مجلة العلوم القانونية و الاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

جرائم الأنترنيت كأحد الأنماط الإجرامية المستحدثة

خربوش فوزية *

أستاذة محاضرة – ب – كلية الحقوق بودواو، جامعة امحمد بوقرة – بو مرداس – (الجزائر)

f.kherbouche@univ-boumerdes.dz

تاريخ ارسال المقال:2023/12/04	تاريخ القبول:2024/02/01	تاريخ النشر: 2024/03/01

*المؤلف المرسل

الملخص:

يشهد المجتمع الدولي المعاصر موجة من التغيرات والتطورات السريعة على كافة الأصعدة أوجدتها الإكتشافات التقنية الحديثة بشكل خاص جعلت العالم اليوم يشهد غزوا تكنولوجيا حقيقيا تغلغل في شتى المجالات الإجتماعية والإقتصادية والسياسية لا سيما الأمنية إذ أن التكنولوجيا الحديثة التي كثيرا ما ساهمت في الكشف عن الجريمة هي نفسها التي تضع اليوم بين أيدي محترفي الإجرام الوسائل المتقدمة لاستخدامها في ارتكاب أخطر جرائمهم ومن ثم إخفائها فظهر مع هذه التكنولوجيا نمط جديد من الجرائم اضحى يعرف بالجرائم ذات التقنية العالية او كما يطلق عليها بمصطلح الجرائم المستحدثة وهي نوع فريد يحتاج إلى تشريعات خاصة ووسائل إثبات تختلف عن الوسائل التقليدية، فأصبحت هذه الجرائم من المعضلات الخطيرة التي تواجه المجتمع الدولي كونها تعتمد على تقنيات حديثة، من ابرز هذه الجرائم جرائم الإنترنت باختلاف صورها

هذه الوسيلة التي أضحت مؤخرا من ضحايا النشاط الإجرامي، وقد شكلت تحديا حقيقيا للسياسات الجنائية السائدة وأجهزتها التشريعية والتنفيذية والقضائية، ونظرا لخطورتها لا سيما على الحقوق الشخصية كان لزاما على الجهات المختصة بمكافحة هذه الجريمة من تطوير اساليبها الأمنية لتتماشى وهذا النوع المستحجث من الجرائم الذي فرض نفسه على مستوى الأفراد والمجتمع وعلى العالم بأكمله

الكلمات المفتاحية: الإنترنت، جرائم مستحدثة، دليل رقمي، إثبات، الحاسب الآلي، معلوماتية

Abstract :

The contemporary international community is witnessing a wave of rapid changes and developments at all levels, created by modern technological discoveries in particular, which have made the world witness a real technological invasion that has penetrated various social, economic and political fields, especially security, as the modern technology that has often contributed to detecting crime is the same one that Today, advanced means are placed in the hands of criminal professionals to use in committing their most serious crimes and then concealing them. With this technology, a new type of crime has emerged that has become known as high-tech crimes, or as they are called by the term “novelty crimes,” which are a unique type that requires special legislation and means of proof that differ from traditional means. These prohibitions have become one of the serious dilemmas facing the international community because they depend on modern technologies. Among the most prominent of these crimes is Internet crime in its various forms. This method, which has recently become a victim of criminal activity, has posed a real challenge to the prevailing criminal policies and its legislative, executive and judicial bodies, and given its danger, especially to personal rights, it has been necessary for the authorities concerned with combating this crime to develop their security methods to be compatible with this emerging type of crime that has imposed itself. At the level of individuals, society and the entire world

Keywords: The Internet, new crimes, digital evidence, proof, computers, informatics

مقدمة:

يشهد المجتمع الدولي المعاصر موجة من التغيرات والتطورات السريعة على كافة الأصعدة أوجدتها الإكتشافات العلمية الحديثة بشكل خاص، جعلت العالم اليوم يشهد غزوا تكنولوجيا حقيقيا تغلغل في شيء المجالات الإجتماعية، الإقتصادية، السياسية وعلى الأخص الأمنية، هذا المجال الأخير تركت التكنولوجيا فيه بصماتها، إذ أنها طويلا ما ساهمت في الكشف عن الجريمة هي نفسها التي تصنع اليوم بين أيدي محترفي الإجرام الوسائل المتقدمة لإستخدامها في إرتكاب أخطر جرائمهم ومن ثم إخفائها. فتظهر مع هذه التكنولوجيا نمط جديد من الجرائم أضحى يعرف بالجرائم ذات التقنية العالمية، أو كما يطلق عليها البعض بمصطلح الجرائم المستحدثة، لم تكن معروفة من قبل، وهي جرائم من نوع فريد تحتاج إلى تشريعات خاصة وإجرءات ووسائل إثبات مختلفة تختلف عن الوسائل التقليدية، وإلى كفاءات مؤهلة على نحو يجعلها قادرة على مواجعة هذا النوع من الإنجرام.

