الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة –
كلية الحقوق والعلوم السياسية
قسم الحقوق

المذكرة

مذكرة مقدمة لنيل شهادة الماستر

الميدان: الحقوق

التخصص: قانون جنائي وعلوم جنائية

العنوان

القواعد الاجرائية لمكافحة الجرمة المعلوماتية

مقدمة من طرف الطالب:

دوايدي عبدالحميد

أمام لجنة المناقشة			
جبيري ياسين	أستاذ التعليم العالي (أ)	جامعة الشهيد الشيخ العربي التبسي	رئيسا
بوراس منير	أستاذ محاضر (أ)	جامعة الشهيد الشيخ العربي التبسي	ممتحنا
بوجوراف فهيم	أستاذ مساعد(أ)	جامعة الشهيد الشيخ العربي التبسي	مشرفا ومقررا

السنة الجامعية: 2024/2023

شكر وعرفان

بسم الله الرحمن الرحيم

الحمد لله الذي بنعمته تتم الصالحات، وأصلي وأسلم على سيدنا محمد خ اتم الأنبياء والمرسلين، وعلى آله وصحبه أجمعين.

أما بعد،

أتقدم بوافر الشكر والتقدير لكل من ساهم في إنجاز هذه المذكرة، فبفضل الله أولًا ثم بفضل دعمكم ومساندتكم، تمكنت من الوصول إلى هذا اليوم الذي أعتبره من أهم محطات حياتي العلمية.

أود أن أعبر عن خالص امتناني وعظيم تقديري إلى مشرفي العزيز، الأستاذ الدكتور: (بوجوراف فهيم)، الذي لم يدخر جهدا في تقديم النصح والإرشاد والتوجيه طوال فترة إعداد هذه المذكرة.

كما لا يفوتني أن أشكر جميع أساتذة قسم الحقوق، كل باسمه وكل بصفته

أخيرًا، أتوجه بالشكر إلى جميع أصدقائي وزملائي، وكل من قدم لي يد العون والمساعدة، ولو بكلمة طيبة، خلال مسيرتي الدراسية.

أسأل الله أن يوفق الجميع لما فيه الخير، وأن يجعل هذا العمل خالصًا لوجهه

الكريم، وأن ينفع به الباحثين والعلماء في مجاله.

إهداء

بسم الله الرحمن الرحيم

إلى من كانوا سندي وسببًا في وصولي إلى هذا اليوم،

إلى والديّ العزيزين، الذين لم يبخلوا عليّ بالدعم والنصح والمساندة، وغمروني بحبهم وتشجيعهم الدائم، أنتم مصدر إلهامي وفخري، وبدونكم لما استطعت تحقيق هذا الإنجاز.

إلى أسرتي الكريمة، لكل فرد منكم، شكرًا على تفهمكم وصبركم ودعائكم المستمر لي .كنتم خير عون لي في كل خطوة من خطوات مسيرتي.

إلى أساتذتي الأفاضل، الذين لم يدخروا جهدًا في تعليمي وتوجيهي، وقدموا لي خلاصة علمهم وخبراتهم، أشكركم جزيل الشكر على دعمكم وثقتكم بي.

إلى أصدقائي وزملائي، الذين شاركوني هذا المشوار بكل ما فيه من تحديات وفرح ، شكرًا لكم على صداقتكم الصادقة ودعمكم المتواصل.

إلى كل من كان له أثر في حياتي العلمية والعملية، أهديكم ثمرة جهودي هذه، وأسأل الله أن ينفع بها، وأن يجعلها في ميزان حسناتكم.

عبد الحميد

مقدمـــــة

مقدمة

إن للتطور التكنولوجي وانتشار وسائل الإعلام مزايا هائلة تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتّى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها، وأصبحت مرتع جديد لظهور أشكال جديدة من الإجرام اصطلح عليه الجرائم المعلوماتية أو الالكترونية.

وما يميز مرتكبي هذه الجرائم دهاءهم ونفوذهم و تحكمهم الكبير في هذه التكنولوجيا مما يصعب من إثبات الجريمة المعلوماتية و يعيق تحديد هوية مرتكبيها وحتى القبض عليهم وهذا ما فطن إليه المجتمع الدولي و أوجـب عليه التعاون الشرطي لمواجهتها من خلال تنسيق الجهود بين الدول و اتخاذ الإجراءات اللازمة لذلك , خاصة أن فشل الدول في مواجهة هذا النوع من الجرائم ليس مرتبطا لا بقوتها ولا تحضرها بل بالعكس فالدول المتطورة تعرف انتشارا واسعا و كبيرا للجرائم الالكترونية , مما اوجب عليها الدخول في علاقات تعاونية فيما بينها من خلال قواعد القانون الدولي بما لا يتنافى مع مبدأ السيادة الدولية وهو ما تنظمه العديد من المعاهدات.

ليس هذا فحسب، بل سهّلت هذه التقنية ارتكاب بعض الجرائم التقليدية وقد ازدادت هذه المخاطر تفاقماً في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات الدولية (الإنترنت) واسعة الانتشار، ما أفرز نوعاً جديداً من الجرائم يتخطى مداها حدود الدول بل والقارات، ولم يعد خطرها أو آثارها محصورة في النطاق الإقليمي لدولة بعينها، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة.

فالدول لا يمكنها أن تواجه هذه الجرائم المتطورة بنفسها دون الحاجة لغيرها لأن المعطيات الجديدة للنظام الدولي لا يمكن للدولة أن تكون منعزلة عن الدول الأخرى، و أصبح التعاون الدولي لا مناص منه ولا غنى عنه، والتضحية بجزء من السيادة وعدم التمسك بالسيادة الوطنية المطلقة أضحى شرطا ضروريا من أجل مصلحة واستمرار الدولة ذاتها وفي سبيل التصدي للتهديدات والأخطار الناجمة عن الجرائم المعلوماتية المهددة لشتى دول العالم، وهذا ما دفع بالدول إلى الاندفاع نحو الإصلاح و تطوير الآليات الوطنية والإقليمية والدولية لملائمة المستجدات الواقعية.

فقد سطر المشرع الجزائري على غرار سائر التشريعات المقارنة، سياسة جنائية اتسمت بالصرامة والحزم، فمن جانب البحث والتحري في هذا النوع من الجرائم أعطى لها المشرع خصوصية

معينة تختلف عن البحث والتحري في الجرائم التقليدية، تتوائم مع الطبيعة التقنية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والأدلة الناتجة عنها والتي تكون في شكل إلكتروني، إيمانا منه بقصور القواعد الإجراءات الجزائية القائمة لمواجهة هذه الجرائم المستحدثة.

حيث تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة وبالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات التي لم تنل حظها على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها، لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها اختيار موضوع المكافحة الإجرائية للجريمة المعلوماتية يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها شخصي والآخر موضوعي.

فالأسباب الشخصية: تمكن في أن مجال الجريمة المعلوماتية مجال حديث وواسع متميز عن الجرائم العادية بوجود إجراءات خاصة وإن إجراءات المتابعة القضائية وإثباتها تختلف كل على ماهية عليه في الجرائم التقليدية.

أما الأسباب الموضوعية : فتكمن فيما يطرحه موضوع المكافحة الإجرائية للجريمة المعلوماتية على المستويين الوطني والدولي، نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال أو الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، والقواعد الإجرائية الحديثة التي جاء بها تعديل الإجراءات الجزائية الجزائري وكذا قانون: 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وكذلك التعاون الدولي في مكافحتها.

وقد واجهتني بعض الصعوبات خلال اعداد هذا البحث تتمثل في ضيق الوقت الذي لم يسمح لي بالإحاطة الكاملة بالموضوع خاصة وأنه من المواضيع المتشعبة وذات الأبعاد القانونية الوطنية والدولية والتطورات الحاصلة في هذا المجال، وكذلك غياب المراجع المتخصصة في القواعد الاجرائية المتعلقة بالجريمة المعلوماتية على المستوى الوطني.

فقد تطرقت عدة دراسات الى الجرائم المعلوماتية من الناحية الموضوعية بدرجة كبيرة، مع وجود بعض الدراسات من الناحية الاجرائية وليس بالتفصيل، ومن بين هذه الدراسات:

– شنتير خضرة، الاليات القانونية لمكافحة الجريمة الالكترونية دراسة مقارنة، اطروحة دكتوراه، جامعة ادرار، 2021/2020، تناولت فيها الاليات الجرائية والاليات المؤسساتية لمكافحة الجريمة الالكترونية.

– بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في الشريع الجزائري، مذكرة ماجستير، جامعة وهران، 2013/2012، تطرقت من خلالها الى الاجراءات الجزائية المتعلقة بالجريمة المعلوماتية من خلال قانون الاجراءات الجزائية الجزائري، وكذلك قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

فبظهور الإجرام المعلوماتي أثار العديد من المشاكل خاصة الإجرائية في مجال الجريمة المعلوماتية باعتبار أن تلك الجرائم هي جرائم صعبة الكشف عنها و متابعة مرتكبها بالإضافة إلى أنها ترتكب على مسرح إلكتروني غير مادي يختلف عن مسرح الجريمة التقليدي، مما يجعل قانون الإجراءات الجزائية قاصرا على إجراءات المتابعة في الجرائم التقليدية فقط ؛ الأمر الذي أدى إلى تدخل المشرع لتعديل قانون الإجراءات الجزائية واستحداث قانون خاص يتضمن القواعد الإجرائية التي يمكن من خلالها لجهات البحث والتحقيق والقضاء التحري من أجل الوصول إلى الدليل المناسب لإثبات الجريمة المعلوماتية، والتمييز بين إجراءاتها وإجراءات المطبقة على الجرائم التقليدية.

ومنه نطرح الإشكالية التالية:

فماهـــي الخصوصية الإجرائية لمكافحة الجريمة المعلوماتيـــة؟

وللإجابة على هذه الاشكالية:

اعتمدنا في دراستنا هذه على المنهج التحليلي، الوصفي، كونه الأنسب لمثل هذه الدراسات من خلال تحليل المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية وكذا وصف وتحليل مختلف الاتفاقيات الدولية من أجل مكافحة هذا النوع من الإجرام المعلوماتي.

فقسمنا هذا البحث الى فصلين تطرقنا في الفصل الأول إلى ماهية الجريمة المعلوماتية، قسم إلى مبحثين:

– المبحث الأول: مفهوم الجريمة المعلوماتية.

– المبحث الثاني: تصنيف وأطراف الجريمة المعلوماتية.

أما الفصل الثاني تطرقنا فيه الخصصوصية الاجرائية لمكافحة الجريمة المعلوماتية، قسم إلى مبحثين:

– المبحث الأول: المتابعة القضائية على المستوى الوطني.

– المبحث الثاني: التعاون الدولي في مكافحة الجريمة المعلوماتية.

لنختم بحثنا بخاتمة للموضوع تناولنا فيها اهم النتائج وبعض التوصيات والاقتراحات.

الفصل الأول:

ماهية الجريمة المعلواتية

تمهيد

لقد شهد العالم في الآونة الأخيرة تطورا في مجال التكنولوجية خاصة المعلوماتية منها مما نتج عنه استخدام الحواسيب الآلية وشبكة الانترنت في مجالات متعددة ومختلفة، وعلى الرغم من أهمية الوسائل الإلكترونية وايجابيات استعمالها، إلا أن الاستخدام غير المشروع لها قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم المعلوماتية، ونظرا لحداثة هذه الجريمة فقد اختلفت آراء الفقهاء في تقديم تعريف موحد لهذه الجريمة، كما تميزت بمجموعة من الخصائص وكذلك تباين تصنيفاتها، وسنحاول التطرق في هذا الفصل إلى ماهية الجريمة المعلوماتية **(المبحث الأول)**، وبيان تصنيفاتها و أطرافها **(المبحث الثاني)**.

المبحث الأول: ماهية الجريمة المعلوماتية

إن الدول المتقدمة في المجال التكنولوجي كانت لها الأسبقية في ظهور الجرائم المعلوماتية فيها لتتطور بعد ذلك وتنتشر في دول أخرى، وبما أنها نوع جديد من الجرائم لارتباطها بالتطورات التكنولوجية الحديثة لذلك أخذت حيزا كبيرا في الدراسة من اجل تحديد مفهومها ووضع دلالات عديدة منها: جرائم التقنية العالية، جرائم الغش المعلوماتي وصولا لجرائم الانترنت ولكن لم تستقر المفاهيم على مصطلح جامع مانع لها.

وللوقوف على ماهية الجريمة المعلوماتية يستلزم علينا التطرق إلى مفهوم الجريمة المعلوماتية في **(المطلب الأول)** وتحديد خصائصها في **(المطلب الثاني)**.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية حديثة النشأة نوعا ما لارتباطها الوثيق بالتكنولوجيا المتطورة أي تكنولوجيا المعلومات " وبالنظر إلى حداثتها وكذا الخصائص والسمات التي تتفرد بها هذه الجريمة عن غيرها من الجرائم الأخرى خاصة أن مرتكبيها يتميزون بصفات غير موجودة عند المجرمين التقليديين جعلت الباحثين فيها يأخذون عدة اتجاهات في تعريفها.

ونتناول من خلال هذا المطلب التعريف الفقهي لها (الفرع الاول)، التعريف القانوني (الفرع الثاني).

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية

تعددت المفاهيم التي تعرضت للجريمة المعلوماتية واختلفت توجهات الفقهاء والدارسين للقانون ومن بين ما تم التوصل إليه.

إن الجرائم التي تنشأ عن طريق سوء استخدام تقنية المعلومات لم يوضع لها مصطلح قانوني جامع مانع يدل على مفهومها واختلف في تعريفها مختلف الباحثين لذا أطلق عليها البعض مصطلح "جريمة الغش المعلوماتي "والبعض الآخر أصطلح عليها بـ:" جريمة الاختلاس المعلوماتي " أما البعض الأخر فضل أن يسميها " بالجرائم المعلوماتية [1]."

إن الجرائم التي تستغل نظم المعلومات من اجل الولوج للمعلومات لتدميرها أو من اجل الاستحواذ عليها وإساءة استعمالها تعتبر جريمة عمدية تترتب عنها إلحاق الأذى بالمجني عليه بالمقابل تحقيق للجاني عائدات طائلة وغير مشروعة .[2]

ونظرا لهذا الاختلاف المصطلحي تطرق لتعريفها مجموعة من العلماء بطرق وجوانب مختلفة والمتمثلة فيما يلي:

1 – نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2008 ، ص 46.

2 – عبد الكريم الردايدة، **الجرائم المستحدثة وإستراتيجية مواجهتها**، دار الحامد للنشر والتوزيع، الطبعة الأولى، الأردن،2013 ، ص 50.

عرفها الفقيه الألماني " تاديمان " **Tiedeman** على أنها : كل سلوك غير مشروع باختلاف أنواعه الذي من شانه إلحاق الضرر بالمجتمع والذي يتم عن طريق استخدام الحاسب، أما الفقيه الإنجليزي" ليزي بول " Lestie D.Ball عرفها بأنها ذلك: "السلوك الإجرامي أداته الرئيسية في ارتكابه هو الحاسوب"، أما الفقيهين "فيفانت و لي ستانس " قالا عن الجريمة المعلوماتية بأنها : " تلك التشكيلة المختلفة من الأفعال الغير قانونية التي لها صلة بالمعلوماتية وتستحق العقاب عليها"[1].

وعرفها الفقيه البلجيكي" ستين ستشيولبيرج " Schiollberg stein بأنها : الجريمة التي تتطلب لارتكابها أن يكون الجاني على اطلاع وإدراك شامل لتقنية الحاسب ونظم المعلومات وحتى التحقيق فيها ومقاضاة فاعليها تستلزم أيضا هذا النوع من المعرفة ، أما الفقيهين " جاك بولوجنا و روبرت لند كويست" فعرفها على أنها : الجريمة التي يكون الحاسب اللآلي وسيلة محفزة في ارتكابها أو هي الجريمة التي يكون الحاسب ضحية لها.[2]

وعرفها الفقه الجزائري بتعاريف متعددة ومن هذه التعاريف ما يلي:" بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال.

وهناك من يعرفها على أنها " كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها. أو انها" استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع.[3]

من خلال هذه التعريف تبنى الفقه الجزائري تعريف مؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية انها جريمة يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية أو داخل نظام حاسوب وتتمثل من ناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[4].

1 – أحمد خليفة الملط، **جرائم المعوماتية**، ط2 ، دار الفكر الجامعي، مصر،2006، ص 18.

2 – رشاد خالد عمر ، **المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)**، المكتب الجامعي الحديث، الطبعة الثانية ، الاسكندرية، 2018، ص 21-22

3 – زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص 42.

4 – راضية عيمور، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، **المجلة الأكاديمية للبحوث القانونية والسياسية**، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد الأول، المجلد السادس، سنة 2022، ص 91.

ومن بين التعاريف الأكاديمية: " كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ترتبت عنه خسارة تلحق بالصحة أو مكسب بحقيقة الجاني، كما يمكن الاعتماد في التعريف للجريمة المعلوماتية[1] على:

1- تكون المعلوماتية موضوعا للاعتداء عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية.

2- عندما تكون المعلوماتية وسيلة عندها يستخدم الجان جهاز معلومات لتنفيذ جريمته.

الفرع الثاني: التعريف القانوني

إن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف النظام المعالج الآلية للمعطيات وأوكل مهمة ذلك إلى الفقه والقضاء إلا أن بعضهم من جهة أخرى اتجهوا إلى وضع تعريف نظام المعلومات وليس النظام معالج الآلية للمعطيات ومن بين التشريعات التي عرفت نظام المعلومات نذكر:

- **قانون المعاملات الالكترونية الأردني رقم 85 لسنة 2001:** حيث عرف هذا القانون بدوره من خلال نص المادة 02 الفقرة 10 نظام معالجة المعلومات على أنه" النظام الالكتروني المستخدم لإنشاء الرسائل معلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه آخر[2]".

