماورد في الفقرتين 7،6 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية [1] ، وكذلك الفقرات 4،3 من المادة الثامنة من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة [2]، وأيضا ماقضت به المادة الأولى من إتفاقية الرياض للتعاون الفضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية ، وفي هضا الإطار صاغ إتفاق شنجن للإتحاد الاوروبي نظاما متكاملا لتبادل المعلومات [3].

ب. نقل الإجراءات: يقصد به قيام دولة ما بناءا على إتفاقية أو معاهدة بإتخاذ إجراءات جنائية وهي بصدد جريمة إرتمبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت شروط معينة من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الجولة الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها، وأيضا أن تكون الإجراءات المطلوب إتخاذها من الأهمية بمكان بحيث تؤدي دورا مهما في الوصول إلى الحقيقة وقد أقرت العديد من الإتفاقيات الدولية والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، والمؤتمر الإسلامي لمكافحة الإرهاب الدولي عام 1999، وأيضا المادة 16 من النموذج الإسترشادي لإتفاقية التعاون القضائي والقانوني الصادر عن مجلس التعاون الخليجي عام 2003 [4] .

1.**صدرت هذه المعاهدة في 1990/3/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة وتقضي بإتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر من المساعدة المتبادلة في التحقيقات وإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في إختصاص السلطة القضائية طالبة المساعدة .**

2.بدري فيصل ، **المرجع السابق**،ص69.

3 Michel quellie : **stratégies en France par la police criminalité organisée** 1996, p199.

4.يوسف حسن يوسف ،**الجرائم الدولية للإنترنت**،ط1،المركز القومي للإصدارات القانونية ،2011،ص151.

ج. الإنابة القضائية الدولية : إتخاذ إجراء قاضئي من إجراءات الدعوى الجنائيةلأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية تعذر على الدولة التي تقدمت بطلب من الإنابة القيان به بنفسها وتهدف إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن إجراء التحقيقات اللازمة لتقديم المتهمين للمحكمة وتجدر الإشارة إلى أن طلب الإنابة عادة مايتم عبر القنوات الدبلوماسية ولكن تفاديا لتعقيد الإجراءات فقد درجت الدول على تعيين سلطة مركزية عادة ماتكون وزارة العدل توجه الطلبات إليها مباشرة، وإن كان التعاون القضائي يشكل أهم الآليات في مجال مكافحة جرائم الإنترنت إلا ان الإتفاقيات الدولية قد تناولت جريمة الإنترنت بدون تعمق وبشكل سَطحي ومنه باتت الحاجة مُلِحّة لِعقد إتفاقيات تواكب التطور السريع لتكنولوجا المعلومات والإتصالات [1] .

د. تسليم المجرمين: يُعد شكلاً من أشكال التعاون الدولي في مجال مكافجة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها وإستقرارها ويعرف إجراء تسليم المجرمين بأنه: عمل بمقتضاه تسلم الدولة التي لجأ إلى أرضها شخص متهم أو محكوم عليه في جريمة إلى الدولة المختصة لمحاكمته أو تنفيذ العقوبة عليه، ولقد تم تعريفه تسليم المحريمن في النظام الأساسي للمحكمة الجنائية الدولية لروما في المادة 102 بقولها " بعني التسليم نقل دولة ما شخصا إلى دولة أخرى بموجب معاهدة أو إتفاقية أو تشريع وطني "، وله صورثلاثة صور وهي: التسليم القضائي، التسليم الإداري، التسليم المختلط، وهناك إجراءات خاصة تتعلق بالجريمة منها التجريم المزدوج ودرجة جسامة الجريمة، وشروط متعلقة بالأشخاص المطلوب تسليمهم وهي عدم جواز تسليم الرعايا وعدم جواز تسليم اللاجئين السياسين وعدم جواز تسليم المحاكمين على ذات الجريمة [2] .

1.بدري فيصل ، **المرجع السابق** ،ص70.

2.للمزيد أنظر بدري فيصل ، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي** ،ص71 إلى ص81 .

3 . الجهود الأمنية والتقنية في مجال مكافحة الجريمة الإلكترونية:

بما أنها جرائم عابرة للحدود لابد من التعاون الدولي والأمني والتقني من أجل مكافحة هذا النوع من الإجرام .

أ. مركز الشرطة الأوروبية (الأوروبول): وهو جهاز على مستوى الإتحاد الأوروبي مقره في مدينة لاهاي بهولندا ،وقد تم إنشاء الأوروبول من قبل المجلس الأوروبي في لوكسمبورغ عام 1991 ليكون بمثابة حلقة وصل بين الشرطة الوطنية في محتلف الدول الأعضاء بهدف تسهيل عملية الملاحقة للجرائم العابرة للحدود، وللأوروبول دور فعّال في مكافحة الجرائم الإلكترونية حيث يقوم مثلا بالتحقيقات المتعلقة بإمتلاك المواقع الإباحية ونشرها عبر الإنترنت في الدول الأوروبية [1] .

ب. الأوروجست: جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مكافحة الجرائم، وينعقد إختصتصه عندما تمس جريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوروبي أو دولة عضو مع دولة من دول العالم الثالث، أو دولة عُضو مع الرابطة الأوروبية، ويعد الأُوروجِست بمثابة الدعامة الفعالة في مجال التحقيقات والمطاردات التي تقوم بها السلطات القضائية الوطنية وخصوصا فيما يتعلق بالإجرام الإلكتروني [2] .

ج. شنجن : إلى جانب الأوروبول والأوروجست، تم إنشاء فضاء جماعي لاحدود له، أطلق عليه هذا الإسم " شنجن Schengen " وهو إسم مأخوذ من الإتفاقية الموقعة عام 1985، وقد استحدثت هذا الإتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي في مواجهة

1.محمد طارق عبد الرؤوف الحن ،**جريمة الإحتيال عبر الإنترنت**،منشورات الحلبي الحقوقية ،بيروت،2011،ص239-240

2.**نفس المرجع** ، ص240 .

التحديات الجديدة ومنها الجريمة الإلكترونية هما: مراقبة المشتبه بهم عبر الحدود، ملاحقة المجرمين [1] .

د . مجلس وزراء الداخلية العرب: حيث أنشأ هذا المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون الشرطي في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود الأنظمة والقوانين المعمول بها في كل دولة بالإضافة لتقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء، حيث أوصى هذه المجلس على سبيل المثال لا الحصر بوجوب وختمية محاربة الجريمة العابرة للحدود والجريمة السيبرانية وذلك بإلزامية تَضافُر المجهودات العربية في هذا المجال في إخْتتام أشغال المؤتمر 36 المُنعقد في الجزائر بتاريخ 10 ديسمبر 2012 [2].

هـ. المنظمة العربية لمكافحة الجريمة الإلكترونية : هي منظمة علمية ومهنية غير حكومية ذات طابع عربي وإهتمامات قانونية وإقتصادية معنية بتنظيم الأطر القانونية والإجرائية والمؤسسية لمكافحة الجرائم التي تتم عبر الإنترنت وكافة الجرائم المعلوماتية، وتم الإتفاق على إنشاء منظمة عربية تحمل إسم المنظمة العربية لمكافحة جرائم المعلوماتية والإنترنت وأهم أهداف هذه المنظمة يتمثل في مكافحة كافة أشكال الجرائم التي تقع ضد المعلوماتية بكافة أشكالها [3].

أما على المستوى المحلي فقد ظهرت العديد من الأجهزة لمكافحة الإجرام الإلكتروني سواء على صعيد الدول العربية أم الأجنبية، نذكر منها :

---

1. بدري فيصل ، **المرجع السابق** ، ص90 .

2.**المرجع نفسه**، ص 91.

3.**المرجع نفسه**، ص91.

1. **الولايات المتحدة الأمريكية:** قامت بإنشاء عدة أجهزة لمكافحة الإجرام الإلكتروني منها:

أ . شرطة الواب (Web Police) ، ب. نيابة جرائم الحاسوب والإتصالات (CTC)

ج.المركز الوطني لحماية البنية التحتية .

2. فرنسا: قامت بتخصيص أجهزة أمنية فعالة في مكافحة الإجرام الإلكتروني فعلى المستوى المركزي فهناك مديرية الشرطة القضائية والمقسمة إلى عدة فروع منها :

أ.فرع خاص بالقضايا الإجرامية الماسة بالأشخاص، الإرهاب واللصوصية، الجريمة المنظمة، المخدرات .

ب. فرع حاص بالقضايا الإقتصادية والمالية: قانون الأعمال، النصب، خيانة الأمانة وغيرها.