هذه الجرائم أضحت من المعضلات الخطيرة التي تواجه المجتمع الدولي كونها تعتمد على إستخدام أساليب حديثة وتقنية عالية في عملياتها الإجرامية، وهي بذلك باتت تؤرق العالم، فكيف إستطاعت أن تجعل التطور التكنولوجي حقلا أساسيا لها، ومن العالم أجمع ميدانا خصبا لها، لا سيما جرائم الإنترنيت التي تعد من أهم الجرائم المستحدثة بمختلف صورها، هذه الوسيلة التي تعد عصب الحياة في القرن الحادي والعشرين نظرا لإستخداماتها المتنوعة في مختلف مجالات الحياة بما فيها المجال القضائي والجنائي عموما، إلا أنها مؤخرا أصبحت من ضحايا النشاط الإجرامي، حيث إستعملت بشكل غير قانوني في إرتكاب بعض الجرائم سواء كانت سياسية، أمنية، أو إقتصادية، كمعرفة المعلومات، غسيل الأموال...الخ، وكل ما يتعلق بالجرائم التي تشكل إعتداءا صارخا على الحياة الخاصة بمختلف أنواعها، وتجدر الإشارة إلى أن بروز ظاهرة هذا النوع من الجرائم المستحدثة التي نحن بصدد دراسته، أصبح يشكل تحديا حقيقيا للسياسات الجنائية السائدة وأجهزتها التشريعية والتنفيذية والقضائية، نحن الآن أمام نمط من أنماط الجرائم التي لم نجد لها نصوصا قانونية موضوعية كانت أم شكلية في كثير من التشريعات الجنائية، خاصة في الدول العربية وحتى وإن كانت هناك بعض النصوص، فهي غير كافية لتحديد الإطار التنظيمي لهذا النوع من الجرائم، وأنها لم تدخل حيز التطبيق بعد.

ولا مراء ان القانون في بداية الأمر قد وقف عاجزا إزاء ردع مثل هذا النوع من الجرائم خصوصا في دولنا العربية، لكن هذا لا يعني تماطل القانون أو أن يقف هكذا بلا حلول، بل أصبح تطوير القانون وإيجاد نصوص تجرم هذه الأفعال وتعطي التكييف القانوني لها أمرا مفروض في التشريعات ولا مفر منه، فعليه مواكبة التطور وإستحداث قوانين تتماشى وهذا التطور، أي يتماشى طرديا وسرعة التكنولوجيا في مكافحة هذا النوع من الجرائم، فإن لم نستطيع التعامل معها بكفاءة عالية فإن ذلك سيهدد الحياة الخاصة، لهذا لابد من وضع برامج علمية جديدة وأساليب فعالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمع على مستوى العالم بأكمله.

وفي حقيقة الأمر، إن هذه الجرائم لا تشكل معضلة قانونية حقيقية من حيث التجريم والعقاب، أو من حيث تصنيف أنماطها وتحديد أركانها فحسب، بل المشكلة تكمن في صعوبة عمليات الترصد والمتابعة وضبط المجرمين

ومخاطر جمع الأدلة والتحقيق مع فئة المجرمين الأذكياء إلى جانب ضعف التشريعات الشكلية وتختلف القواعد العامة للبنية أو الدليل.

بالإضافة إلى ذلك، فعلى التشريع التأقلم مع هذا الوضع الجديد حتى ولو كان يمس نوعا ما الحريات الشخصية، وتقنين ما يجب تقنينه لمكافحة هذا النوع من الجرائم.

فعلى المشرع أن يضع تنظيما وإطارا قانونيا بحيث يمنع الحدود الفاصلة بين ما هو مشروع وما هو غير مشروع، لأنه يصطدم أحيانا بعوائق دستورية، وبمبادئي قانونية، كمبدأ الشرعية، وأيضا الحقوق الأساسية للشخص وحرمة الحياة الخاصة عموميا.

إنطلاقا من كل هذا ستتم دراسة الموضوع من خلال إبراز النقاط الآتية :

- تحديد مفهوم الجرائم المستحدثة أو الجرائم ذات التقنية العالية.
- طبيعة الجرائم المستحدثة وأنواعها بالتركيز على جرائم الإنترنيت كمثال.
- إجراءات التحقيق في هذه الجرائم، وتحديد المسؤولية فيها.
- المشكلات التي تشيرها الجرائم المستحدثة بصورة عامة وجرائم الإنترنيت بصورة خاصة.
- الحلول وآليات مكافحة هذه الجرائم.

المبحث الأول: مفهوم الجرائم المستحدثة :

سنركز في هذا المبحث على نوع من الجرائم المستحدثة، والمتمثلة في جرائم الأنترنيت، هذه الأخيرة تمثل مجموعة من الأنماط الإجرامية التي تتم عبر شبكة المعلومات الدولية (الإنترنيت) مثل الفيروسات، السطو على بطاقات الإئتمان، وإساءة إستغلال البريد الإلكتروني وغيرها، لكن قبل الخوض في هذا الموضوع يجب تحديد بعض المفاهيم، إذ يتساءل البعض ربما لما سميت بالجرائم المستحدثة، هي جرائم ذات تقنية عالية جلبتها التكنولوجيا الحديثة، يمكن أن نكتفي بهذه التسمية وإنما عبارة أو مصطلح عبارة مستحدثة تدل على جرائم جديدة ، وهي عبارة فنية كثر تداولها مؤخرا مع انتشار أنماط جديدة من الجرائم لم تكن مذكورة من قبل، إن هذه العبارة ليست مصلح قانونيا يحدد أركان وعناصر جريمة معينة وينص عليها أو يعاقب عليها القانون، وإنما هي عبارة تصف أنماطا مختلفة من الجرائم لا يجمع بينها سوى حداثها من حيث الأسلوب والأدوات المستعملة في إرتكابها، وتطلق — كما يرى البعض– على الجرائم المرتكبة بأساليب تقنية، كجرائم الحاسب الآلي والجريمة المنظمة التي تستغل التكنولوجيا في إرتكاب جرائمها.

