محاضرات في مقياس الجريمة الالكترونية

السنة الثانية ماستر-علوم جنائية-

أ. مشري سلمى

مفهوم الجريمة الالكترونية

الجريمة بوجه عام

تعتبر الجريمة فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبير وهي فعل غير مشروع صادر عن شخص مدرك أو غير مدرك سوي أو غير سوي.

انطلاقا من هذا التعريف يتضح أن الجريمة بوجه عام تقتضي تواجد سلوك إجرامي غير مشروع منصوص عليه في قانون العقوبات الذي يجرم كل فعل يتعارض مع القانون أو يخالف النظام العام، وهذا السلوك يشكل ما يسمى بالركن المادي للجريمة والذي يتضمن أفعالا إيجابية وسلبية تكون عمدية أو غير عمدية وتشكل الركن المادي للجريمة الذي يعد من أصعب أركان الجريمة وخاصة في تحديد النية الاجرامية، أو القصد الجنائي.

أما الركن الشرعي فيتمثل في النص التجريمي الذي يعد عصب وأساس التجريم والعقاب، فلا جريمة ولا عقوبة بغير قانون، وإلا انعدم الركن الشرعي. وعلى القاضي تجنب الخروج عن النص التجريمي، أو خلق نصوصا أخرى فينهدم مبدأ الشرعية.

انطلاقا من تعريف الجريمة بوجه عام يتضح تماما مدى تطابق أو اختلاف المفاهيم المرتبطة بهذه الأخيرة ،و بين الجريمة الالكترونية ومدى احتوائها على العناصر الاجرامية العامة أم أنها تدخل ضمن مجال إجرامي آخر سمي بالجريمة الالكترونية المرتبطة بالعالم الشبكي والافتراضي الذي أضحى ضرورة حتمية لاستخدام التكنولوجيا التقنية والرقمية، التي أنشأت حالة من التعامل الالكتروني عبر استخدام الوسائط الالكترونية المتمثلة في الحاسوب وشبكة الانترنت أو الهاتف النقال، وكلها تمتد عبر العالم لتؤلف شبكة هائلة لنقل المعلومات بحيث يمكن للمستخدم الدخول إليها في أي وقت وفي أي مكان من العالم، وهنا يكمن مربط الفرس؛ إذ تشكل شبكة الانترنت ووسائل التواصل المختلفة أهمية بالغة للأفراد ترتبط بحياتهم اليومية وبطرق عيشهم عبر استخدام حقهم في الولوج إلى المعلومات والاستفادة منها في قضاء حاجاتهم ولكن بالمقابل نجد أن التعامل الالكتروني خلق تحديات خطيرة أثرت على حياتهم وتعاملاتهم المالية التي تهدف إلى تطوير المعارف بأقل التكاليف مما أدى إلى تضاعف حجم المعلومات ووفرتها وتراكمها بشكل سريع.

والجريمة الالكترونية تبعا للقواعد العامة للجريمة بوجه عام قائمة على توافر عناصر أساسية مادية ومعنوية تكمن في استخدام الحاسب الآلي أو الهاتف والنظام المعلوماتي عبر شبكة الانترنت ووسائل البريد الالكتروني بالطريقة غير المشروعة أو المخالفة لنصوص

قانون العقوبات؛ فتشكل اعتداء قانونيا إما بنية الاضرار بالغير أو بنية تحقيق الربح أو بدافع الانتقام عبر استخدام ما يسمى بالاحتيال والنصب الالكتروني، السرقة، الإرهاب الالكتروني، القرصنة الالكترونية، التجسس الالكتروني الابتزاز الالكتروني... وغيرها.

1- تعريف الجريمة الالكترونية

تعرف الجريمة الالكترونية عموما بأنها كل فعل إجرامي معتمد أيا كانت صلته بالنظام المعلوماتي ينشأ عن خسارة تلحق بالمجني عليه ومكسب يحققه من جهة أخرى، فخلف ما يسمى بالجريمة الالكترونية التي سوف نسلط الضوء على مفهومها وخصائصها ومقارنتها بالجرائم العادية بالتطرق إلى النصوص الجزائية التقليدية والتشريعات الحديثة الخاصة والمعاصرة في ضوء القانون العقابي الجزائري، وخاصة الأساس القانوني لهذه الجريمة والمسؤولية الجزائية المترتبة عنها.

أولا-مفهوم الجريمة الالكترونية

ويقصد بها جريمة الانترنت أو الجريمة التي تتخذ من الفضاء الافتراضي مكانا لها عبر استخدام الحاسوب كوسيط إلكتروني وكأداة لتنفيذ الجريمة- تلعب فيها البيانات دورا بالغا إلى جانب برامج المعلوماتية، هذه الأخيرة نتجت عن التطور السريع لتكنولوجيا المعلومات وأضحت عنصرا أساسيا من عناصر التفاعل الشبكي للأفراد بشكل متبادل الذي يتخطى الحدود الزمانية والمكانية للوصول إلى المعلومات من خلال الشبكة الالكترونية المعتدي، أو هي تلك الجرائم التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا لارتكاب الجرائم ذات الطابع التقني، وفي المقابل نجد أنها كل فعل يستهدف إلحاق الضرر إما بالوسيلة المستخدمة أو عبرها بالاستناد إلى شبكة الانترنت.

أ- التعريف الفقهي للجريمة الالكترونية

تعرف بأنها "كل فعل أو امتناع عن فعل عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات وبهدف الاعتداء على الأموال والحقوق المعنوية"، أو هي "عمل أو امتناع عن عمل بنية الاضرار بمكونات الحاسوب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقوبة"

وتشكل عند البعض الآخر من الفقهاء جريمة مرتبطة بـ" كل فعل ضار بالآخرين عن طريق الوسائط الالكترونية وهي شبكة الانترنت، الهاتف النقال، شبكات نقل المعلومات، الاستخدامات غير المشروعة للحاسوب"

ب- التعريف القانوني للجريمة الالكترونية

تعرف الجريمة الالكترونية في القانون كونها فعل أو سلوك مادي يصدر عن إدارة جنائية عمدية يقرر لها قانون العقوبات عقوبة أو جزاء، أو هي فعل أو امتناع عن فعل يصدر عن مجرم ذكي يستخدم الوسيط الالكتروني لارتكاب أفعال غير مشروعة، وقد تطرق إليها

المشرع الجزائري في المادة02 من القانون 09-04 باعتبارها من قبيل الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات وهي "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو اتصالات إلكترونية"

ونجد أن مختلف التعريفات تستند إما إلى موضوع الجريمة وأخرى إلى الوسيلة المستخدمة، أو لصفات شخصية لدى مرتكب الفعل المجرم، أما المشرع الجزائري فحصر تعريف الجريمة الالكترونية في جانبها المعلوماتي فقط، بحيث ركز على أنظمة المعالجة الآلية للمعطيات الشخصية، دون التطرق إلى جوانب أخرى ترتبط بها، كالجانب الشخصي والجانب التقني، لذلك تختلف الجريمة الالكترونية عن الجريمة المعلوماتية في هذا التعريف.

غير أنه يتفق كل من التعريف الفقهي والقانوني في كون الجريمة الالكترونية هي فعل أو امتناع الهدف منه تحقيق الضرر وتتم عن طريق الحاسوب، هذا الأخير تتكون من مكونات مادية كأدوات ومستلزمات الكمبيوتر كالأقراص والشاشة، فهذه المكونات أو العناصر لا تتم عبر الولوج إلى شبكة الانترنت فقد يتم التعدي عليها عبر السرقة أو الكسر أو التفجير، ومن طرف شخص لا يفقه في التقنية أو استخدامها بشكل أو بآخر، على خلاف العناصر التي تشكل محلا للجريمة الالكترونية كالبيانات والبرامج والمعلومات المختزنة داخله سواء بسرقتها أو تدميرها أو الاطلاع على أرقامها السرية والدخول إليها أو إرسال فيروسات عبر برامج ضارة.