ج. المديرية الفرعية الخاصة بمكافحة الجريمة المنطمة والإجرام المالي .

د. المديرية الفرعية الخاصة بمكافحة الإرهاب . وتم إنشاء الفرعين الآخرين في 2006 ، ولها أقطاب متخصصة كل حسب وظيفته والمهام التي أُنشأ من أجلها .

3 . بريطانيا: قامت بتخصيص وحدة تضم نُخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن جرائم الإنترنت وتضم هذه الوحدة 80 عُنصراً على درجة عالية من الكَفاءة في المجال التقني وبدأت نشاطها عام 2001 ومقرها لُندن .

4. إسبانيا: قامت الحكومة الإسبانية بتأسيس وحدة التحريات المركزية المعنية بالإجرام الإلكتروني وهي تعمل مع الإدراة المركزية في وزارة الداخلية على مراقبة مرتكبي هذه الجرائم وملاحقتهم .

5.هونكونغ: قامت بتأسيس مايعرف " بقوة مكافحة قَرْصَنة الإنترنت" وذلك في 1999 وتمكنت هذه القوة من إلقاء القبض على 12 شخص في 5 قضايا خلال 6 أشهر .

6. الصين : قامت بتأسيس مايعرف " القوة المضادة للهاكرز "، وهي تختص برقابة المعلومات التي يسمح لمواطنبها الدخول إليها عبر الإنترنت .

7. الإمارات العربية المتحدة: لم تقم بإنشاء جهاز خاص وإنما قامت بإحكام الرقابة على الإنترنت عن طريق مايعرف بنظام **PROXY**.

8. الأردن: أنشأت قسما خاصا بجرائم الحاسوب تابعا لمديرية الأمن ويتعامل مع مختلف الجرائم الإلكترونية.

9. مصر: قامت مصر بتكليف بعض الجهات بمكافحة الجرائم الإلكترونية ومنها :

أ. الإدارة العامة لمباحث الأموال وتختص بمكافحة الجرائم الإقتصادية .

ب. الإدارة العامة للتوثيق والمعلومات وهي من أكبر الإدارات بوزارة الداخلية للتعامل مع الإجرام الإلكتروني .

ج. الإدارة العامة للمصنفات الفنية وتهتم بجرائم النسخ والتقليد التي تشكل أكثر الجرائم شيوعا في مجال المعلومات [1] .

أما بالنسبة للجهود التقنية في مكافحة الجرائم الإلكترونية:

يقصد بها رسم سياسة جنائية ترتكز على التقنية الرقمية تحد من وقوع الجرائم الإلكترونية من ناحية وفي تقديم معالجة ناجعة لآثارها إذا كانت في طور الشروع أو أنها قد وضعت بالفعل من ناحية أخرى وهذا كله يتم عبر وسائل الإستقصاء وجمع الأدلة وهي :

أ . الإرشاد الجنائي عبر الإنترنت وهي قيام عناصر الضبطية بالولوج للإنترنت .

ب. المراقبة الإلكترونية وذلك بجمع المعلومات عن المشتبه به .

---

1. بدري فيصل ، **المرجع السابق** ، ص93-98.

ج. المعاينة وهي الكشف الحسي المباشر لإثبات حالة شيء أو شخص [1] .

المطلب الثاني: الآليات الوطنية لمكافحة الجرائم الإلكترونية (في التشريعين الجزائري والفلسطيني) :

أولا : الهيئة الوطنية للوقاية من الجرائم المتصلة يتكنولوجيات الإعلام والإتصال ومكافحته:

نصت على إنشاء هذه الهيئة **المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها** " تنشأ هيئة وطنية للوقاية من الجرام المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته .

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم " ، أما مهامها فقد أوردتها المادة 14 من نفس القانون .

أ . **تنظيم الهيئة :** بإستقراء نصوص القانون **04/09** فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية ، والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهه الهيئة .

ب مهام الهيئة : لهذه الهيئة دوران مهمان تلعبهما :

1. الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال : وذلك بتوعية مستعملي تكنولوجيات الإعلام والإتصال بخطورة الجرتءم التي يمكن أن يكونو ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات .

1.بدري فيصل ، **المرجع السابق**،ص97.

2. مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال : حسب نص المادة 14 من القانون 04/09 فهناك نوعان من النمافحة هما :

أ. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاو الخبرات القضائية .

ب. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجبات الإعلام والإتصال وتحديد مكان تواجدهم [1] .

ثانيا: دور الضبطية القضائية في إجراءات مواجهة الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال :

لها دور فعال في ذلك وبالنسبة للجرائم المستحدثة فإنها تلقي المزيد من الأعباء على عاتق الضبطية القضائية وكذلك الأمر بالنسبة للسلطات القضائية، وذلك نظرا لضعف خبرة كل منهما في مواجهة هذه الجرائم، فمن المتصور أن يجد ضباط البشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الإستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، وقد يفشل جهاز الضبط اقضائي في تقدير أهمية الجريمة نظرا لنقص الخبرة والتدريب، وللسبب اته سيفشل الحقيق في الجرائم الإلكترونية، ونتيجةً لذلك فقد قام الدرك الوطني وَبَاشر مُنذ 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال فبموجب هذا العمل فإن الكثيرمن إطارات الدرك الوطني إستفادو من تكوين خاص في جامعات سويسرا وأمريكيا وكندا. سواء في المجال التقني أو القانوني، كما أن إطارات الدرك الوطني تساهم في عدة مُلتقيات وطنية ودولية تَنصبّ

1.أحمد مسعود مريم ، **آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 04/09** ، مذكرة ماستر – تخصص قانون جنائي ، بإشراف الدكتور قريشي محمد ، جامعة ورقلة ، 2013،ص44.

موضوعاتها في إطار الجرائم الإلكترونية وكذلك المشاركة والمساهمة في مُلتقيات ومُؤنمرات وطنية ودولية تتناول بالخصوص حقوق المؤلف في البيئة الرقمية [1] .

ثالثا: السلطة القضائية في مواجهة الجرائم الإلكترونية :

إن السلطة القضائية ستتعامل تأكيدا مع قضايا الجرائم الإلكترونية ولاسيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين بينما بتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعّالة في هذه المواد التي تجتاح المجال العقابي [2] .

ومنذ 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليواكب التطور القانوني الجاري الخاص بالجرائم المعلوماتية ولأجل هذا تم إجراء دمج مادة الجريمة المعلوماتية في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل مُلتقيات يُنشّطها خبراء، والعديد من دورات التكوين في مختلف الجرائم الإلكترونية المُنظمة بالخارج لصالح القضاة وإطارات وزارة العدل في إطار التعاون الثنائي .

وهناك هيئات أخرى لمكافحة الجريمة الإلكترونية بالجزائر سنذكرها فقط وهي :

1. المعهد الوطني للأدلة الجنائية وعلم الجرائم .

2.المديرية العامة للأمن الوطني [3] .

1.أحمد مسعود مريم ، **المرجع السابق** ، ص46.

2. Myriam quemener, Yves chrpenel : **cybercriminalité, droit pénal appliqué,** 2010, economica, paris – France, page206

3. أحمد مسعود مريم ، **المرجع السابق** ،ص48.

رابعا : وحدة نيابة الجرائم الإلكترونية في فلسطين :

كما قلنا سابقا أنها وحدة في جهاز الشرطة الفلسطيني متخصصة بالجرائم الإلكترونةي ومتابعة مرتكبيها، وأن إنشاء هذه الوحدة مهد لإصدار قانون خاص بهذه الجرائم، وشكّل قرار النائب العام الفلسطيني إنشائ نيابة للجرائم الإلكترونية دفعة جديدة في تهيئة الظروف القانونية والتسريع بإصدار قانون خاص بهذا النوع من الجرائم التي ترتفع سنويا بنسبة 40 %، والنيابة العامة الفلسطينية أوْلَت إهتماماً لهذا الموضوع كونه متخصص وجديد حيث تم تدريب نحو 146 عضو نيابة من مستويات مختلفة، وبناءا على قرار النائب العام تم تخصيص التدريب لأعضاء النيابة المتخصصين بحيث يكونو على قدرة وكفاء بإدارة وبناء الملف التحقيقي، وإتخاذ القرار المناسب فيه وأن هناك أمام المحاكم الفلسطينية مامجموعه 1142 قضية متعلقة بالجرائم الإلكترونية وتقنيات الإتصالات حتى شهر أوت لعام 2018، وقد تعاملت هذه الوحدة في العام 2017 مع 1619 قضية تتعلق بالفيسبوك والإنترنت أنجز منها 908، أي أن هناك مئات القضايا التي لاتصل إلى الشرطة الفلسطينية ويتم حلها من خلال القضاء غير الرسمي[1]، وأيضا دَور المؤسسات الأمنية في مواجهة الجرائم الإلكترونية لابدّ منه من خلال تأهيل كوادر أمنية متخصصة بإستخدام التقنيات الحديثة والفضاء الإلكترونية في عمليات البحث والتحري والمراقبة، لمنعها وضبطها والتوعية الثقافية الأمنية من مخاطر إنتشارها، وبالتالي فإن هناك كثير من المؤسسات الرسمية التي لها الدور الكبير في مكافحة الجرائم الإلكترونية بالإضافة إلى الأجهزة الداخلية في الشرطة الفلسطينية [2] .