- **قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم 02 لسنة 2002:**

حيث عرف هذا القانون هو الآخر من خلال نص المادة 2 الفقرة 06 مصطلحات نظام المعلومات الالكتروني على أنه" نظام الكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل الكترونيا[3]"

ومن خلال التعريفين نلاحظ أنها تنطبق على نظام المعالجة الآلية للمعطيات أكثر منها على نظام المعلومات ككل، كذلك لأنها انصبت في مجرى واحد معتمدة في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها وينجزها هذا النظام والتي تمثل طرق المعالجة المعلوماتية معتبرة المعالجة الآلية مجرد وظيفة من تلك الوظائف[4].

التشريع الجزائري: المشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة الإلكترونية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، معتبرا أن النظام المعلوماتي

---

1 – راضية عيمور، **مرجع سابق**، ص 91.

2 – قانون رقم 85 لسنة 2001، المملكة الأردنية الهاشمية، **الجريدة الرسمية** رقم:4524 بتاريخ 2001/12/31.

3 – قانون امارة دبي رقم 02 لسنة 2002 المتعلق بالمعاملات والتجارة الالكترونية، صادر بتاريخ 2002/02/12.

4 –أحمد خليفة الملط، **مرجع سابق**، ص 12.

في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، حيث يمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة.

كما لم يتطرق قانون العقوبات الجزائري المعدل والمتمم لتعريف جرائم الإنترنت، بل اكتفى بالعقاب على بعض الأفعال تحت عنوان الجرائم الماسة بنظام المعالجة الآلية للمعطيات[1].

فقد تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية.

وهذا يظهر واضحا من خلال نص المادة الثانية (02) الفقرة 01 من القانون رقم 09-04 الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي جاء فيها: "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية** "[2].

فقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال عديدة من الإجرام التي لم تشهدها البشرية من قبل، وهذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر: 66-156 المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 8 مواد من المادة 394 مكرر وحتى المادة 394مكرر 7.

كما استحدث المشرع الجزائري القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمتخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها.

ويقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال.

1- فضيلة عاقلي، **الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، أعمال المؤتمر الرابع عشر للجريمة الالكترونية، طرابلس، 24-25 مارس 2017، ص 05.

2 – المادة 02 من القانون رقم:09-04، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، ع 47، 2009.

المطلب الثاني: خصائص الجريمة المعلوماتية

لقد خلقت تكنولوجيا المعلومات أشكالا جديدة لارتكاب الجرائم فهناك تشابه كبير بين الجرائم المعلوماتية وبين الجرائم التقليدية فهي جميعا تحتاج الى إجراءات تتشابه في عمومها مثل: المعاينة، التفتيش، المراقبةالكترونية، التحريات والاستجواب بالإضافة إلى جمع وتحليل الأدلة.

قد لا يشير مصطلح "الجريمة المعلوماتية" بالضرورة إلى وجود سلوك إجرامي جديد، بل يعتمد إلى حد كبير على الأسلوب السيبراني الذي يمثل طريقًا جديدًا لارتكاب السلوك الإجرامي.

يمكن القول إن هذا النموذج أقرب إلى الطريقة التقليدية في تحديد وتصنيف الجرائم، إلا أن الجرائم المعلوماتية تتميز عن الجرائم التقليدية من حيث إثباتها بشكل عام، وإجراءاتها، وطبيعتها بشكل خاص [1].

فالجرائم المعلوماتية لها ما يميزها عن غيرها من الجرائم، هذه المميزات التي أصبحت تمثل حاجزا للسلطات القضائية الذين يهتمون بمصداقيتها في اكتشاف هذه الجرائم وإثباتها والوصول لمرتكبها ناهيك عن تقييم نطاقها.

وسنقسم هذه الخصائص الى خصائص متعلقة بكشف الجريمة أي من حيث صعوبة كشفها وإثباتها والخصائص المتعلقة بطبيعتها.

وبالتالي نتناول هذا المطلب من خلال تقسيم ه الى فرعين نتحدث في (**الفرع الأول**) عن الخصائص المتعلقة بكشف الجريمة المعلوماتية و(**الفرع الثاني**) نتطرق الى الخصائص المتعلقة بطبيعتها.

الفرع الأول: الخصائص المتعلقة بكشف الجريمة المعلوماتية

يصعب متابعة جرائم الحاسب الآلي والانترنت وكذا كشف عنها ومعظم هذه الجرائم تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها كما أن الجرائم لم تكتشف هي أكثر بكثير من تلك التي كشف عنها وتعود أسباب صعوبة اكتشاف وإثبات هذا النوع من الجرائم من الأمور التالية:

أولا– صعبة الاكتشاف : تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة[2].

حيث أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إن الوسيلة المستخدمة بارتكاب الجريمة هي نبضه الكترونية ينتهي دورها خلال أقل من من ثانية واحدة

1 – مراد عبد الفتاح، **شرح جرائم الكمبيوتر والانترنيت**، دار الكتب والوثائق، الإسكندرية، 2007، ص 43.

2 – الصغير جميل عبد الباقي، **القانون الجنائي والتكنولوجيا الحديثة**، ط1 ، دار النهضة العربية، القاهرة،1992 ، ص17 .

وأن الجان يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء ودون إحداث أي ضجة وتلك على خلاف الكثير من الجرائم التي نعرفها [1].

الجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس عسيرا بالكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها[2].

كما أن المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض وأنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم كشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون إبلاغ عنها للسلطات المختصة تجنبا للإظرار بسمعتها ومكانتها وهز الثقة في كفاءاتها[3].

ثانيا– صعبة الإثبات : ويعني صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أنّ الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، فهي تحتاج لخبرة فنية، يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل وذلك بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل، وقد يلجا مرتكبيها لتشفير التعليمات لمنع إيجاد أي دليل يدينه[4].

إن الجريمة المعلوماتية لا تخلف آثار مادية، يكون دليل الإثبات في الجريمة التقليدية مرئيا من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب، وكذلك المادة السامة التي تستعمل في القتل، أو المحرر ذاته الذي تم تزويره، أو النقود التي زيفت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه[5].

---

1 –المطردي مفتاح بوبكر، **الجريمة الالكترونية**، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23 –25 أيلول 2012، ص8 .

2 – نهلا عبد القادر المومني، **مرجع سابق**، ص .54.

2– هشام فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية**، ط1 ، مكتبة الآلات الحديثة، أسيوط،1992 ، ص16.

2– مراد عبد الفتاح، **شرح جرائم الكمبيوتر والانترنيت**، دار الكتب والوثائق، الإسكندرية، 2007، ص 65.

5– صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة تيزي وزو، 2013، ص124 .

الفرع الثاني: الخصائص المتعلقة بطبيعتها

لقد أتاحت شبكة الانترنت إمكانية الاتصال بين عدة حاسبات مهما كانت المسافة الفاصلة بينهما. حيث لم يعد هناك ما يحول دون تبادل المعلومات ونقلها بكميات مذهلة بسرعة هائلة وقد ادى ذلك الى نتيجة مفادها أن عدة أماكن متفرقة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة وفي آن واحد. حيث غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الظاهر متحصل في بلد الثالث في الوقت نفسه، وعليه تعتبر الجريمة المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية و الإقليمية والقارية[1].

كما أتاحت في نفس الوقت سهولة في ارتكاب هذا النوع من الجرائم ومرونة في التنفيذ بمجرد توفر جهاز حاسب آلي وخدمة انترنت يتيح إمكانية التصرف على مستوى العالم.

أولا- الطبيعة الدولية للجريمة المعلوماتية : يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكة المعلومات لم تعد الحدود مرئية وملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل كميات كبيرة من المعلومات بين أنظمة يفصل بينهما آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية بان واحد[2].

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجان عن هذه المعلومات والأموال قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[3].

لقد أثارت الطبيعة الدولية للجرائم المعلوماتية مسائل مهة تتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، هل هي الدولة التي وقع بها النشاط الإجرامي أم تلك التي توجد بها معلومات الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب[4].

إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية في الجرائم المتصلتة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبي وتستهدف الدولة أو الدفاع

1- هشام فريد رستم، **مرجع سابق**، ص 22.

2- **المرجع نفسه**، ص 23.

3- مراد عبد الفتاح، **مرجع سابق**، ص 70.

4- المطردي مفتاح بوبكر، **مرجع سابق**، ص 12.

الوطني والمصالح الإستراتيجية للاقتصاد الوطني المادة 15 من القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة . فقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة مجرمي المعلوماتية ، والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى كما أن هذا التعاون يجب أن يمتد الى مكافحة الجريمة المعلوماتية[2].

ثانيا- جريمة هادئة : أن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج الى العنف ، يتصرف المجرم المعلومات خارج العتبة حيث تقلل تقنيات المعلومات من عتبة الإجراءات ولم يعد الجان يجد نفسه وجها لوجه مع الضحية ، حيث يصبح الضحية مجهو ل الهوية بالنسبة له إذ لم يعد هناك خطر التعرض الجسدي للضحية أو السلطات.

كل ما تحتاج إليه هو القدرة على التعاون مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير مشروعة، كما تحتاج كذلك الى وجود الانترنت مع وجود مجرم موظف خبرته أو قدرته على التعاون مع الشبكة للقيام بجرائم مختلفة واختراق خصوصيات الغير أو التجسس أو الاحتيال[3].

من ناحية أخرى لا تكون مهارات التقنية الخاصة مطلوبة دائما ولكن يمكن الحصول عليها عبر الإنترنت بدلا من ذلك، كما يمكن تنزيل الأدلة والبرامج العملية مجانا أو مقابل الدفع أو يمكن الوصول الى الخدمات الأخرى التي تسهل ارتكاب الجريمة. وبالتالي يمكن شراء المعلومات المتعلقة بأحدث الفقرات الأمنية في البرامج أو حتى البيانات الشخصية.

1- المادة 15 من القانون رقم 09-04، المؤرخ في 05 أوت 2004، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، عدد 47، الصادر بتاريخ 16 اوت 2009.

2- سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الإنترنت**، دار الفكر الجامعي، دط، الإسكندرية، مصر،2007 ، ص16 .

3- نهلا عبد القادر المومني، **مرجع سابق**، ص 58.

المبحث الثاني: تصنيف وأطراف الجريمة المعلوماتية

تعد الجرائم الإلكترونية من الجرائم الحديثة التي أثارت جدلاً فقهياً حول تصنيفها إلى تقسيمات متعددة، حيث لم تراعَ أغلب التصنيفات خصائص وموضوعات الجرائم المعلوماتية.

ما يميز هذه الجرائم هو استهدافها للبيانات المعنوية للحاسوب الآلي وارتكابها بواسطة أجهزة إلكترونية، ويعود الاختلاف بين الفقهاء في تقسيم الجرائم الإلكترونية إلى ظهور جرائم جديدة باستمرار، مما يجعل من الصعب حصر أصنافها وأشكالها وخصائصها، إذ تتغير وتتجدد باستمرار مع تطور استخدامات الحاسب الآلي[1].

المطلب الأول: تصنيف الجرائم المعلوماتية

توجد عدة تصنيفات للجرائم المعلوماتية وأبرز هذه الجرائم، الجرائم الواقعة على الأشخاص (الفرع الأول)، أوعلى الأموال (الفرع الثاني)، أوعلى أمن الدولة (الفرع الثالث).

الفرع الأول: الجرائم الواقعة على الأشخاص

وهي من الجرائم المتعلقة بإتلاف وتعطيل الممتلكات الخاصة بالناس على الانترنيت، ويطلق بعض الفقهاء على هذا النوع من الجرائم مصطلح الاعتداء على جريمة الحياة الخاصة للأفراد باعتبار حق حماية الحياة الخاصة من أهم الحقوق و ذلك لما له من ارتباط وثيق بحرية الفرد، وقد جاء تجريم هذا النوع من الأفعال كحماية من التهديد الحقيقي الذي تشكله تكنولوجيات المعلومات لحق الأفراد في احترام حياتهم الخاصة مع انتشار ما يسمى ببنوك المعلومات بمختلف أنواعها[2].

وعليه يمكن أن يستخدم النظام المعلومات في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد بصور متعددة من أهمها:

- جمع البيانات وتخزينها على نحو غير مشروع.
- إساءة استعمال البيانات أو المعلومات الاسمية.
- الإفشاء غير المشروع للبيانات والمعلومات الاسمية.
- الاعتداء على سرية الاتصالات والمراسلات .

سنحاول من خلال هذا العنصر التعرض إلى بعض الجرائم التي ترتكب بواسطة النظام المعلوماتي عن طريق الانترنيت من بينها ما يلي:

أولاً: جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي

1 – محمد ابراهيم حسن، **الجرائم الالكترونية وجرائم الحاسب اللآلي**، د ط، دار النشر والتوزيع، الاردن،2006، ص 26.

2 – مدحت رمضان، **جرائم الاعتداء على الاشخاص والانترنت**، دار النهضة العربية، القاهرة، 2000، ص 38.

أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة[1].

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية[2].

اما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية[3].

هكذا أصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من أسرار الإنسان التي يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك و المؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها ،فالبيانات الخاصة بشخصية المستخدم يمكن الوصول إليها عن طريق زيارة بعض المواقع على شبكة المعلومات ، لان شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الأجهزة وتسمى هذه البروتوكولات الخاصة مثل بروتوكولات HITP الذي يمكن عن طريقها الوصول الى رقم جهاز الحاسب الشخصي ومكانه وبريده الالكتروني ، كما أن هناك بعض المواقع التي يؤدي الاشتراك في خدماتها الى وضع برنامج على القرص الصلب للحاسب الشخصي وهو ما يسمى cookies وهدفه جمع معلومات عن المستخدمين[4].

وعلية فإن القوانين المقارنة اهتمت بهذه المسألة واتجهت إلى تبني العديد من الضمانات التي يمكن تلخيصها في:

---

1 – مدحت رمضان، **مرجع سابق**، 41.

2– ممدوح خليل عمر، **حماية الحياة الخاصة والقانون الجنائي**، دار النهضة العربية، القاهرة، 1983، ص 207.

3– أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة، 1994، ص 48

4– أسامة عبد الله قايد، **مرجع سابق**، ص 50.

1 مبدأ الأخطار العام : وهو أن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومات التي تقوم بتسجيلها فيجب أن تكون هناك قيود على إنشاء الأنظمة المعلوماتية المختلفة لمعالجة البيانات[1].

2 شرعية الحصول على المعلومة: يجب أن يتم الحصول على المعلومة بطريقة تخلو من الغش والاحتيال.

3 التناسب بين المعلومات الشخصية المسجلة والهدف من ذلك التسجيل، فعلى الجهة الراغبة في إقامة أي نظام معلوماتي أن تحدد الهدف من إقامته[2].

ثانيا: جرائم السب والقذف عبر الإنترنت:

تعد جريمة السب والقذف والتعرض للحياة الشخصية للأفراد بغرض التشهير والخوض في أعراضهم، من أكبر الجرائم التي تم تجريمها في كافة القوانين، سواء في الدول العربية أو الدول الأجنبية، وترجع أسباب التجريم إلى تجريح الأشخاص في أعراضهم ومبادئهم وشرفهم ونسب أمور غير صحيحة إليهم بغرض التشهير بهم، والخوض في أعراضهم وفي حياتهم الخاصة[3]. والجرائم تتم إما عبر البريد الإلكتروني أو عن طريق شبكة الويب حيث ترتكب جريمة الذم والقدح إذا قام المعتدي بإسناد مادة للعلنية، أو بإسناده حكما أو صفة عامة في القدح إلى المعتدى عليه في أحد مواقع الشبكة الإلكترونية أو عن طريق مجموعات الأخبار كما يلاحظ أن صور الذم والقدح يمكن أن تمارس من خلال مجموعات الأخبار في نشر التعليقات والمشاركة على مواضيع منشورة، وتتحقق علنية الذم والقدح إذا كانت رؤية ما يرد في الرسائل والتعليقات متاحة للجميع في مجموعات الأخبار أو عبر غرف الدردشة والمحادثة[4].

الفرع الثاني: جرائم الاعتداء على الأموال

إن تجريم الاعتداء على الأموال في صوره التقليدية كالسرقة والنصب وخيانة الأمانة واختلاس الأموال العامة ، قد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات في عصر المصارف التقليدية ذات المقر المحدد مكانيا وقد كان أقصى ما وصلت إليه من تقدم متمثلا في إجراء التحويلات المصرفية بإجراءات ورقية معقدة و مقابل رسوم مالية معينة[5].

1- رحاب عميش، **الجريمة المعلوماتية**، الندوة الاقليمية حول الجرائم الالكترونية، طرابلس، 2011/02/27. ص 11.

2- ممدوح خليل عمر، **مرجع سابق**، ص 213.

1- مدحت رمضان، **مرجع سابق**، 46.

4- أسامة عبد الله قايد، **مرجع سابق**، ص 54.

5 - رحاب عميش، **مرجع سابق**، ص 11.

لكن في ظل هذا التطور الهائل عرفت جريمة الاعتداء على الأموال تزايدا كبيرا، وذلك باستخدام وسائل فنية للاختلاس التي ترتكب عن طريق التقنية المعلوماتية.

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الإشارة إلى أكثرها انتشاراً.

1- استخدام برامج معده خصيصا لتنفيذ الاختلاس : أشهر هذه الوسائل هو تصميم برامج معينة تهدف الى إجراء عمليات التحويل الآلي من حساب الى آخر سواء كان ذلك من المصرف نفسه أو من حساب أخر في مصرف آخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام احد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بِالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات التي حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله ، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا[1].

2- التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور ،أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار الى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات و مرتبات وهمية وتحويلها إلى حساب الجاني ،ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية فهناك بعض الأنظمة الى تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات الكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها[2].

وهو ما نصت عليه المادة 05 من اتفاقية بودابست

1- هشام فريد رستم، ص 81.

2- محمد سامي الشوا، **ثورة المعلومات وانعكاسها على قانون العقوبات دار النهضة العربية**، القاهرة، 1994، ص 70-72 وما بعدها

3- التلاعب بالبطاقات المالية.