صور الجريمة الالكترونية

1/صور العنف الالكتروني المعلوماتي في إطار الملكية الفكرية

وهذا يعتبر نوع من العنف المرتكب على شبكة الانترنت تتفاوت درجاته حسب درجة خطورته ويكون محله المعلومات والبيانات باستخدام أساليب تكنولوجية متطورة يتم من خلالها سرقة أو تخريب وتعديل معلومات وبيانات موجودة على الحاسب الآلي أو مخزنة في برامجه وعلى الرغم من إقرار بعض الفقهاء في القانون الجنائي على عدم إمكانية خضوع المعلومات في حال سرقتها أو اختلاسها باعتبارها شيء معنوي غير مادي وجريمة السرقة لا تطبق إلا على كل ما هو مادي محسوس وملموس، تتم فيه نقل الحيازة من المجني عليه إلى الجاني وهنا تعتبر جريمة الحيازة في حد ذاتها فعلا غير مشروع يستوجب المحاسبة الجزائية. أما الجريمة المعلوماتية أو سرقة المعلومات يغيب فيها عنصر الحيازة لأن المعلومات لا تزال في حوزة المجني عليه وإنما تم سرقتها عن طريق النقل والنسخ في قرص مدعم أو أي وسيلة الكترونية.

ويتم تعديلها وتخريب شيء منها لأجل الإضرار بصاحبها، ولكن يرى جانب آخر أن السرقة في جانب المعلومات مرتبطة بفكرة المال المعلوماتي أي أن المعلومة لها أثر مادي إذ ترتب عنها ضرر ملموس. وبالنظر أيضا إلى أن نشاط الجاني المتمثل في الدخول غير المشروع

والبقاء من أجل النسخ والنقل أو التغيير في المعلومات والبرامج والبيانات دلالة على تحقق الركن المادي للجريمة واكتمال تحقق الإيجابية في ارتكاب الجريمة، فبمجرد الاطلاع ولو كان ذهنيا وبطريقة غير قانونية يعاقب عليه وفقا لنص المادة 394 من قانون العقوبات الجزائري.

وتظهر خطورة السرقة المعلوماتية في طبيعة البرامج والمعلومات المرتبطة ببراءة الاختراع الصناعي والفكري (أي حق الابتكار وحق التأليف) ولقد استبعد المشرع الجزائري صراحة برامج الحاسوب من مجال الحماية المقررة لبراءة الاختراع في المادة 7 من الأمر 05/03 المؤرخ في 2003/7/19 "لا تعد من الاختراعات في هذا الأمر برامج الحاسوب".

غير أن المشرع اعتبر المصنفات الأدبية والفنية في مجال العلوم أي كان نوعها أو طريقة التعبير عنها من قبل حق المؤلف، وتمنح له الحماية مهما كانت أهميتها، قيمتها أو الغاية منها فقد تطرق إلى تعريف المصنف في المادة 4 من الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة له واشترط لكي يضيف هذا القانون أن تدخل هذه الحقوق في شكل مصنف مبتكر أي لابد أن تتوفر على عنصر الابتكار سواء كان ذهنيا أو ماديا.

كما يجب منح الحماية لكل مؤلف يعمد إلى إنتاج فكري هادف ومنظم أي ليس بطريقة عشوائية لأنه في هذه الحالة لا يمكن حمايته.

والحماية في هذه الحقوق الأدبية والفنية تحتوي على صعوبة كبيرة أي حماية حق المؤلف على برنامجه أو ملكياته الفكرية لأنه بإمكان أي شخص محترف للوسائط الالكترونية أن يستخدم أساليب غير مشروعة لتعديل وتغيير محتوى البرنامج ويطالب هو بنفسه الحماية له على اعتبار أنه هو صاحب الحق.

لذلك تجد المشرع الجزائري كغيره من المشرعين قد أكد على ضرورة حماية حقوق المؤلف من خلال تعديل قانون حق المؤلف بمقتضى الأمر 10/97 والأمر 05/03 وأدمج البرامج وقواعد البيانات ضمن المصنفات الأصلية، وقام بتشديد العقوبات في حال المساس بالمصنفات المعلوماتية من خلال المادة 151 من الأمر 10/97 حيث أن التعدي على الملكية الفكرية يخضع لقانون العقوبات في المواد 390، 394 من قانون العقوبات الجزائري.

وتم التأكيد في الأمر 10/97 على خلاف قانون العقوبات على عقوبة الحبس والغرامة بدلا من الغرامة وفقا لنصوص قانون العقوبات وذلك بوضعها في قانون خاص، استنادا أو توافقا على ما ورد في أحكام الاتفاقية المتعلقة بالتجارة الدولية والتي انضمت إليها الجزائر، ضمانا لحماية حقوق المؤلفين الأجانب في الخارج. ونستنتج هنا أن المعلومة ذات طابع مالي واقتصادي أي من قبل المال المعلوماتي وكذا البرامج على اعتبارها محمية بحق المؤلف.

وهذا يعني أنه تعرض المعلومة أو البرنامج للاستحواذ أو السرقة عن طريق تشغيلها ووضعها في جهاز الحاسب الآلي وتشغيل هذا الأخير عن طريق مفتاح السر ومعرفة الرقم

السري اللازم للتشغيل يعتبر في حد ذاته فعلا جرميا تتوفر فيها جميع أركان الجريمة حتى وإذ مخله معنوي معلوماتي، وبالتالي يتعرض صاحبه للمسؤولية الجنائية، لأنها تعتبر ككيان مادي يمكن رؤيته على شاشة الكمبيوتر، وبالتالي لا يمكن تجريدها من الحماية القانونية.

2/ التجسس الالكتروني:

تعريف جريمة التجسس الالكتروني: هي جريمة تستخدم فيها التكنولوجيا كأداة للجوسسة، تتسم بميزة خاصة هي السهولة والحرية في تحقيق النتيجة، بعيدا عن رقابة من جهة معينة، وهو مفهوم عام يشمل الأفراد والجماعات والدول.

1- **التجسس الالكتروني الفردي:** "هذا الاطلاع على معلومات خاصة بالغير محفوظة في جهاز الكتروني وليس مسموحا لغير المخولين بالاطلاع عليها".

أو هو "قيام أحد الأشخاص غير المصرح بهم بالدخول إلى نظام التشغيل في مختلف أجهزة الاتصالات بطريقة غير مشروعة ولأغراض غير سوية حيث يتاح للشخص المتجسس أن ينقل أو يمسح أو يضيف ملفات أو برامج، فيتحكم في نظام التشغيل بإصدار الأوامر مثل إعطاء أمر بالطباعة أو التخزين أو التصوير ولكن لا بد أن تتم هذه العمليات في شكل منظم أو فردي بالتجسس على الأشخاص... أو الدول أو المنظمات باستخدام الأنظمة الالكترونية.

2- **التجسس الالكتروني الدولي:** وهو استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح به أو غير قانوني إلى أنظمة المعلومات الالكترونية الخاصة بالدول والحكومات والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها مثل التحسيس على العمليات العسكرية والأمنية والسياسية والاقتصادية والاجتماعيةهناك مجالات عديدة للتجسس الالكتروني فيكون في مجال التجارة عبر كشف المعلومات التجارية والتجسس الصناعي والتقني مثل كشف أبحاث ونتائج الأبحاث والتطور والبيانات المتعلقة بعمليات الإنتاج، ثم المجالات الأمنية والعسكرية مثل نشاطات التحسيس على الدولة كالاستخبارات المتمثلة في معلومات وبيانات ترتبط بأمن الدولة واستقرارها السياسي.

أساليب التجسس الالكتروني:

- **الأساليب التقليدية:** تكمن في سرقة الأسطوانات التي تخزن فيها البيانات والمعلومات المخزنة داخل الحاسوب.

أما الأساليب الحديثة فتكمن في إتلاف المحتويات داخل الجهاز بأساليب مثل الأسطوانات الممغنطة، اختراق البيانات للتجسس والالتقاط والتسجيل. ص 133. وكذا البيانات التي يتم نقلها عبر الأسلاك المعدنية أو خطوط الهاتف المخصصة لنظام الاتصالات الالكترونية. أو ما يسمى بأجهزة التقاط الصوت.