1.معالي موسى ، **التجربة الفلسطينية في التأمين والحماية للفضاء السيبراني** ، ورقة عمل مقدمة إلى الندوة العلمية حول حوكمة الإنترنت وإدارة المواقع ،بيروت ، 2018،ص11 .

2.حمدان هاني ، **دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية** ، مجلة الدراسات الأمنية ، أكاديمية الشرطة الملكية ، الأردن ، العدد 1 ، 2004 ،ص37 .

المطلب الثالث: آليات الوقاية من الجرائم الإلكترونية :

الفرع الأول: الوقاية المؤسساتية من الجريمة الإلكترونية :

أولا: دور المؤسسات الإعلامية في الوقاية من الجريمة الإلكترونية :

يساعد الإعلام كسُلطة رابعة على ترسيخ أمن المجتمع والتأثير فيه من خلال إثارة الرأي العام لمواجهة الجرائم بكافة أشكالها، من خلا تسليط الضوء على اأفعال والتصرفا تالسلبية وتوعية المجتمع بهذه الجرائم ومخاطر الوقاية منها، بواسطة الصصحافة الإلكترونية وإصدار الصحف والمحلات التوعوية ونشرها في أروقة المجتمع، ولإنجاح ذلك يتطلب وضع خطة إعلامية من أجل التعرف على ظاهرة الجرائم المعلوماتية في المجتمع لمُواجهتها وتنمية الوعي المجتمعي بمخاطرها، وحثّ المواطنين على إبلاغ الجهات المختصة حال تَعرضه لهذه الجرائم وتَعاوُنِهم مع الجهات المختصة، وبالإضافة إلى نَشر وتركيز الجهود على أداء المؤسسات الأمنية والقَضائية في مجال مكافحة هذه الجرائم [1] .

ثانيا: دور المؤسسات التعليمية والثقافية في الوقاية من الجريمة الإلكترونية :

تلعب دوراً هاماً في مواجهة الجرائم الإلكترونية، وتَحد من إنتشار السلوك غير المرغوب فيه مُجتمعياً، وتمنع إنحراف الإشخاص نحو إرتكاب الجرائم وتوجيههم إلى السلوك الإجتماعي الصحيح وتعزيز القيم والإخلاق من خلال الإخلاص بالعمل وحسن التربية والتوجيه، وفرض الرقابة والمتابعة على أفرادها لرصدها ومعرفة أسبابها من أجل الوصول إلى طرق ووسائل علاجها والتركيز بالمناهج الدراسية على الأخلاق الحميدة كون الطفل أكثر إستجابة في هذه

1. نبيل أبو الرب ، **المرجع السابق** ،ص82.

المرحلة ،وتساهم هذه المؤسسات من حلال إيجاد مقررات تعمل على توعية أفراد المجتمع ، ونشر الكتب والمجلات حول هذه الجرائم ومخاطرها [1] .

ثالثا : دور المؤسسات الدينية للوقاية من الجرائم الإلكترونية :

تلعب المؤسسات الدينية دوراً هاماً في الوقاية من هذا النوع من الجرائم من خلال التربية الإحلاقية وتقوية الإيمان بين أفراد المجتمع والتنشئة السليمة للأفراد عبر وسائل التوعية الدينية المختلفة، ومن خلال وضع مؤلفات وكتب ذات بُعد ديني عن مخاطرها، وتنظيم دورات ومحاضرات إرشادية حول هذه الجرائم في أماكن العبادة والمدارس والجامعات وغيرها من المؤسسات، وتعزيز دور الخطباء في المساجد بالتعاون مع وزارة الأزقاف بتوعية الناس حول هذه الظواهر، وبيان المخاطر التي تنشأ عن السلوكيات التي تتعارض مع الدّينْ الإسلامي ومبادئ الشريعة الإسلامية، والمساهمة في تنمية الوازع الديني والأخلاقي [2].

الفرع الثاني : الوقاية الذاتية من الجريمة الإلكترونية :

على الرغم من أن الجرائم الإلكترونية تشكل خطراعلى مختلف المناطق في العالم، إلا أن هناك عدة خطوات وطرق تمكنك من حماية نفسك وعائلتك من مثل هذه الجرائم .

أولا . الوقاية من الجرائم الإلكترونية على الصعيد الشخصي :

1. إستخدام التحديثات المعتادة لبرامج مُضادات الفيروسات ومُضادات التّجَسُسْ على جميع أجهزتك الإلكترونية حتى لاتقع فريسة تحت هذا النوع من الجرائم .

2.الحرص على تحديث المُتصفح الخاص بالإنترنت بشكل مستمر.

---

1. نبيل أبو الرب، **المرجع السابق** ص83 .

2. **المرجع نفسه**، ص82.

3. عدم التواصل مع أي جهات أو مواقع إلكترونية لايوجد فيها الأمان العالي، والتواصل مع جهات موثوقة والتي تقوم بحماية معلومات وبيانات المرور الخاصة بالشخص.

4.عدم الضغط على أي روابط أو إعلانات أو مُلحقات، وعدم الرد على أي رسائل إلكترونية من مصادر غير معروفة وغير موثوق بها.

5.عدم الرد على رسائل يتم فيها السؤال عن البيانات الشخصية أو المعلومات الأمنية الخاصة بالشخص مص المعلومات البنكية، وعدم جعل البيانات منشورة على مواقع التواصل والإنترنت حتى لايقع الشخص ضحية في المستقبل لمصل هذه الجرائم .

6. كما يمكن للشخص حماية نفسه من اللصوص الإلكترونيين من خلال عدم مشاركة إعدادات الخصوصية والأمان لتحديد من يمكنهم مشاهدة نشاطك الإلكتروني [1] .

ثانيا : دور الأسرة في الوقاية من الجرائم الإلكترونية :

تساهم الأسرة في مواجهة هذه الجرائم بإعتبارها أكثر تأثيرا بوصفها المؤسسة الأولى التي تؤثر في تحديد سلوك الطفل وشخصيته، ومن خلال تنشأة وتربية وتوعية أفرادها وتوجيههم نحو السلوكيات الإيجابية وإبعادهم عن الجريمة، وتقديم النصائويفرض هذا الدورج لهم حول مخاطر هذه الجرائم كما تساهم الأسرة في مواجهة ومكافحة الجرائم الإلكترونية عن طريق مُعاقبة أفرادها حال وقوعها من قبل أحدهم ويفرض هذا الدور على مختلف الدول وضع برامج أُسَرِيّة ضمن خُططها التنموية والإجتماعية من أجل بناء جيل صالح [2].

---

1. **Assawsana.com** ، تاريخ الإطلاع على الموقع : 2019/5/21.(الجرائم الإلكترونية .. طرق الحماية) .

2. نبيل أبو الرب ، **المرجع السابق**، ص83.

ثالثا : الحماية التقنية للوقاية من الجرائم الإلكترونية :

وهي متعددة الأشكال فعلى سبيل المثال للوقاية من الإصابة بفيروس الحاسب الآلي يجب إتباع إجراءا الأمن التالية :

1. عدم إستخدام برامج مَجهولة الأصل .

2.عدم إستخدام اسطوانات تتضمن برامج متغيرة وقابلة للتغيير الأمر الذي يشكك في أنها حاملة للعدوى .

3.مراقبة إستخدام الجاسب للذاكرة للتيقن من عدم وجود فيروسات مختبئة فيها .

4. ويرى البعض أنه يجب إنشاء مركز قومي لأمان الحاسبات والمعلومات كإجراء أمني للوقاية من هذه الجرائم الإلكترونية.