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات[1].

4- جرائم الاستيلاء على النقود الالكترونية: يمكن تعريف النقود الالكترونية بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الائتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الالكترونية أن تحل فعليا محل تبادل العملات النقدية [2]، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[3].

الفرع الثالث: الجرائم الواقعة على أمن الدولة:

لقد أصبحت عدة دول أمنها مهدد بفعل التطور التكنولوجيا الحاصل، وتنوعت الجرائم في هذا المجال بحسب طبيعتها، ومن بين أهم الجرائم الواقعة في على أمن الدولة، جريمة التجسس (أولا)، جرائم الإرهاب(ثانيا)، الجريمة المنظمة(ثالثا).

أولا: جريمة التجسس

التجسس هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر وليس مسموحا لغير المخولين بالاطلاع عليها .وقد سهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية و الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية وهي :التجسس العسكري، التجسس السياسي، والتجسس الاقتصادي، كما تستخدم العديد من الدول التجسس باستخدام

1- رحاب عميش، **مرجع سابق**، ص 15.

2 – منير الجنبيهي – ممدوح الجنبيهي، **البنوك الالكترونية**، ط 2 – 2006 دار الفكر الجامعي – الإسكندرية ص47.

3- عبد الفتاح بيومي حجازي، **صراع الكمبيوتر والانترنت – في القانون العربي النموذجي**، دار الكتب القانونية، دار للنشر والبرمجيات، القاهرة 2007، ص 609.

التقنية المعلوماتية،وهذه الأنشطة تمارس من قبل دولة على دولة أو دول أخرى، أو من قبل الدول على مواطنيها، أو من قبل شركة على شركات أخرى منافسة[1].

ثانيا: جرائم الإرهاب

يتم بث ثقافة الإرهاب عبر الإنترنت والوسائل الحديثة عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية احدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة من منظمات أو جهات دولية أخري .وتجند الجماعات الإرهابية من خلال الإنترنت عبر وسائل وأنظمة الحواسيب الآلية عناصر ارهابية جديدة تساعدهم على تنفيذ أعمالهم الإجرامية، وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر[2].

ثالثا: الجريمة المنظمة

الجريمة المنظمة ليست وليدة التقدم وان كانت استفادت منه، فالجريمة المنظمة بسبب تقدم وسائل الاتصال والتكنولوجيات الحديثة أصبحت غير محدودة لا بقيود الزمان ولا بقيود المكان، وأصبح انتشارها على نطاق واسع وكبير كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة على وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية بسهولة، فقد اكتشفت هذه الجماعات أن استخدام شبكات الإنترنت والتكنولوجيا تستطيع أن تؤمن فرص جديدة وفوائد حية لأعمالهم وأرباح غير مشروعة عما يقومون به[3].

المطلب الثاني: أطراف الجريمة المعلوماتية

ينظر إلى المعلوماتية دائما بوصفها أداة محايدة وأن مصدر ضعفها وانتهاكها هو الإنسان الذي يقوم باستغلال الوسيلة المعلوماتية، لأن الحاسوب ليس بإمكانه ارتكاب الجرائم بمفرده، ولكن يمكن أن يستخدم كوسيلة لارتكابها، وكما هو معلوم فلكل جريمة طرفان مرتكبها المجرم المعلوماتي (الفرع الأول)، والمرتكب ضده الفعل الإجرامي الذي يقع ضحية له المجني عليه في الجريمة المعلوماتية (الفرع الثاني).

الفرع الأولى: المجرم المعلوماتي

تتميز الجرائم المعلوماتية عن الجرائم التقليدية باختلاف صفات مرتكبيها عن غيرهم من المجرمين ، لأنهم في الغالب أشخاص على مستوى عال من العلم والمعرفة، ولا يمكن حصر مرتكب الجريمة في طبقة أو فئة معينة، فقد يكون من الراشدين كما هو الشأن لمجموعة من الطلبة في معهد

1- رحاب عميش، **مرجع سابق**، ص 22.

2- يوسف صغير، **مرجع سابق**، ص .55

3- **المرجع نفسه**، ص 56.

دولي للدراسات العليا بالرباط، إذ قاموا بقرصنة أرقام بطائق ائتمان وأدوات بواسطتها ثمن مقتنيات عبر شبكة الإنترنت وتمت العملية انطلاقا من أجهزة حواسيب في حوزة المعهد الذي يدرسون به يكون مرتكب الجريمة حدثا ، وكنموذج على ذلك قيام أحد الأحداث بالاستيلاء على أموال مجموعة من الأشخاص بالولايات المتحدة الأمريكية، وذلك بعد أخذه كل المعلومات الخاصة بحساباتهم البنكية من خلال شبكة الإنترنت على إثر استمارة قاموا بملئها بعدما وزعها عليهم عبر الشبكة، ولما توصل بجميع المعلومات خزنها في الحاسوب ثم وضعها على بطائق بنكية وقام بسحب مبالغ مالية مهمة من المؤسسات البنكية بالمغرب ، وذلك بمساعدة زميل له إذ قدر مجموع المبالغ المختلسة ثلاثين مليون سنتيم، كل عملية سحب تفوق أربعة آلاف درهم، يتسلم منها هذا الأخير ثلاثمائة درهم عن كل عملية وهو بدوره تلميذ ولا يكبره إلا بفارق أشهر جعلت منه راشدا عند عرض النزاع أمام المحكمة[1].

هذا وقد انتهت بعض الدراسات المتعلقة بمجرمي نظم المعلومات إلى تقسيم هذه الفئة لأربع فئات:

- **الفئة الأولى:** العاملون على أجهزة الحاسب الآلي في منازلهم لسهولة اتصالهم به دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.
- **الفئة الثانية:** الموظفون الساخطون على منظماتهم كتخريب المواقع الخاصة بها على شبكة الإنترنت أو إتلافها أو التشهير بها.
- **الفئة الثالثة:** فئة المتسللين " Hackers" ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت تحت هذه الفئة بقسميها.
- **الفئة الرابعة:** العاملون في الجريمة المنظمة.

ومن السمات العامة لمجرمي المعلومات التي تميزهم عن غيرهم من المتورطين في أشكال الانحراف والإجرام الأخرى[2]:

– السن: إذ تتراوح أعمار مقترفي تلك الجرائم عادة ما بين 17 و46 سنة والمتوسط العمري 25 سنة؛

– المعرفة والقدرة الفنية الهائلة والحرص الشديد مع ارتفاع مستوى الذكاء؛

– الحرفية الفنية العالية، ويختفي أغلب مرتكبي هذه النوعية من الجرائم عبر دروب الإنترنت بحيث يمكن أن يختفوا تحت قناع فني يظهرهم من دولة لأخرى[3].

1 – كوثر فرام، **الجريمة المعلوماتية على ضوء العمل القضائي المغربي**، مذكرة نهاية التدريب، المعهد العالي للقضاء، المملكة المغربية، 2009/2007، ص 17.

2– كوثر فرام نفسه، ص18.

3 – محمد محمد الألفي، **المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت**، المكتب المصري الحديث، القاهرة، ط1، 2005، ص 30.

وتختلف دوافع ارتكاب الجرائم المعلوماتية بين دوافع ذاتية تتعلق بالرغبة في تحقيق الربح المادي بطريقة غير مشروعة كقرصنة بطائق ائتمان زبناء المطاعم، أو المراكز التجارية الكبرى، أو المحطات المتواجدة بالمطارات وذلك بتمرير بطائق المسافرين الذين يسددون فواتير سفرهم بواسطتها بآلة مخصصة لقرصنة المعلومات الخاصة بحساباتهم، أو زبناء الفنادق، وذلك بمساعدة المستخدمين بهذه المراكز مقابل مبالغ مالية تمنح لهم، كما قد تكون هذه الدوافع نفسية مرتبطة بالرغبة في إثبات الذات والتفوق، كالذي استفزه أحد الأشخاص بعرضه عليه وصل بضاعة توصل بها من الخارج عن طريق الشراء عبر الإنترنت باستعمال بطائق ائتمانية تخص أشخاصا أجانب مقيمين خارج المغرب حصل على أرقامها عبر شبكة الإنترنت، فاتصل هو بدوره بوكالة وسترن يونيون بالولايات المتحدة الأمريكية التي حولت لفائدة ذلك الشخص مبلغ 800 دولار حتى يؤكد تفوقه عليه إذا كانت الجرائم المعلوماتية بها العديد من الفوارق التي تميزها عن نظيرتها التقليدية إلا أنها لا تختلف عنها في وجود ضحية تتضرر مصالحه عندما يكون مستهدفا من قبل مرتكبيها[1].

الفرع الثاني: المجني عليه في الجريمة المعلوماتية

ليس من السهل تحديد نطاق الجرائم المعلوماتية على نحو دقيق إذ يمكن أن يقع الأشخاص سواء منها الطبيعية أو المعنوية العامة أو الخاصة، ويرتبط جميع هذا النوع من الجرائم بالأنشطة المالية والتجارية والشخصية، ويتخذ المجني عليه الأنماط التالية[2]:

- **المؤسسات المالية:** حيث تمس هذه الجرائم المركز الحسابي والإداري والمالي والاستثمارات وتنقلات الأموال في المؤسسات العامة أو الخاصة.
- **المؤسسات التجارية والصناعية:** وتمس هذه الجرائم الدراسات الخاصة بالأسواق ومشروعات الاستثمارات والتصنيع والإنتاج والتجارة والتوزيع ومراكز البيع. الأنظمة الشخصية: تقع الاعتداءات فيها على المعلومات الشخصية المخزنة في ذاكرات الأنظمة المعلوماتية لدى البنوك وشركات التأمين. ونشير إلى أن ضحايا الجرائم المعلوماتية ليسوا محصورين في هذه الفئات، بل هناك آخرين يختلفون باختلاف الهدف من الجريمة، فهناك مجرمين يستهدفون أشخاصا أو جهات بشكل مباشر عن طريق التهديد أو الابتزاز أو التشهير وتشويه السمعة، وذلك بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحاياهم عبر إنشاء موقع على شبكة الإنترنت يضم تلك المعلومات، كما قد يستهدفون الأطفال من خلال استغلالهم جنسيا ولفت انتباههم للإباحية ، وتتمثل عناصر قيام هذه الجريمة في وجود[3]:

1- كوثر فرام، **مرجع سابق**، ص 20.

2- محمد سامي الشوا، **مرجع سابق**، ص 58.

3- محمد محمد الالفي، **مرجع سابق**، ص 37.

1- قاصر (ذكر أو أنثى) لم يبلغ من العمر 18 سنة.

2- عرض مرئي أو مسموع يتضمن عرضا لطفل يقوم بارتكاب فعل أو سلوك جنسي سواء كان عرضا حقيقيا أو مجرد تمثيل.

3- الهدف منها هو عرض المادة الإباحية وتوزيعها ونشرها وكذا تحقيق الربح منها، وتتمظهر الأفعال المؤثمة قانونا في إنتاج مواد إباحية وفاضحة للأطفال بهدف توزيعها باستخدام جهاز كمبيوتر، وتسهيل عرضها للآخرين عن طريق هذا الجهاز ثم شراء هذه المواد الإباحية وأخيرا حيازتها أو تخزينها على قاعدة معلومات شخصية 50، والاستغلال الجنسي للأطفال له عواقب وخيمة إذ يخلف نتائج مباشرة وغير مباشرة، الأولى جسدية كالجروح والكدمات، أو انفعالية كمشاعر الرعب والقلق والعجز والغضب، أما الثانية فتتمثل في الآثار اللاحقة للاستغلال الجنسي وتشمل أثارا انفعالية ومعرفية واجتماعية، كظهور حالات من القلق والاكتئاب وضعف القدرة على ضبط الانفعالات والشعور بالذنب والخجل الشديد، فيكون هؤلاء الأطفال قليلي الثقة بأنفسهم وعدوانيين مع أقرانهم في المدرسة ومع أفراد أسرهم[1].

تأسيسا على ما سبق يتبين أن الجرائم المعلوماتية تأخذ تمظهرات مختلفة، منها معرفة الوسائل المستخدمة في ارتكابها والمسهلة لقيامها ومدى إمكانية إثباتها.

1 – كوثر فرام، **مرجع سابق**، ص 21.

خلاصة الفصل الأول

في ختام هذا الفصل حول الجريمة المعلوماتية، يمكننا التأكيد على أن التطور التكنولوجي السريع قد أوجد بيئة جديدة ومعقدة لارتكاب الجرائم، حيث أصبحت الجريمة المعلوماتية تهديدًا عالميًا يتطلب استراتيجيات مبتكرة لمواجهته، تميزت هذه الجرائم بخصائص فريدة مثل الطبيعة الافتراضية وصعوبة التتبع، مما يجعلها تحديا كبيرا للجهات الأمنية والقانونية، التصنيف المتنوع لهذه الجرائم وأطرافها المتعددة يعقدان ذلك، حيث يمكن أن يكون الجناة أفرادا، جماعات، أو حتى دولا، لهذا من الضروري تعزيز التعاون الدولي، وتطوير التشريعات، وزيادة الوعي المجتمعي للحد من هذه الجرائم وحماية المجتمعات من آثارها السلبية، وعليه فإن فهمنا العميق للجريمة المعلوماتية وخطورة تأثيرها يسهم في بناء مستقبل آمن وأكثر استقرارا في عالم رقمي متزايد التشابك.

الفصل الثاني:

الخصوصية الإجرائية لمكافحة الجريمة المعلوماتية

تمهيد

في ظل تزايد التهديدات الناتجة عن الجريمة المنظمة والجريمة المعلوماتية، أصبح من الضروري التركيز على الجوانب الإجرائية لمكافحة هذه الجرائم، يتناول هذا الفصل الخصوصية الإجرائية لمكافحة الجريمة المنظمة، مع التركيز على الجريمة المعلوماتية، سيتم استعراض كيفية معالجة القوانين الوطنية هذه الجرائم، وأهمية التعاون الدولي لتعزيز فعالية مكاحة الجريمة المعلوماتية.

يتم تقسيم الفصل إلى مبحثين؛ الأول يتناول المتابعة القضائية في الجريمة المعلوماتية ضمن القانون الوطني، من حيث القواعد المتعلقة بالاستدلال والتحقيق والإثبات، أما المبحث الثاني فيسلط الضوء على التعاون الدولي لمكافحة الجريمة المعلوماتية، بما في ذلك التعاون القضائي وآليات تسليم المجرمين.

المبحث الأول: المتابعة القضائية في الجريمة المعلوماتية في القانون الوطني

سعى المشرع الجزائري إلى التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أثار وأضرارمعتبرة على الأفراد وعلى مؤسسات الدولة من جهة، إذ نجد المشرع قام بإصدار نصوص قانونية لقمع الجريمة المعلوماتية وذلك بسبب تزايد الاعتداءات على الأنظمة المعلوماتية، وكذلك استعمال المنظومة المعلوماتية لأغراض إجرامية، حيث خص المتابعة القضائية للجريمة المعلوماتية بقواعد إجرائية خاصة.

وهو ماسنتناوله من خلال: القواعد المتعلقة بالاستدلال والتحقيق **(المطلب الأول)**، الإثبات في الجريمة المعلوماتية **(المطلب الثاني)**.

المطلب الأول: القواعد المتعلقة بالاستدلال والتحقيق في الجريمة المعلوماتية

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، الأمر الذي يتطلب على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية من إنشاء قواعد إجرائية حديثة إلى جانب القواعد الموضوعية ونظرً لاتسام هذه الجرائم المعلوماتية بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات الإجرائية والتي جعلت القواعد الإجرائية التقليدية قاصرة في مواجهة تلك المشاكل، لهذا قام المشرع الجزائري بتعديل بعض القواعد الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية خاصة المتعلقة بالاختصاص القضائي **(الفرع الأول)**، وأساليب البحث والتحري **(الفرع الثاني)**.

الفرع الأول: قواعد الاختصاص القضائي

أولا: قواعد الاختصاص المحلي

إن الاختصاص المحلي هو ذلك المجال الإقليمي الذي يمارس فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة، ذلك في حدود الدائرة التي يباشر وظيفته وذلك يتعين أن يكون في مكان وقوع الجريمة أو محل القبض على المتهم أو مكان إقامته[1]، حيث عالج المشرع الجزائري الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه، وقام بالاعتماد على عناصر تربط من الاختصاص الجهات القضائية بالنظر في الخصومة الجزائية وتتمثل في المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، و نظرا لاعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود فغالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما قد يحصل الضرر في بلد ثالث في الوقت نفسه، لهذا السبب نجد المشرع الجزائري قد أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة الإلكترونية

1 – حرزون ليلى، هدروق أسماء، **التنظيم القانوني للجريمة الالكترونية في القانون الجزائري**، مذكرة لنيل شهادة الماستر، جامعة بجاية، 2022/2021، ص 56.

بموجب القانون: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 155-66 المتضمن قانون الإجراءات الجزائية[1].

أولا: الاختصاص المحلي للنيابة العامة

وفقاً لنص المادة 37 من قانون الإجراءات الجزائية الجزائري، فإنه يتحدد الاختصاص المحلي للنيابة بمكان وقوع الجريمة أو محل القبض على أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو القبض على هؤلاء الأشخاص حتى ولو تم القبض عليهم لسبب أخر، وبالتالي فإن اختصاص وكيل الجمهورية لا يتعدى مكان وقوع الجريمة أو مكان القبض على الأشخاص المشتبه في مساهمتهم في الجريمة أو محل إقامة أحد هؤلاء الأشخاص، لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر، فإن المشرع الجزائري أجاز بتمديد الاختصاص المحلي لوكيل الجمهورية بموجب المادة 37 فقرة 2 من قانون الإجراءات الجزائية إلى دائرة الاختصاص المحاكم الأخرى، كما أن المشرع قضى في أحكام نص المادة 40 مكرر فقرة 2 من قانون الإجراءات الجزائية على أنه يتعين على ضابط الشرطة القضائية إخبار وكيل الجمهورية لدى المحكمة الكائن في مكان الجريمة ويبلغونه بإجراءات البحث ويرسل هذا الأخير فوراً بنسخة ثانية إلى النائب العام لدى محكمة المجلس القضائي التابعة له المحكمة المختصة، والذي يطالب وفق المادة 40 مكرر فقرة 2 من قانون الإجراءات الجزائية التي تتعلق بإجراءات تحريك الدعوى العمومية أو مباشرتها أو رفعها بمجرد أن يتبين للنائب العام أن الجريمة ضمن المحكمة المختصة التابعة لها وهذا ما نصت عليه المادة 40 في الفقرة 03 من نفس القانون[2].