- أيضا التجسس عبر استخدام الأقمار الصناعية من منظمة أو دولة إلى أخرى بهدف اعتراض المراسلات أو التقاط الأخبار.

1- **جريمة التجسس عبر الاعتراض غير القانوني للبيانات:** نصت عليه المادة 3 من اتفاقية بوكسيت لعام 2001، "يجب على كل طرف أن... الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها وفقا لقانونه الداخلي... من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسوب أو في داخل النظام المعلوماتي..."

والهدف من المادة كان حماية الحق في الخصوصية وفي حرية الاتصالات. وذلك بالنقل أو التسجيل باستعمال أي من الأجهزة الفنية للإرسال غير العلني للمحادثات أو البيانات أو الملفات. سواء كان ذلك عن طريق الحاسوب أو الهاتف أو الفاكس وهي محمية بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الانسان..

2- **خصائص جرائم التجسس:** تعتبر من الجرائم الواقعة على أمن الدولة الداخلي والخارجي ويكون الاعتداء على مصالح الأفراد وحرياتهم وأيضا سرية المعلومات على مستوى أمن الدولة محل للاعتداء أو ارتكاب جريمة التجسس، سواء ما تم التطرق إليها من حريات في الاتفاقيات الدولية والدساتير والقوانين المتعلقة بالحق في الخصوصية وحرية الرأي والتعبير أو تلك التي تستهدف الأمن القومي للدولة مثل معلومات أمنية محتفظة لدى جهاز المخابرات بالدولة أو معلومات عسكرية تتعلق بالجيش ودرجة تسليحه، أو كل ما يتعلق بالأجهزة السياسية وباقتصاد الدول. ص 19

وتعتبر جرائم التجسس أيضا من الجرائم المستمرة، حيث يمتد فيها السلوك الاجرامي إلى خارج نطاق الدولة ويدل على طول ارتكاب السلوك الاجرامي إلى غاية تحقيق النتيجة. أي لحظة القبض على الجانب وتسليمه للسلطات.

إن جرائم التجسس الالكتروني من بين أهم الجرائم التي يتحقق فيها العنصر الإيجابي للجريمة ويكتمل في آن واحد، مثل: الشخص الذي يقوم بعملية التجسس فإنه تام فعلا بارتكاب فعل التجسس أي الركن العادي للجريمة وفي نفس الوقت تكون النتيجة متحققة بمجرد الاطلاع على المعلومة، وحتى وإن لم يتجسد الركن المادي في سلوك ملموس، فإنه يحصل بمجرد الاطلاع على المحكومة ونقلها.

كذلك تعتبر جرائم التجسس من قبيل جرائم الاعتياد فهي ترتكب لأكثر من مرة وخلال مدة زمنية قصيرة.

تعتبر جرائم التجسس الالكتروني من الجرائم العمدية التي يتوفر فيها كل من القصد الجنائي الخاص والهام أن يوضح النية الاجرامية وسهولة كشفها فهي جرائم لا تقع عن طريق الخطأ.

التجسس الالكتروني من بين أهم الجرائم التي يعاقب عليها القانون لمجرد التخطيط والتفكير الجرمي أي الاتفاق الجنائي مثال: لو اتفق شخصان على سرقة معلومات ترتبط

بالدولة عن طريق التخابر وقاما بالاطلاع غير المشروع فإنهما يعاقبان على أساس الاشتراك في ارتكاب جريمة التجسس في تلك الخطة حتى ولو لم يتم تسليم هذه المعلومات بعد إلى دولة أجنبية أو أشخاص آخرين.

3- **أركان جريمة التجسس الالكتروني:** تتلخص أركان جريمة التجسس الالكتروني في ثلاثة أركان كما هو الشأن بالنسبة للجرائم التقليدية التي تتم بصورة عادية، يكمن الركن الأول في توافر مبدأ الشرعية الذي لا تقوم الجريمة بدونه، فهو المعيار الذي يتم من خلاله التمييز بين الفعل المباح قانونا والفعل المحظور وفقا لنصوص قانون العقوبات أو القوانين المستقلة عنه، فتقوم من خلاله أجهزة العدالة بمباشرة إجراءاتها في التحقيق، وهي من تقوم بالكشف عن شرعية أو عدم ذلك، من خلال الاستناد إلى النص التجريمي العقابي الذي لا بد من توافره حتى يتم تحقيق العقوبة على مرتكب الفعل غير المشروع.

3- **الركن المادي لجريمة التجسس الالكتروني:** هي الصورة التي يتم من خلالها ارتكاب جريمة التجسس الالكتروني سواء عن طريق الشروع في ارتكابها أو تنفيذها فعلا، وكون لها أثر مادي ملموس غير أنه في مثل هذا النوع من الجرائم غالبا ما يكون الفعل معنوي أي لا يترتب عنه ضرر خارجي وإنما يتأثر المجني عليه تأثرا معنويا قد يؤدي إلى ضرر مادي ونظرا لقيام الجاني بفعل التجسس فهذا يعني أن كل عناصر الركن المادي من فعل ونتيجة وعلاقة سببية قد تم تحققها بمجرد الاطلاع غير المشروع كما ذكرنا سابقا. ص 24

4- **الركن المعنوي لجريمة التجسس الالكتروني:** يعتبر الركن المعنوي في جريمة التجسس الالكتروني مفتاح أو حجرة الأساس في اثبات وقوع الجريمة من عدمها، فهو الدليل على علم الفاعل بالطبيعة القانونية لفعله الإجرامي، أي اتجاه إرادته للقيام بالفعل، وهو سيبقى في ذلك ظهور الركن المادي للجريمة.

5- لأن النية الاجرامية تكون هي الأسبق وهي تأكيد فعلي لارتكاب الجريمة وهنا الأمر يختلف عن الجرائم المادية التي يصعب في الغالب كشف النية الاجرامية من خلالها لأنها لا ترتكب بفعل الوسائط الالكترونية.

ثانيا-تجريم جرائم التجسس الالكتروني في قانون العقوبات: قبل أن نتطرق إلى المجال القانوني لجرائم التجسس الالكتروني في قانون العقوبات نعرج أولا إلى مجموع النصوص والمواثيق الدولية التي تضمنت هذه الجريمة بالإعلان العالمي لحقوق الانسان عام 1948، والعهد الدولي للحقوق المدنية والسياسية لعام 1966، وخاصة في المادة 17 منه التي تنص على "الحق في حرمة الحياة الخاصة وأنه لكل شخص الحق في عدم التعرض بحياته على نحو تعسفي أو غير مشروع للتدخل في خصوصياته أو شؤون أسرته أو بيئته أو مراسلاته" أي ضمان سلامة وسرية المراسلات قانونا وفي الواقع وهي ترتبط بشخصية صاحبها ولا يجوز المساس بها بأي طريقة أو أخرى كقراءتها وفتحها ومسحها ويصدق القول هنا أيضا على سرية المعلومات الالكترونية التي تكون محزنة في الجهاز الالكتروني، لأنه تم حظر الرقابة بالوسائل الالكترونية أو غيرها

وأيضا على اعتراض الاتصالات الهاتفية والبرقية، وضرورة حمايتها من التنصت حتى ولو كان الكترونيا.

كما استوجب في مجال الجريمة الالكترونية تنظيم القانون لعمليات حفظ المعلومات الشخصية عن طريق الحاسوب ومصارف البيانات.

1- **دور الجمعية العامة للأمم المتحدة في حماية الحق في الخصوصية الرقمية:** تحت عنوان "الحق في الخصوصية في العصر الرقمي" تناولت الجمعية العامة هذه المسألة الناشئة ضمن القرار رقم 68/167 المؤرخ في 2013/12/18، حيث أكدت على أن الحق في الخصوصية هو حق من حقوق الانسان الأساسية يجب حمايته على الانترنت ودعت الدول إلى احترام وتعزيز حماية الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية.