كما قدمت الباحثة إسراء جبريل مرعي من المركز الديمقراطي العربي جُملة من الأساليب في بحثها المنشور إلكترونياَ وذكرت من أبرز هذه الأدوات الوقائية :

1.إستعمال مايطلق عليها جدار الحماية (**firewall**)، ويكون بمثابة الدور الذي تقوم به جَمارك الحُدود للحيلولة دون دخول الأجسام الغريبة والضارة.

2. إستخدام تقنية التشفير لمنع كشف المعلومات.

3.إستعمال تقنية التوقيع الرقمي لمنع تزوير الرسائل الإلكترونية.

4. العناية بتوظيف أنظمة كشف مختلف الإختراقات وإيجاد حلول للثغرات الأمنية.

5. ضرورة إمتلاك نُسخ إحتياطية، لِمُختلف المَلفات الهامّة والحسّاسة ووضعها في أماكن آمِنة.

6.ضرورة إستخدام بعض البرامج التي ضممت خصيصا للكشف والوقاية من الفيروس والبُعد عن إستعمال كلمة السر البسيطة .

7. التعامل بحذر بالغ عند فتح البريد الإلكتروني، وذلك بالتأكد من هوية باعث الرسالة، فقد يكون فيروساً مُدمراً لايُبقي ولايذر [1].

وبهذا نكون قد بينّا آليات الوقاية من الجرائم الإلكترونية كل حسب دوره سواء مؤسسة أو أسرة أو تبيان الدور التوجيهي من أجل الإستخدام السَّليم للحاسب الآلي وعدم إستخدامه بشكل ضارّ، وبهذا يبقى ضَرورة حُضور الضمير الأخلاقي بِتَحرّي الموضوعية والنزاهة استشعاراً بِعِظَم المسؤولية الكاملة وأن مايلفُظه أو يفعله الإنسان في هذا الوجود إلا ولديه رقيبٌ عتيد، على كل أفعاله مع إستغلال هذه الوسائل في عملية التربية والتوجيه وتبليغ الرسالة الصحيحة المَرجُوة منها وأن تكون خالية من كل الشوائب التي تَزُجّ في مستنقعات الجريمة الإلكترونية .

خلاصة الفصل الثاني :

إن الجريمة الإلكترونية كغيرها من الجرائم تمر في مراحل متعددة إجرائية وهي مرحلة جمع الإستدلالات والبحث والتحري ولها أجهزة خاصة تقوم بهذه المهمة وتقع على عاتق رجال الضبطية القضائية ،وأن هناك نطاق إختصاص لسلطة البحث والتحري عن الجرائم الإلكترونية بينها المُشرع ووسّع منها ووضع لذلك إستثناءات في بعض الجرائم ومنها الجريمة الإلكترونية كونها عابراة للقارات وتضرّ بأكثر من دولة، وأن هناك إجراءات تقليدية كلاسيكية وإجراءات حديثة للكشف وجمع الإستدلالات عن الجريمة الإلكترونية، وهناك آليات للإثبات الجنائي لعل

1. سليمان قوراري ، سعاد رحلي ، **دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية** ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية ، طرابلس 24 -25 مارس 2017،ص6-7 .

أهمها الدليل الإلكتروني الذي يعد أهم الأدلة في هذا النوع من الجرائم وأن للقاضي سلطة التقدير لهذا الدليل والجريمة الإلكترونية صعبة الإثبات، وأن الجريمة الإلكترونية تمر بعدة مراحل منها التحقيق والمحاكمة وبينا أيضا كيفية إتصال قاضي التحقيق بملف الجريمة الإلكترونية وماهي سلطاته فيها وأن هذا النوع من الجرائم يتطلب ويحتاج رجال تحقيق مدربون وأصحاب خبرة وإختصاص في الإجهزة الإلكترونية فهي تختلف كل الإحتلاف عن التحقيق في الجرائم التقليدية وأن المحقق تواجه صعوبات إثناء عمله نظراً لما يفرضه قانون الإجراءات الجزائية عليه من قيود والتي قد تعرقل عمل المحقق في الجريمة الإلكترونية، وأن القانون وضع عقوبات رادِعة للجريمة الإلكترونية من خلال قانون العقوبات الجزائري وقانون الجرائم الإلكترونية في فلسطين وماهي إجراءات ملاحقة مرتكبي الجرائم الإلكترونية، ويتبين ان هناك جهود دولية وإحرى إقليمية تحاول التصدي للجرائم الإلكترونية حيث تسعى كل الدول جاهدة لمواكبة هذه الإتفاقيات الدولية، وذلك بسن تشريعات جديدة تتلائم والتطورات التكنتولوجية الحاصلة، وأن هذا التطور التكنولوجي ألقى مسؤولية كبيرة على عَاتق المشرع الجنائي لمواجهة الجريمة الإلكترونية الناشئة عن إستخدام الأنظمة الإلكترونية في ظل قُصور قانون العقوبات عن الإحاطة بهذه الجرائم، ولأن تنظيم مجال المعلوماتية وسن تشريعات بهذا الخصوص يساهم في زرع الثقة في المجتمع عامة فكان على المشرع الوطني مكافحتها بكل السُّبل والوسائل وأيضا أن مؤسسات المجتمع المدني تقع على عَاتقها الحِماية من الوقوع في الجرائم الإلكترونية ووضع خُطط مُناسبة للوقاية من هذه الجرائم .

الخاتمة

لقد تم بحمد الله وفضله في ثنايا هذه الدراسة المقارنة، التعرف على واقع الجريمة الإلكترونية في فلسطين والجزائر وكيف عالجها المشرعين من خلال سن النصوص القانونية التي تخص هذا النوع من الجرائم كونها من الجرائم العصرية المستحدثة، ومما سبق يمكن أن نصل إلى نتيجة مفادها أن الجريمة الإلكترونية هي آفة العصر، والأخطبوط الذي أنتجته الحضارة التقنية والثورة التكنولوجية، الذي تمتد أذرعه في جميع أنحاء العالم ولم تفلت من قبضته لا الدول الضعيفة ولا المتطورة واستشرى خطره المدمر على مختلف القطاعات الحياتية الإقتصادية منها والإجتماعية والسياسية، وحتى الشخصية وأن جميع الأفراد في العالم مستهدفون على إختلاف فئاتهم وأعمارهم ومرجعياتهم الفكرية والدينية والثقافية، فنحن نعيش في زمن الإستعمار الإلكتروني بكل أشكاله ومظاهره الذي يستهدف التأثير بشكل مباشر وغير مباشر على سلوكيات الناس فالجرائم الإلكترونية ليست جرائم تقليدية بثوب جديد أو أنها طبعة جديدة لجرائم قديمة بوسائل حديثة، فهي جرائم مستحدثة أنتجها التطور التكنولوجي، وبعد الإنتهاء من هذا البحث توصلنا إلى وجود مشكلة حقيقة في واقع الجرائم الإكترونية في فلسطين والجزائر، وبناءا على ذلك توصلنا إلى النتائج والتوصيات التالية :

النتائج :

1. تعرف الجريمة الإلكترونية بأنها عبارة عن إعتداء يُطال معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، وتكون بإستخدام إحدى الوسائل الإلكترونية بشكل غير مشروع يلحق ضررا بالغير يعاقب عليه المشرع الجزائي، ولحد الآن لايوجد تعريف محدد لها إتفق عليه المختصون .

2. إن محل الجريمة الإلكترونية وموضوعها هو المعطيات والمعلومات الكمبيوترية والذي تستهدفه إعتداءات الجناة بشكل عام إذ أن هذه الجرائم إما أن تقع على الكمبيوتر ذاته وإما بواسطته وذلك بإعتباره محل للجريمة تارة ووسيلة لإرتكابها تارة أخرى .

3. تتسم الجريمة الإلكترونية بصعوبة إكتشافها، لأنها لاتترك دليل مرئي كما أن الجاني ذكي يخفي آثار جريمته وأنها أيضا ترتكب في دول مختلفة، وأن فقدان الأثر من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية .

4. يتم ملاحقة مرتكبي الجرائم الإلكترونية عن طريق تطبيق القوانين السارية المفعول والتي أقرها المشرع ألا وهي قانون الجرائم الإلكترونية وقانون المساس بأنظمة المعالجة الآلية للمعطيات .

5. تم إنشاء وحدة للجرائم الإلكترونية في فلسطين تابعة للمباحث العامة في الشرطة الفلسطينية سنة 2013 بهدف مواجهة التحديات القائمة في هذا المجال لمكافحة الجرائم الإلكترونية كظاهرة من الظواهر الإجرامية المستحدثة، كما أنشئت هيئة خاصة بالجزائر مهمتها متابعة المجرمين الإلكترونيين .