ثانياً :الاختصاص المحلي لقاضي التحقيق

الاختصاص المحلي لقاضي التحقيق يقصد به التحقيق في المجال الذي يباشر فيه قاضي التحقيق مهامه والذي يتحدد طبقاً للمادة 40 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم على اقترافها أو محل القبض على أحد من هؤلاء الأشخاص حتى ولو كان هذا القبض حصل لسبب أخر، غير أن المشرع الجزائري قام بإلغاء في التعديل الجديد الفقرة 2 و 3 من المادة 40 وأصبحت تنص الفقرة الثانية على جواز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى في الجرائم الماسة بأنظمة المعالجة

1 - **المرجع نفسه**، ص 57.

2- أمر رقم: 66-155 مؤرخ في 18 جوان 1966، **يتضمن قانون الاجراءات الجزائية**، ج.ر، عدد48 ، معدل ومتمم بموجب الأمر رقم: 15-02 مؤرخ في 2015/07/23، ج.ر، عدد 40.

الآلية للمعطيات، ونستخلص من هذا أن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم اخرى[1].

ثالثا: الاختصاص المحلي لمحاكم الجنح

يتحدد الاختصاص المحلي للمحاكم الجنح طبقاً للمادة 329 من ق، إ، ج، ج، بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المتهمين أو شركائهم أو بمكان الذي في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر.

كما أضاف المشرع الجزائري فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحاكم إلى اختصاص محاكم أخرى.

وبالتالي فإن المشرع الجزائري أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص لوكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح.

تعد مشكلة الاختصاص القضائي في الجريمة المعلوماتية من المشكلات التي تصعب الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين وتنتج أثارها في مكان أخر داخل الدولة أو خارجها، وإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقامة أو مكان وقوع الجريمة، فأي مكان من هذه الأماكن ينعقد الاختصاص الجنائي لسلطات التحقيق والمحاكمة في الجريمة المعلوماتية، لكن على المستوى الدولي فإن الأمر بحاجة إلى اتفاقيات دولية، فقد شرعت بعض الدول في عقد اتفاقيات قضائية لتسهيل مهمة التحقيق في جرائم الحاسوب الآلي،غير أنه بالرغم من ذلك لم يتحقق تقدماً في معالجة الاختصاص القضائي بهدف الحاجة الماسة إلى قوانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسوب الآلي في كل المجالات[2].

رابعا :الاختصاص النوعي للقطب الجزائي الوطني

يختص هذا القطب حصرياً بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها وفق نص المادة 211 مكرر24 من نفس القانون حيث يختص هذا القطب في[3]:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني

1- حرزون ليلى، هدروق أسماء، مرجع سابق،57.

2- محمد الأمين البشري، **التحقيق في جرائم الحاسوب الآلي**، المجلة العربية للدراسات الأمنية والتدريب، العدد 30 نوفمبر 2000، ص 373.

3- أمر رقم: 66-155 مؤرخ في 18 جوان 1966، **يتضمن قانون الاجراءات الجزائية**، ج.ر، عدد48 ، معدل ومتمم بموجب الأمر رقم: 15-02 مؤرخ في 2015/07/23، ج.ر، عدد 40.

– جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة– العامة أو استقرار المجتمع.

– جرائم نشر وترويج أنباء معرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أوالعابرة للحدود الوطنية.

– جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

– جرائم الاتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين.

– جرائم التميز وخطاب الكراهية وخير دليل قضية اغتيال جمال بن سماعيل.

كما يختص أيضا القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بالإعلام والاتصال الأكثر تعقيداً والجرائم المرتبطة بها وفق لنص المادة 211 مكرر25 ، حيث يختص هذا القطب بالمتابعة والتحقيق والحكم في القضايا الموصوفة بالجرائم الإلكترونية الأكثر تعقيداًن ففي هذه الجرائم أعطى المشرع الجزائري للضبطية القضائية ووكيل الجمهورية استعمال وسائل خاصة للتحري أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي وهذا في مثل هذه الحالات.

خامسا :حالة الاشتراك في الاختصاص

تطبيق في هذه الحالة الإجراءات المنصوص عليها في المادة 211 مكرر 4 إلى211 مكرر 14من هذا القانون أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

يمارس هذا القطب الجزائي الوطني اختصاصا مشتركاً مع الاختصاص الناتج من تطبيق المواد (37 و 40 و 329 من ق، إ، ج، ج) بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها المتعلقة في الجرائم المتمثلة في المخدرات، الفساد، تبيض الأموال، الجريمة التي تمس بمعالجة الآلية للمعطيات، جريمة الصرف، فالاختصاص هنا مشترك بين هذه الأقطاب وهذا ما قضت به المادة 211 مكرر 27 [1].

– إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، يتنازل القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث يؤول الاختصاص للقطب الاقتصادي والمالي وجوباً حسب نص المادة 211 مكرر 28 من القانون:21-11 ، أما في حال ما إذا كان

1– حرزون ليلى، هدروق أسماء، **مرجع سابق**،62.

الاختصاص مشتركاً بين القطب الجزائي الوطني مع الجرائم التي يختص بها القطب الجزائي الاقتصادي والمالي، فيؤول الاختصاص لهذه الأخيرة[1].

– إذا كان الاختصاص مشتركا بين القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقاً للأحكام المواد 211 مكرر 16 إلى 211 مكرر 21 من هذا القانون، فإن الاختصاص يؤول لمحكمة مقر المجلس قضاء الجزائر وفق المادة 211 مكرر 29 من القانون 21–11.

نستنتج مما سبق أن الاختصاص الوطني يكفل كامل القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، ولتخفيف العبء عمد المشرع الجزائري بالتعاون مع الأقطاب الأخرى ماعدا في الاختصاص الحصري المنصوص عليه في المواد 211 مكرر 25 والجرائم الأكثر تعقيداً المنصوص عليه في المادة 211 مكرر25 [2].

الفرع الثاني: القواعد المتعلقة بالاستدلال والتحقيق

يصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الأدلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم المعلوماتية.

ومما لا شك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها أساليب التحري في ظل القانون 09– 04 المتعلق الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها : التفتيش وضبط الأشياء، المعاينة والمراقبة الالكترونية، التزامات مقدمي الانترنت[3].

وكذلك القواعد الإجرائية الحديثة في قانون الإجراءات الجزائية: التسرب أو الاختراق، اعتراض المراسلات وتسجيل الأصوات والتقط الصور.

وهو ماسنتطرق له من خلال مايلي:

أولا :أساليب التحري في ظل القانون 09–04

01– التفتيش والحجز في الجريمة المعلوماتية

يهدف التفتيش الى البحث عن الأدلة التي تفيد في كشف الحقيقة وهو من بين الإجراءات التي ثمنها المشرع الجزائري من خلال القانون09–04 ، أما الضبط أو الحجز كما أطلق عليه المشرع في

1– المادة 211مكرر 28 من القانون 21–11، المؤرخ في 25 غشت 2021، المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال، ج ر، عدد 65.

2– حرزون ليلى، هدروق أسماء، **مرجع سابق**، ص 60.

3– احمد سعود مريم، **اليات مكافحة جرائم تكنولوجيا الاعلام والتصال في ضوء القانون رقم 09–04**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة ورقلة، 2013/2012، ص 183.

إطار القانون 09-04 إجراء جديد خاص بالمعطيات والذي يتناسب مع طبيعة اللامادية واللامحسوسة لجرائم الانترنت.

أ- التفتيش في جرائم الانترنت

يعرف التفتيش على أنه البحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة التي وقعت ونسبتها الى مرتكبيها "وهو إجراء من إجراءات التحقيق التي تهدف الى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص .وذلك بهدف إثبات ارتكابها أو نسبتها الى المتهم وفقا لإجراءات قانونية محددة"، وعرفه البعض الآخر بأنه " :البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون [1] ".

من خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات إجراؤه من خلاله سيتم البحث عن الأدلة المادية الملموسة.

- حالات تفتيش المنظومة المعلوماتية

أن تفتيش المنظومات المعلوماتية على جهة المشرع الجزائري في أحكام القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائد المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث برجوع الأحكام نص المادة خمسة من هذا القانون فان تنص صراحة على جواز الدخول ولو عن بعد للمنظومة المعلوماتية بغرض تفتيش هي كليا أو جزء منها وتفتيش المعطيات المخزنه فيها وكذا تفتيش منظومة تخزين المعلومات لذا فإن هذا التفتيش مقيد ولا يمكن اللجوء إليه إلا في جرائم محددة على سبيل الحصر ويرد على الجهاز الذي ارتكبت بواسطته الجريمة[2].

- من حيث نوع الجريمة:

بالرجوع إلى نص المادة 05 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه....."[3]

حيث باستقراء نص هذه المادة نجدها تنص صراحة على جواز تفتيش المنظومات المعلوماتية في حالات معينة مذكورة في أحكام المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويمكن حصر تلك الحالات فيما يلي:

1 – خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 182

2 – حمداش شمس الدين، القواعد الاجرائية لتفتيش المنظومة المعلوماتية في القانون الجزائري، **مجلة صوت القانون**، المجلد 09، العدد02، 2022، ص100.

3- المادة 05 من القانون 09-04، **مرجع سابق**.

– الوقاية من الأفعال المنصوبة بجرائم الإرهاب أو التخريب او الجرائم الماسة بامن الدولة.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني ومؤسسات الدولة والاقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

– من حيث مكان وجود جهاز الذي ارتكبت به الجريمة

ان عملية تفتيش المنظومة المعلوماتية اوعيتها المختلفة بغرض البحث بأي شيء يتصل بجريمة معلوماتية مال كشف عنها ويدخل هذا الأمر في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها الا ان هناك حالات خاصة للتفتيش في هذه المكونات هي:

– **الحالة الاولى:** في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص مسكن المتهم أو أحد ملحقاته فانها تاخذ نفس الاحكام المقررة تفتيش المسكن وبنفس العاملات المقررة قانونا في مختلف التشريعات.

– **الحالة الثانية :** إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز او نهايه طرفية في مكان آخر كمسكن غير مسكن المتهم بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا نظام فإن عملية الكشف تصبح صعبة جدا ربما مستحيلة لذلك حتى تتم عملية تفتيش هذه الاجهزة المرتبطة بأجهزة في أماكن أخرى يتعين مراعاة القيود والضمانات التي يجيبها المشرع تفتيش هذه الأماكن[2]

الحالة الثالثة : إذا وجدت مكونات الحاسوب المادية في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة لسيارات الاجرة فان تفتيشها لا يكون الا في الحالات التي يجوز فيها تفتيش الاشخاص وفي نفس الضمانات والقيود المنصوص عليها في هذه الحالات[3].

– الشروط والاجراءات القانونية للتفتيش المنظومة المعلوماتية

أن تفتيش المنظومة المعلوماتية أحاطها المشرع الجزائري بمجموعة من الضوابط القانونية إذ لا يكون مطلقا نظرا لما فيه من مساس بحقوق وحريات الأفراد كما أن إخضاع المنظومة المعلوماتية

1 – المادة 04 من القانون:04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة الرسمية العدد 47.

2 – طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة ماجستير في القانون الجنائي، كلية الحقوق جامعة الجوائر 1، 2012/2011، ص 215.

3 – طارق الدسوقي عطية، **الامن المعلوماتي النظام القانوني للحماية المعلوماتية**، الطبعة الاولى، دار الجامعة، 2009، ص 385.

للتفتيش يكون وفق الإجراءات معينة وفيما يلي سنتناول الشروط والإجراءات الخاصة بتفتيش المنظومة المعلوماتية[1].

-الشروط القانونية للتفتيش المنظومة المعلوماتية

بالرجوع إلى أحكام قانون الإجراءات الجزائية فإن المشرع وضع جملة من الشروط الشكلية والاخرى موضوعيه التي يجب على القائم بالتفتيش أن يلتزم بها تحت طائلة بطلان إجراءات التفتيش

*** الشروط الموضوعية**

يشترط أن يتوافر في التفتيش سببا له وان يكون محله الحاسوب في كل مكوناته المادية والمنطقيه والشبكة الالكترونية بالاضافة الى وجود سلطة المختصة بالقيام به وعلى ضوء ما سبق فإن القواعد الموضوعية لتفتيش النظم المعلوماتية تتمثل فيما يلي:

***سبب التفتيش:**

ان السبب التفتيش المنظومة المعلوماتية كما سبق ذكره يكون إما لحماية النظام العام أو لمستلزمات تحريات او لاجل التحقيقات القضائية الجارية إليه في أحكام نص المادة 44 من قانون الإجراءات الجزائية غير أنه وخلافا لذلك فان المشرع الجزائري خرج عن هذه القواعد العامة بخصوص الجريمة المعلوماتية وجعل من التفتيش المنصب على المنظومة المعلوماتية إجراء وقائي في مواجهة ما يقدم عليه المجرم المعلوماتي واستعمال الوقاية التقنية لإرسال اتصالات الإلكترونية قد تكون سابقة ارتكاب أي جرم ودون توجيه الاتهام لأي شخص وقد أوضحت المادة 05 من القانون 04/09[2].

*** محل تفتيش نظم المعلوماتية:**

لكي يكون التفتيش صحيحا يجب أن يرد على المحل الذي قد يكون الشخص فيه وبحوزته الحاسب الالكتروني وهذا المحل يجب ان يكون محددا أو قابل للتحديد وجائزا قانونا وبالتالي فالشخص الذي يقوم بتفتيش نظم المعلوماتية قد يكون من خبراء البرنامج سواء كانت برامج نظام او برامج تطبيقات أو من مشغل او مستخدمي الحاسب أو مقدمي الخدمة أو المهندسين للصيانه والاتصالات أو من مديري نظم المعلوماتية اما الاشخاص الذين يقومون عليهم التفتيش هم اي اشخاص اخرين يكونوا بحوزتهم معدات وأجهزة معلوماتية وأجهزة حاسب آلي محمول او تليفونات متصلة بجهاز المودم او مستندات وفي كل الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به.

1- حمداش شمس الدين، **مرجع سابق**، ص 102.

2- زيبحة زيدان، **مرجع سابق**، ص 139.

وتشمل مكونات الحاسوب المادية على الاشياء الملموسه وملحقاته [1]، والتي تتمثل بشكل وحدات كوحدة الذاكرة لوحة المفاتيح والشاشة ووحدة التحكم وكل واحدة لها مهمة محددة فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية والتي يمكن إيجاده في مسكن المتهم أو مسكن غير المتهم والتي قد تتواجد أيضا في مكان عام فهي في ذلك تخضع لقواعد التي تحكم ذلك المكان وسواء كان الشخص الحائز المالك أو الغرامات بالنسبه للمكونات الحاسوب المعنوية المتمثلة في المعلومات والبيانات المعالجة آليا فهي محل خلاف باعتبارها غير مادية[2].

- الشروط الشكلية لتفتيش النظم المعلوماتية

يستخلص من نص المادة خمسة من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام بأن التفتيش في مجال جرائم المعلوماتية يدرجه المشرع في إطار أحكام قانون إجراءات جزائية والاختلاف الوحيد الموجود عن التفتيش العادي يكمن في طبيعة المكان الذي يوجد فيه الكمبيوتر ومكوناته فيما إذا كان خاصا وعاما هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أم أجنبيا.

ففي الحاله الاصليه يكون التفتيش ويكون بالانتقال الى مسكن المتهم أو المكان الذي تتواجد فيه الأجهزة المقصوده او في الاماكن العامة حال حيازة الشخص لجهاز الحاسوب الآلي واحد مكوناته المادية وسائط التخزين مثل الأقراص المرنة والأقراص الصلبة والأقراص المضغوطة والأشرطة الممغنطة فواضح أن القانون حال هذه الإجراءات للقواعد العامة في قانون الإجراءات الجزائية.[3]

*** صفة القائم بالتفتيش للمنظومة المعلوماتية**

الاصل ان تقوم باجراء تفتيش المنظومة المعلوماتية سورة التحقيق الأصلية المتمثلة في قيد التحقيق أو النيابة العامة باعتبار سلطه قضائيه إلا أنه يجوز لطلبات السلطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر عن السلطة المختصة وهو الأمر الذي أكدته المادة خمسة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم بالتكنولوجيات الإعلام وحددت الأشخاص المؤهل لهم قانونا بتفتيش المنظومة المعلوماتية وحضارتهم فيما يلي:

*** السلطات القضائية**

باعتبار ان الامر باجراء تفتيش هو مخول حصريا للسلطات القضائيه دون سواها فان التحقيق باعتباري مختص بإجراء كل التحقيقات بما فيها التفتيش لكن في كل الحالات التي يقوم فيها بهذا الاجراء لابد من يختار وكيل الجمهورية الذي له الحق في مرافقته باستثناء أن يقوموا ببعض إجراءات

1- حمداش شمس الدين، **مرجع سابق**، ص 104.

2- **المرجع نفسه**، ص 105

3- احمد سعود مريم، **مرجع سابق**، ص 192.

التحقيق لان الاختصاص الاصيل مباشره يعود التحقيق وحده دون سواه ولا يكفي توافر صفة قاعدة تحقيق ليقوم بإجراء تفتيش بل لابد ان يكون مختصا سواء من ناحية الاختصاص المكان او النوع ويتحدث اختصاص قاده تحقيق محليا اما بمكان وقوع الجريمه أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على احد هؤلاء الاشخاص حتى ولو كان القبر قد حصل لسبب آخر.