أيضا أكدت الجمعية العامة على هذا الحق من خلال تقريرها رقم 69/166 المؤرخ في 2014/12/18 الذي قام من خلاله بحث الدول على:

- حماية واحترام الحق في الخصوصية بما في ذلك في سياق الاتصالات الرقمية.
- أن تتخذ ما يلزم من التدابير لوضع حد لانتهاكات تلك الحقوق، وأن تعمل على تهيئة الظروف الملاءمة والكفيلة بالحيلولة دون حدوث هذه الانتهاكات، بطرق تضمن من خلالها توافق تشريعاتها الوطنية في هذا الصدد مع التزاماتها بموجب القانون الدولي لحقوق الانسان.
- إعادة النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجميع البيانات على نطاق واسع.
- إنشاء آليات رقابة محلية قضائية، إدارية، برلمانية نزيهة ومستقلة وفعالة على أن يتم تزويدها بموارد كافية وقادرة على ضمان الشفافية حسب الاقتضاء والمساءلة بشأن مراقبة الدولة للاتصالات واعتراضها وجميع البيانات الشخصية.
- إتاحة الفرصة للأشخاص الذين انتهك حقهم في الخصوصية نتيجة المراقبة التعسفية أو غير القانونية سبل الإنصاف الفعالة بما يتسق مع الالتزامات الدولية في مجال حقوق الانسان.

ومن أمثلة التعاون الدولي أيضا تقديم كل من ألمانيا والبرازيل مشروع قرار رقم 68/67، عام 2013 إلى الجمعية العامة للأمم المتحدة حول الحق في الخصوصية في العصر الرقمي نتيجة انتشار التنصت على الاتصالات الرئيسية في الو.م.أ وبريطانيا والبرازيل، مما يشكل انتهاكا صارخا للحق في الخصوصية عبر توظيف تكنولوجيات تسمح بالوصول إلى الكثير من سجلات المكالمات عبر الانترنت والعناوين الالكترونية للأفراد، كما تم استخدام برنامج تجسس رقمي Prism وهو سري للغاية من قبل الوكالة الأمريكية للأمن القومي منذ عام 2007، والذي أعطى الوكالة صلاحية جمع وتحليل البيانات الرقمية ومعرفة محتواها.

ثانيا-جهود المفوضية السامية لحقوق الانسان ومختلف المنظمات الدولية الأخرى في حماية الحق في الخصوصية الرقمية: لقد صدر تقرير عن المفوضية السامية لحقوق الانسان بتاريخ 2022/09/16 حذر من خطورة تعرض الحق في الخصوصية لضغوط متزايدة بسبب استخدام التكنولوجيات الرقمية الحديثة المتصلة بالشبكات التي حولتها إلى أدوات للمراقبة والسيطرة والقمع، حيث تناول هذا التقرير ثلاث مسائل رئيسية هي:

- إساءة سلطات الدول استخدام أدوات الاختراق الحاسوبي "برامج التجسس".
- تفشي ظاهرة الرصد الرقمي للأماكن العامة، خاصة في ظل جائحة كوفيد 19 عبر عديد الدول وذلك باستعمال أحدث التكنولوجيا في تتبع الأشخاص ورصد أماكن تواجدهم.
- دور التشفير "تشفير البيانات" في ضمان حماية حقوق الانسان عبر الانترنت.
- نظم معلوماتية قوية جيدة التصميم وتفعيل مراقبتها لمنع محاولات اختراقها.

1- **تعيين مقرر خاص بحماية الحق في الخصوصية الرقمية على مستوى المفوضية:** لقد تم تعيين مقرر خاص يعنى بمتابعة جهود حماية الحق في الخصوصية ابتداء من سنة 2015، حيث يتمتع هذا المقرر بولاية واسعة لتغطية الجوانب المتعددة للجق في الخصوصية، ومن أهم مهامه ما يلي:

- المراجعة المنهجية للسياسات الحكومية التي تعترض الاتصالات الرقمية وتجمع البيانات الشخصية وإبراز السياسات التي تتدخل في الخصوصية دونما مسوغ مقنع.
- التحقق من مسؤوليات القطاع الخاص باحترام حقوق الانسان في ظب "إطار عمل الحماية والاحترام، والإنصاف" للمبادئ التوجيهية للأمم المتحدة للمؤسسات وحقوق الانسان في سياق محدد من تكنولوجيا الاتصالات والمعلومات الرقمية.
- المساعدة على تطوير المعايير الدولية التي تعالج بشكل أكثر فعالية التفاعل بين الخصوصية وحرية التعبير... وغيرها من حقوق الانسان في السياق الرقمي.
- التركيز على العوامل التي تسهل المراقبة الفضفاضة، بما في ذلك الممارسات المتفاوتة على نطاق واسع ومستويات الشفافية حول ما تحتفظ به الشركات من بيانات، وكيف لهذه الممارسات في كثير من الحالات التأثير المباشر على ما تجمعه الحكومات وترصده، والعمل مع خبراء الأمم المتحدة الآخرين على حماية حرية التعبير وحرية التجمع السلمي.
- تشجيع مجلس حقوق الانسان على أن يبقى باب المناقشة مفتوحا بهدف تحديد وتوضيح المبادئ والمعايير وأفضل الممارسات فيما يتعلق بتعزيز وحماية الحق في الخصوصية وأن ينظر في إمكانية وضع إجراء خاص لهذا الغرض.

2- جهود مجلس حقوق الانسان في حماية الحق في الخصوصية الرقمية: أكد مجلس حقوق الانسان في القرار رقم 32/13 المؤرخ في 2016/07/01 تحت عنوان "تعزيز وحماية حقوق الانسان على الانترنت والتمتع بها" في فقرته الثامنة على دعوة الدول إلى التصدي للشواغل الأمنية على الانترنت وفقا لالتزامها الدولية في مجال حقوق الانسان من أجل ضمان حرية التعبير، وضمان حرية تكوين الجمعيات والحق في الخصوصية

وغير ذلك من حقوق الانسان على شبكة الانترنت، عن طريق مؤسسات وطنية وديمقراطية شفافة وعلى أساس سيادة القانون، وبطريقة تكفل الحرية والأمن على شبكة الانترنت، لكي يتسنى لهذه الشبكة أن تظل قوة حيوية تولد التنمية الاقتصادية والاجتماعية والثقافية.

وفي سبيل تفعيل استخدام التقنيات الرقمية وحكومتها، أكد البيان مفوضية الأمم المتحدة لحقوق الانسان عام 2021، كيف أن الحياة الخاصة للأفراد أضحت وسيلة لقمع حقوقهم وحرياتهم عبر استخدام شبكة الانترنت وانتشار الترهيب والاعتداءات العنيفة التي تنجر عن استخدامها، وتطورت قرارات مجلس حقوق الانسان بشأن الحق في الخصوصية وخاصة فيما يتعلق بحماية الصحفيين واحتوائه على مبادئ توجيهية أساسية للأمم المتحدة في إطار تحقيق التعاون بين الدول والشركات التكنولوجية والمجتمع المدني مثل دعم ما يسمى بمركز الأمم المتحدة لحقوق الانسان والتكنولوجيا الرقمية.

2/ جريمة النصب والاحتيال

سُميت جريمة الاحتيال بجريمة النصب في العديد من التشريعات، منها التشريع الجزائري. وهي عبارة عن استيلاء على مال منقول للغير بخداع المدين وحمله على تسليمه. جريمة النصب هي من جرائم الغش والاحتيال، أو هي كل تدليس يقصد فاعله من خلاله إيقاع شخص في الغلط أو استغلال ذلك الغلط الذي وقع فيه لحمله على تسليم المال. ويتم ذلك بتسليم المال للفاعل أو لغيره سواء عن طريق التدليس بالقول، أو الكتابة، أو الإرشاد.

وعليه، يتحقق فعل الاحتيال بجريمة النصب على الأشخاص الطبيعيين والمعنويين على حد سواء. يُعد الحاسوب ووسائل الاتصال من أهم الوسائل المستخدمة للاحتيال من قبل الشركات العامة والخاصة، مما يجعلها عرضة للتلاعب والاحتيال على معطياتها أو نظامها المعلوماتي.