6. إن الإجراءات الخاصة بالتحري والتفتيش والضبط قد تنطوي على كشف خصوصية البيانات المخزنة في النظام، فإذا لم تكن ضمن الإطار المبين في أوامر التفتيش والضبط فإنها تذهب بإتجاه البطلان وبالتالي بطلان الدليل الذي إستمد منه، كما أنه لايكتفي الإعتماد على التشريعات القائمة لتجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم الإلكترونية بل لابد من تدعيمها بنصوص خاصة تلائم طبيعة هذا الشكل الجديد من الإجرام.

7. من أسباب إنتشار الجريمة الإلكترونية هو الإنترنت لأنه جعل العالم كقرية صغيرة فالجريمة الإلكترونية قد ترتكب في دولة وتتحقق نتيجتها في دولة أخرى .

8. الإستعانة بالخبراء أمر لابد منه في جميع مراحل الدعوى الجزائية .

9. تتخذ إجراءات المحاكمة في الجريمة الإلكترونية نفس الإجراءات التي تتم في الجرائم التقليدية، مع إختلاف الأدلة والتي تكون على هيئة معطيات إلكترونية .

10. إن تعاون وتكاتف الجهود الدولية و الإقليمية في حقل الجرائم الإلكترونية ساعد في تخطي العقبات التي تطرحها هذه الجرائم كونها جرائم عابرة للقارات، كما أنه يوجد صعوبة في التعاون القضائي الدولي في الجرائم الإلكترونية والقانون الواجب التطبيق والمحكمة المختصة بذلك .

11. لايوجد سيادة كاملة للفضاء الإلكتروني في فلسطين كون أن الإحتلال الإسرائيلي يسيطر على النسبة الكبرى منها، وهذا ماأدى إلى صعوبة ملاحقة المجرمين الإلكترونيين في فلسطين.

12. إن إنضمام فلسطين للإنتربول مؤخراً سيساعد على ملاحقة جميع المطلوبين الجنائيين للقضاء الفلسطيني على المستوى الدولي، وهذا مايتيح فرصة لتبادل المعلومات وزيادة خبرة الشرطة الفلسطينية وتطوير قدراتها لتصبح في مصافِ الدول الأخرى في مكافحة الجرائم الإلكترونية .

التوصيات :

1. لابد من وضع تعريف عام وشامل للجريمة الإلكترونية حتى يتسنى لذوي الإختصاص التعامل مع هذه الجرائم لأن مصطلحاتها زئبقية صعب حصرها في تعريف واحد، لذا لابد من رجال القانون والمتخصصين أن يضعوا تعريف يحيط بالجريمة الإلكترونية من جميع نواحي هذا المصطلح .

2. ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين في الإدعاء العام(النيابة) والقضاء على كيفية التعامل من هذا النوع من الإجرام وتحقيق التعاون مع التقنيين من أصحاب الخبرو ، وذلك بعقد دورات تدريبية بشكل دوري دائم للإستفادة من خبراتهم وإرشاداتهم إبتداءا من مرحلة الإستدلال وجمع الأدلة وإنتهاءا بقرارات المحاكم .

3. إعداد خطة وطنية وشاملة للوقاية والحد من الجرائم الإلكترونية في فلسطين، كما يجب بسط السيطرة على الفضاء السيبراني في فلسطين، كما ويجب وضع حماية إلكترونية للمواقع

الحكومية والمهمة في الدولة مثل الوزارات كون هذه الجرائم قد تمس بمصالح الدولة العليا .

4. ضرورة تعزيز وتكاتف التعاون الدولي أكثر من ذلك للسيطرة على الجرائم الإلكترونية قدر الإمكان ولتسهيل متابعة المجرمين الإلكترونيين، وأيضا تعزيز التعاون الدولي الشرطي والقضائي بهدف تبادل المعلومات والخبرات والتدريب فضلا عن المساعدة المتبادلة في كشف هذه الجرائم .

5. تطوير قانون الإجراءات الجزائية لينظم الإجراءات التي تتعلق بالتحري والتحقيق في الجرائم الإلكترونية، كما ويجب رفع سقف العقوبات على بعض الجرائم الإكترونية والعمل على تصنيف الجرائم الإلكترونية بين الجنح والجنايات لأنها ينتج عنها آثار جسيمة .

6. نشر الوعي والثقافة بين المواطنين بخطورة الجرائم الإلكتونية وكيفية التصدي لها في حال وقوعها وإحاطتهم بإرشادات خاصة للتبليغ عن مثل هذه الجرائم كون أن الفرد في المجتمع هو المسؤول الأول عن حماية نفسه من الجرائم حتى لايقع ضحيتها .

7. إنتهاج سياسة جنائية واضحة وكفيلة بمواجهة الجرائم الإلكترونية بحيث يتوفر لهذه السياسة مقومات النجاح من المناقشة المستفيضة والتخطيط الشامل والجهات التنفيذية القادرة والناشطة، والأدوات التشريعية والقضائية المتخصصة والفاعلة لتتكلل الجهود المبذولة بالنجاح في الإطار العام لهذه السياسة في مواجهة الجرائم الإلكترونية بصورة متكاملة تتناسب ومستجدات العصر وتتوائم مع مبادرات التعديل والتطوير ومراكمة الإنجازات .

8. نقترح بزيادة قدرة الخبير على نقل الأدلة غير المرئية وتحويلها بشكل صحيح إلى أدلة مقروءة أو المحافظة على دعائمها لحين القيام بأعمال الخبرة بغير أن يلحقها أي تدمير، وإتقان مأموريته دون أن يترتب على ذلك أي مشاكل أو تدمير للأدلة المتحصلة من الوسائل الإلكترونية، ووضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة ورصد الإتصالات الهاتفية من وإلى مسرح الجريمة حتى لايضيع أي دليل وللتمكن من الوصول

إلى الحقيقة والفاعل، أي بمعنى إستحداث وتطوير مهنة خبير البحث التقني القانوني للحاسب الآلي .

9. التّريث عند التوقيع على الإتفاقيات المختلفة للحيلولة دون التوقيع على بنود تصطدم بالقانون الأساسي في فلسطين " الدستور " .

10. يجب العمل من خلال برنامج محدد على تنمية قدرات القضاة الفلسطينيين والجزائريين حول الجرائم الإلكترونية وآليات إكتشافها وإكتشاف أدلتها .

11. الإعتماد على مبدأ العالمية بالنطلر لطبيعة الجرائم الإلكترونية العابرة للحدود ونرى أنه أطثر ملائمة من مبدأ اللإقليمية المطبق في أغلب التشريعات الجنائية الحالية .

12. نقترح بالإستفادة من المجرمين الإلكترونيين بعد معاقبتهم أو تخفيف الحكم عنهم وذلك لأن لهم قدرات مميزة وخاصة، بحيث يمكن الإستفادة منها لتعزيز الحماية الإلكترونية للمؤسسات المختلفة وذلك بإشراكهم في الدفاع عن الفضاء الإلكتروني للدولة .

13. عند وضع النصوص القانونية يجب أن يدقق في حماية المواطن، على أساس أن حماية الأمن الرقمي يمكن أن تحيل على مفاهيم متعددة تتراوح مابين حماية الأشخاص تتراوح مابين حماية الأشخاص وحماية المحموعات وغيرها، وبالتالي وضع نصوص قانونية واضحة خالية من الغموض لأنها ستؤطر ظواهر إجتماعية جديدة مستقبلا .

" والله وليّ التوفيق "

تم بحمد الله الإنتهاء من هذه المذكرة وأتمنى أنني قمت بمعالجة هذا الموضوع من بعض النواحي الهامة بالشكل الصحيح، وفي النهاية لأملك إلا أن أقول أنني قد عرضت رأيي وأدليت ببعض الأفكار في هذا الموضوع لعلي أكون قد وفقت في كتابته والتعبير عنه، وأخيرا ما أنا إلا بشر قد أخطئ وقد أصيب فإن كنت قد أخطأت فذلك من الشيطان وإن أصبت فهذا كل مأرجوه من الله عز وجل .

قائمة المصادر والمراجع

أولا : الإتفاقيات والمعاهدات الدولية :

1. الإتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض في 1904/5/18 .

2. إتفاقية العهد الدولي الخاص لحقوق الإنسان لعام 1966 .

3. إتفاقية برن لحماية المصنفات الأدبية والفنية والتي عقدت في برن بسويسرا عام 1886 وتم التعديل عليها في مؤتمرات مختلفة آخرها في باريس عام 1979 .

4. إتفاقية الرياض للتعاون القضائي العربي بشأن تبادل المعلومات لعام 1983 .