- التفتيش عن بعد

هو الذي نصت عليه الفقرة 02 من المادة 05 والتي قضت بأنه في الحالة المنصوص عليها في الفقرة –أ– من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة اخرى، وان هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد اعلام السلطه القضائية المختصه مسبقا بذلك[1].

فقد صرحت المادة 02/05 بامكانية الدخول الى منظومة معلوماتية موجودة على جهاز آخر متصل بالجهاز الاول ، ولكن في مكان مختلف تماما عنه داخل الدولة متصلا فيما بينها بشبكة اتصالات أيا كانت يمكن الدخول الى هذه المنظومة سواء كان الجهاز الثاني ملك المتهم او لشخص اخر فلا فرق ما دامت هناك دلائل على إمكانية وجود المعطيات المبحوث عنها في ذلك النظام وعليه فإن التفتيش عن بعد في هذه الفرضية يشترط[2]:

- وجود دلائل أو أسباب تدعو للاعتقاد بين الكشف عن المعطيات يكون البحث في المنظومة الثانية.

- اعلام السلطة القضائية فلما يفرض المشرع الطلب إذن ثاني يسمح بهذا التفتيش وإنما مجرد اعلام السلطة القضائية التي تولد أمر هذا التفتيش.

ب- الضبط في الجرائم الالكترونية

لما أقر المشرع الجزائري تفتيش المنظومة المعلوماتية كما سبق وأن فصلنا فبالضرورة كان لابد له أن يقر ضبط الأشياء المستخلصة من تفتيش البيئة الافتراضية بما يناسبها وهو الحجز بأنواعه، والحجز هنا هو كل ما يتعلق بإجراءات التحقيق أي التفتيش عن بعد والضبط هنا يعد من إجراءات التحقيق حيث أن الضبط يعد في الأصل من إجراءات الاستدلال[3].

1- المادة 05 من القانون 09-04، **مرجع سابق**.

2- حمداش شمس الدين، **مرجع سابق**، ص 103.

3 - خضرة شنتير، **الاليات القانونية لمكافحة الجريمة الالكترونية دراسة مقارنة**، اطروحة دكتوراه، جامعة ادرار، 2021/2020 ، ص 101.

حيث نظم المشرع الجزائري الضبط في المادة 06 من القانون 04 – 09 والتي تتمكن من خلالها السلطة التي تباشر التفتيش من ضبط أو حجز المعطيات تكون مفيدة في كشف الجرائم أو مرتكبيها، والضبط يعني وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها[1].

02- المعاينة والمراقبة الإلكترونية

بالإضافة الى التفتيش والضبط تأتي إجراءات تتعلق بالمعاينة والمراقبة:

أ- المعاينة في الجريمة المعلوماتية

المعاينة هي إجراء ينتقل بمقتضاه المحقق أو القاضي لمكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة ويعرف كيف وقعت ويقوم بجمع الأشياء التي تفيد في كشف الحقيقة، حيث أن جوهر المعاينة هو ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة[2] ، ويعد مسرح الجريمة بمثابة الشاهد الصامت الذي إذ أحسن المحقق استنطاقه حصل على معلومات مؤكدة.

ب- المراقبة الالكترونية للاتصالات

تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا كبيرا في الكشف عن الجرائم الالكترونية وهي وسيلة هامة من وسائل الإرشاد الجنائي، ويقصد به المراقبة الأمنية التي محلها الاتصالات الالكترونية التي عرفها المشرع الجزائري في إطار القانون 04 – 09 وهي التي ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية[3].

وقد استعمل المشرع الجزائر مصطلح مراقبة الاتصالات الالكترونية بالرغم أن معظم أحكام قانون09-04 هي مستمدة من اتفاقية بودابست والتي استخدمت مصطلح اعتراض معطيات المحتوى[4].

والشيء المراقب هو شبكة الانترنيت، حيث يرقَاب من خلالها الاتصالات الإلكترونية للمشتبه فيه التي تتم عن طريق الانترنيت، كمراسلاته مثلا عبر البريد الإلكتروني، والجدير بالذكر أن شرطة أمريكا الشمالية تعد قائمة بالأشخاص المشتبه بهم والمبحوث عنهم توضع في ملف مركزي وترسل إلى

---

1 – خالد عياد الحلبي، **مرجع سابق**، ص 168.

2 – منير محمد الجنبيهي، **مرجع سابق**، ص 63.

3 – المادة 02، القانون 09-04، **مرجع سابق**.

4 – دلال مولاي، **اشكالية الاثبات في جرائم النترنت في التشريع الجزائري، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية**، جامعة ابوبكر بلقايد تلمسان، 2018/2017، ص209.

مئات المواقع، حيث تسمح هذه التقنية بالوضع اليومي للصور في الواجهة، مما تساعد جهات البحث في عملية المراقبة، كما أ ن هذه الطريقة تستلهم رجال التحريات الأولية لأنها بكل بساطة تنشر عبر الانترنيت آراء للبحث؛ كما يراقب القائم بإجراء المراقبة الإلكترونية البيانات غير المشروعة[1].

– أحكام المراقبة الإلكترونية:

يحمي المشرع الجزائري على غرار التشريعات الأخرى الحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة وذلك عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة في المادة 303 مكرر من قانون العقوبات والتي جاء فيها أ نه (:يعاقب بالحبس 06 أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

– بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

– بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه...

غير أن المشرع الجزائري أباح الاعتداء على هذه الحرمة بسبب وقاية أفراد المجتمع من خطورة بعض الجرائم، وذلك في المادتين 3 و 4 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومن خلال استقراء هذه المواد نجد أن المشرع أحاط هذه الإباحة ببعض الضمانات القانونية الفعالة لحماية الحرية الفردية، وحماية حق الإنسان في سرية اتصالاته بمختلف أنواعها وتتمثل هذه الضمانات في:

–إباحة المراقبة بإذن القانون:

نصت المادة 03 من القانون السابق الذكر على إباحة المراقبة الإلكترونية كما يلي: (مع مراعاة

الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها...).

تنص المادة 01/04 الحالات التي تتيح اللجوء إلى عملية مراقبة الاتصالات الإلكترونية، وهي كالتالي (يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية[2]:

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .

1– عمر محمد يونس، **الاجراءات الجنائية عبر الانترنت في القانون الامريكي**، ددن، دب ن، 2005، ص 366.

2– المادة 03 من القانون 09–04، **مرجع سابق**.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الاقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهتم الأبحاث الجارية دون اللجوء إلى المارقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة....

03– التزامات مقدمي الخدمات

إن الدليل في الشكل الإلكتروني يمتاز بأنه سريع التبخر أو التعديل، حثت الاتفاقية العربية لتقنية المعلومات، على ضرورة أن تتبنى الدول الأعضاء في تشريعاتها الداخلية إجراء التجميع الفوري للمعطيات المتعلقة بحركة المرور، و يلزم بهذا التجميع مزودي الخدمات، بمعنى أن يقوم هذا الأخير بجمع المحتويات المتعلقة بالاتصال في فترة الإنتاج وتجميعها لحظة النقل عبر الاتصال ولقد نص المشرع الجزائري على هذا الإجراء في المواد 10 و 11 و 12 من الفصل الرابع من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحت عنوان التزامات مقدمي الخدمات، حيث يلتزمون بمساعدة السلطات في تجميع وتسجيل المعطيات وحفظ المعطيات المتعلقة بحركة السير، حيث تقرر المواد السابقة تحملهم المسؤولية في حالة الإخلال بالتزاماتهم[1].

مساعدة السلطات:

وفقا للمادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإن

مزود الخدمات يلتزم بما يأتي:

– تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، بحيث انه لما كان مزود الخدمات بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها، ومن ثم فإنه ملزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها 23، وذلك بتجميعها أو تسجيلها.

– وضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من ذات القانون تحت تصرف السلطات المكلفة بالتحريات القضائية.

–الحفاظ على السرية، إذ يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من

المحققين وكذا المعلومات المتصلة بها.

1– احمد سعود مريم، **مرجع سابق**، ص 207.

-حفظ المعطيات المتعلقة بحركة السير:

تنص المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

على: (مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدموا الخدمات بحفظ[1]:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها

ثانيا: أساليب التحري في ظل قانون الإجراءات الجزائية الحديثة.

نظرا لخطورة الجريمة الالكترونية وصعوبة اكتشاف المجرم الالكتروني وإيجاد الآلية المناسبة للتحقيق التقليدي، قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية الجديد المعدل والمتمم بالقانون 06 - 22 وهي: التسرب أو الاختراق الإلكتروني واعتراض المراسلات وتسجيل الأصوات.

01- التسرب:

عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 كمايلي: يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف[2].

وعرفه الفقه بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنظمتهم الإجرامية وذلك بإخفاء الهوية الحقيقية، وبتقديم المتسرب على أنه فاعل أو شريك[3].

1- المادة 11 من القانون 09-04، **مرجع سابق**.

2- المادة 65 من القانون 06-22 مؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006، يتمم الأمر 66-156 المؤرخ في 18 صفر 1386الموافق 8 يونيو 1966، المتضمن قانون الاجراءات الجزائية، **الجريدة الرسمية**، العدد 84، الصادرة بتاريخ 4 ذي الحجة 1427 الموافق 24 ديسمبر 2006.

3- الهام بن خليفة، **القواعد الاجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال** مداخلة حول الجرائم الالكترونية واليات مكافحتها، كلية الحقوق والعلوم السياسية، جامعة الوادي، ص 06.

أ- شروط التسرب

ينطوي إجراء التسرب على المساس بالحريات الفردية وحقوق الإنسان لذا نجد أن المشرع الجزائري وضع له ضوابط أو شروط تكون بمثابة ضمانات يتعين مراعاتها عندما تقتضي ضرورة التحقيق للقيام بمثل هذا الإجراء وتتمثل هذه الشروط فيما يلي[1]:

1 – أن تتم هذه العملية بإذن من وكيل الجمهورية المختص إقليميا أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية، وهو ما جاء في المادة 65 مكرر 11.

2 – يجب أن يكون الإذن مكتوبا ومسببا، وإذا خلا من هذا الشرط فان التسرب قد يقع تحت طائلة البطلان، ويجب أن يتضمن التسبيب العناصر التي يستند إليها القاضي الآمر به، مع ذكر الجريمة موضوع التسرب، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وهو ما ورد في الفقرات الأولى والثانية من المادة 65 مكرر 15.

3 – يجب ألا تتجاوز المدة المطلوبة لعملية التسرب الأربعة أشهر، والتي يمكن تجديدها حسب مقتضيات التحري والتحقيق، والتجديد يكون بإذن مكتوب ومسبب ويكون بنفس المدة وهي ألا تتجاوز أربعة أشهر، كما يجوز للقاضي الذي أمر بالتجديد أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، وهو ما حدده المشرع في الفقرات الثالثة والرابعة والخامسة من المادة 65 مكرر 15.

4 – يشترط المشرع كذلك في المادة 65 مكرر 13 وجود تقرير مسبق يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض المتسرب للخطر، وذلك من أجل أن يطلع القاضي بشكل مفصل عن ظروف القضية ومتطلباتها.

وحسب المشرع الجزائري وطبقا للمادة 65 مكرر فإن إجراء التسرب، يتخذ في حال التحقيق أو التحري في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.

02- اعتراض المراسلات وتسجيل الأصوات والتقط الصور

جعل المشرع الجزائري من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور أهم الأساليب المستحدثة للكشف عن الجرائم الالكترونية وهي جرائم ترتكب بشكل خفي وذلك تماشيا مع التقدم

1- الهام بن خليفة، **مرجع سابق**، ص 08-09

العلمي والتكنولوجي المعاصر لاسيما في مجال الاتصالات الإلكترونية، مما أفرز أساليب عملية جديدة عالية الكفاءة والفعالية أحدثت ثورة في مجال التحريات[1].

استحدث المشرع الجزائري بموجب القانون رقم 06 – 22 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر الى المادة 65 مكرر10 وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه[2].

نص المشرع الجزائري على إجراء الاعتراض في المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية.

لم يضع المشرع الجزائري تعريف لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ويعرف البعض الاعتراض بأنه عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب الجريمة[3].

إذ تتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض.

أما تسجيل الأصوات والتقاط الصور فيقصد بها تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وتكمن أهمية إجراء الاعتراض في كون أن التكنولوجيات المعلوماتية قادرة على نقل كميات ضخمة من البيانات في شكل نصوص أو صور أو أصوات، فإنها في المقابل تقدم إمكانيات واسعة لارتكاب الجرائم، والتي تأخذ شكل بث محتوى غير قانوني كمستند يحتوي على بيانات مزورة، إذ أن مثل هذه الجرائم تفترض النقل والاتصال، وعليه فمن غير الممكن تحديد الوقت الفعلي لهذه البيانات غير المشروعة إلا من خلال اعتراض محتوى المستند، وإن لم يتم تدارك هذه البيانات بالاعتراض سوف تقع الجريمة تامة، وبذلك يعد الاعتراض من أهم الإجراءات التقنية اللازمة لتعقب الدليل في الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والمحافظة عليه[4].

---

1 – بومدين كعيش، أساليب التحري الخاصة في جرائم الفساد، **مجلة القانون**، جامعة ابو بكر بلقايد تلمسان، العدد7، ديسمبر 2016، ص 304.

2 – بومدين كعيش، **مرجع سابق**، ص 311.

3 – **مرجع نفسه**، ص312.

4 – هلالي عبد اللاه احمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية اتفاقية بودابست**، دار النهضة العربية، القاهرة، 2006، ص 271–272

- أحكام اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أورد المشرع الجزائري عدة قيود حال القيام بهذا الإجراء تتمثل في:

1 - يجب أن تتخذ هذه الإجراءات حيال جرائم محددة على سبيل الحصر.

2 - ضرورة أن تتم هذه الإجراءات بناءا على إذن مكتوب من وكيل الجمهورية المختص إقليميا أو من قاضي التحقيق وتحت مراقبته المباشرة في حالة فتح تحقيق قضائي، وهذا وفقا للمادة 65 مكرر 5؛ وحسب المادة 65 مكرر 7 فإنه يجب أن يتضمن الإذن المكتوب كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها[1].

3 - يجب أن يكون الإذن لمدة أقصاها 04 أشهر قابلة للتجديد، حسب مقتضيات التحري والتحقيق، حيث أن التجديد يكون بإذن مكتوب ومتضمن العناصر السابقة ومدة التجديد وهو ما جاء في الفقرة الأخيرة من المادة 65 مكرر 7.

4 - إمكانية الدخول إلى كل الأماكن العامة والخاصة بغير علم أصحابها وموافقتهم وفي كل وقت وهو ما أشار إليه المشرع في المادة 65 مكرر 05.

- يمكن للقائم بالاعتراض المأذون به أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعملية، وهو ما جاء في المادة 65مكرر8.

- حسب المواد 65 مكرر 9 ، و 65 مكرر 10 فإن القائم بالاعتراض يحرر محضرا بعد الانتهاء من هذه العملية يضمن فيه محتوى العملية والترتيبات التقنية المتخذة، ويذكر فيه تاريخ وساعة بداية ونهاية العملية، ويقوم بنسخ المراسلات أو المحادثات أو الصور المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض[2].

المطلب الثاني: الإثبات في الجريمة المعلوماتية

من المعلوم أن إثبات الجريمة يكتسي أهمية بالغة إذ أن الغاية في الإثبات هي الوصول إلى الحقيقة، فالجريمة واقعة من الماضي وليس بالإمكان معاينتها والتعرف على حقيقتها وإسنادها للمتهم والقضاء بشأنها لا يتم إلا بالاستعانة بوسائل تجسد صورتها كما حدثت وهذه الوسائل هي ما يسمى بأدلة الإثبات فالاهتمام يبدأ في صورة الشك والقاضي يمحص هذا الشك بأدلة الإثبات فيصل بالشك إلى اليقين.

1- الهام بن خليفة، **مرجع سابق**، ص 10.

2 - الهام بن خليفة، **مرجع نفسه**، ص 10.

إن الأدلة الالكترونية إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات، أو الراسم، وإما أن تكون مخرجات غير ورقية أو أن تكون الكترونية : كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الالكترونية غير التقليدية، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به، أو الانترنت بواسطة الشاشات او وحدة العرض المرئي، ويكون الدليل باطلا إذا تحصل عليه عن طريق مخالفة القانون. ولذلك يجب أن يتم الحصول على الدليل وفق الإجراءات والشروط المنصوص عليها قانونا، وذلك لأجل أن يكتسب حجيته في إثبات الجرائم الالكترونية.

وهو ماسنتناوله في هذا المطلب من خلال: مفهوم الدليل الرقمي (الفرع الأول)،

الفرع الأول: مفهوم الدليل الرقمي

يقصد بالدليل لغة المرشد وما يستند به أما عن الدليل قانونا فهو إقامة البينة والبرهان والحجة على الشخص أمام القضاء وفقا لأحكام القانون على واقعة قانونية متنازع عليها بين الخصوم وهذا التعريف يتعلق بالدليل الجنائي بوجه عام أما الدليل الرقمي فهو وإن كان متشابها مع الدليل الجنائي في الغاية فإنه يختلف عنه في المضمون.

أولا: تعريف الدليل الرقمي

تعددت التعريفات التي قيلت بخصوص الدليل الرقمي وتباينت بين التوسيع والتضييق، ويرجع ذلك البيئة التي ينشأ فيها الدليل الرقمي والمجال الذي يستخدم فيه هذا الدليل، فاختلف الباحثين في تعريفهم للدليل الرقمي فمنهم من عرفه من منظور تقني بحت ومنهم من عرفه تعريف قانوني مركزا على إجراءات استخلاصه ومدى اعتماده كوسيلة إثبات لدى مختلف التشريعات، يقصد بالتعريف التقني للدليل الرقمي تلك التعريفات التي اعتمدت على الجانب الشكلي دون الجانب الإجرائي وجعلت من محل استخلاصه الحاسب الآلي أساسا لتعريفه من هذه التعريفات نجد أن الدليل الرقمي هو:

" الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل المجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات تكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات او الأشكال أو الرسوم وذلك من اجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون[1]."