ونجد أن الاحتيال والنصب الإلكتروني يأخذ صورًا عديدة ومتطورة بتطور التكنولوجيا الحديثة ووسائل الاتصال، التي تسهل انتشارها وسرعة الوقوع فيها. مثل:

- مجالات التبادل التجاري.
- تحويل الأسواق الإلكترونية.
- الدفع باستخدام بطاقات الائتمان.

ومن أمثلة ذلك انتحال الأسماء الكاذبة، وتبني صفة أو شخصية وهمية، أو إنشاء مشروع وهمي أو كاذب بهدف تحقيق الربح السريع..

ونجد أن أساس جريمة النصب والاحتيال الإلكتروني هو التلاعب الوهمي والخداع، مثل إنشاء مواقع وهمية تتشابه مع مواقع أصلية لشركات أخرى واستقبال المعلومات، خاصة في مجال البطاقات الائتمانية، حيث قد يستخدم حامل البطاقة طرقًا احتيالية من بينها القيام بتحويلات مالية عبر البنوك بأسماء وهمية.

وبالتالي يرتبط الاحتيال الإلكتروني في مجال المعلوماتية بإيقاع الأشخاص والمؤسسات للحصول على أموالهم بطرق غير شرعية.

ولا تزال هذه الجريمة تُنفذ بأساليب احترافية في ظل غياب أو قصور في التشريعات الجزائرية لمواجهة هذا النوع من الجرائم التقنية. فالمشرع الجزائري تعامل مع فعل الاحتيال في حد ذاته واعتبره عنصرًا أساسيًا من عناصر الركن المادي في جريمة الاحتيال بالطرق العادية وليس الإلكترونية أو المعلوماتية، وهذا ما ورد في نص المادة 372 من قانون العقوبات.

إلى جانب ذلك، هناك غياب للنصوص الإجرائية الكفيلة بملاحقة مرتكبي هذه الجرائم التي تتعدد صورها ومجالاتها، مثل:

- جرائم الاعتداء على الأموال أو الأنظمة المالية.
- جرائم الاحتيال باستخدام بطاقة الدفع الإلكتروني والاستيلاء على الأموال الموجودة في هذه البطاقات.
- جرائم الاحتيال المعلوماتية أو الغش المعلوماتي الذي يؤدي إلى حدوث أضرار مادية.

وهذا الأخير قد يجد حماية من خلال ما ورد في نص المادة 394 المرتبطة بالدخول والبقاء غير المشروع، ولكن في غير هذه الحالة نعود إلى نفس القوانين العادية والإجراءات التقليدية.

وعليه، يتحقق فعل الاحتيال بجريمة النصب على الأشخاص الطبيعيين والمعنويين على حد سواء. يُعد الحاسوب ووسائل الاتصال من أهم الوسائل المستخدمة للاحتيال من قبل الشركات العامة والخاصة، مما يجعلها ضحية للتلاعب والاحتيال على معطياتها أو نظامها المعلوماتي.

ونجد أن الاحتيال والنصب الإلكتروني يأخذ صورًا عديدة ومتطورة بتطور التكنولوجيا الحديثة ووسائل الاتصال، التي تسهل من انتشارها وسرعة الوقوع فيها، مثل:

- مجالات التبادل التجاري.
- تحويل الأسواق الإلكترونية.
- الدفع باستخدام بطاقات الائتمان.

ومن أمثلة ذلك انتحال الأسماء الكاذبة، وتبني صفة أو شخصية وهمية، أو إنشاء مشروع وهمي أو كاذب بهدف الوصول إلى الربح السريع.

ونجد أن أساس جريمة النصب والاحتيال الإلكتروني هو التلاعب الوهمي والخداع، مثل إنشاء مواقع وهمية تتشابه مع مواقع أصلية لشركات أخرى واستقبال المعلومات، خاصة في مجال البطاقات الائتمانية. حيث قد يستخدم حامل البطاقة طرقًا احتيالية، من بينها القيام بتحويلات مالية عبر البنوك بأسماء وهمية.

وبالتالي يرتبط الاحتيال الإلكتروني في مجال المعلوماتية بإيقاع الأشخاص والمؤسسات للحصول على أموالهم بطرق غير شرعية.

ولا تزال هذه الجريمة تُنفذ بأساليب احترافية في ظل غياب أو قصور في التشريعات الجزائرية لمواجهة هذا النوع من الجرائم التقنية. فقد تعامل المشرع الجزائري مع فعل الاحتيال في حد ذاته واعتبره عنصرًا أساسيًا من عناصر الركن المادي في جريمة الاحتيال بالطرق العادية وليس الإلكترونية أو المعلوماتية، وهذا ما ورد في نص المادة 372 من قانون العقوبات.

إلى جانب ذلك، هناك غياب للنصوص الإجرائية الكفيلة بملاحقة مرتكبي هذه الجرائم، التي تتعدد صورها ومجالاتها، مثل:

- جرائم الاعتداء على الأموال أو الأنظمة المالية.
- جرائم الاحتيال باستخدام بطاقة الدفع الإلكتروني والاستيلاء على الأموال الموجودة في هذه البطاقات.
- جرائم الاحتيال المعلوماتية أو الغش المعلوماتي الذي يؤدي إلى حدوث أضرار مادية.

وقد يجد هذا الأخير حماية من خلال ما ورد في نص المادة 394، المرتبطة بالدخول والبقاء غير المشروع. ولكن في غير هذه الحالة، نرجع إلى نفس القوانين العادية والإجراءات التقليدية.

الأساس القانوني للجريمة المعلوماتية الإلكترونية في قانون الإجراءات الجزائية:

إن المتعارف عليه بالنسبة للجريمة الإلكترونية هو قلة أو غياب النصوص الجزائية المحددة لطرق المتابعة القضائية، وأن كثيرًا منها أخفى طرق إجراءات التحقيق بالنسبة للجرائم العادية. إلا أن المشرع الجزائري تطرق في نص المادة 65 مكرر من قانون الإجراءات الجزائية إلى غاية المادة 65 مكرر 5 إلى إجراءات تخص الجريمة الإلكترونية، مثل انتهاكات حرمة الحياة الخاصة، اعتراض المراسلات، تسجيل الأصوات، والتقاط الصور، مغلبًا في ذلك حق الدولة في المتابعة والعقاب على حق الأفراد.

وهذا ما قصده المشرع الجزائري في نص المادة 65 مكرر 5 التي تنص على ما يلي:
"إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أثناء التحقيق الابتدائي في جرائم الإرهاب والمخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وغيرها، يجوز لوكيل الجمهورية المختص أن يؤذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات دون موافقة، من أجل التقاط، تثبيت، وبث تسجيل الكلام أو الحديث من طرف شخص أو عدة أشخاص في أماكن عمومية، أو التقاط صور لأشخاص في أماكن خاصة.

ويسمح وكيل الجمهورية، عن طريق الإذن ووضع الترتيبات التقنية، بالدخول إلى المحلات السكنية أو غيرها حتى لو كان ذلك خارج المواعيد المحددة في المادة 47 من هذا القانون.

عليه، تتم هذه الإجراءات بموافقة وكيل الجمهورية وتحت إشرافه ومراقبته، كما أنه هو من يحيل لقاضي التحقيق فتح تحقيق قضائي إذا تم حدوث واقعة من الوقائع المذكورة أعلاه".

كما لا يمكن لضابط الشرطة القضائية أن يقوم بأي إجراء من الإجراءات السابقة إلا بعد حصوله على إذن وكيل الجمهورية، ويجب أن يكون مكتوبًا. ويسمح لهم هذا الإذن أيضًا بالتفتيش مع مراعاة الوقت، أي قبل الساعة 8 ليلًا وبعد الساعة 5:00 صباحًا.

أي عدم انتهاك الحق في الخصوصية الذي أكد عليه المشرع في المادة 303 من قانون العقوبات، حيث نص على أن:

"كل من يفض ويتلف رسائل أو مراسلات موجهة إلى الغير، وذلك سواء بعمد أو في غير الحالات المنصوص عليها قانونًا، يعاقب بالحبس من شهر إلى سنة، وبغرامة تتراوح بين 25,000 إلى 100,000 دينار جزائري، أو بإحدى هاتين العقوبتين فقط".