إذن عبارة مستحدثة لا لأن المشرع إستحدثها وإنما إستحدثتها التكنولوجيا الحديثة مؤخرا وهي أحدث من سابقتها بمعنى أنه مع ظهور الحاسب الآلي والإنترنيت، ظهرت جرائم بالمقارنة مع هذه الجرائم المستحدثة التي أضحت تقليدية، هذا من جهة ومن جهة أخرى بإستمرار في تنفيذ الجرائم فالإستحداث يرجع إلى الوسيلة والأسلوب في إرتكابها، فجرائم القتل والإرهاب والإتجار بالبشر والمخدرات كلها جرائم عرفت منذ القدم، إلا أن المستحدث والجديد فيها هو إستخدام العلوم التقنية الحديثة في التخطيط والتنفيذ وإخفاء معالم الجريمة بمهارة فائقة فجريمة القتل مثلا، لما عرفها الإنسان كانت ترتكب بوسائل بسيطة بساطة المجتمعات آنذاك، كالعصى والحجارة والآلات الحادة،

حتى عهد الأسلحة النارية، إلى أن تطورت هذه الأخيرة فأصبحت ترتكب عن طريق كاتمات الصوت والمزودة بالمناظير وأجهزة التصويب عن بعد، وما يمسى بالقتل الإلكتروني ... الخ.

وعلى هذا الأساس سنوضح في هذا المبحث من خلال مطلبيه، طبيعة هذه الجرائم وأنواعها.

المطلب الأول: طبيعة جرائم الإنترنيت

قبل الحديث عن طبيعة هذه الجرائم، تجدر الإشارة إلى كيفية ظهورها، والتي بدأت مع ظهور الحاسب الآلي في فترة السبعينات، إذ كان عالم أمريكي (دون باركر) أول المهتمين بهذا النوع من الجرائم و من الذين نبهو لخطورتها، فساهم بذلك في وضع أول قانون لجرائم الحاسب الآلي في سنة 1978 في ولاية " فلوريدا" الأمريكية، وأطلق عليها اسم " الجريمة الإفتراضية " وقسمها إلى أربع مجموعات هي كالآتي:

1- جرائم يكون فيها جهاز الحاسب الآلي وملحاقته هدفا للنشاط الإجرامي، كالسرقة إتلاف البيانات.

2- جرائم يكون فيها جهاز الحاسب الآلي أداة لتنفيذ الجريمة والتخطيط لها مثل تزوير الوثائق والدخول على أنظمة محمية.

3- جرائم يكون في الحاسوب موضوع الجريمة، كأن يشكل البيئة التي ترتكب فيها الجريمة، مثل إصابته بفيروسات هدامة.

4- جرائم تستغل فيها سعة الحاسوب للغش والإحتيال.

لكن " باركر" أهمل أنذاك دور الحاسب الآلي في أن يكون دليلا للإثبات أو مصدرا مساهما فيها بعد الأدلة الجنائية الرقمية التي تتماشى وطبيعة هذه الجرائم.

- أما المرحلة الثانية فكانت مرحلة التسعينات، حيث ظهر تصنيفا جديدا لهذه الجرائم لا يختلف كثيرا عن التصنيف الذي وضعه " باركر" حيث جاء العالم الأمريكي – كارنر- ليطور من التصنيف السابق، فتكلم عن دور الحاسوب كمصدر للأدلة الجنائية.

- أما المرحلة الثالثة فكانت سنة 1994م أين طورت وزارة العدل الأمريكية هذه التصنيفات وجعلتها أكثر وضوحا للتمييز بين هذه الجرائم الإفتراضية، حيث فرقت بين جهاز الحاسوب ومكوناته من جهة، وبين البرامج والمعلومات من جهة أخرى، مع التركيز على دور الحاسوب و شبكات الإتصال في الإثبات فوضعت هذا التصنيف.

- جرائم يكون فيها جهاز الحاسوب هو جسم الجريمة.

- جرائم يكون فيها جهاز الحاسوب كدليل في الإثبات.

- جرائم يكون فيها جهاز الحاسوب الوسيلة التي نفذت بها الجريمة.

- جرائم يكون فيها معلومات الحاسوب هي جسم الجريمة.

- جرائم تكون المعلومات هي وسيلة لإرتكاب الجريمة.

- جرائم تكون المعلومات هي دليل للإثبات.

مما سبق نستخلص أن هناك تعريف فني وآخر قانوني فمن الناحية الفنية، تعرف هذه الجريمة بأنها كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود،

أما من الناحية القانونية، فلا يمكن إيجاد تعريف شامل لهذه الجريمة لأن تعدد إستعمالات الحاسب الآلي وإختلاف عناصرها وعملياتها يقتضي إيجاد تعريف لكل عنصر أو عملية، فهناك تعاريف مثلا تخص العبث بالحاسب الآلي، الإخلال بأمن الحاسوب، الغش المعلوماتي وهو أبسط هذه الجرائم وأكثرها تداولا وإنتشارا ... الخ.

على العموم يمكن القول " أن جرائم الأنترنيت تعد مجموعة الأفعال والأعمال غير القانوني التي تتم عبر شبكة الأنترنيت أو تبث محتوياتها ".