كما عرف بأنه عبارة عن معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها

1 – نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، **مجلة الباحث للدراسات الأكاديمية**، جامعة باتنة، العدد الحادي عشر، جوان 2017، ص 911

وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شخص له علاقة بجريمة أو جان أم مجني عليه[1].

والملاحظ من خلال التعريفات السابقة للدليل الرقمي أنها تحصر مفهومه على ذلك الذي يتم استخراجه من الحاسب الآلي، ولا شك أن ذلك فيه تضييق لدائرة الأدلة الرقمية، فهي كما يمكن أن تستمد من الحاسب الآلي، فمن الممكن أن يتحصل عليها من أية آلة رقمية أخرى، فالهاتف وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدرا للدليل الرقمي، وعليه يمكننا تعريف الدليل الرقمي على أنه:

" الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة وأدوات الحاسب الآلي، أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها الى القضاء بعد تحليلها علميا باستخدام برامج وتطبيقات خاصة أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور أو أشكال وأصوات لإثبات وقوع الجريمة وتقرير بالبراءة أو الإدانة فيها مما يضفي عليه طابع وسيلة إثبات جنائي[2]."

وانطلاقا من هذا التعريف الذي أعطى للدليل الرقمي يتضح لنا أنه من الأدلة الجنائية الرقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعديا لحدود الزمان والمكان ويبدو أن الدليل الرقم يعتمد على التطور التلقائي وهذا راجع لبيئته التقنية المتطورة بطبيعتها ومن خلال الدليل الرقمي يمكن رصد المعلومات عن الجانب وتحليلية في ذات الوقت.

ثانيا: تحديد نطاق استخدام الدليل الرقمي في الإثبات الجنائي

لقد تعاظم دور الإثبات العلم للدليل مع ظهور الجرائم المعلوماتية وضرورة اشتقاق الدالة الرقمية المطلوبة للإثبات في هذه الجرائم وكشف أنماط الجرائم المرتكبة باستخدام الحاسب الآلي وهو الدور الذي يختص به الخبراء القضائيين فأصبح إنشاء المعامل الجنائية الرقمية مطلبا ملحا لفحص الأدلة الرقمية والتقييم عملية الإثبات الرقمي وتحليل الجرائم في نطاق ما يعرف باسم نظم الخبرة الأمنية فكان الاهتمام الذي حظي به الدليل الرقمي قياس بغيره من الأدلة الأخرى المستمدة من الآلة مرده انتشار استخدام تقنية المعلومات الرقمية التي تعاظم دورها مع دخول الانترنت شتى مجالات الحياة وأصبح بذلك هذا الوسط طول أداة الفعالة التي يستغلها المجرمون المعلوماتيين في الجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الرقمي ولذا كان الدليل الرقمي هو الدليل الأفضل لإثبات هذا النوع من الجرائم لأنه من طبيعة الوسط الذي ارتكبت فيه ومن هنا بدأت أهمية

1 – محمد الأمين البشري، **التحقيق في الجرائم المستحدثة**، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص88

2 – نور الهدى محمودي، **مرجع سابق**، ص 912.

هذا النوع من الأدلة لكن هل يعني أن الدليل الرقمي ينحصر مجاله كدليل إثبات فقط على الجريمة المعلوماتية[1].

فإذا كانت الجرائم المعلوماتية تختلف عن الجرائم التقليدية في طريقه الحصول على الدليل حيث أن هذه الأخيرة يتم استخلاص الدليل منها بواسطة رجل الشرطة العلمية الذي ينتقل الى مسرح الجريمة ليقوم بوصف كل شيء وصفا دقيقا موضحا مكان الدليل والشكل الذي وجد عليه وكل ما يتعلق به حسب ما يشاهده أمامه ثم يتم تصوير الدليل المادي فوتوغرافيا وكذلك حركيا عن طريق كاميرا الفيديو وبعدها يتم تحريز الدليل في حرز خاص موضحا به نوعه ومكان العثور عليه و من قام بتحريره وينقل إلى المختبر الجنائي لاستكمال فحصه وإصدار تقرير فني يوضح به جميع ما يتوصل إليه من نتائج كذلك فإن الأمر لا يختلف كثيرا بالنسبة للدليل الرقمي في الجريمة المعلوماتية الذي يمر بمرحلة التحديث ثم التحليل ثم التقديم والعرض.

والملاحظ أن الجريمة المعلوماتية رغم شدة صلتها بالدليل الرقمي إلا أن إثباته لا يقتصر عليه فمن الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرها ولذلك فإن التلازم بين مشكلة الدليل الرقمي لإثبات الجريمة المعلوماتية ليس له أي فعاليه هنا في الجريمة المعلوماتية وإثباتها تثير إشكالات أخرى لا شأن لها بالدليل الرقمي فإن كانت غاية الدليل عموما هي إثبات الجريمة ونسبتها إلى مرتكبها فإن هذا الدليل لا يكون قاصرا لأنه إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها إذ مع ذلك تصح تسميته كدليل وتبدو أهمية هذا النوع من الأدلة بالنسبة للجريمة المعلوماتية لصعوبة إثبات وقوعها عادة[2].

وعليه فإن العلاقة بين نطاق العمل بالدليل الرقمي من جهة والجريمة المعلوماتية من جهة أخرى هي علاقة تلازم. لأن الدليل الرقمي مثل ما يصلح لإثبات الجريمة المعلوماتية ويعتبر في ذات الوقت الدليل الأفضل لإثباتها فإنه من ناحية أخرى كذلك يصلح لإثبات الجرائم التقليدية، ونطاق العمل بالدليل الرقمي وإشكالية قبولها كدليل إثبات في الجريمة المعلوماتية يختلف تبعا لطبيعة الجريمة وموضوعها[3].

ثالثا: شروط قبول الدليل الرقمي كدليل إثبات في الجريمة المعلوماتية

يتعين على القاضي بقبول هذه الأدلة كأساس تستند إليه الحقيقة في الدعوى العمومية سواء كان الحكم فيها بالإدانة أو البراءة توافر بعض الشروط أهمها:

1 – نور الهدى محمودي، **مرجع سابق**، ص 99.

2 – محمد الأمين البشري، **مرجع سابق**، ص98.

3 – نور الهدا محمودي، **مرجع نفسه**، ص 100.

1- أن تكون هذه الأدلة يقينية وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وان تبتعد عن الظنون والتخمينات.

2- يتعين مناقشة الدليل الرقمي تطبيقا لمبدأ شفوية المرافعة، فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى في الجريمة المعلوماتية، فإنه يجب مناقشتها أمام الخصوم إذ تنص المادة 02/212 من قانون الإجراءات الجزائية الجزائري " لا يسوغ أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه[1]."

وهذا يعني أنه للقاضي الاجتهاد في الحكم في الجرائم المعلوماتية وعدم الاعتماد على رأي الغير، إلا إذا كان الغير من الخبراء وقد ارتاح ضميره الى التقرير المحرر منه، وقرر الاستناد إليه ضمن حكمه حيث يكون متولدا من عقيدته وليس من تقرير الخبير[2].

3- يجب أن يكون الدليل الرقمي مشروعا ويقصد بذلك أن إجراءات جمع الأدلة الرقمية المتحصل عليها من الحاسب الآلي إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الأدلة في المواد الجزائية.

رابعا: خصائص الدليل الرقمي:

على اعتبار أن الدليل الرقمي وليد البيئة الالكترونية الحديثة وينتمي لعالم افتراضي ويرتبط بالجريمة الإلكترونية التي تختلف عن الجريمة التقليدية الأمر جعله يتميز بخصائص تختلف عن الأدلة الأخرى تتمثل فيما يلي:

1- **الدليل الرقمي دليل علمي وتقني:** الدليل الرقمي هو الواقع التي تنبئ عن وقوع جريمة أو عمل غير مشروع في العالم الافتراضي فهذه الخاصية تفيد أنه لا يمكن الحصول على الدليل الرقمي او الاطلاع على فحواه إلا باستخدام الوسائل العلمية والتقنية عن طريق عملية البحث والتحري حول هذا الدليل وفق أسس علمية بطريقة تجعله يتجاوب مع الحقيقة بصفة كلية ونفس الأمر فيما يتعلق بحفظ هذا الدليل وفق أساليب علمية مما يجعل تحرير المحاضر يختلف عن المحضر الذي يبنى على شهادة الشهود مثلا في المحضر بالدليل العلمي يعني وجوب توافر طريقة عملية متوافقة مع ظاهر الدليل العلمي أثناء تحريره فمن غير المنطق أن يتخذ سورة المحضر التقليدي.

وعليه فالدليل الرقمي ليس كالدليل العادي، ففي الدليل الرقمي يتم التعامل مع نبضات الكترونية تقنية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه لذلك فكل ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي[1].

1 – المادة 212 من الامر رقم 66-155 المؤرخ في 1966/06/08، والمتضمن قانون الإجراءات الجزائية المعدل والمتمم.

2 – نور الهدى محمودي، **مرجع سابق**، ص 99.

2- **الدليل الرقمي دليل يصعب التخلص منه** : هذه الخاصية والميزة من أهم خصائص الدليل الالكتروني في الأوراق والأشرطة المسجلة التي تكون كاملة تقليدية يمكن حرقها وتمزيقها كما أنه من المستطاع التخلص من بصمات الأصابع بمسحها من موضعها أما بالنسبة للأدلة الالكترونية فان الأمر مختلف حيث انه يمكن استرجاعها بعد محوها وإصلاحها بعد تلفها أو بعد إخفائها مما يؤدي لصعوبة التخلص منه فكل هذا يشكل صعوبة إخفاء الجريمة أو التخفي عن أعين العدالة أو غيرها بعدما يتمكن رجال البحث والتحقيق الجنائي من اكتشاف الجريمة

3- **الدليل الرقمي دليل متنوع متطور** : مصطلح الدليل الالكتروني يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقميا إما أن يكون متنوعا كان يكون في شكل صوره ثابتة أو متحركة أو معده بنظام التسجيل السمعي المرئي أو أن تكون مخزنة في نظام البريد الالكتروني.

تتكون الأدلة الرقمية من بيانات ومعلومات ذات بيئة الكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب إدراكها الاستعانة بالأجهزة والمعدات والأدوات الآلية واستخدام نظام برمجية حاسوبية أي أنها أدلة رقمية خاصة بالشبكة الدولية للمعلومات.

يعد الدليل الرقمي من طبيعة تقنية وهذا ما يميزه عن الدليل التقليدي فالدليل الرقمي ينتج نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي تتكون منها الحاسب الآلي مهما كان نوعه.

الفرع الثاني: سلطة القاضي في قبول الدليل الرقمي

تتنوع نظم الأدلة الجنائية في الإثبات بين التي تأخذ نظام الأدلة القانونية في الإثبات واخرى تعتنق نظام الإثبات الحر والقائم على حرية القاضي الجزائي في تكوين اقتناعه وتلك التي تجمع بين نظامين بما يسمى النظام المختلط.

ففي نظام الأدلة القانونية يتقيد القاضي في الإثبات بادل ة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها[2].

أما في نظام الأدلة الاقتناعية فان القاضي لا يقيده المشرع بأدلة إثبات معينة، وإنما يترك له حرية الإثبات وفقا للسلطة التقديرية في تقدير الدليل ويترتب عن ذلك أن للقاضي الجزائي قبول أي دليل يمكن أن يتولد من اقتناعه[3].

1- روابح الهام شهرزاد، الدليل الرقمي بين مشروعية الاثبات وانتهاك الخصوصية، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة 02، المجلد 05ن العدد10ن جوان 2016ن ص 195.

2 – نور الهدى محمودي، **مرجع سابق**، ص920.

3 – روابح الهام شهرزاد ، **مرجع سابق**، ص197.

وعلى الرغم من سيادة هذا النظام الأخير للإثبات الجنائي في جل التشريعات منها الجزائر إلا أن المشرع قد طبق في إثبات بعض الجرائم نظام الأدلة القانونية عندما نص على تقييد سلطة القاضي في الإثبات بأدلة معينة ومثال ذلك إعطاء حجية كاملة لبعض المحاضر محاضر الحجز و المعاينة الجمركية التي تكون صحيحة إلى أن يثبت العكس وهنا ينتقل عبئ الإثبات من النيابة إلى المتهم ومثال ذلك الاعترافات والتصريحات في المحاضر الجمركية[1].

تعد حرية القاضي في تقدير وسائل الإثبات المطروحة أمامه في الدعوى نتيجة حتمية ومنطقية لمبدأ القناعة الوجدانية للقاضي الجزائي، فإن اقتناعه وجب أن يكون منطقيا وغير مبني على التصورات الشخصية للقاضي، حيث أنه إذا اعتمد في تفكيره على أساليب ينكرها المنطق السليم، فإنه يعرض حكمه للنقض.

وعليه فقيمة الدليل الإلكتروني يمكن حصرها في نقطتين تتمثل الأولى في أن يكون هذا الدليل معترف به أو بمعنى آخر أن القانون يجيز للقاضي الاستناد إليه في تكوين عقيدته، أما النقطة الثانية فهي أن يتوفر على مجموعة من الشروط التي تضفي عليه المشروعية.

وأخيرا فإن مبدأ حرية القاضي في إقناع نفسه بالدليل العلمي هو أساس التبرير بالوسائل العلمية، بحيث يحق له قبول أي دليل مشروع يكتسب يقينا، حتى ولو كان هذا الدليل مستمدا من الوسائل العلمية الحديثة ، وبالرغم من أن القاضي حر في اختيار أي دليل، فإن هذا لا يعني أنه قادر على إصدار أحكام مطلقة ، ول ذلك هناك حدود يجب احترامها والضمانات التي يمنحها القانون للإدانة الشخصية هي : مراجعة المحكمة العليا للأحكام الصادرة عن المحكمة ، بحيث تعتمد سلطة المحكمة العليا المذكورة على التحكم في التطبيق الصحيح للقانون على الخلاصة الجيدة للوقائع من قبل القاضي الذي تم ضبطه وفقا للمنطق القضائي ، وبالتالي تعتبر العلاقة السببية المنطقية آداة فعالة تبرز الأحكام وأصالتها[2].

فالدليل الرقمي وحتى يتم قبوله كدليل إثبات يجب أن يتم الحصول عليه بطريقة مشروعة، وذلك من خلال أن يكون الإجراء المتبع في استخلاص الدليل الجنائي الرقمي مشروعا، عن طريق مراعاة القواعد الموضوعية والشكلية أثناء اتخاذ أي إجراء، حيث تتمثل القواعد الموضوعية في أن يكون الإجراء الذي يستهدف استخلاص الدليل الجنائي الرقمي عملا إراديا صادرا من شخص له صلاحية

1 – حسن بوسقيعة، **المنازعات الجمركية**، دار هومة، الطبعة 2005، ص147.

2 – عمر خوري، عقيلة لاغة، الرقابة على سلطة القاضي الجنائي في تقدير لدليل العلمي، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية** جامعة الجزائر1، المجلد03، العدد 11، سبتمبر 2018، ص 545.

القيام به بناء على سبب معين، زيادة على ذلك يجب أن يكون المحل الذي يرد عليه الإجراء محددا أو قابل للتحديد وأن يكون مشروعا[1].

وقد تدخل المشرع الجزائري لحماية التعاملات الرقمية حين وضع القانون رقم 09-04 المؤرخ في 5 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومن خلال هذا القانون أدرج المشرع طريق الضبط الأدلة الرقمية والتي تتخذ صورتين الصورة الأولى تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على أن تكون هذه المعطيات مهيأة بشكل يجعلها قابلة لحجزها وضعها بإحراز حسب ما هو مقرر في قواعد التحرير دليل المنصوص عليها في قانون الإجراءات الجزائية والصورة الثانية تتمثل في الاستعانة بالتقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال منظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة صعوبة الحصول على هذه الأدلة وفقا للصورة الأولى.

المبحث الثاني: التعاون الدولي لمكافحة الجريمة المعلوماتية

تتجاوز الجريمة المعلوماتية جميع الحواجز الجغرافية والسياسية والاقتصادية للدول، إذ تنتقل كميات هائلة من المعلومات عبر الحدود على شكل إشارات إلكترونية لا تعيقها أي عقبات. ومع تزايد الحاجة إلى مواجهة الإجرام الدولي المنظم والنشاطات المرتبطة بالجريمة المعلوماتية، يصبح من الضروري مكافحة هذه الجرائم من خلال تحقيق التعاون الدولي. يُعَد هذا التعاون أحد أهم الوسائل لمكافحة جرائم الإنترنت وملاحقة مرتكبيها، ويتم ذلك عبر التعاون القضائي (المطلب الأول) وتسليم المجرمين (المطلب الثاني)

المطلب الأول: التعاون القضائي

إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تقتضي تتبع النشاط الإجرامي الأمر الذي يستوجب تقصي آثار الجريمة من مصدرها إلى غاية تنفيذها وتحديد مواقع الأضرار التي مستها[2] ، وذلك من خلال مجموعة متنوعة من مقدمي خدمات للإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة [3] ، ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة

1 – سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الإنترنت**، دار الفكر الجامعي، دط، الإسكندرية، مصر، 2007 م، ص43 .

2 – قزران مصطفى، **الأليات الدولية لمكافحة الجريمة الالكترونية**، الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية، جامعة زيان عاشور، الجلفة، 27-28 أفريل 2009، ص 09.

3 – يوسف حسن يوسف، **الجرائم الدولية للانترنت**، الطبعة الاولى، المركز القومي للاصدارات القانونية، 2011، ص 143.

إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها ، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت أجرائه، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى، بمعنى الحاجة إلى ما يسمى بالتعاون القضائي[1].

من أهم صور التعاون القضائي: التعاون الأمني والمساعدة القضائية الدولية.