أيضًا، ما ورد في نص المادة 303 مكرر من قانون العقوبات بشأن الحماية الجنائية للحق في الخصوصية وحرمتها، حيث نص على أن: "يعاقب بالحبس من سنة إلى ثلاث سنوات، وبغرامة تتراوح بين 50,000 إلى 300,000 دينار جزائري، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية".

يلاحظ من خلال هذه النصوص أنها لا تتعلق بحماية عقابية أو جزائية للجريمة الإلكترونية في جرمها. إذا نظرنا إلى مفهوم أو مضمون المادة 303 من القانون العام، نجد أنها تشكل حماية للخصوصية في الحالات المادية وليس الإلكترونية المعلوماتية. أما المادة 303 مكرر فتضمن من خلالها حماية هذا الحق من الناحية التقنية عن طريق ذكر عبارة "بأي تقنية"، أي يمكن أن يقصد بها المشرع أي وسائل إلكترونية أخرى.

ومادام أنه لم يصرح أو لم يتضمن بشكل واضح عقوبات أو جزاءات تشمل الجريمة الإلكترونية والمعلوماتية في حد ذاتها، فإنه تبقى الإجراءات المتعارف عليها في الجريمة التقليدية تطبق على الجريمة الإلكترونية.

الاختصاص الجزائي للجريمة الإلكترونية:

ويقصد به الجهات المختصة لإجراء الدعوى الجزائية، أو ما يسمى بإجراءات الملاحقة أو المتابعة الجزائية، ونظر المحكمة في الجريمة المعلوماتية، وخاصة من ناحية القانون الداخلي والقانون الدولي. ويكتسب القانون الدولي أهمية خاصة في هذا السياق لأن أغلب الجرائم المعلوماتية هي جرائم عابرة للحدود.

الاختصاص الداخلي:

يقصد به توزيع الدعاوى الجزائية على المحاكم، وينعقد الاختصاص تبعًا لنوع الجريمة والاختصاص الشخصي الذي يحدد تبعًا لنوعية الجريمة، والاختصاص المحلي الذي يحدد بمكان وقوع الجريمة (محل الإقامة أو مكان القبض على الجاني) حسب المواد 37، 40، 329، 248، 451 من قانون الإجراءات الجزائية.

وعادةً لا يوجد إشكال في معالجة الجرائم الناتجة عن حاسوب متصل بشبكة واحدة أو داخل الدولة نفسها. إنما يثور الإشكال بخصوص الجرائم المتعددة الشبكات أو التي تتخطى حدود الدولة عبر الإنترنت المتصلة بجميع دول العالم، مما يستدعي تدخل القانون الدولي. أي أن تكون الجريمة غير مرتبطة بإقليم واحد، وبالتالي تعاقب كل دولة الجاني المرتكب لهذه الجريمة وفقًا لقانونها الداخلي، كما هو الحال بالنسبة للجريمة التقليدية.

مبدأ إقليمية القوانين:

وفقًا لنص المادة 03 من قانون العقوبات، يطبق القانون الجزائي على الجرائم المرتكبة على أرض الجمهورية، حتى بالنسبة للجريمة الإلكترونية أو المعلوماتية، فإن يُؤَوَّل الاختصاص وفق قواعد القانون الجزائي الجزائري شريطة تحديد مكان ارتكابها، سواء كانت جرائم وقتية أو مستمرة. وعليه، يُسند الاختصاص إلى المحاكم الجزائية الجزائرية.

فإذا انطلق الفعل الجرمي من الإقليم الجزائري، ينعقد الاختصاص للمحاكم الجزائرية، خاصة في حال اكتمال عناصر الركن المادي أو جزء منه، مثل الدخول والتخريب، أو ارتكاب غش معلوماتي، أو احتيال، أو اعتداء على نظام

المعالجة الآلية للمعطيات. يُقال الاختصاص للقضاء الجزائري، مثلما يحدث عند اختراق المعلومات داخل الشبكة المفتوحة لشركة أو منظمة حكومية انطلاقًا من الإقليم الجزائري، أو نشر فيروس من الإقليم الجزائري وانتشاره في باقي الدول.

أما بالنسبة للجريمة الواحدة أو الجرائم المتجزئة المستمرة أو الممتدة خارج الدولة، مثل الجريمة المتتابعة، وجريمة الاعتياد، والجريمة المركبة، ففي هذه الحالة يكفي أن يتحقق في الجزائر حالة من حالات الاستمرار أو الاعتياد. كذلك في حال القبض على الجاني إذا استقر وجوده في الإقليم الجزائري.

كما ينطبق قانون العقوبات على كل شريك موجود في الأراضي الجزائرية في جناية أو جنحة مرتكبة في الخارج، وفقًا لنص المادة 585 من قانون الإجراءات الجزائية.

وسائل إثبات الجريمة الالكترونية

ونقصد بالدليل الالكتروني هو تلك المعطيات اللصيقة بالملف أو البرنامج في المعلومات الالكترونية المتواجدة على جهاز الكمبيوتر ، وهي بمثابة معطيات رقمية يلجأ إليها المحققون لأجل الحصول على أدلة رقمية تساعد في الوصول إلى حل الخصومة المعروضة على القاضي إلا أنه في هذه الحالة يختلف الدليل الالكتروني عن الدليل العادي في الجريمة العادية وخاصة من ناحية الإثبات كون أن الجرائم الالكترونية تتميز بخصائص السرعة والكثافة أو غزارة المعلومات وتشبعها وبالتالي تكون في غالب الأحيان معقدة وذلك كونها عرضة للتحويل والتبديل والإلغاء أو الحذف والتغيير...

أنواع الدليل الالكتروني: تشتمل الدليل الالكتروني مخرجات ورقية ومخرجات الكترونية

1- **الدليل الالكتروني الورقي**: أي أنه ذا طبيعة ورقية تسجل فيها المعلومات على الورق عبر استخدام الطابعات والرسومات.
2- **الدليل الالكتروني**: الذي يستخرج من المعلومات المخزنة في جهاز الحاسوب بدلا من الوثائق الورقية كالأشرطة المغناطيسية والأوراق والدعامات الالكترونية وتستخدم عند عرضها على جهاز الحاسوب، أي عرض المعطيات المعالجة آليا.

وهذا يعني أن هناك أدلة تعد لتكون وسيلة للإثبات كالسجلات المعالجة والموجودة في الجهاز أو الآلة، وأيضا المعلومات المخزنة، وهي سهلة الاكتشاف لأن صاحبها يترك أثرا بمجرد الدخول أو البقاء أو المساس بالمعلومة ودون أن يعلم بذلك.

والدليل الرقمي يحدد ما إذا تم العبث بالمعلومات أو تعديلها عند مقارنتها بالنسخة الأصلية.

كما يمكن استرجاع الدليل حتى بعد حذفه من جهاز الكمبيوتر وذلك عن طريق استخراجه بالاعتماد على برامج الاسترجاع. ص267.

مثال: لو حاول الجاني إخفاء نشاطه الاجرامي أو حذفه في سبيل محو الدليل فإن هذه العملية بذاتها يمكن استخلاصها بالرجوع إلى ما يسمى بسجلات التدقيق LOG.

يمكن للمحققين استغلال الأدلة على مستوى عالمي لأن المجرم المعلوماتي أو الالكتروني لا يقوم على مسرح واحد للجريمة وفي إطار واحد، فقد تتعدد الأمكنة وتختلف باختلاف المناطق والدول المرتكب على متنها مثل هذا النوع من الجرائم.

3- الدليل القضائي والدليل الالكتروني:

يتميز الدليل القضائي بالطابع القضائي واجراءاته تكون قضائية إجرائية بحتة تقوم على حجة اثبات واقعية وحقيقية بينما الدليل الالكتروني فهو ذو طابع تقني لا بد أن يستند على القضاء حتى يتم اعتماده لدليل الكتروني وقضائي، وذلك بخروج الواقعة من الطابع التقني إلى الطابع القضائي وهذا يتوقف على الأساس القانوني ومدى تواجده بالنسبة للكثير من الوقائع الإلكترونية.