إن هذه الجرائم في تطور مستمر، وهي منتشرة في دولنا العربية وتعد حديثة، وقد أضحت تقليدية بالنسبة إلى الدول المتطورة، بعد أن كانت مجرد ظاهرة فردية تنصب مثلا على سرقة برامج وكتب ومستندات وملفات تطورت حتى أصبحت ظاهرة عامة في تصميم الفيروسات لتصيب مكونات الشبكة، وسرعة إنشار الصناعة التكنولوجية وهكذا، (الأمر الذي لفت الإنتباه إبل أهمية تطبيق نظم الأمان برغم تكلفته الكبيرة)، بل وصل الأمر إلى أبعد من ذلك (وكأنها الحرب على الأنترنيت)، لأنه وصل الأمر إلى أنه من خلال إستغلال الإنترنيت في إرتكاب الجرائم أيضا من خلاله نشأت حرب باردة بين بعض الدول كما هو عليه الحال بين أمريكا وروسيا والصين، و باكستان والهند حيث اقتحم بعض القراصنة المجهولين الهوية مواقع حكومية على الإنترنيت في دولة باكستان لسرقة بعض البيانات والمعلومات السرية خصوصا على بعض الوزارات في هذه الدولة، سواء كان هؤلاء الأشخاص بين دولتين أو ثلاثة في هذه الحرب على الإنترنيت، المشكل هنا أن الأخطار معروفة ولو أنها في بعض الأحيان تكون خفية ولكنها تعرف في نهاية المطاف نتائجها، ولكن من إرتكب هذه الجريمة يبقى مجهولا ومن الصعب الوصول إليه، خصوصا أنهم يستعملون أسماء مستعارة، هذا كله غرضه التجسس على المنشآت النووية للهند، وعلى كيفية إطلاق الصواريخ وغير ذلك فرغم أن دولة باكستان إستعانت بمختصين في هذا المجال لكن لم تصل إلى حل ولازالت لتتعرض لخطر التجسس، فيجب حماية هذه المواقع على الإنترنيت وإستعمال أسلوب التشفير من هذه القرصنة ولتحديد هوية الفاعل، وهذا العجز في إكتشاف الجريمة يعد إحدى المشاكل التي يشريها هذا النوع من الجرائم ذو التقنية العالية.

الفرع الأول: أنواع جرائم الحاسب الآلي والإنترنيت

يقدم الحاسب الآلي والأنترنيت خدمات جليلة غير محدودة للإنسان في حياته اليومية، وفي عصر المعلوماتية، إلا أنه بالمقابل أصبحت هذه الوسائل مؤخرا من ضحايا النشاط الإجرامي، كالجرائم التي ترتكب عن طريق شبكة الإنترنيت نفسها من سرقة المعلومات وإستغلال الإنترنيت بشكل غير قانوني، وغسيل الأموال، وكل أنواع الجرائم سواء كانت إقتصادية، أمنية أو سياسية.

وبالأخص الإجرام المنظم والجرائم الإرهابية التي تعد من أكثر الجرائم رواجا تحتاج إلى وسائل علمية جد متطورة للتقليص من النشاط الإجرامي للمجموعة الإرهابية.

وتتمثل إذن أنواع جرائم الإنترنيت في جرائم ولت تقليدية وترتكب عن طريق وسائل فنية وتقنية كالإستيلاء على الأموال عن طريق الإحتيال المعلوماتي، أو جرائم القتل بإستخدام شبكات الإتصال عن بعد، بالإضافة إلى كل الجرائم التي تشكل إعتداء صارخا على حرية الحياة الخاصة، مثل القذف والسب على شبكات التواصل الإجتماعي، وأخرى مستحدثة في مجال المعلوماتية، كإختراق شبكة المعلومات، الإستيلاء على المعلومات الموجودة في قواعد

البيانات، والدخول أو البقاء في الأنظمة المعلوماتية بطريق غير مشروع، وكل الوسائل التقنية المجتمعة للإجراء المنظم من غسيل أموال وجرائم إرهابية وغيرها.

أغلب هذه الجرائم بعضها يرتكب على شبكة الإنترنيت، وهي التي تتعلق بين نقل أو تبادل المعلومات، والقتل عن طريق استخدام البريد الالكتروني، وكل جرائم الإعتداء على الحياة الخاصة أما البعض الآخر يرتكب بواسطة الإنترنيت أي يجعله بمثابة وسيلة لإرتكاب الجريمة الإرهابية مثلا والجريمة المنظمة وسوف أقتصر على ذكر هذه الجرائم من خلال النقاط التالية :

الفرع الثاني: الإشكاليات الإجرائية لجرائم الإنترنيت

نظرا للخصائص المميزة التي تتسم بها هذا النوع من الجرائم، نظرا لكونه عابر للحدود إلى جانب السرعة في تنفيذه والسرعة في إتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين، أو كما يطلق عليهم باسم " المجرم المعلوماتي "، لهذا أغلب التشريعات وعلى غرارها التشريع الجزائري قد خصص لها إجراءات خاصة نظرا لكونها ترتكب في بيئة معلوماتية افتراضية، وهو ما يرتب العديد من الصعوبات من الناحية التطبيقية ويجعل الإجراءات العادية عاجزة عن إثبات هذه الإجراءات من مرحلة لأخرى من مراحل الدعوى الجزائية، وعليه سنخصص المطلب الأول أهم القواعد الخاصة بإجراءات التحقيق القضائي، وفي المطلب الثاني إلى طرح بعض المشكل التي يشيرها هذا النوع من الجرائم مع الحلول المقترحة في سبيل مكافحتها، وذلك على هذا النحو.

المطلب الثاني : القواعد الإجرائية في التحقيق في هذا النوع من الجرائم

تعد إجراءات التحقيق الجنائي العام هي الأساس في التحقيق في هذا النوع من الجرائم تماما كما هو الحال عليه في الجرائم التقليدية، إلا أن إجراءات التحقيق في جرائم الحاسوب والإنترنيت تتميز بنوع من الخصوصية سنتطرق إليها لاحقا.

إن أغلب التشريعات في الدول المتطورة عرفت هذه الجريمة كصورة من صور الجريمة المعلوماتية ووصلت إلى وضع قوانين خاصة تتماشى وطبيعة هذه الجرائم أما في دولنا العربية، فقد عرفت هي الأخرى هذا النوع من الجرائم لكنها لم تصل إلى وضع قانون خاص قائم بذاته يعاقب عليها، بداية كانت الجريمة تخضع للقواعد العامة في التجريم والعقاب، ولكن هذه النصوص التقليدية لم تكن كافية في مكافحة هذه الجرائم، هذا ما دفع ببعض الدول وعلى رأسها دولة الإمارات التي كانت في الطليعة بالنص على تجريمها ثم حذت حذوها مصر و الجزائر، بالنسبة للجزائر، فإن المشرع الجزائري لم يكن يعرف هذا النوع من الجرائم إذ مؤخرا مع دخول شبكة الإنترنيت سنة 1998، بداية عالجها ضمت الجريمة المنظمة بموجب إتفاقية مصادق عليها بتحفظ وهي إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بمقتضى مرسوم رئاسي يحمل رقم 22-55 الصادر في 05 فبراير سنة 2002.