5. إتفاقية شنجن للإتحاد الأوروبي بشأن تبادل المعلومات لعام 1985 .

6. معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية لعام 1990 .

7. معاهدة الأمم المتحدة النموذجية بشان نقل الإجراءات في المسائل الجنائية لعام 1990.

8. إتفاقية تريبس حول الجوانب التجارية لحقوق الملكية الفكرية لعام 1994 .

9. معاهدة الويبو لعام 1996 وتنقسم إلى ثلاثة أقسام :

- معاهدة الويبو بشأن حقوق المؤلف .
- معاهدة الويبو بشأن الأداء والتسجيل الصوتي .
- معاهدة الويبو بشأن الحماية الدولية لحق الموؤلف والحقوق المجاورة .

10. المؤتمر الإسلامي لمكافجة الإرهاب الدولي لعام 1999 .

11. إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود (باليرمو)، المعتمدة من طرق الجمعية العامة في 2000/11/15 .

12. إتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام 2001 .

13.القانون العربي النموذجي الإسترشادي لإتفاقية التعاون القضائي والقانوني لمكافحة جرائم تقنية المعلومات الصادر عن مجلس التعاون الخليجي عام 2003 .

14. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي صادقت عليها الجزائر وفلسطين عام 2010 .

ثانيا : النصوص التشريعية الوطنية والمقارنة (القوانين) :

1. الدستور الجزائري لعام 1963 المعدل والمتمم بالقانون رقم 16-01 في 6 مارس 2016، في الجريدة الرسمية رقم 76 المؤرخة في 8 ديسمبر 1996 .

2. الأمر رقم 66-155 المورخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، والمنشور بالجريدة الرسمية الحزائرية عدد 49 .

3. الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم، والقانون رقم 17-07 المؤرخ في 28 جمادى الثانية عام 1438 الموافق 27 مارس سنة 2017 .

4. القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، والمنشور في الجريدة الرسمية الجزائرية العدد 06 المؤرخة في 20 ربيع الثاني عام 1436هـ الموافق 10 فبراير لسنة 2015 .

5. القانون رقم 09 -04 المؤرخ في 14 شعبان 1430الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمنشور في الجريدة الرسمية الجزائرية العدد 47 المؤرخة في 25 شعبان عام 1430 الموافق 16 غشت سنة 2009 .

6. الدستور الفلسطيني (القانون الأساسي) سنة 2005 المعدل والصادر في مدينة غزة بتاريخ 2005/08/13، عن رئيس دولة فلسطين محمود عباس .

7. قانون العقوبات الفلسطيني رقم 74 لسنة 1936، والمنشور في الوقائع الفلسطينية في العدد 652 المؤرخ في 1936/12/12، والمعدل بقانون رقم 16 لسنة 1960 المعمول به حالياً، والساري التطبيق في الأراضي الفلسطينية، والصادر في تاريخ 1960/4/10.

8. مشروع قانون العقوبات الفلسطيني لسنة 2010 .

9.قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 ، ومعه قرار رقم (17) لسنة 2014، الصادر بمدينة غزة بتاريخ 2001/5/12، عن رئيس دولة فلسطين ياسر عرفات.

10. قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الإلكترونية ، والصادر عن رئيس دولة فلسطين في رام الله، والمنشور في الجريدة الرسمية الفلسطينية ممتاز عدد 14بتاريخ 2017/7/9 .

11. قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية الصادر عن رئيس دولة فلسطين في رام الله، والمنشور في الجريدة الرسمية الفلسطينية ممتاز عدد14 بتاريخ 7/9 /2017 .

12. قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية ، والصادر في مدينة رام الله عن رئيس دولة فلسطين والصادر بتاريخ2018/4/29، والمنشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 16 بتاريخ 2018/5/3 .

13. قرار بقانون رقم (9) لسنة 2018 بشأن محكمة الجنايات الكبرى الصادر عن رئيس دولة فلسطين في رام الله، والمنشور في الجريدة الرسمية الفلسطينية ممتاز عدد 16 بتاريخ 2018/5/3 .

14. قانون تشكيل المحاكم النظامية الفلسطينية رقم (5) لسنة 2001 الصادر عن رئيس دولة فلسطين بمدينة غزة بتاريخ 2001/5/12، والمعدل بقرار قانون رقم (19) لسنة 2014 والصادر عن رئيس دولة فلسطين في مدينة رام الله بتاريخ 2014/9/4 ، والمنشور على المقتفي .

15. قانون رقم (3) لسنة 1996 بشأن الإتصالات السلكية واللاسلكية ، والصادر في مدينة غزة عن الرئيس ياسر عرفات بتاريخ 1996/1/18 والمنشور في المقتفي .

16. مشروع قانون الإنترنت والمعلوماتية لعام 2002 في فلسطين .

17. قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996.

18. قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001 ، والمنشور على الصفحة 6010 من عدد الجريدة الرسمية رقم 4524 بتاريخ 2001/12/31 .

19. قانون إمارة دبي رقم (2) الخاص بالمعاملات والتجارة الإلكترونية لسنة 2002، والصادر عن حاكم دبي بتاريخ 12 فبراير 2002 .

20. قانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته والمؤرخ في 21 محرّم عام 1427 النوافق 20 فبراير سنة 2006 والمنشور في الجريدة الرسمية الجزائرية العدد 14 بتاريخ 8 مارس 2006 .

21. قانون العقوبات الفرنسي الجديد .

ثالثا : قائمة الكتب باللغة العربية :

أحمد خليفة الملط :

1. الجرائم المعلوماتية ، ط2 ، دار الفكر الجامعي ، 2006 ، مصر .

أحمد فتحي سرور:

2.الوسيط في قانون الإجراءات الجنائية ، ط8، دار النهضة العربية ، 2012 ، القاهرة .

أحسن بوسقيعة :

3.الوجيز في القانون الجزائي الخاص ، الجزء الأول ، ط1 ، دار هومة ، 2008، الجزائر.

أحمد عزمي الحروب :

4.السندات الرسمية الإلكترونية ، ط1، دار الثقافة للنشر والتوزيع ، 2010، عمان.

أسامة عبد الله قايد :

5.شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، 2007 ، القاهرة .

أسامة المناعسة وأخرون:

6.جرائم الحاسب الآلي والإنترنت ، ط1 ، دار وائل للنشر ، 2001 ، الأردن.

أشرف عبد القادر قنديل:

7. الإثبات الجنائي في الجريمة الإلكترونية ، دار الجامعة العربية ، 2015 ، مصر.

آمال قارة :

8.الحماية الجزائية المعلوماتية في التشريع الجزائري ،ط2 ، دار هومة ، 2007 ، الجزائر.

أمير فرج يوسف :

9.الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت ، ط1 ، مكتبة الوفاء القانونية ، 2011 ، الإسكندرية .

10.الجرائم المعلوماتية على شبكة الإنترنت ،دار المطبوعات الجامعية ، الإسكندرية ، 2008.

أيمن عبد الله فكري :

11.جرائم نظم المعلومات ، دار الجامعة الجديدة ، 2007، الإسكندرية .

جميل عبد الباقي الصغير :

12.الجرائم الناشئة عن إستخدام الحاسب الآلي ، ط1 ، دار النهضة العربية، 1992، مصر.

حسن صادق المرصفاوي :

13.أصول الإجراءات الجنائية ،منشأة المعارف ، 2000 ، الإسكندرية.

خالد ممدوح إبراهيم :

14.أمن الجريمة الإلكترونية ، دار الجامعية ، 2008، الإسكندرية .

15.الجرائم المعلوماتية ،ط1، دار الفكر الجامعي ،2009 ،الإسكندرية .

16. فن التحقيق الجنائي في الجريمة الإلكترونية ط1 ، دار الفكر الجامعي ، 2009 ، الإسكندرية.

خليفة علي الكعبي :

17.البصمة الوراثية وأثرها على الأحكام الفقهية ، ط1 ،دار الثقافة للنشر والتوزيع ، 2003، الأردن.

خالد عياد الحلبي :

18.إجراءات التحري والتحقيق في المسائل الجنائية والمعاملات المدنية والتجارية ، دار الفكر والقانون ، 2010 ، مصر.

رشاد خالد عمر :

19. المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية ، المكتب الجامعي الحديث، 2013، الإسكندرية .

زيبحة زيدان :

20. الجريمة المعلوماتية في التشريع الجزائري والدولي ،دار الهدى ، 2011، الجزائر.

سامي علي حامد عياد:

21.الجريمة المعلوماتية وجرائم الإنترنت ، دار الفكر الجامعي ، 2008، الإسكندرية.