كما أنه الدليل الالكتروني يمكن إثباته بعد عرضه على خبراء تقنيين ومختصين في مجال التقنية والقضاء بهدف الوصول إلى الحقيقة أما الدليل القضائي فهو مرتبط بمدى تطبيق قانون الإجراءات الجزائية (أي الملف الجزائي) وقد ينتهي إما بالبراءة أو الإدانة.

أما الدليل الالكتروني فينتظر ما تم التوصل إليه من الخبير التقني من وقائع إلكترونية وأدلة، فتكون لدى القاضي هنا سلطة تقديرية واسعة في تقدير البراءة أو الإدانة، أو يطبق قاعدة تفسير الشك لصالح المتهم أي بمعنى آخر الدليل القضائي يكون قويا من حيث الحجة مقارنة بالدليل الالكتروني، كما يجب على القاضي أن يكون على دراية بالأدلة الالكترونية لأن عدم تمكنه من ذلك يشكل قصورا في التسيير، وعجزا في إثبات الجريمة.ص299

لذلك تعتبر الأدلة الالكترونية أداة اثبات ولكنها ليست فعالة إلى حد كبير نظرا للصعوبات التي تثأر حول طبيعتها التقنية ولغة فهمها أو إعطاء وصف قانوني لها، مما جعل منها أدلة لا يمكن إدراجها ضمن الأدلة ..... تقليديا.

جهات التحري والتقصي والبحث عن الأدلة الالكترونية:

أنشأ المشرع الجزائري القانون 09/04بموجب المادة 13منه، هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وذلك من خلال تطبيق فكرة الاستباقية في الوقاية من الاجرام التكنولوجي بمساعدة السلطات القضائية ومصالح الشرطة القضائية، وذلك بإجراء تحريات عبر جمع المعلومات وإنجاز الخبرة القضائية وتبادل المعلومات على المستوى الخارجي في سبيل الحصول على معلومات أو تبادل المعطيات للتعرف على مرتكبي هذه الجرائم وأماكن تواجدهم.

- قد تضمنت المادة 45من قانون 04/09المؤرخ في 2009/8/5 مهام جهات التحقيق من بينها اجراء التحريات وضمان المراقبة والوقاية للاتصالات الالكترونية وخاصة فيما يتعلق

بالجرائم الماسة بأمن الدولة تحت سلطة القاضي المختص، وأيضا تسجيل وتجميع وحفظ المعطيات الرقمية.

وهناك فرق متخصصة على مستوى الشرطة تمتلك سلطة التدقيق في جرائم الاعلام الآلي وكذلك الدرك الوطني.

إجراءات التقصي:

تختلف الأدلة الالكترونية كأدلة إثبات عن الأدلة المادية في الجرائم العادية أو التقليدية.

فجرائم الانترنت يتم اثباتها عن طريق الأدلة الرقمية أو الالكترونية، المستخرجة من الحاسبات الآلية والمستخدمة في تنفيذ أفعال جريمة مثل: سجلات الحفظ (log fils) وهي تلك التقنية التي تختص بتسجيل الإجراءات وكافة الأنشطة التي سبق اتخاذها من طرف مستخدم الانترنت، أو هي البريد الالكتروني الذي يكمن في مجموع الرسائل المتبادلة بين المتهم والمجني عليه والتي تكشف عن المراسلات والاتفاقيات والوعود الالكترونية والتهديدات وهي بدورها قد تشكل دليلا يحدد هوية المتهم.

- وفي حال التأكد من هذه الأدلة بعد الحصول عليها من طرف الأجهزة الأمنية والفنية وضبطها بناء على اذن النيابة العامة التي تأمر بدورها بضبط الجهاز في حد ذاته لأنه بمثابة الوسيلة المستخدمة في تنفيذ الجريمة الالكترونية.

- وقد سبق وأن أشرنا أن المشرع الجزائري لم يتطرق إلى الأدلة كوسيلة للإثبات بالنسبة للجرائم المعلوماتية والالكترونية، إلا أنه في هذه الأخيرة ركز على اعتبارها كوسيلة للإثبات في مجال التصرفات القانونية المادية كالمواد التجارية والمعاملات المصرفية مثل: الدفع الالكتروني والبطاقات البنكية من أجهزة الحاسوب.

وهي الوحيدة التي تشكل دليل اثبات يعكس تصنيف قانون الإجراءات الجزائية في الدعوى العمومية.

- وبالتالي هناك نوعين من الأدلة الالكترونية من حيث تطبيق قانون الإجراءات الجزائية تتمثل في:

1- المحررات الالكترونية: وتعتبر كدليل اثبات الكتروني واقعي وله الحجة في الاثبات سواء كان مدنيا أو جزائيا كالتوقيع الالكتروني في مجال المعطيات المعالجة آليا، وخاصة في مجال التجارة الدولية إذ أضحت تعتمد على تقنيات الكمبيوتر والسندات الالكترونية في ربط المتعاملين عبر الشبكة. ص351 ومن بين المحررات الالكترونية التي يعتمدها المشرع الجزائري هي المحررات الالكترونية المكتوبة والمرتبطة بحروف متسلسلة ترابط من حيث المعنى، وهي تشتمل على معلومات ومعطيات محتواه في الأقراص المضغوطة أو الدعامة الالكترونية التي يتم كتابتها بواسطة الكمبيوتر وارسالها ونشرها.

واشراط المشرع الجزائري في الكتابة الالكترونية أ تكون واضحة أي لا تحتوي على رموز أو خوارزميات أو إشارات لأنه يصعب اثباتها وبالتالي تخرج عن كونها محررا الكتروني لعدم صحته.

- ومع ذلك لم يحدد المشرع الجزائري نصوصا قانونية تنظم شروط الكتابة أو كيفياتها، أو إمكانية قبولها من عدم ذلك كالتعاملات العقدية والتجارية وخاصة في مجال الشروط الشكلية.

إجراءات التحقيق في الجرائم المعلوماتية

إن وسائل أو طرق إتباع قضايا الجرائم المعلوماتية أو الالكترونية لا تختلف كثيرا عن إجراءات التحقيق في الجرائم العادية من حيث مشروعية البحث عن الدليل أي مرحلة الاستدلال والبحث عن الدليل والذي يكمن في الجريمة بالاعتماد على الوسائط الالكترونية كالحاسوب والهاتف أو أي دعمة أخرى، وأيضا تطبيق نفس إجراءات التحقيق من سماع الأقوال والاستجواب..... الخبراء كما هو الحال في الجرائم التقليدية. وكما تم التطرق إليه سابقا أن هناك إجراءات أولية ينطلق منها جهاز العدالة للكشف عن الجريمة ومرتكبها والتقصي عن تفاصيل ارتكابها والمتمثلة في إجراءات التحقيق التمهيدي الذي يقوم بها جهاز الضبطية القضائية كاختصاص أصل لها. وذلك عبر المرور ببعض المراحل والإجراءات الازمة للسير في التحقيق وهي:

1- الإبلاغ عن الجريمة:

الجريمة الالكترونية هي أيضا تخضع لإجراء الإبلاغ عنها بنفس طريقة الإبلاغ في الجريمة التقليدية وبخاصة إجراءات التحقيق من صحة وقوعها فعلا وطرق اثباتها والكشف عنها، وصولا إلى مرتكب الجريمة أو الحصول على معلومات أو وثائق تبرز وقوع الجريمة فعلا.

وكما سبق الذكر فإن عنصر المعلومات والوثائق قد يشكل محلا لارتكاب الجريمة المعلوماتية وتتلخص هذه الإجراءات المرتبطة بالإبلاغ عن الجريمة فيما يلي:

أ- **اجراء الإبلاغ:** (أو الاخبار) وهو اجراء قانوني يشكل التزاما قانونيا أخلاقيا يستوجب على كل شخص شاهد أو علم يوقع جريمة الكترونية أو عاينها بنفسهأو تعبيرا على جهاز الحاسوب أو أي وسط الكتروني آخر أن يعلم جهات التحقيق وأن يتقرب إلى أقرب مركز للضبطية القضائية ويبلغ عن مرتكبها. ومن شروط هذا البلاغ أن يكون شفهيا كما يمكن أن يكون مكتوبا وهذا الأخير يصدق تماما مع الجرائم الالكترونية في شقيها المعلوماتي، مثلا:

كأن يتم ضبط عملية تزوير إلكتروني على جهاز الحاسوب أو مستخرج منه، أو عقود إلكترونية مزورة غير مطابقة للشروط القانونية أو توقيعات إلكترونية متلاعب فيها...وغيرها.