الفرع الأول: التعاون الأمني

إنه من البديهي أن تقف الحدود الجغرافية ومشكلة الاختصاص الإقليمي حجر عثرة أمام الإجراءات الجنائية لملاحقة مرتكبي الجرائم لا سيما في جريمة الانترنت التي تتميز بكونها جريمة عابرة للحدود فقد يكون مرتكب الهجوم يحمل جنسية دولة ما وينفذ جريمته من أجهزة دولة أخرى وتقع آثار هذه الجريمة في دولة ثالثة ولهذا تبرز الحاجة الملحة لتوحيد الجهود فيما يتعلق بتبادل المعطيات المتعلقة بالجريمة والمعلومات التي تسمح بكشف هوية المجرمين ما دام أنه يستحيل على الدولة بمفردها القضاء على هذه الجريمة فأجهزة الشرطة لا يمكنها تعقب مرتكبي الجرائم وملاحقتهم إلا من نطاق حدودها أي أنه متى فر المجرم خارج حدود الدولة فإنه يبقى في مأمن من المتابعة ونجد في هذا الإطار أن هناك عدة أوجه لإقامة هذا التعاون[2] :

أولا: ضرورة التعاون الأمني الدولي

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من النظام والأمن، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن الدولة، أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة [3]. فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الانترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم المعلوماتية [4]، التي باتت تشكل خطرا لا على سرية وطن حاسوبية او سلامتها او توافرها فحسب بل تعدت الى امن البنى الأساسية الحرجة

1 – الغافري حسين بن سعيد، **الجهود الدولية في مواجهة جرائم النترنت**، ورقة عمل مقدمة للامانة العامة لمجلس التعاون الخليجي لدراسة سبل مكافحة الجرائم الالكترونية، الرياض، 04-05 افريل 2004، ص03.

2 – قزران مصطفى، **مرجع سابق**، ص 06.

3 – يوسف حسن يوسف، **مرجع سابق**، ص 144.

4 – الغافري حسين بن سعيد، **المرجع نفسه**، ص 03.

ومع تميزها العالمية فان مكافحتها لا تتحقق الا بوجود تعاون دول يعدل المستوى الإجرامي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكب الجرائم المتعلقة بالإنترنت وتعميمها[1].

ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى وتقع آثار مدمرة لهذا الهجوم في دوله ثالثة.

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يتولى هذه المهمة، بالتعاون مع أجهزة الشرطة في الدول المختلفة. ينبغي أن يركز هذا الكيان على تبادل المعلومات المتعلقة بالجرائم والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من العدالة.

01- جهود المنظمة الدولية للشرطة الجنائية الانتربول

ان البدايات الاوليه للتعاون الدولي الشرطي ترجع الى عام 1904 عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 18 مايو 1904 والتي نصت في مادتها الاولى على تتعهد كل الحكومات المتعاقدة بإنشاء او تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعاره في الخارج ولهذه السلطة الحق في تخاطب مباشر الاداره المماثلة لها في كل الدول الأطراف المتعاقدة.

لم تمر سنة على إبرام هذه الاتفاقية إلا وكانت سبع دول من الدول المتعاقدة مثل تلك الأجهزة يتبادر من خلالها المعلومات والبيانات الخاصة باستخدام النساء لغرض عارة في الخارج من أجل القضاء على هذه الجريمة في إقليمها بعد ذلك اخذ التعاون الشرطي الدولي ياخذ صور المؤتمرات الدولية ولها واسبقها تاريخيا كان مؤتمر موناكو 14-1914/4/18 والذي وضع رجال الشرطة والقضاء والقانون من 14 دولة وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية خاصة ما يتعلق بمدى امكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين إلا أنه هو نتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية[2].

وبعد انتهاء الحرب العالمية الأولى وتحديدا عام 1919 حاول الكولونيل فان هوتين أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولي الشرطي وذلك بالدعوة لعقد مؤتمر دولي لمناقشة هذا الموضوع غير انه لم يوفق في مسعاه[3].

1 – الغافري حسين بن سعيد، **المرجع نفسه**، ص 06.

2 – **المرجع نفسه**، ص07.

3 – حسن يوسف حسن، **مرجع سابق**، ص 146.

بنهاية عام 1923 تم عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في الفترة 1923/9/7 بحضور مندوبي 19 دولة وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (ICPO).

إلا أنه اندلاع الحرب العالمية الثانية توقفت اللجنة عن أعمالها حتى وضعت الحرب أوزارها عام 1946 وتهدف المنظمة الدولية للشرطة الجنائية طبقا للمادة 2 من القانون الاساسي الى:

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

2. إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها[1].

بالتالي تهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة.

كما يحظر على المنظمة أن تنشط أو تتدخل في مسائل ذات طابع سياسي أو عسكري أو ديني أو عنصري وهذا طبقا للمادة 3 من القانون الأساسي للمنظمة.

من بين الأمثلة على دور الأنتربول فيما يتعلق بالجرائم المعلوماتية ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الانترنت وذلك أثر تلقي النيابة اللبنانية برقية من الأنتربول في ألمانيا بهذا الخصوص.

لقد مرت جهود المنظمة في هذا المجال بمراحل عديدة إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي ويضاف إلى ذلك مركز إقليمي فرعي في بانكوك[2].

02- تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة

واجه جميع دول العالم احتمالية وقوع كوارث ضخمة ومفاجئة لا يمكن التنبؤ بتوقيتها أو مواجهتها بالإمكانات الوطنية للدولة المنكوبة وحدها. هذا يستدعي تكثيف الجهود والخبرات والإمكانات بشكل يتطلب تضافر الجهود الدولية. هذه الصورة من التعاون الأمني تُعَد من أهم الأشكال في مكافحة جرائم الإنترنت، خاصة وأن أجهزة العدالة الجزائية ليست على نفس المستوى والجاهزية في

1 – الغافري حسين بن سعيد، **مرجع سابق**، ص09.

2 – محمد طارق عبدالرؤوف الحن، **جريمة الاحتيال عبر النترنت**، منشورات الحلبي، بيروت، 2011، ص39.

جميع الدول، إذ تتفاوت فيما بينها. فبعض الدول تتمتع بتقدم تكنولوجي كبير وصيت واسع في مواجهة الجرائم المعلوماتية، بينما تفتقر دول أخرى إلى هذا المستوى من القدرات[1].

رابعا: القيام بعمليات أمنية مشركة

حيث يتم تعقب جريمة الانترنت وتتبع الأدلة الرقمية وضبطها والقيام بعمليات التفتيش العابر للحدود لمكونات أجهزة الإعلام الألى والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تتضمنه من أدلة وبراهين وهذه الإجراءات تستدعي كلها تعاونيا دوليا مكثفا لا سيما العمليات الفنية والأمنية كما من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم[2].

الفرع الثاني: المساعدة القضائية

تعرف 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 الجنائي عدة صور منها:

ثانياً : تبادل الخبرات والمساعدة التقنية :

لتحقيق التكامل مع الاتجاه العام لحوسبة عمليات العدالة الجنائية، وتطوير المعلومات وتحليلها على الوجه الذي يخدم أهداف السياسية الجنائية الحديثة لمكافحة الإجرام عموماً .... ينبغي تبادل العناصر الإدارية ، والتقانات الفنية ، وتعزيز القدرات لأجهزة العدالة وتحليل ونشر البيانات والمعلومات المتاحة حول الجريمة والسبل و الآليات المبتكرة لمكافحة ما هو تقليدي وغير تقليدي منها ، ويجب التركيز على الأساليب الجديدة كدعم التعاون الفني ، و تقديم الخدمات الإستشارية الواسعة لتشمل كافة المجالات كتلك المتعلقة بإخفاء أثر الأموال ، لمواجهة جريمة غسيل الأموال بهدف حرمان المنظمات الإجرامية من عائدات الجرائم ، لأن السياسة الوقائية ستظل قاصرة ، ما لم تضبط كافة عناصر السلوك الإجرامي المفترض.[3]

أولاً: تبادل المعلومات:

عرف العصر الحالي ثورة في مجال المعلومات مما حتم على المجتمع الدولي أن يولي تبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما، والجريمة المعلوماتية خصوصاً، لما توفره المعلومات الصحيحة و الموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في

1 – علي حسن الطوالبة، **التعاون القضائي الدولي في مكافحة الجريمة الالكترونية**، جامعة العلوم التطبيقية، الاردن، دس، ص 123.

2 – علي حسن الطوالبة، **مرجع نفسه**، ص 133.

3 – مصطفى القللى، **الصلات القضائية**، الدار الجامعية للكتاب، دط، د ب ن، 1991 ، ص 127.

ذلك متابعة نشاط المنظمات الإجرامية، ومصادر الأموال في كافة المجالات، لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصراً رئيسياً من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، و أوصى بأنه على منظمة الأمم المتحدة أن تنشئ قاعدة معلوماتية للإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة.

وهكذا ينبغي للتعاون في المسائل المتعلقة بالجريمة المعلوماتية أن يدعم بتوظيف نظم تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب على تنفيذ القوانين والمعاهدة المتعلقة بالعدالة الجنائية، على الصعيد الدولي.

و يجب ألا تحول مركزية المعلومات دون نشرها وتبادلها فيما بين الدول ، بعد ترتيبها ودراستها ومعالجتها ، على النحو يسمح بالإفادة منها في مرحلة التحقيقات والمحاكمة ، ولمتابعة الأشخاص المشبوهين سواء أكانوا أشخاصا أم هيئات، مع كفالة الحريات الشخصية، وتشمل كذلك ما يتعلق بتحركات المجرمين المنظمين في جماعة إجرامية عبر الحدود وما يتعلق بالوثائق المزورة والمسروقة التي قد يلجؤون إلى استخدامها وكافة المعلومات المتصلة بما يرتكبون من أنشطة إجرامية كتهريب الأجانب ، للتنسيق فيما بين أجهزة مكافحة التهريب المنظم للأشخاص عبر الحدود الوطنية[1].

ثانيا: نقل الإجراءات

يقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة، وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدي دورا مهما في الوصول إلى الحقيقة[2].

ثالثا: الإنابة القضائية الدولية

1- فائزة يونس الباشا، **الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية**، دار النهضة العربية، ط1، الجماهيرية الليبية، 2001، ص142.

2- سعيداني نعيم، **اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماجيستر، كلية الحقوق والعلوم السياسية، جامعة حمة لخضر، باتنة، 2013/2012/، ص 90.

وهي ناتجة عن الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات ، لمصلحة السلطة القضائية المختصة في الدول الطالبة ، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالمياً ، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل ، و احترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية ، وتعني الإنابة وفقاً للمادة السادسة من اتفاقية الإعلانات والإنبات القضائية أنه: لكل من الدول المرتبطة بهذه الاتفاقية أن تطلب إلى أية دولة منها أن تباشر في أراضيها نيابة عنها أي إجراء قضائي متعلق بدعوى قيد النظر ، وفقاً لأحكام المادتين السابعة والثامنة[1].

تجدر الإشارة إلى أن طلب الإنابة عادة ما يتم عبر القنوات الدبلوماسية إلا أنه تفاديا لتعقيد الإجراءات وبطئها وبغية التعجيل والتبسيط منها درجت الدول على تعيين سلطة مركزية عادة ما تكون وزارة العدل توجه الطلبات إليها مباشرة.

أما فيما يتعلق بالتعاون القضائي يمكن أن نخلص إلى نتيجة مفادها أن التعاون القضائي وإن كان يشكل أهم آليات مكافحة جرائم الانترنت إلا أن الملاحظ أن غالبية الاتفاقيات في مجال التعاون القضائي قد تناولت جريمة الانترنت بدون تعمق وبشكل سطحي ومنه باتت الحاجة ملحة لعدة اتفاقيات تواكب التطور السريع لتكنولوجيا المعلومات والاتصالات[2].

الحكم الأجنبي:

من المفاهيم التي يجب تجاوزها لدعم أواصر التعاون الدولي : عدم قابلية الحكم الأجنبي للتنفيذ بحجة أن الحكم الجنائي في حقيقته مظهر لسيادة الدولة ولحقها في توقيع العقاب ، إلا أنه لا ينبغي أن يقتصر الأمر علىما يرتبه الحكم الجنائي الأجنبي من أثار سلبية تتعلق بعدم جواز محاكمة الشخص على الفعل الواحد مرتين ، حيث يدعوا الفقه الجنائي إلى ضرورة الاعتداد بالسوابق القضائية للحيلولة دون إفلات الجناة من العقاب،إتفاقاً مع متطلبات العدالة[3].

1 – فائزة يونس الباشا، **مرجع سابق**، ص 145.

2– علي حسن الطوالبة، **مرجع سابق**، ص 151

3 ـ مصطفى القللى، **مرجع سابق** ، ص 133

المطلب الثاني: تسليم المجرمين

لقد أتت هذه الصورة من صور التعاون الدولي كنتيجة حتمية للتطور الهائل الذي شهدته كافة المجالات وبوجه خاص مجال الاتصالات والمعلوماتية حيث لم تعد الحدود الإقليمية تشكل حاجزا أمام مرتكبي جرائم الإنترنت حيث أضحى في مكان المجرم أن يشرع في التحضير لجريمته في بلد معين ويبدأ بالتنفيذ في بلد آخر ويمتد نشاطه الاجرامي الى بلدان اخر[1].

أصبحت جريمة الإنترنت ذات طابع دولي، وحيث إن أجهزة العدالة لا تستطيع تجاوز الحدود الإقليمية لملاحقة المجرمين الفارين، كان لا بد من إيجاد آلية للتعاون بين الدول تكفل ملاحقة هؤلاء المجرمين واتخاذ كافة الإجراءات القضائية ضدهم. عند التمعن في نظام تسليم المجرمين، نجد أنه يحقق مصالح الدول بشكل كبير. فالدولة التي يتواجد في إقليمها المتهم بارتكاب جريمة عابرة للحدود، مثل جريمة الإنترنت، ينبغي أن تحاكمه إذا كان تشريعها يسمح بذلك، ولا يتوجب عليها تسليمه لدولة أخرى لمحاكمته[2].

الفرع الاول: صور تسليم المجرمين

درجت الممارسة الدولية على وجود ثلاث انظمة من الأنظمة المتبعة في تسليم المجرمين:

اولا: التسليم القضائي

ويقصد به ذلك النوع من التسليم الذي تكون فيه المحاكم الجهه المختصه الوحيدة المخول لها إصدار قرار التسليم للدولة التي تطلبه وبالرغم من الايجابيات التي يوفرها هذا النهج حيث انه يمكن للشخص المطلوب تسليمه بأوجه دفاعاته كاملة أمام السلطات القضائيه المختصه إلا أنه يعاب عليه بطل إجراءات وهما ينعكس سلبا على ما تستوجبه سرعة ملاحقة مرتكبي جرائم الانترنت لسهولة اندثار أدلة الإثبات عليها[3].

ثانيا: التسليم الإداري

في هذا النظام، يُكلف السلطة التنفيذية بمهمة تسليم المتهمين، حيث تتمتع بالصلاحية المطلقة لاتخاذ قرار التسليم. على الرغم من أن هذا النظام يسهل تفادي الإجراءات المعقدة والبطيئة، إلا أن النقمة تتعلق بالإهمال لحقوق الأفراد الدفاعية. كما يثير قضية خضوع قرار التسليم لاعتبارات سياسية أو قواعد المجاملات الدولية.

1 ـ الغافري حسين بن سعيد، **مرجع سابق**، ص 10.

2 ـ فائزة يونس الباشا، **مرجع سابق**، ص 165.

3 ـ يوسف حسن يوسف، **مرجع سابق**، ص 162.

ومن الجهة الأخرى، يدير نظام التسليم الإداري السلطة التنفيذية، التي قد لا تمتلك الخلفية القانونية المناسبة لاتخاذ قرارات في مثل هذه القضايا[1].

ثالثا: التسليم المختلط

وهو الاسلوب الاكثر انتشارا حيث انه يمزج بين مزايا النظامين السابقين فهو يسهل الإجراءات ويسرعها كما يضمن للشخص المتهم حق الدفاع

الفرع الثاني: شروط تسليم المجرمين

تجدر الاشارة الى ان نظام تسليم المجرمين يخضع الجمله من الشروط ينبغي توافرها مثل صدور قرار التسليم وتكمن أهمية الشروط في توضيح حدود العلاقة بين الدول والأطراف في عملية التسليم ويمكن إجمال هذه الشروط فيما يلي:

أولا: الشروط المتعلقة بالجريمة:

01-التجريم المزدوج:

ويقصد به ان يكون الفعل مجرما في كلتا الدولتين ولا عبرة بالتكييف القانوني لهذه الجريمة وشرط التسليم المزدوج يجد اساسه في أن الدولة طالبة التسليم تهدف من خلال طلبها الى محاكمة من نسب إليه ارتكاب السلوك الاجرامي او تنفيذ العقوبه المحكوم بها عليه وهذا يفترض في بداية ان السلوك المجرم في تشريعاتها وإلا كان لوجه لوجود متابعة جنائية أو تحريك دعوى عمومية ومن ناحية أخرى لا يتصور مطالبة الدولة ما تسليم شخصا لتوقيع عقوبة على سلوك غير مجرم أساسا في قوانينها العقابية وعلى هذا الأساس تتبع الدول في تحديد الجرائم نظام الحصر وذلك بإعداد قائمة تدرج فيها على سبيل الحصر الجرائم المعنية بالتسليم[2].

02-درجة جسامة الجريمة:

حيث نجد أن بعض الدول تشترط درجة معينة من جسامة الجريمة او اشتراط حد أدنى من العقوبة الموافقة لهذه الجريمة وفق تشريعاتها الداخلية حتى يقع التسليم وهذا الشرط بالذات ورد في بعض الاتفاقيات الدولية كما هو عليه الحال في المادة اثنين من المعاهد النموذجية بشأن تسليم المجرمين المادة 24 اتفاقية الأوروبية الإجرام المعلوماتي[3].

1 – الغافري حسين بن سعيد، **مرجع سابق، ص 18**.