بعد ذلك واجه المشرع الجزائري هذه الجريمة بإستحداثه لنصوص قانونية تضفي قواعد خاصة للوقاية من هذه الجرائم، مكرسا حماية خاصة وتجريم المساس بأنظمة المعالجة الآلية للمعطيات، فكان أول تدخل له بموجب القانون رقم 01-09 المؤرخ في 26 يونيو 2001 المعدل والمتمم لقانون العقوبات حيث قرر عقوبات في هذا المجال من خلال المواد 144-144 مكرر إلى المادة 144 مكرر2 بعدها صدر القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل

والمتمم لقانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، ولقد إعتبر المشرع هذه الجريمة جريمة مستقلة قائمة بذاتها، بدليل تخصيصه لها قسما كاملا خاصا بها في قانون العقوبات وهو القسم السابع مكرر والذي تضمن ثماني (08) مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 وهي مواد إحتوت أهم الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد حدد لها العقوبة من خلال المادة 394 مكرر، بعد ذلك سن المشرع قانون رقم 09-04 المؤرخ في 05 اوت 2009، يتضمن القواعد الخاصة للوقاية، من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، لما تشكله هذه الجرائم من إعتداء على أنظمة المعالجة الآلية للمعطيات، لذا إستحدث المشرع قانون خاصا يتضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ووضع قواعد إجرائية خاصة تسمح برصدها وآليات مكافحتها ومتابعة مرتكبيها.

كما جاء المشرع بالقانون رقم 16-02 المؤرخ في 19 يونيو 2016 المعدل والمتمم لقانون العقوبات بمادتين وهما 87 مكرر 11 و 391 مكرر 08، فإستعمل في الأولى عبارة (تكنولوجيا الإعلام والإتصال)، وفي الثانية عبارة (مقدم خدمات الإنترنيت)، حيث وضع عقوبات خاصة بشأنها.

دون أن ننسى الإشارة إلى قانون الإجراءات الجزائية لسنة 2006 الذي أشار إلى هذه الجريمة في الفصل الرابع منه من خلال المادة 65 مكرر 05 ضمن الجرائم الخمس الخطيرة والتي خصها المشرع بإجراءات خاصة بالبحث والتحري وأساليب المتابعة، حيث سمح المشرع فيها بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، والتسرب، من طرف الشرطة القضائية أثناء البحث التفتيش القضائي، كلها أساليب فيها نوع من المساس بالحرية الشخصية للمتهم، رغم ذلك تتخذ هذه الإجراءات بشأن هذا النوع من الجرائم المستحدث، كل ذلك في سبيل الوصول إلى الحقيقة في وقت قياسي، فمصلحة المجتمع أولى بالرعاية في مصلحة الفرد.

الفرع الأول: الإشكاليات الإجرائية للجريمة

نظرا للخصائص المميزة التي تتسم بها لهذه الجريمة كونها عابرة للحدود، وإلى جانب السرعة في إتلاف الأدلة ومحو آثارها ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين، فإنها آثارت إشكالات عدة في مجال البحث والتحري عنها ومتابعتها والتحقيق فيها، كما نلاحظ أن المشرع تطرق إلى نوع واحد من إجرام الإنترنيت أو الجريمة المعلوماتية بصورة عامة، إذ حصر هذا النوع من الجرائم في جريمة واحدة فقط، دون التطرق إلى باقي الأنواع أو الصور و المتعلقة بسرقة البيانات والمعطيات وسماها بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كون هذه الجريمة أكثر إنتشارا في الجزائر بعد دخول شبكة الإنترنيت، أما في الأنواع التي فاقت التقنية لا يزال المشرع وحتى المجتمع بعيد كل البعد عن معرفتها والوصول إليها. وذلك على هذا النحو.

- بخصوص مرحلة البحث والتحري، مثلا نركز على أهم الإجراءات في التبليغ عن الجريمة والمعاينة.

-التبليغ : إن إكتشاف جرائم الحاسوب والإنترنيت لا يكون بسهولة، حيث أن الأشخاص العاديون لا يمكنهم إكتشاف هذه الجرائم والتبليغ عنها، بل تستدعي متخصصين في مجال الإنترنيت، مثال على ذلك أن بعض الشركات عندما تكتشف وقوعها ضحية لسرقة البيانات على موقعها على الإنترنيت فإنها لا تقوم بالتبليغ وذلك خوفا على سمعتها، وهنا يبقى دور رجال الأمن بالتدخل بالبحث والتحري عنها، فمصدر البلاغ يجب أن يكون على درجة

من الوعي والمعرفة بتفاصيل ما يدلي به من معلومات لأنه لا يكفي التبليغ وحده على أنه ثمة وقوع جريمة، بل أن يعطي وصف علمي محدد لهذه الجريمة.

-المعاينة ومسرح الجريمة: في الغالب هذه الجرائم تعد من الجرائم المستمرة، وطبيعته هذه تثير إشكالات في إجراء المعاينة، وبالتالي تكون معاينة فنية تستلزم مختصين وإلى جهاز خبراء فنيين بكل ملحقاته أما بخصوص مرحلة التحقيق، فهي كذلك تعتمد على قضاة تحقيق مؤهلين ومدربين في تكوين خبرتهم في مجال الإنترنيت.