والابلاغ عن جريمة الكترونية- معلوماتية هو بمثابة اخبار عن وقوعها فعلا.

ب- الشكوى: كأن يتقدم الطرف المتضرر بنفسه إلى جهاز العدالة شاكيا بوقوع جريمة الكترونية معه أو مع غيره، ويكون هو طرف فيها فيقوم من خلالها جهات التحقيق ببدأ التحقيق فيها بناء على شكوى المتضرر.

وشرط فيها أن تكون بخط اليد أو مطبوعة بواسطة الحاسوب أو أي آلة كتابة وتكون موقعة من الشاكي أي الطرف المتضرر من الجريمة بخلاف البلاغ الذي يقع لمجرد القيام بعملية الإخبار.

وتقوم جهات التحقيق بعد المرور بهذه الإجراءات بالقيام بالتحقيق الالكتروني للتعرف على هوية المبلغ وكذلك على صحة البلاغ أو الشكوى، فقد يكون البلاغ مجهولا غير معلوم وقد تكون الشكوى عبارة عن رسالة مجهولة، وبالتالي يتعذر القيام بعملية التحقيق.

مراحل التحقيق التمهيدي في الجريمة الالكترونية:

وهي عبارة عن إجراءات أولية يقوم بها جهاز الضبطية القضائية لا يختلف كثيرا في إجراءات التحقيق التمهيدي في الجرائم العادية وهي عملية يتم فيها التقصي والتحري عن مرتكب الجريمة وما يدور حولها من تفاصيل تساهم في الكشف عنها والحصول على أدلة لإثباتها، ويكون ذلك بالرجوع إلى الملفات المخزنة في الحاسوب والسجلات الالكترونية والملفات المسجلة ووسائط التخزين الخاصة الموجودة في الدعامات الالكترونية التابعة لجهاز الحاسوب، أو شركة الاتصالات إذا كانت معلومات هاتفية كالسب والقذف أو الصور الإباحية، فتقوم جهات التحقيق باستخراجها عن طريق أخذ صور أو تفريغ محتواها في محضر الاستدلال. وعند القيام بهذه الإجراءات يتم استدعاء المعني إذا كان معروفا لأجل التحقيق معه أوليا عبر سماع أقواله ورده على تلك الرسائل أو المعلومات المخزنة التي شكلت محلا لارتكاب الجريمة.

2- تحديد مكان ارتكاب الجريمة الالكترونية:

إن الجريمة الالكترونية تتميز بطابع الكتروني رقمي على وجود وتعدد أمكنة القيام بالجريمة غير أن الجاني لا يبذل أي مجهود جسدي لأنه يقوم بارتكاب الفعل غير المشروع عبر جهاز الكتروني ويحقق النتيجة أو جزء منها في نفس اللحظة الزمنية، أي لا تعتبر من قبل الجرائم المستمرة أو المركبة التي تقوم على عنصر التنقل من جهة إلى أخرى، أو من منطقة إلى أخرى، هذا من جهة ومن جهة أخرى لا تعتبر الأدلة الرقمية أو الالكترونية دليل حتمي أو يأتي من مكان محدد، بل تستطيع أن نتحصل عليه من أي دعامة الكترونية أخرى كالهاتف، وسائل التخزين المتعارف عليها أي جهاز أو قطعة تعمل بواسطة التكنلوجيا المعلوماتية فهي الأخرى تعتبر محلا للحصول على الدليل الرقمي.

3- إجراءات المعاينة:

إن اجراء المعاينة واضح في الجريمة المعلوماتية وأكثر إدراكا مقارنة واجراءاته بسيطة مقارنة مع المعاينة في الجريمة التقليدية إذ تتم في حضور الضبطية القضائية أو وكيل

الجمهورية أو حتى قاضي التحقيق، لمعاينة مسرح الجريمة أي في الغالب لدينا جثة أو ضحية مغدور بها أو عاهة مستديمة، أما المعاينة الالكترونية فتتم عبر توثيق نشاط على جهاز الحاسوب، ويقوم بها خبير الكتروني (تقني خبير بالأمور والتقنيات المرتبطة بالوسائط الالكترونية) فيقوم بالتصوير والتخزين والاستخراج، ووقف تشغيل الحاسوب خوفا لضياع الدليل الالكتروني أو حفظ جهاز الحاسوب من التعرض للتخريب أو ارسال فيروسات مخربة للنظام أو برامج خبيثة تساهم في محو الدليل، كما يقوم جهاز الضبط القضائي بمصادرة أو حجز جميع لوازم الحاسوب ومتتبعات المكتب، الالكترونية من طابعات وكاميرات وأجهزة الفاكس والهاتف للتعرف على المكالمات المسجلة، وأيضا البريد الالكتروني للتأكد من الرسائل المتبادلة والصور المعتمدة في ارتكاب جرائم إلكترونية.

4- سماع الشهود:

إن جهات التحقيق الاولي للجريمة هدفها التعرف على جميع الأشخاص المحيطة بارتكاب الفعل غير المشروع واحتجازهم في مرحلة الاشتباه لأجل القيام بسماع أقوالهم فيما يتعلق بالمعلومات الضرورية عن كيفية ارتكاب الجريمة الالكترونية والعلاقة التي تربط بين الشهود ومرتكب الفعل والضحية في سبيل الحصول على الدليل الذي يجرم الواقعة كما هو الحال بالنسبة للجريمة التقليدية، الاختلاف يكون فقط في محل ارتكاب الجريمة المعلوماتية بالوسائل.

5- التفتيش:

إن الجريمة التقليدية تحتوي على صلاحيات واسعة للقيام بعملية التفتيش وبشكل واضح منصوص عليه في قانون الإجراءات الجزائية وذلك في الحالات العادية وحتى في حالات التلبس، وأجاز خلالها المشرع الدخول إلى المنازل أو الشركات أو مكان ارتكاب الجريمة شريطة بعد اخطار وكيل الجمهورية، وأيضا أجاز المشرع التفتيش الالكتروني عبر الدخول إلى منظومة معلوماتية أو الاطلاع على ما يحتويه جهاز الكمبيوتر أو الهاتف وذلك من خلال نص المادة 394من قانون المج الجزائية، وكذلك بعد الحصول على اذن وكيل الجمهورية، وذلك بتسخير أشخاص يكونون على دراية بمهارات وفن التعامل الالكتروني حتى يتمكن من مساعدة أعضاء الضبط القضائي على جمع المعلومات والحصول على المعطيات اللازمة التحقيق، خاصة وأن هذه الأخيرة لا يمكن حجزها أو مصادرتها (أي المعلومة) كما هو الحال في إجراءات التفتيش التقليدي، إلا ما كان منها عبارة عن وثائق الكترونية مستخرجة من جهاز الحاسوب أي في شكل ورقي أو دعامة مادية (flash) المحفوظ بها المعطيات (carte mémoire) أو قرص مضغوط فهذه الأخيرة يجوز حجزها كما هو موضح في المادة السادسة من القانون 06/09.

ويجوز تمديد التفتيش إلى أي مكان تتواجد فيه المعلومات أو المعطيات في حدود الإقليم حتى ولو كان خارج التراب الوطني بمساعدة السلطات الأجنبية، وهذا خروجا عن القيود الإجرائية بخصوص الاختصاص الإقليمي بغرض التفتيش عن بعد، وبالتالي يمكن نسخ

المعلومات وتسجيلها في دعامة كي تكون قابلة للحجز. ص402..... غير أنه تثار صعوبة من حيث استكمال إجراءات التحقيق التي تكمن في احضار المشتبه فيه والتحقيق معه وتفتيشه إذا كان خارج الوطن مما يعيق مهمة التحقيق.