2 – قرزان مصطفى، **مرجع سابق**، ص 10.

3 – محمد ارزقي عبلاوي، **تسليم المجرمين في نطاق المعاهدات الدولية والتشريع الجزائري**، رسالة دكتوراه، جامعة الجزائر 01، 2010، ص 183.

ثانيا: الشروط المتعلقة بالأشخاص المطلوب تسليمهم

01-عدم جواز تسليم الرعاية:

لقد استقر الفقه الدولي ومعظم التشريعات الوطنية على مبدأ عدم جواز تسليم الرعاية الوطنيين الى دول الأجنبية أيا كان نوع الجريمة المتبعين بها في هذه الحالة تكون الدولة التي ينتمي إليها المتهم بارتكاب الجريمة أولى ومحاكمته وتوقيع العقوبة المناسبة وفقا لمبدأ شخصية القوانين[1]

02-عدم جواز تسليم اللاجئين السياسيين

ويعتبر هذا المبدأ عرفا دوريا درجة الممارسة الدولية على اتباعه كما اقرته الاتفاقيات الدولية والتشريعات الوطنية واعتبرته استثناء على واجب الالتزام بتسليم المجرمين ولعل الأساس الذي يقوم عليه هذا المبدأ هو تحقيق العدالة وحماية حقوق الإنسان خشية أن تكون التهمه ملفقه من قبل السلطات الدولة طالبة التسليم[2].

03-عدم جواز تسليم المحكومين على ذات الجريمة

وذلك اقرارا لمبدا عدم تكرار العقوبه على ذات المجرم الذي اقرته القوانين الوطنية واكدته الاتفاقيات الدولية فمتى كان الشخص المطلوب تسليمه قد حكم من قبل عن الجريمة المطلوب تسليمه لأجلها بمقتضيات العدالة تقتضي أنه إذا كان برئ او قضى عقوبته فانه لا يجوز تسليمه حتى لا يتعرض هذا الشخص عقوبة مزدوجة[3].

1 – محمد ارزقي عبلاوي، **المرجع نفسه**، ص 211.

2 – يوسف حسن يوسف، **مرجع سابق**، 165.

3 – قرزان مصطفى، **مرجع سابق**، ص10.

خلاصة الفصل الثاني:

في هذا الفصل، تم تناول الخصوصية الإجرائية لمكافحة الجريمة المعلوماتية، حيث في المبحث الأول، تم استعراض المتابعة القضائية في القانون الوطني، حيث تم التركيز على القواعد المتعلقة بالاستدلال والتحقيق في الجريمة المعلوماتية، والتي تشمل القواعد الاجرائية الحديثة في قانون الاجراءات الجزائية، وكذلك القانون 09-04 ، كما تم تناول موضوع الإثبات في الجريمة المعلوماتية، موضحا كيفية توثيق الأدلة الرقمية وتقديمها أمام القضاء، وفي المبحث الثاني، تم تسليط الضوء على أهمية التعاون الدولي في مكافحة الجريمة المعلوماتية، حيث شمل ذلك التعاون القضائي بين الدول وآليات تسليم المجرمين لتجاوز الحدود الجغرافية التي يستغلها الجناة، واخيرا بالتأكيد على أن مواجهة الجريمة المعلوماتية تتطلب نهجا شاملا يجمع بين التشريعات الوطنية والتعاون الدولي الفعال لضمان العدالة والأمن في المجتمع الرقمي العالمي.

الخاتمـــة

الخاتمة

تعدّ الجرائم المعلوماتية من أخطر أنواع الجرائم، حيث تمثّل إرهابًا إلكترونيًّا يهدّد الأمن على كافة الأصعدة، فمع تطوّر الفضاء الإلكتروني، أصبحت هذه الجرائم تشكل تهديدًا إستراتيجيًا على المجتمع الدولي اقتصاديًا وسياسيًا وثقافيًا وأمنيًا واجتماعيًا، حيث تعتمد هذه الجرائم على تقنيات متقدّمة مثل أجهزة التنصت على شبكات الاتصال، وبرمجيات التشفير، وبرمجيات اختراق أنظمة أمن الشبكات والحواسيب، ويمكن لشبكة آلية واحدة أن تضم عشرات أو مئات الآلاف أو حتى ملايين الحواسيب والأجهزة المتصلة بالإنترنت، والتي يمكن استخدامها بشكل غير مشروع لشن هجمات متنوعة لأغراض إجرامية مثل: التخريب، والسرقة، والإرهاب، والتهديد، والابتزاز.

كما تكمن خطورة هذه الجرائم فيما تتميّز به من خصائص إستثنائيّة ومنفردة أضفت عليها لوناً وطابعاً قانونياً خاصا وجعلها تشكّل تحدّياً كبيراً للقوانين والقضاء وجميع الجهود والآليات الوطنيّة والدوليّة لمكافحتها حيث ظلّت هذه الجهود رغم أهميّتها عاجزة عن التصدي لها والحدّ منها.

ومن خلال ما تقدم توصلنا إلى جملة من النتائج والتوصيات والمقترحات كما يلي:

النتائج:

– أنّ الجرائم المعلوماتيّة ظاهرة إجرامية حديثة وليدة التطورات الهائلة في نظم تقنية المعلومات والإتّصالات وتُعدّ من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكونها تتمثّل في إعتداءات خطيرة على الأفراد والمؤسسات وأمن الدول، وهو ما يترك في النفوس شعورًا بعدم الثقة وإنعدام الأمن في التعامل والإستفادة من الثورة الرقميّة.

– أن الجرائم المعلوماتية تختلف عن الجرئم العادية من حيث أسلوب إرتكابها فهي جرائم ناعمة لا تحتاج مجهود بدني بل إلى الموهبة والمهارة الفنية والتقنية وكما تختلف من حيث شخص مرتكبها والوسيلة المستعملة في إرتكابها وهي من الجرائم الصعبة الاكتشاف والّتي تحتاج إلى خبراء مختصين في التحقيق فيها لأنّ المجرم لا يترك أثرًا عند ارتكابها.

– ان القواعد الاجرائية لمكافحة الجرائم المعلوماتية على المستويين الوطني والدولي لابد ان تكون متماشية مع التطور الكبير الذي تشهده التكنولوجيا للحد منها وتقليل اضرارها.

التوصيات والمقترحات:

في ختام هذا البحث، فإننا نورد بعض التوصيات قد يكون من المناسب العمل بها لمواجهة تهديدات الجرائم المعلوماتيّة المتزايدة. وتتمثّل فيما يلي:

– وجوب تعديل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم المعلوماتيّة وخطورتها وطرق مكافحتها.

– إنشاء محاكم أو دوائر متخصّصة في الجرائم المعلوماتيّة في كل المجالس القضائية لمجابهة هذه الظاهرة.

– عقد المؤتمرات الدولية ذات العلاقة بالجرائم المعلوماتية وإعداد الإتّفاقيات الدولية أيضاً ذات الصلة بالموضوع.

– إبرام إتّفاقية دوليّة لتعزيز التعاون الدولي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم المعلوماتية عبر الوطنية.

– تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الإنترنت.

قائمة المراجع

قائمة المصادر والمراجع

1/القوانين:

01- الأمر رقم: 66-155 مؤرخ في 18 جوان 1966، يتضمن قانون الإجراءات الجزائية ج.ر ، عدد48، 1966.

02- القانون رقم 09-04، المؤرخ في 05 أوت 2004، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، عدد 47،2009.

03- قانون إمارة دبي رقم 02 لسنة 2002 المتعلق بالمعاملات والتجارة الالكترونية، 2002

04- قانون رقم 85 لسنة 2001، المملكة الأردنية الهاشمية، الجريدة الرسمية رقم:4524 بتاريخ 2001/12/31.

2/الكتب:

01- الصغير جميل عبد الباقي، **القانون الجنائي والتكنولوجيا الحديثة**، ط 1، دار النهضة العربية، القاهرة، 1992.

02- أحمد خليفة الملط، **جرائم المعوماتية**، ط 2، دار الفكر الجامعي، مصر،2006.

03- أحسن بوسقيعة، **المنازعات الجمركية**، دار هومة، الطبعة 2005، الجزائر.

04- أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة، 1994.

05- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي، مصر، 2009.

06- رشاد خالد عمر، **المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة**، المكتب الجامعي الحديث، ط02، مصر، 2018.

07- زيبحة زيدان، **الجريمة المعلومتتية في التشريع الجزائري والدولي**، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

08- سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الإنترنت**، دار الفكر الجامعي، دط،، مصر، 2007.

09- عبد الفتاح بيومي حجازي، – **صراع الكمبيوتر والانترنت** – في القانون العربي النموذجي دار الكتب القانونية – دار للنشر والبرمجيات – القاهرة 2007 .

10- عبد الكريم الردايدة، **الجرائم المستحدثة وإستراتيجية مواجهتها**، دار الحامد للنشر والتوزيع، الطبعة الأولى، الأردن، 2013 .

11- علي حسن الطوالبة، **التعاون القضائي الدولي في مكافحة الجريمة الالكترونية**، جامعة العلوم التطبيقية،دط، الأردن، دس ن.

12- فائزة يونس الباشا، **الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين** الوطنية، دار النهضة العربية ، ط1، الجماهرية الليبية، 2001.

13- محمد الأمين البشري، **التحقيق في الجرائم المستحدثة**، جامعة نايف للعلوم الأمنية، الرياض، 2004.

14- منير الجنبيهي، – ممدوح الجنبيهي – **البنوك الالكترونية**، ط 2، 2006 دار الفكر الجامعي، الإسكندرية .

15- محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، 1994، د ب ن،

16- محمد طارق عبدالرؤوف الحن، **جريمة الاحتيال عبر النترنت**، منشورات الحلبي، بيروت، 2011.

17- محمد محمد الألفي، **المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت**، المكتب المصري الحديث، القاهرة، ط1، 2005.

18- مراد عبد الفتاح، **شرح جرائم الكمبيوتر والانترنيت**، دار الكتب والوثائق، الإسكندرية ، 2007.

19- ممدوح خليل عمر، **حماية الحياة الخاصة والقانون الجنائي**، دار النهضة العربية، القاهرة، 1983،

20- مصطفى القللى، **الصلات القضائية** ، الدار الجامعية للكتاب ، دط، د ب ن، 1991 .

21- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2008.

22- هلالي عبد اللاه احمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية اتفاقية بودابست** ، دار النهضة العربية، القاهرة، 2006.

23- هشام فريد رستم، **قانون العقوبات مخاطر المعلومات**، مكنة الآلات الحديثة أسيوط، 1992.

24- يوسف حسن يوسف، **الجرائم الدولية للانترنت**، الطبعة الأولى، المركز القومي للإصدارات القانونية، 2011.

3/الرسائل والمذكرات:

أ/رسائل الدكتوراه:

01- خضرة شنتير، **الآليات القانونية لمكافحة الجريمة الالكترونية دراسة مقارنة**، اطروحة دكتوراه، جامعة ادرار، 2021/2020 .

02- دلال مولاي ملياني، **إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري**، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة ابوبكر بلقايد تلمسان، 2018/2017.

03- محمد ارزقي عبلاوي، **تسليم المجرمين في نطاق المعاهدات الدولية والتشريع الجزائري**، رسالة دكتوراه، جامعة الجزائر 01، 2010.

ب/مذكرات الماجستير :

01- أحمد سعود مريم، **اليات مكافحة جرائم تكنولوجيا الاعلام والتصال في ضوء القانون رقم 09-04**، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة ورقلة، 2013/2012.

02- سعيداني نعيم، **اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجوائري**، مذكرة ماجيستر، كلية الحقوق والعلوم السياسية،جامعة حمة لخضر،باتنة، 2013/2012.

03- صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة تيزي وزو، 2013.

ج/مذكرات الماستر

01-حرزون ليلى، هدروق أسماء، **التنظيم القانوني للجريمة الالكترونية في القانون الجزائري**، مذكرة لنيل شهادة الماستر، جامعة بجاية، 2022/2021

4-المقالات:

01- بومدين كعيبش، أساليب التحري الخاصة في جرائم الفساد، **مجلة القانون**، جامعة ابو بكر بلقايد تلمسان، العدد7، ديسمبر 2016.

02- حمداش شمس الدين، القواعد الاجرائية لتفتيش المنظومة المعلوماتية في القانون الجزائري، **مجلة صوت القانون**، المجلد 09، العدد02، 2022.

03- راضية عيمور، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، **المجلة الأكاديمية للبحوث القانونية والسياسية**، كلية الحقوق والعلوم السياسية، جامعة الأغواط، العدد الأول، المجلد السادس، سنة 2022.

04- روابح الهام شهرزاد، الدليل الرقمي بين مشروعية الاثبات وانتهاك الخصوصية، **مجلة البحوث والدراسات القانونية والسياسية**، جامعة البليدة 02، المجلد 05ن العدد10ن جوان 2016.

05- محمد الأمين البشري، التحقيق في جرائم الحاسوب الآلي، **المجلة العربية للدراسات الأمنية والتدريب**، العدد 30 نوفمبر 2000.

5/مداخلات:

01- الغافري حسين بن سعيد، **الجهود الدولية في مواجهة جرائم الانترنت**، ورقة عمل مقدمة للأمانة العامة لمجلس التعاون الخليجي لدراسة سبل مكافحة الجرائم الالكترونية، الرياض، 04-05 أفريل 2004.

02- المطردي مفتاح بوبكر، **الجريمة الالكترونية**، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 25- 23 أيلول2012.

03- الهام بن خليفة، **القواعد الاجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال**، مداخلة حول الجرائم الالكترونية واليات مكافحتها، كلية الحقوق والعلوم السياسية، جامعة الوادي.

فهرس المحتويات

العنوان	الصفحة
شكر وعرفان	
إهداء	
مقدمة	05-02
الفصل الأول: ماهية الجريمة المنظمة	06
تمهيد	07
المبحث الأول: ماهية الجريمة المعلوماتية	08
المطلب الأول: مفهوم الجريمة المعلوماتية	08
المطلب الثاني: خصائص الجريمة المعلوماتية	12
المبحث الثاني: تصنيف وأطراف الجريمة المعلوماتية	16
المطلب الأول: تصنيف الجرائم المعلوماتية	16
المطلب الثاني: أطراف الجريمة المعلوماتية	21
خلاصة الفصل الأول	25
الفصل الثاني: الخصوصية الإجرائية لمكافحة الجريمة المنظمة	26
تمهيد	27
المبحث الأول: المتابعة القضائية في الجريمة المعلوماتية في القانون الوطني	28
المطلب الأول: القواعد المتعلقة بالاستدلال والتحقيق في الجريمة المعلوماتية	28
المطلب الثاني: الإثبات في الجريمة المعلوماتية	44
المبحث الثاني: التعاون الدولي لمكافحة الجريمة المعلوماتية	51
المطلب الأول: التعاون القضائي	51
المطلب الثاني: تسليم المجرمين	57
خلاصة الفصل الثاني	61
الخاتمة	26
قائمة المراجع	65
فهرس المحتويات	70
ملخص	

ملخص:

تعتبر الجرائم المعلوماتية من أهم جرائم العصر الحديث التي نشأت من خلال سوء استخدام التكنولوجيا فهي جريمة مختلفة عن الجرائم الكلاسيكية من حيث طريقة ارتكابها والوسائل المستخدمة في ارتكابها فهي وسائل مختلفة عن الوسائل التقليدية في ارتكاب الجرائم،وكذا الأشخاص مرتكبيها لهم سيمات تميزهم عن غيرهم من المجرمين التقليديين فسلاحهم الذكاء والمهارة في استخدام التقنية ومما زادهم تفردا أن لهم قدرة الاختفاء والتمويه، كما أن دليل هده الجريمة يتسم بالحساسية فهو غير مادي وقابل للإتلاف في غضون توان، كما أنها جريمة جديدة وصعبة الإثبات من حيث الأشخاص والأدلة فهي عابرة للحدود الدولية أي يمكن للمجرم المعلوماتي ارتكابها على بعد القارات، فأصبح الضرر الناجم عنها يمس بالأشخاص وبالدول والتحقيق فيها بات يستلزم تجاوز الحدود الدولية في سبيل التصدي والوقاية من الجرائم المعلوماتية ضرورة حتمية في ظل المعطيات الجديدة للعالم الجديد لمكافحة الإجرام.

بالإضافة إلى ذلك فقد استحدث المشرع إجراءات أخرى للكشف عن الجريمة المعلوماتية،

و من قبيل ذلك إجراء التسرب الإلكتروني و الذي يقوم به ضباط الشرطة القضائية دعما لجهات التحقيق، بالإضافة إلى اعتراض المراسلات و المراقبة الإلكترونية، والحفظ والإفشاء العاجلان للمعطيات الإلكترونية، بالإضافة إلى إنتاج المعطيات المعلوماتية، و تجميع معطيات المرور بوقتها الفعلي.

الكلمات المفتاحية:

الجرائم المعلوماتية – التعاون الدولي –البيئة الرقمية – الدليل الرقمي – التحقيق

Abstract:

Information-related crimes are contemporary crimes that have arisen due to the misuse of technology, they are unique from conventional crimes in terms of how they were committed and the means used for the competent, and the people who committed them have a reputation that sets them apart from other traditional criminals, whose weapons are smart and skill in the use of technology, which has added to their uniqueness, is that they have the ability to vanish and camouflage. The evidence of this crime is sensitive and non-material and can be destroyed in seconds, furthermore it is a new crime which is difficult to prove in terms of people and transnational evidence, damage to people and states and the investigation of them would have crossed international borders, which poses a lot of problems, so international cooperation has been established internationally through the consolidation of efforts to combat and prevent crimes, in the new world of crime control.

In addition, the legislature has introduced other procedures to uncover information crime, such as the electronic leakage procedure that some judicial police officers perform in support of the investigation authorities, in addition to intercepting correspondence and electronic surveillance, and the urgent preservation and disclosure of electronic data, in addition to the production of data Informatics, and collecting traffic data in real time.

Keywords:

-information crimes -international cooperation - digital environment - digital evidence - investigation.