وهذه المرحلة تثير إشكالات مهمة جدا تتعلق بنوع الأدلة المطلوبة في إثبات هذا النوع من الجريمة، إذ لا يمكن الإعتماد على أدلة الإثبات التقليدية في مجال إثبات جريمة مستحدثة ذات تقنية عالية، فهي تحتاج إلى أدلة فائقة التقنية في الإثبات تتماشى وحداثة هذه الجريمة كالإثبات عن طريق الدليل الرقمي.

الفرع الثاني: الإثبات عن طريق الأدلة الرقمية:

وشهود وقرائن ولكنها غير كافية بخصوص إثبات هذا النوع المستحث من الجرائم لذا تبقى على سبيل الإستئناس يلجأ إليها القاضي إلى جانب أدلة ذات صيغة علمية فقط لطمئنة نفسية وضمير القاضي الجزائري، فالحاسوب يمكن ان يشكل بذاته دليلا للإثبات بكل ملحقاته والمعلومات المخزنة في ذاكرته، مفتاح الحاسوب، الشاشة، الطابعات، كلها وسائل تشكل دليل للإثبات، لكن اليوم مع التطور التكنولوجي الذي جلب معه أفاق جديدة ولت هذه الأدلة السالفة الذكر تقليدية بمقارنتها مع الأدلة التي ظهرت مؤخرا التي أطلق عليها مصطلح " الأدلة الجنائية الرقمية " في مواجهة الجرائم المستحدثة لكنها لم تدخل حيز التطبيق، تبقى مجرد أدلة إفتراضية نظرا لحداثة مفهومها وصعوبتها وندرة المراجع فيها.

فقد عرفها " كيسي " وهو عالم أمريكي بأنها تلك " الأدلة التي تشمل جميع البيانات الرقمية التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة من رسومات، خرائط، الصوت، الصورة والتي يمكن أن تثبت أن هناك جريمة قد إرتكبت، أو توجد علاقة بين الجريمة والجاني، أو بين الجريمة والمتضرر منها".

بمعنى أنها معلومات يقبلها المنطق تعتمد على العلم يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في جهاز الحاسوب وملحقاته وشبكة الإتصال، وفي حقيقة الأمر هي أدلة إفتراضية في شكلها وحجمها ومكان تواجدها غير معين، لأنها تتكون من دوائر وحقول مغناطسية ونبضات كهربائية غير ملموسة ولا تدرك بالحواس الطبيعية للإنسان.

أما بخصوص مرحلة المحاكمة: فإن هذه المرحلة تثار فيها بشكل أساسي مشكلة تنازع الإختصاص من حيث المحكمة المختصة وبالتالي تتساءل عن القانون الواجب التطبيق.

وكون جريمة الإنترنيت عابرة للحدود وقد يرتكب جزء من ركنها المادي أي السلوك الإجرامي في بلد وتتحقق النتيجة في بلد آخر، وهنا تثار مسألة تطبيق مبدأ الإقليمية أو مبدأ الشخصية مثلا شبكة الإنترنيت ليس لها مقر في دولة معينة ولا تضمن شخصي محدد، بل توجد موزعة على الكرة الأرضية، لذا تقع جريمة في مكان معين وتنتج آثارها في مناطق أخرى داخل الدولة أو خارجها وهنا تثار مشكلة أخرى تتمثل في تحديد المسؤول عن الجريمة والبحث عن

الأدلة الجنائية خارج دائرة الإختصاص التي سجل فيها البلاغ وتتم فيها تحريك الدعوى بالإضافة إلى مشكلة فحص البيانات وإجراء التحقيق.

مثال: إذا تم بث فيروس معلوماتي (السلوك الإجرامي) في مكان والنتيجة هي تدمير المعلومات في مكان آخر، فهل ينعقد الإختصاص لمكان السلوك أو لمكان النتيجة؟ إن التشريعات الجنائية الساوية اليوم في معظم الدول تميل إلى الطابع الإقليمي، أي تطبيق مبدأ الإقليمية مع إحترام سيادة الدول، ويكون عن طريق عقد إتفاقيات جنائية لتسهيل مهمة التحقيق في هذا النوع من الجرائم وكيفية تسليم المجرمين وغير ذلك مع تبادل الأدلة أيضا.

إذن يجب أن يكون هناك تعاون دولي لما لا أو إستحداث ما يسمى بشرطة الإنترنيت تختص بهذه الجريمة وضبطها لأن في حقيقة الأمر مكافحة هذه الجرائم تقتضي توحيد التشريعات المختلفة وأن يكون هناك ما يسمى بنظام الإثبات بالدليل الإلكتروني واحد، أي موحد بين الدولة التي وقعت فيها الجريمة والأخرى التي يقيم فيها المتهم وتتولى محاكمته.

المطلب الثاني: آليات مكافحة جريمة الإنترنيت

إن إستخدام الإنترنيت في المجال الجنائي قد يؤدي إلى ظهور مشاكل قانونية، ما دفع ببعض الدول إلى البحث عما إذا كانت القوانين القائمة هي كافية لمكافحتها أم يتعين على المشرع أن يتدخل لكي يضع تنظيما وإطارا قانونيا حتى يوضع الحدود الفاصلة بين ما هو مشروع وما هو غير مشروع عند التغامل مع هذه الوسيلة الجديدة من وسائل الإتصال، لكن حتى لو تدخل المشرع فإنه يصطدم أحيانا بعوائق دستورية تتعلق بالحقوق الأساسية للشخص في الإعلام وحرية التعبير وحرية الحياة الخاصة.