سامي محمد الشوا:

22.ثورة المعلومات وإنعكاساتها على قانون العقوبات ، ط2، دار النهضة العربية 1994،القاهرة.

سليمان عبد المنعم ومحمد أبو عامر:

23.القسم العام من قانون العقوبات ، دار الجامعة الجديدة ، 2002، الإسكندرية .

سماتي الطيب :

24.حماية حقوق الضحية في الدعوى الجزائية في التشريع الجزائري، ط1، البديع للنشر والخدمات الإجتماعية ، 2008، الجزائر .

سالم أحمد الكرد :

25.أصول الإجراءات الجزائية في التشريع الفلسطيني ،ط3، كلية الشرطة الفلسطينية ، فلسطين غزة ، 2008.

شنّة محمد :

26.إجراءات البحث والتحري ، محاضرات ألقيت على طلبة السنة الأولى ماستر تخصص القانون الجنائي ، كلية الحقوق والعلوم السياسية ، جامعة خنشلة ، 2018.

علي عبد القادر القهوجي :

27.شرح قانون العقوبات (القسم العام) دراسة مقارنة ، منشورات الحلبي الحقوقية ، 2002،لبنان.

28.الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعية للطباعة والنشر ، 1999،بيروت.

عبد الفتاح بيومي حجازي :

29.مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي ، دار الكتب القانونية ، 2007،مصر .

عبد القادر جرادة:

30.موسوعة الإجراءات الجزائية في التشريع الفلسطيني ، مكتبة آفاق ، 2009، فلسطين.

علي حسين الخلف وسلطان عبد القادر الشاوي :

31. المبادئ العامة في قانون العقوبات ، مطابع الرسالة ، 1982 ، الكويت .

عائشة بن قارة:

32. حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، 2006 ، الإسكندرية .

عبد الفتاح الصيفي :

33.الأحكام العامة للنظام الجنائي في الشريعة والقانون ، دار النهضة العربية ، 2004 ، القاهرة.

عبد الرحمن أحمد الرفاعي :

34. البصمة الوراثية وأحكامها ف الفقه الإسلامي والقانون الوضعي (دراسة مقارنة) ،منشورات الحلبي الحقوقية ، 2013 ،لبنان .

علي حسن محمد الطوالبة :

35. التفتيش الجنائي على نظم الحاسوب والإنترنت ، ط1 ،عالم الكتب الحديثة ، 2004 ، الأردن.

عبد الرحمن خلفي :

36. الإجراءات الجزائية في التشريع الجزائري والمقارن ، دار بلقيس للنشر ، الجزائر.

فتحي محمد أنور عزت :

37.الأدلة الإلكترونية في المسائل الجنائية و المعاملات المدنية والتجارية ،دار الفكر والقانون، مصر، 2010.

محمود المسعدي :

38.القاموس الجديد للطلاب ، معجم مدرسي الفبائي ،ط7 ،المؤسسة الوطنية للكتاب،1991، الجزائر .

محمد حماد مرهج الهيتي :

39.التكنولوجيا الحديثة والقانزن الجنائي ، ط1 ، دار الثقافة للنشر والتوزيع ،2004،الأردن.

ابن منظور (أبو الفضل جمال الدين محمد بن مكرم) :

40.لسان العرب ، ط1 ، دار صادر ، لبنان ، م3.

41.لسان العرب ، ط1،دار صادر ، لبنان ، م10 .

محمد عبيد الكعبي :

42.الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، ط2 ، دار النهضة العربية، 2007 ، القاهرة .

منير الجنبيهي ومحمد الجنبيهي :

43.جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، 2005 ، الإسكندرية .

محمد علي العريان :

44.الجرائم المعلوماتية ، دار الجامعة الجديدة ، 2011 ، الإسكندرية .

محمود نجيب حسني :

45.شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 2013.

ممدوح خليل البحر :

46.مبادئ قانون أصول المحاكمات الجزائية ، دار التثافة ، 1998 ، عمان .

مولود ديدان :

47.قانون الإجراءات الجزائية ، دار بلقيس ، 2014 ،الجزائر .

محمد خليفة :

48.الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن ، دار الجامعة الجديدة، الإسكندرية، 2008.

محمد طارق عبد الرؤوف الحن :

49.جريمة الإحتيال عبر الإنترنت ، منشورات الحلبي الحقوقية ، 2011،بيروت .

نهلا عبد القادر المومني:

50.الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، ط2 ،2010، عمان.

نائلة قورة :

51.جرائم الحاسب الآلي الإقتصادية ، ط1 ، منشورات الحلبي الحقوقية ، 2005، بيروت.

نبيلة هبة هروال :

52.الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات ، دار الفكر الجامعي ، 2013 ، الإسكندرية .

نصر الدين مبروك :

53.محاضرات في الإثبات الجنائي ، دار هومة للطباعة والنشر والتوزيع ، الجزائر ، 2003.

هدى حامد قشقوش :

54.جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ، 1992

يونس عرب :

55.دليل أمن المعلومات والخصوصية ، ط1،ج1، إتحاد المصارف العربية ، 2002 .

يوسف حسن يوسف :

56.الجرائم الدولية للإنترنت ، ط1 ، المركز القومي للإصدارات القانونية ، 2011.

رابعا : قائمة الكتب باللغة الأجنبية :

1. Stein Schiollberg, computer and penal legislation, A study of the legal politics of a new technology, Oslo, Universitets for lagest, 1983, p.401.

2. David Thompson, Current trends, in computer control crime, computer quarterly, vol 9, no 12, 1991. P.2

3. Ulrich Sieber. Op. Eit. P. 27.39 and 58.

4. Michel quellie : stratégies en France par la police criminalité organisée 1996, p199 .

5. Myriam quemener, Yves chrpenel : cybercriminalité, droit pénal appliqué, 2010, economica, paris – France, page206.

خامسا : الرسائل الجامعية (الأطروحات ، الرسائل ، المذكرات) :

أ. أطروحات الدكتوراه :

إبراهيم الطنطاوي :

1.سلطات مأمور الضبط القضائي (دراسة مقارنة) ، رسالة دكتوراه ، دار النهضة العربية، 1993، القاهرة .

براهيمي جمال :

2.التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة دكتوراه – تخصص قانون ، بإشراف الأستاذ الدكتور إقلولي محمد ، جامعة مولود معمري – تيزي وزو ، 2008.

بدري فيصل :

3.مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي ، أطروحة دكتوراه – تخصص قانون عام ، بإشراف البروفيسور البقيرات عبد القادر ، كلية الحقوق ، جامعة الجزائر 1– بن يوسف بن خدة ، 2018

بن شهرة شول :

4.الحماية الجنائية للتجارة الإلكترونية ،أطروحة دكتوراه ،كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر بسكرة ، الجزائر ، 2011.

ب: رسائل الماجستير :

بن مكي نجاة :

5.السياسة الجنائية لمكافحة الجرائم المعلوماتية ، رسالة ماجستير – تخصص القانون الجنائي الدولي ، بإشراف الدكتور زواقري الطاهر ، كلية الحقوق والعلوم السياسية ، جامعة خنشلة،2009.

سعيداني نعيم :

6.آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،رسالة ماجستير– تخصص علوم جنائية ، بإشراف الأستاذ الدكتور زرارة صالحي الواسعة ،كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ، 2013.

عبد الله دغش العجمي :

7. المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة) ،رسالة ماجستير – تخصص قانون عام ، إشراف الدكتور أحمد اللوزي ،جامعة الشرق الأوسط ، الكويت ، 2014.

لهوة رابح :

8.البحث والتحري في الجريمة المعلوماتية ، رسالة ماجستير– تخصص علوم جنائية ، بإشراف الدكتورة ميموني فايزة ، كلية الحقوق والعلوم السياسية ، جامعة خنشلة ، 2014.

محمد بن حميد المزمومي :

9.جريمة الإعتداء على الأموال عن طريق الحاسب الآلي ، رسالة ماجستير – تخصص قانون إقتصادي ، كلية الإقتصاد والإدارة ، جامعة الملك عبد العزيز ، جدة – السعودية ، 2007.

مجراب الذاودي :

10.أساليب البحث والتحري على ضوء القانون 22/06 المتضمن تعديل قانون الإجراءات الجزائية ، رسالة ماجستير ، كلية الحقوق ، بن عكنون – جامعة الجزائر 1 ، 2012.