لهذا ثار جدل كبير بشأن الحاجة إلى تدخل المشرع لتنظيم الإنترنت، وهل تكفي النصوص القائمة لمواجهة هذه الظاهرة العلمية الجديدة أم لا؟

إن كل من المشرع الأمريكي والفرنسي قد تدخلا لوضع نصوص خاصة لتجريم الدخول سواء بطريق مباشر أو غير مباشر على شبكة الإنترنت لتوفير حماية خاصة للمعلومات وبرامج الكمبيوتر من كشفها أو الإطلاع عليها والتلاعب بها، بل جرم الدخول غير المشروع على أجهزة الحاسب ذاته دون النظر فيما إذا كان الجاني قد استهدف الإضرار أم لا، وهناك رأي آخر يرى أن النصوص القائمة أي الموجودة في قانون العقوبات لا تكفي بذاتها لمواجهة جرائم الإنترنت، ولبعض الآخر يرى أنها كافية فحسب رأيهم الإنترنت يعد غابة بلا قانون.

وهناك من يرى حلا وسطا حيث أن الكثير من النصوص الموجودة بالقوانين العقابية تواجه أغلب الجرائم التي ترتكب بطريق الإنترنت، إضافة إلى استحداث قوانين جديدة تتماشى وطبيعة هذه الجريمة تكون إلى جانب القوانين التقليدية السابقة لتدعيمها.

المطلب الأول: موقف بعض الدول وتشريعاتها

تجد ظاهرة الجريمة الإلكترونية – كما سلف ذكره- اهتماما كبيرا في جميع أنحاء العالم، لكن ولعهد قرب قلة من الدول من قامت بإصدار تشريعات شكلية وموضوعية تساعد على مواجهة هذه الجريمة ففي بداية التسعينات بدأت الحكومة البريطانية بالتعاون مع بعض شركات تقنية المعلومات في تطوير مشروع قانون للجريمة الإلكترونية، أما في

الهند فكانت من الدول الأوائل التي قامت بخطواتها بإصدار قانون تقنية المعلومات في عام 2000م، أما في اليابان فقامت الشرطة القومية بإتخاذ تدابير فنية وإدارية وقانونية لمكافحة هذه الجريمة، ولهذا الصين وكوريا الجنوبية التي إعترفت بالمخاطر الأمنية الناجمة عن هذه الجريمة بالإضافة إلى دول أخرى قد توصلت إلى وضع قانون خاص بهذا النوع من الجرائم. أما بخصوص الدول العربية فرغم التباطؤ في إصدار تشريعات تنظم التعامل مع تقنية المعلوماتية إلا أننا نجد أجهزة الشرطة قد فتحت في بعض الدول العربية تحقيقات في جرائم تتعلق بالحاسوب والإنترنيت وهي تحاول اليوم إلى وضع قانون للقضاء على الجريمة نهائيا وعلى رأسهم، دولة الإمارات، مصر، تونس، والجزائر مؤخرا رغم ذلك لا زالت بعيدة كل البعد على وضع قوانين تتماشى وردع هذا النوع من الجرائم نظرا لصعوبة الجريمة المتشعبة وقصور قوانينها.

المطلب الثاني: موقف المشرع الجزائري

سبق وأن رأينا أنه لم يعد خطر هذا النوع من الجرائم وآثارها محصورا على المستوى الإقليمي بل تخطى خطرها حدود الدول والقارات الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة مكافحة الجريمة ولا سيما خطورة هذه الجريمة وإعتدائها على مبدأ الحق في الخصوصية، وعلى الشرعية الإجرائية.

وأمام هذا الخطر الذي تركبه الإجرام الافتراضي والرقمي، كان لابد على المشرع الجزائري أن يواكب هذا التطور ويتدخل لوضع حد لهذه الكوارث التقنية التي باتت تهدد أمن وإستقرار الدول، فعليه أن يتدخل لمواجهتها بنصوص تجريمية جديدة نظرا لخصوصيتها المستحدثة، وقد رأينا في المبحث الأول من هذه الدراسة مجموعة القوانين التي جاء بها المشرع في مجال مكافحة الجريمة المعلوماتية ونظرا لتطورها المستمر، فهي تحتاج إلى إجراءات متابعة مستجدة تتماشى وهذا النوع الجديد من الجرائم، ولا يمكن إخضاعها للقواعد العامة، حتى من حيث الجهة المختصة بالنظر فيها فهي لا تخضع للقضاء العادي، بل تخضع لجهات خاصة، وهذا ما جاء به المشرع الجزائري مؤخرا من خلال إنشائه لقطب وطني جزائي متخصص بالنظر في هذا النوع من الجرائم ومكافحتها وذلك بموجب الأمر 21-11 المؤرخ في 25 أوت 2021، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 65.

لقد ترتب على إنتشار الإنترنت والكمبيوتر صعوبات وإشكالات قانونية عديدة لاسيما في مجالات الإثبات، والحماية القانونية والجنائية لبرامج الكمبيوتر، لذا أصبح على رجال القانون التعامل مع نوع جديد من الجرائم يسمى بجرائم المعلوماتية لذا أصبح لزاما على الجهات الأمنية والتشريعية والقضائية من تطوير أساليبها ووسائلها وإخضاعها لهذا التطور كي تتمكن من التعامل والتعايش مع عصر الثورة المعلوماتية وفي ظل التقدم العلمي الذي فتح أفاقا جديدة وجلب معه أيضا مشكلات ومخاطر جديدة، إن لم نستطع التعامل معها بكفاءة عالية فإن ذلك سيهدد الحياة الخاصة.