نبيل أبو الرب :

11.الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين ، رسالة ماجستير – تخصص قانون عام ، بإشراف الدكتور أنور جانم ، كلية الدراسات العليا ، جامعة النجاح الوطنية ، نابلس – فلسطين ، 2018 .

نداء المصري :

12.خصوصية الجرائم المعلوماتية ، رسالة ماجستير – تخصص قانون عام ، بإشراف الدكتور فادي شديد، كلية الدراسات العليا،جامعة النجاح الوطنية ، نابلس – فلسطين ، 2017.

يوسف العفيفي :

13.الجرائم الإلكترونية في التشريع الفلسطيني (دراسة مقارنة) ، رسالة ماجستير– تخصص قانون عام جنائي ، بإشراف الدكتور أيمن عبد العال ،الجامعة الإسلامية ، غزة – فلسطين ، 2013.

ج. مذكرات الماستر :

أحمد مسعود مريم :

14.آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون 04/09 ، مذكرة ماستر – تخصص قانون جنائي ، بإشراف الدكتور قريشي محمد ،جامعة ورقلة ، 2013.

إبتسام موهوب :

15.جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري ، مذكرة ماستر – تخصص قانون جنائي للأعمال ، بإشراف الأستاذة كوثر شريط ، جامعة أم البواقي 2014.

إلهام بوالطمين :

16.الإثبات الجنائي في مجال الجرائم الإلكترونية ،مذكرة ماستر– تخصص جنائي أعمال ، بإشراف الأستاذ اليزيد بومعراف ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي– أم البواقي ،2018

بن الأخضر محمد :

17.جرائم الكمبيوتر والإنترنت ، مذكرة لنيل رتبة ضابط ، المدرسة العليا للشرطة ،2008، بن عكنون .

بعرّة سعيدة :

18.الجريمة الإلكترونية في التشريع الجزائري ، مذكرة ماستر – تخصص قانون جنائي، بإشراف الأستاذ بنشوري الصالح ، جامعة محمد خيضر – بسكرة ، 2016.

لبيض عادل ، نزلي بشرى :

19.إثبات الجريمة الإلكترونية ، مذكرة ماستر – تخصص قانون جنائي ، بإشراف الأستاذ خويلدي السعيد ، جامعة قاصدي مرباح – ورقلة ، 2018.

معمش زهية ، غانم نسيمة :

20.الإثبات الجنائي في الجرائم المعلوماتية ، مذكرة ماستر – تخصص قانون خاص ، بإشراف الأستاذ بن فردبة محمد ، كلية الحقوق والعلوم السياسية ، جامعة عبد الرحمن ميرة – بجاية ، 2013 .

د. مذكرات الليسانس :

عرشوش سفيان :

21.جرائم المساس بأنظمة الكمبيوتر ،مذكرة ليسانس ، بإشراف الدكتور سعيد فكرة ، معهد العلوم القانونية ، المركز الجامعي – خنشلة، الجزائر، 2006 .

سادسا : المجلات العلمية :

1.لورنس سعيد الحوامدة ، الجرائم المعلوماتية أركانها وآلية مكافحتها،مجلة الميزان للدراسات الإسلامية والقانونية، صادرة عن عمادة البحث العلمي في جامعة العلوم الإسلامية – الأردن ، 2017.

2. مانع سلمى ، التفتيش كإجراء للتحقيق في الجرائم الإلكترونية ، مجلة العلوم الإنسانية ، جامعة محمد خيضر –بسكرة ، العدد 22 ، 2011.

3.حمدان هاني ، دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية ، مجلة الدراسات الأمنية ، أكاديمية الشرطة الملكية ، الأردن ، العدد 1 ، 2004 .

سابعا : المؤتمرات الدولية والوطنية (المقالات والأبحاث والأعمال) :

1.أمحمدي بوزينة آمنه ، إجراءات التحري الخاصة في الجريمة المعلوماتية ، أعمال الملتقى الوطني لآليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر،29 مارس 2017.

2.سليمان قوراري ، سعاد رحلي ، دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية ، طرابلس 24 –25 مارس 2017 .

3. عبد اللطيف ربايعة، الجرائم الإلكترونية ، بحث مقدم الى المؤتمر الأول للجرائم الإلكترونية في فلسطين والمنعقد في جامعة النجاح الوطنية – نابلس ، 2016 .

4.الغافري حسين بن سعيد ، الجهود الدولية في مجال جرائم الإنترنت ، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي خلال إجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية الأول، المنعقد بالأمانة العامة بالرياض خلال الفترة 4–5 / أبريل/ 2003.

5. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية، طرابلس ، 24–25 مارس 2017.

6. محمد الشلالدة،عبدالفتاح أمين،الجرائم الإلكترونية في دولة فلسطين،بحث مقدم لكلية القانون جامعة جرش حول الجرائم المعلوماتية،5-2015/5/7.

7.معالي موسى ، التجربة الفلسطينية في التأمين والحماية للفضاء السيبراني ، ورقة عمل مقدمة إلى الندوة العلمية حول حوكمة الإنترنت وإدارة المواقع ،بيروت ، 2018 .

8.نشناش منية،مداخلة حول الركن المفترض في الجريمة المعلوماتية،جامعة بسكرة-الجزائر،2015-2016.

9. هشام محمد فريد رستم،الجرائم المعلوماتية،بحث مقدم لمؤتمر الكمبيوتر والإنترنت في جامعة الامارات العربية المتحدة،ط3، 2004.

ثامنا : المواقع الإلكترونية :

1. **AL araby. Co. uk / العربي الجديد**
2. **AL merja.Netالمرجع الإلكتروني للمعلوماتية.**
3. **Blogs, Najah, edu**
4. **Ar.m.wikipedia.org.**
5. **Assawsana.com**
6. **Muqtafi. Birzeit. Edu**
7. **Blogs. Aljazeera.com**
8. **www.palpolice.psجهاز الشرطة الفلسطيني**
9. **www.pgp.ps/ar/pagesالنيابة العامة الفلسطينية**
10. **palinfo.com المركز الفلسطيني للإعلام**
11. **www.courts.gov.ps مجلس القضاء الأعلى الفلسطيني**

فـــهـــرس الموضـــوعـــات

ملخص :

الجريمة الإلكترونية من الجرائم المستحدثة التي بدأت في الإنتشار بشكل واسع في الآونة الأخيرة وقد إختلف الفقهاء في تعريفها، فهناك من عرفها على أنها كل فعل إجرامي يستخدم الكمبيوتر في إرتكابه كأداة رئيسية كما وقع إختلاف في تسميتها لأنها مصطلح زئبقي صعب الإمساك والإحاطة بتعريف خاص بها، كما يتسم مجرم الجريمة الإلكترونية بأنه متخصص وله القدرة الفائقة والمهارة التقنية، ويعد الدليل الإلكتروني كدليل إثبات جنائي وله قوته الثبوتية فيها، وقد تضمنت هذه الدراسة معطيات قانونية وأخرى فنية وتقنية نظرا لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الحاسوب والنظم المعلوماتية والعلوم القانونية، كما أن كافة الدول تسعى إلى تحقيق التعاون الدولي من أجل التصدي لهذه الجريمة، وهناك محاولات لتطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال إستحداث تشريعات نموذجية لمكافحة الجريمة الإلكترونية حتى لايبقى الأفراد تحت مقصلة الجريمة الإلكترونية .

Résumé :

La cybercriminalité est un crime émergent qui a commencé à se répandre largement ces derniers temps, et le Fuqaha ' ont différé dans sa définition, parce qu'il est défini comme tout acte criminel utilisé par l'ordinateur comme un instrument majeur, ainsi que d'une différence dans son nom parce que c'est un terme de mercure qui est difficile à attraper et à entourer Avec sa propre définition, le cybercriminel est caractérisé comme un spécialiste et a une grande capacité et des compétences techniques, et la preuve électronique est considérée comme une preuve médico-légale et a son propre pouvoir probant, et cette étude comprenait des données juridiques, techniques et techniques en raison de la nature du sujet, qui est un point de passage entre Informatique, systèmes informatiques et sciences juridiques, tous les pays cherchent à obtenir une coopération internationale pour lutter contre ce crime, et des tentatives sont entreprises pour développer le système juridique et l'adapter aux données internationales en introduisant une législation modèle pour lutter contre la cybercriminalité, même Les individus ne restent pas sous la guillotine de la cybercriminalité .

فهرس المصادر والمراجع

الفصل الأول

الأحكام الموضوعية للجريمة الإلكترونية

الفصل الثاني :

الأحكام الإجرائية للجريمة الإلكترونية

مقدمة

الخاتمة

فهرس الموضوعات