مما تقدم، لاحظنا أن المشرع الجزائري ورغم الترسانة القانونية التي حاول وضعها من أجل القضاء على هذا النوع الخطير من الإجرام المنظم، إلا أن لها لا تتلائم مع هذا النوع من الجرائم خصوصا المتعلقة بالأنترنيت، فالنصوص الراهنة لازالت تقليدية مقارنة مع النصوص المستحدثة التي إعتمدتها الدولة المتطورة التي تتبنى تكنولوجيا جد متطورة،

بالإضافة إلى أن المشرع الجزائري حصر هذه الجرائم في صورة واحدة كما إقتصرت حمايته الجزائية على مجالين من مجالات الحاسب الآلي، أما بقية الجرائم المتعلقة بالأنترنيت فلم يشملها بحمايته الجنائية، وهكذا تبقى النصوص القانونية فيها قصور، إذ لا نجد نص شاهد جامع يحدد النموذج القانوني لكل أنواع هذه الجرائم، فضباب النص يثير مشكلة التكييف القانوني للجريمة، كل هذا يعود إلى صعوبة السيطرة عن شبكة الأنترنت وعلى الجرائم التي ترتكب عليها، حيث من الصعب اكتشافها فهناك من يستخدم الشيكة من الجناة يحملون أسماء مستعارة أو يرتكبون سلوكهم الإجرامي من خلال إحدى مقاهي الإنترنت، صعوبة تحديد إذن هوية المتدخلين في هذه الشركة وتحديد دورهم وطبيعة عملهم والمسؤولية الجنائية لكل منهم، بالإضافة إلى سرعة نشر المعلومات وتسجيلها لذلك جرائم الأنترنت غالبا ما تقيد ضد مجهول، وفي حالة اكتشاف هذا المجهول فمن الصعب إقامة الدليل عليه ومحاكمته مثل الجرائم الإرهابية والجواسيس الذين يستخدمون البريد الإلكتروني في ارتكاب جرائمهم المتمثلة في الإرهاب والتخريب و الإغتيالات...الخ

فيكون من الصعب إن لم يكن من المستحيل مراقبتهم، فظهور الإنترنت إذن يزيد من مخاطر الإعتداء والمساس بالحريات الشخصية والعامة يوجعل مسألة المراقبة موضوع الساعة وصعبة لا سيما عندما يتعلق الأمر بالمساس بالنظام العام والآداب العامة كنشر المعلومات التي تحض على الكراهية والعنصرية وإهانة الأديان، ونشر الصور الخليعة عن طريق الإنترنت والمواقع الإباحية كما ذكرنا جعلت أمر الرقابة على هذه الشبكة بالشبه مستحيل في تفعيلها، لذا لا بد من وضع برامج علمية جديدة وأساليب فعالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمع على مستوى العالم.

في الأخير نصل إلى بعض المقترحات وذلك على هذا النحو:

- يجب إعداد مشروع قانون ينظم جرائم الإنترنت بصورة عامة وآليات مكافحتها
- تدخل المشرع بنص صريح وتجريم كل فعل غير مشروع يرتكب عبر الكمبيوتر مثل إلتقاء البرامج أو الدخول أو البقاء غير المشروع أو أفعال التزوير والاستخدامات اللاأخلاقية مثل الإتجار بالبشر وخطف الأطفال، تجارة المخدرات وغسيل الأموال، وكل ما يتعارض مع الأخلاق والدين.
- تشديد العقوبات لهذا النوع الخطير من الجرائم
- توحيد المصطلحات من أجل تحديد تعريف وتكييف الجريمة المعلوماتية
- إسناد عملية البحث والتحري لفرق متخصصة في مجال المعلوماتية والرقمنة التابعة للضبطية القضائية
- خصوصية إجراءت المتابعة
- إمكانية استعانة الصبطية بوسائل التحري المستجدة في مجال مكافحة هذه الجريمة.
- استحداث مجموعة من التدابير والإجراءات الوقائية الخاصة لتفادي وقوع الجريمة أصلا
- لا بد من تعاون دولي، إبرام اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسب الآلي والأنترنت من أجل معالجة مشكلات الإختصاص وتبادل الأدلة الجنائية وتسليم المجرمين فالأمر يحتاج إلى قوانين جنائية أكثر مرونة تواكب مرونة التعامل مع هذه الجرائم في مختلف المراحل

- في الأخير التعاون مع شرطة الأنتربول للقضاء على الجريمة ولما لا استحداث ما يسمى بشرطة الإنتربول.

- **قائمة المراجع:**

أولا: الكتب

1. جميل عبد الباقي الصغير، الجوانب الإجرامية لجرائم الإنترنت.

2. حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، دار حامد للنشر والتوزيع، عمان، الأردن، 2014.

3. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، المجلة العربية للعلوم والمعلومات، الطبعة الأولى، سنة 2001، ص133 – 141.

4. عاد عبد الجواد محمد، إجرام الإنترنت، مجلة الأمن والحياة، العدد221، السنة 20، ديسمبر 2000، يناير 2001، أكاديمية نايف العربية للعلوم الأمنية الرياض من ص 70 -73.

5. محمد الأمين البشري، التحقيق في الجرائم المستحدثة.

ثانيا: القوانين

1. الأمر رقم 09 -04 المؤرخ في 16 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، الجريدة الرسمية رقم47.

2. قانون رقم 06 -22 المؤرخ في 29 ذو القعدة عام 1427هـ الموافق ل20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66- 155 المؤرخ في 08 يونيو 1966.

3. قانون رقم 06 – 23 المؤرخ في 29 ذو القعدة عام 1427هـ الموافق ل 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 18 صفر 1336 الموافق ل 08 يونيو، سنة 1966 والمتضمن قانون العقوبات.

4. الأمر رقم 21 – 11 المؤرخ في 25 أوت 2021، المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65.